Guia do Usuário do Lenovo XClarity Administrator

Versão 4.0.0

Primeira edição (Fevereiro 2023)

Conteúdo

Tabelas

Resumo de alterações

Versões de acompanhamento do software de gerenciamento Lenovo XClarity Administrator oferecem suporte aos novos aprimoramentos de hardware, software e correções.

Consulte o arquivo de histórico de alterações (*.chg) fornecido no pacote de atualizações para obter informações sobre as correções.

Esta versão oferece suporte aos seguintes aprimoramentos feitos no software de gerenciamento.

Para obter informações sobre alterações nas versões anteriores, consulte O que há de novo na documentação online do XClarity Administrator.

Função	Descrição
Administrando	É possível pressionar o nome de domínio totalmente qualificado (FQDN) do servidor de gerenciamento do XClarity Administrator e informações DNS para servidores gerenciados com IMM2, XCC e XCC2 para que os servidores gerenciados possam encontrar o servidor de gerenciamento usando essas informações (consulte Configurando o acesso à rede).
Monitoramento	É possível exibir dados adicionais do inventário para componentes de memória persistente (PMEM) (consulte Visualizando os detalhes de um servidor gerenciado). É possível exibir dados de inventário adicionais para dispositivos de armazenamento (consulte Visualizando os detalhes de um servidor gerenciado).
Gerenciamento de dispositivos	É possível exibir e configurar o modo de segurança para servidores específicos separados do XClarity Administrator (Definindo as configurações de segurança de um servidor gerenciado e Definindo configurações de criptografia no servidor de gerenciamento). Os endereços IP secundários são compatíveis com o Baseboard Management Controller nos servidores ThinkSystem aplicáveis (consulte Visualizando os detalhes de um servidor gerenciado).
Atualizações de firmware	Você pode atualizar o firmware em bibliotecas de fita IBM TS4300 (consulte Atualizando firmware em dispositivos gerenciados).
Implantação do sistema operacional	É possível implantar os seguintes sistemas operacionais em servidores gerenciados (consulte Sistemas operacionais suportados). • Microsoft Windows Client 10 21H2, 10 22H2 e 11 22H2 • RedHat Enterprise Linux 9.x • Ubuntu Server 22.04.x

Capítulo 1. Visão geral do Lenovo XClarity Administrator

O Lenovo XClarity Administrator é uma solução centralizada de gerenciamento de recursos que simplifica o gerenciamento de infraestrutura, acelera as respostas e melhora a disponibilidade dos sistemas e soluções de servidor da Lenovo®. Executado como um dispositivo virtual que automatiza descoberta, inventário, rastreamento, monitoramento e fornecimento de servidor, rede e hardware de armazenamento em um ambiente seguro.

Saiba mais:

- XClarity Administrator: gerenciando o hardware como software
- XClarity Administrator: Visão Geral

O XClarity Administrator fornece uma interface central para executar as seguintes funções para todos os dispositivos gerenciados.

Gerenciamento de hardware

O XClarity Administrator fornece gerenciamento de hardware livre de agente. Pode descobrir automaticamente dispositivos gerenciáveis, incluindo o servidor, a rede e o hardware de armazenamento. Os dados do inventário são coletados para dispositivos gerenciados para proporcionar uma visão geral do inventário e status de hardware gerenciado.

Existem várias tarefas de gerenciamento para cada dispositivo suportado, incluindo visualização de status e propriedades, definição de configurações do sistema e de rede, ativação das interfaces de gerenciamento, ativação e desativação do sistema e controle remoto. Para obter mais informações sobre o gerenciamento de dispositivos, consulte Gerenciando chassi, Gerenciando servidores e Gerenciando comutadores.

Dica: O servidor, a rede e o hardware de armazenamento que podem ser gerenciados pelo XClarity Administrator são chamados de *dispositivos*. O hardware que está sob gerenciamento do XClarity Administrator é chamado de *dispositivos gerenciados*.

É possível usar a exibição do rack do XClarity Administrator para agrupar seus dispositivos gerenciados e refletir a configuração física do rack em seu datacenter. Para obter mais informações sobre racks, consulte Gerenciando racks.

Saiba mais:

- XClarity Administrator: descoberta
- XClarity Administrator: inventário
- XClarity Administrator: controle remoto

Monitoramento de hardware

O XClarity Administrator fornece uma visão centralizada de todos os eventos e alertas gerados dos dispositivos gerenciados. Um evento ou alerta é transmitido ao XClarity Administrator e exibido no log de eventos ou de alertas. Um resumo de todos os eventos e alertas é visível no painel e na barra de status. Eventos e alertas de um dispositivo específico estão disponíveis na página de detalhes Alertas e eventos desse dispositivo.

Para obter mais informações sobre o monitoramento de hardware, consulte Trabalhando com eventos e Trabalhando com alertas.

Saiba mais: XClarity Administrator: monitoramento

Gerenciamento de configuração

É possível fornecer rapidamente e pré-provisionar todos os servidores usando uma configuração consistente. Definições de configuração (como armazenamento local, adaptadores de E/S, configurações de inicialização, firmware, portas e configurações UEFI e de controlador de gerenciamento) são salvas como um padrão de servidor que pode ser aplicado a um ou mais servidores gerenciados. Quando os padrões de servidor são atualizados, as mudanças são implantadas automaticamente nos servidores aplicados.

Os padrões de servidor também integram suporte para virtualizar endereços de E/S. Assim, é possível virtualizar conexões de malha do Flex System ou redefinir servidores sem interromper a malha.

Para obter mais informações sobre configuração de servidores, consulte Configurando servidores com padrões de configuração.

Saiba mais:

- XClarity Administrator: bare metal para cluster
- XClarity Administrator: padrões de configuração

Atualizações de firmware e conformidade

O gerenciamento de firmware é simplificado designando políticas de conformidade de firmware para dispositivos gerenciados. Quando você cria e atribui uma política de conformidade para dispositivos gerenciados, o XClarity Administrator monitora alterações no inventário para esses dispositivos e sinaliza todos os dispositivos que estão fora de conformidade.

Quando um dispositivo está fora de conformidade, é possível usar o XClarity Administrator para aplicar e ativar as atualizações de firmware para todos os dispositivos nesse dispositivo em um repositório de atualizações de firmware que você gerencia.

Nota: Atualizar o repositório e baixar atualizações de firmware requer uma conexão com a Internet. Se o XClarity Administrator não tiver conexão com a Internet, importe manualmente atualizações de firmware no repositório.

Para obter mais informações sobre atualização de firmware, consulte Atualizando firmware em dispositivos gerenciados.

Saiba mais:

- XClarity Administrator: bare metal para cluster
- XClarity Administrator: atualizações de firmware

- XClarity Administrator: fornecimento de atualizações de segurança de firmware

Implantação do sistema operacional

É possível usar o XClarity Administrator para gerenciar um repositório de imagens do sistema operacional e implantar imagens do sistema operacional em até 28 servidores gerenciados simultaneamente.

Para obter mais informações sobre implantação de sistemas operacionais, consulte Instalando sistemas operacionais em servidores bare-metal.

Saiba mais:

- XClarity Administrator: bare metal para cluster
- XClarity Administrator: implantação do sistema operacional

Gerenciamento de usuários

O XClarity Administrator fornece um servidor de autenticação centralizado para criar e gerenciar contas de usuário e para gerenciar e autenticar credenciais do usuário. O servidor de autenticação é criado automaticamente quando você inicia o servidor de gerenciamento pela primeira vez. As contas do usuário que você cria para o XClarity Administrator também podem ser usadas para fazer login no chassi gerenciado e nos servidores no modo de autenticação gerenciada. Para obter mais informações sobre usuários, consulte Gerenciando contas de usuário.

O XClarity Administrator suporta três tipos de servidor de autenticação:

- **Servidor de autenticação local**. Por padrão, o XClarity Administrator é configurado para usar o servidor de autenticação local que reside no nó de gerenciamento.
- **Servidor LDAP externo**. Atualmente, apenas o Microsoft Active Directory é suportado. Este servidor deve residir em um servidor do Microsoft Windows externo conectado à rede de gerenciamento. Quando um servidor LDAP externo for usado, o servidor de autenticação local será desativado.
- **SAML externo 2.0 provedor de identidade**. Atualmente, apenas o Microsoft Active Directory Federation Services (AD FS) é suportado. Além de inserir um nome de usuário e senha, a autenticação de vários fatores pode ser configurada para ativar segurança adicional exigindo um código PIN, a leitura de um cartão inteligente e o certificado de cliente.

Para obter mais informações sobre tipos de autenticação, consulte Gerenciando o servidor de autenticação.

Ao criar uma conta de usuário, designe um grupo de funções predefinido ou personalizado à conta do usuário para controlar o nível de acesso desse usuário. Para obter mais informações sobre grupos de funções, consulte Criando um grupo de funções personalizado.

O XClarity Administrator inclui um log de auditoria que fornece um registro histórico de ações do usuário, como efetuar logon, criar novos usuários ou alterar senhas de usuário. Para obter mais informações sobre o log de auditoria, consulte Trabalhando com eventos.

Autenticação do dispositivo

O XClarity Administrator usa os seguintes métodos para autenticar com o chassis e servidores gerenciados.

- **Autenticação gerenciada**. Quando a autenticação gerenciada é habilitada, as contas do usuário que você cria no XClarity Administrator são usadas para autenticar chassis e servidores gerenciados.

  Para obter mais informações sobre usuários, consulte Gerenciando contas de usuário.
- **Autenticação local**. Quando a autenticação gerenciada está desabilitada, as credenciais armazenadas definidas no XClarity Administrator são usadas para autenticar servidores gerenciados.

As credenciais armazenadas devem corresponder a uma conta do usuário ativa no dispositivo ou no Active Directory.

Para obter mais informações sobre credenciais armazenadas, consulte Gerenciando credenciais compartilhadas.

Segurança

Se o ambiente deve obedecer aos padrões NIST SP 800-131A, o XClarity Administrator pode ajudá-lo a obter um ambiente totalmente compatível.

O XClarity Administrator oferece suporte aos certificados SSL autoassinados (que são emitidos por uma autoridade de certificação interna) e certificados SSL externos (que são emitidos por uma CA privada ou comercial).

Firewalls no chassi e servidores podem ser configurados para aceitar solicitações de entrada apenas do XClarity Administrator.

Para obter mais informações sobre segurança, consulte Implementando um ambiente seguro.

Serviço e Suporte

O XClarity Administrator pode ser configurado para coletar e enviar arquivos de diagnóstico automaticamente ao provedor de serviço preferencial quando determinados eventos que podem ser reparados ocorrerem no XClarity Administrator e nos dispositivos gerenciados. É possível optar por enviar arquivos de diagnóstico ao Suporte da Lenovo utilizando Call Home ou outro provedor de serviço que usar SFTP. Também é possível coletar arquivos de diagnóstico manualmente, abrir um registro de problemas e enviar arquivos de diagnóstico ao Centro de Suporte da Lenovo.

Saiba mais:  XClarity Administrator: serviço e suporte

Automação de tarefas usando scripts

O XClarity Administrator pode ser integrado no gerenciamento externo de alto nível e em plataformas de automação por meio de interfaces de programação de aplicativos (APIs) abertas REST. Usando as APIs REST, o XClarity Administrator pode integrar se facilmente à sua infraestrutura de gerenciamento existente.

O kit de ferramentas do PowerShell fornece uma biblioteca de cmdlets para automatizar o fornecimento e gerenciamento de recursos em uma sessão do Microsoft PowerShell. O kit de ferramentas Python fornece uma biblioteca Python de comandos e APIs para automatizar o fornecimento e gerenciamento de recursos em um ambiente OpenStack, como Ansible ou Puppet. Os dois kits de ferramentas fornecem uma interface para as APIs REST XClarity Administrator para automatizar funções como:

- Efetuando login no XClarity Administrator
- Gerenciar e cancelar o gerenciamento de chassi, servidores, dispositivos de armazenamento e comutadores top-of-rack (dispositivos)
- Coletar e exibir dados do inventário para dispositivos e componentes
- Implantar uma imagem do sistema operacional em um ou mais servidores
- Configurar servidores com padrões de configuração
- Aplicar atualizações de firmware a dispositivos

Integração com outro software gerenciado

Os módulos XClarity Administrator integram XClarity Administrator ao software de gerenciamento de terceiros para oferecer funções de descoberta, monitoramento, configuração e gerenciamento para reduzir o custo e complexidade de administração rotineira de sistema para dispositivos suportados.

Para obter mais informações sobre o XClarity Administrator, consulte os documentos a seguir:

- Lenovo XClarity Integrator para Microsoft System Center

- Lenovo XClarity Integrator para VMware vCenter

Para considerações adicionais, consulte Considerações sobre gerenciamento na documentação online do XClarity Administrator.

Saiba mais:
- Visão geral do Lenovo XClarity Integrator para Microsoft System Center
- Lenovo XClarity Integrator para VMware vCenter

Documentação

A documentação do XClarity Administrator é atualizada regularmente online em inglês. Consulte o Documentação online do XClarity Administrator para obter as informações e os procedimentos mais atualizados.

A documentação online está disponível nos seguintes idiomas:
- Alemão (de)
- Inglês (en)
- Espanhol (es)
- Francês (fr)
- Italiano (it)
- Japonês (ja)
- Coreano (ko)
- Português do Brasil (pt_BR)
- Russo (ru)
- Tailandês (th)
- Chinês simplificado (zh_CN)
- Chinês tradicional (zh_TW)

Você pode alterar o idioma da documentação online das maneiras a seguir:

- Alterar a configuração de idioma em seu navegador da Web
- Anexar `?lang=<language_code>` ao final do URL, por exemplo, para exibir a documentação online em chinês simplificado:
  `http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html?lang=zh_CN`

Efetuando login no XClarity Administrator

Faça login na interface da Web do Lenovo XClarity Administrator usando um navegador compatível.

Antes de iniciar

Use um dos seguintes navegadores da Web suportados:
- Chrome™ 48.0 ou posterior (55.0 ou superior para o Console Remoto)
- Firefox® ESR 38.6.0 ou posterior
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 ou posterior (IOS7 ou posterior e OS X)

Nota: Iniciar as interfaces do controlador de gerenciamento do XClarity Administrator usando o navegador da Web Safari não é permitido.

Efetue login na interface da Web do XClarity Administrator em um sistema que tenha conectividade de rede com o nó de gerenciamento do XClarity Administrator.

Procedimento

Conclua as seguintes etapas para fazer login na interface da Web do XClarity Administrator.

Etapa 1. Aponte seu navegador para o endereço IP do XClarity Administrator.

Dica: O acesso à interface da Web é feito por uma conexão segura. Certifique-se de usar **https**.

- **Para contêineres**. Use o endereço IPv4 especificado para a variável ${ADDRESS} para acessar o XClarity Administrator usando o seguinte URL:
  `https://<IPv4_address>/ui/login.html`

  Exemplo:
  `https://192.0.2.10/ui/login.html`

- **Para dispositivos virtuais**. O endereço IP utilizado depende de como seu ambiente é definido.

  Se você tiver as redes Eth0 e Eth1 em sub-redes diferentes e se DHCP for usado nas sub-redes, use o endereço IP de *Eth1* ao acessar a interface da Web para configuração inicial. Quando o XClarity Administrator é iniciado pela primeira vez, Eth0 e Eth1 obtêm um endereço IP designado por DHCP e o gateway padrão do XClarity Administrator é configurado para o gateway designado por DHCP para *Eth1*.

  Usando um endereço IPv4 estático

  Se você especificou um endereço IPv4 em eth0_config, use esse endereço IPv4 para acessar XClarity Administrator usando o seguinte URL:
  `https://<IPv4_address>/ui/login.html`

  Exemplo:
  `https://192.0.2.10/ui/login.html`

  Usando um servidor DHCP no mesmo domínio de transmissão como XClarity Administrator

  Se um servidor DHCP estiver configurado no mesmo domínio de transmissão como XClarity Administrator, use o endereço IPv4 que é exibido no console de máquina virtual de XClarity Administrator para acessar XClarity Administrator usando o seguinte URL:
  `https://<IPv4_address>/ui/login.html`

  Exemplo:
  `https://192.0.2.10/ui/login.html`

  Usando um servidor DHCP em um domínio de transmissão diferente como XClarity Administrator

  Se um servidor DHCP *não estiver* configurado no mesmo domínio de transmissão, use o endereço de link local (LLA) IPv6 que é exibido para eEth0 (rede de gerenciamento) no console de máquina virtual de XClarity Administrator para acessar XClarity Administrator, por exemplo:

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
```

```
2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
x. To continue without changing IP settings
… …
```

Dica: O endereço de link local (LLA) do IPv6 é derivado do endereço MAC da interface.

Atenção: Se estiver configurando XClarity Administrator remotamente, você deverá ter conectividade com a mesma rede de camada 2. Ela deve ser acessada de um endereço não roteado até a configuração inicial ser concluída. Portanto, considere acessar XClarity Administrator de outra VM que tenha conectividade com XClarity Administrator. Por exemplo, é possível acessar XClarity Administrator de outra VM no host em que XClarity Administrator está instalado.

– **Firefox:**

  Para acessar a interface da Web do XClarity Administrator em um navegador Firefox, faça login usando o URL a seguir. Observe que os colchetes são necessários ao inserir endereços IPv6.

  `https://[<IPv6_LLA>/ui/login.html]`

  Por exemplo, com base no exemplo anterior mostrado para Eth0, insira o seguinte URL em seu navegador da Web:

  `https://[fe80:21a:64ff:fe12:3456]/ui/login.html`

– **Internet Explorer:**

  Para acessar a interface da Web do XClarity Administrator em um navegador Internet Explorer, faça login usando o URL a seguir. Observe que os colchetes são necessários ao inserir endereços IPv6.

  `https://[<IPv6_LLA>%25<zone_index>]/ui/login.html`

  em que <*zone_index*> é o identificador do adaptador Ethernet conectado à rede de gerenciamento do computador no qual você iniciou o navegador da Web. Se você estiver usando um navegador no Windows, use o comando `ipconfig` para localizar o índice da zona, que é exibido após o sinal de porcentagem (%) no campo **Endereço IPv6 Local de Link** do adaptador. Neste exemplo, o índice da zona é "30."

```
PS C:> ipconfig
Configuração de IP do Windows

Adaptador Ethernet vEthernet (teamVirtualSwitch):

   Sufixo DNS específico da conexão  . :
   Endereço IPv6 local do link . . . . . : 2001:db8:56ff:fe80:bea3%30
   Endereço IPv4 de autoconfiguração. . : 192.0.2.30
   Gateway Padrão . . . . . :
```

  Se estiver usando um navegador no Linux, use o comando `ifconfig` para localizar o índice da zona. Você também pode usar o nome do adaptador (normalmente Eth0) como o índice da zona.

  Por exemplo, com base nos exemplos mostrados para Eth0 e o índice da zona, insira o seguinte URL em seu navegador da Web:

  `https://[2001:db8:56ff:fe80:bea3%2530]/ui/login.html`

A página de login inicial de XClarity Administrator é exibida:

Etapa 2. Selecione o idioma desejado na lista suspensa **Idioma**.

Nota: Os parâmetros de configuração e os valores que são fornecidos pelos dispositivos gerenciados podem estar disponíveis apenas em inglês.

Etapa 3. Insira um ID de usuário e senha válidos, e clique em **Fazer Login**.

Na primeira vez que você fazer login em uma conta do usuário, será necessário alterar a senha. As senhas devem satisfazer os seguintes critérios:

- (1) Deve conter pelo menos um caractere alfabético e não deve ter mais de dois caracteres sequenciais, incluindo sequências de caracteres alfabéticos, dígitos e teclas de teclado do QWERTY (por exemplo, "abc", "123" e "asd" não são permitidos).
- (2) Deve conter pelo menos um número (0 a 9).
- (3) Deve conter pelo menos *dois* dos caracteres a seguir.
  - Caracteres alfabéticos maiúsculos (A – Z)
  - Caracteres alfabéticos minúsculos (a – z)
  - Caracteres especiais ; @ _ ! ' $ & +
- (4) Não deve repetir nem reverter o nome do usuário.
- (5) Não deve conter mais de dois caracteres consecutivos (por exemplo, "aaa", "111" e "..." não são permitidos).

Depois de concluir

A página do painel de XClarity Administrator é exibida:

Nota: Se o sistema operacional do host for desligado inesperadamente, você poderá receber um erro de autenticação ao tentar fazer login em XClarity Administrator. Para resolver esse problema, restaure XClarity Administrator do backup mais recente para acessar o servidor de gerenciamento (consulte Fazendo backup do Lenovo XClarity Administrator).

É possível executar as ações a seguir no menu de ação do usuário (ADMIN_USER) na barra de título XClarity Administrator.

- Encontre informações sobre como usar o XClarity Administrator no sistema de ajuda integrado, clicando em **Ajuda**.

  A documentação do XClarity Administrator é atualizada regularmente online em inglês. Consulte o Documentação online do XClarity Administrator para obter as informações e os procedimentos mais atualizados.
- Exiba a licença do XClarity Administrator clicando em **Licença**.
- Exiba informações sobre a versão do XClarity Administrator clicando em **Sobre**.
- Altere o idioma da interface do usuário clicando em **Alterar idioma**.
- Faça logout da sessão atual clicando em **Fazer logout**.
- Envie ideias ou forneça comentários sobre o XClarity Administrator clicando em **Enviar ideias** ou **Enviar feedback**.
- Faça perguntas e encontre respostas no Site do fórum da comunidade do Lenovo XClarity clicando em **Visitar fórum**.

Dicas e técnicas de interface do usuário

Considere estas dicas e técnicas ao usar a interface do usuário do Lenovo XClarity Administrator

Visualizando mais ou menos dados por página

É possível alterar o número de linhas exibidas por página usando os links na parte inferior direita da tabela. É possível exibir **10**, **25**, **50** ou **Todas** linhas

Localizando dados em listas grandes

A maioria dos campos pode aceitar até 128 caracteres.

Há várias maneiras de exibir um subconjunto de uma lista grande com base em critérios específicos.

- É possível classificar as linhas da tabela clicando no cabeçalho da coluna.

  Alterar a ordem de classificação de uma coluna de tabela é permanente nas sessões do usuário.
- É possível usar os ícones **Filtrar Por** e a lista suspensa **Mostrar** disponíveis em algumas páginas para exibir um subconjunto de dados com base nos critérios selecionados.
- É possível refinar ainda mais o subconjunto inserindo texto (como um nome ou endereço IP) no campo **Filtros** para localizar os dados encontrados em qualquer coluna disponível.

  É possível escolher entre as 10 últimas pesquisas selecionando as pesquisa no menu da lista suspensa no campo **Filtros**. A última pesquisa ativa em uma página é permanente nas sessões do usuário.

Visualizando dados da coluna

Se o tamanho da coluna evitar que todas as informações sejam exibidas na célula da tabela (indicada por reticências), você poderá exibir as informações completas em um pop-up passando o mouse sobre o texto na célula.

Configurar colunas da tabela

É possível configurar tabelas para mostrar informações que são importantes para você.

- É possível escolher quais colunas mostrar ou ocultar clicando em **Todas as Ações → Alternar Colunas**.
- É possível reordenar colunas arrastando os cabeçalhos de coluna para o local preferencial.

Alterando o idioma da interface do usuário

Você tem a opção de definir o idioma da interface do usuário ao fazer login pela primeira vez.

Depois de fazer login, é possível alterar o idioma da interface do usuário clicando no menu de ações do usuário (

) e, em seguida, em **Alterar idioma**. Selecione o idioma que você deseja exibir.

Nota: O sistema de ajuda é exibido no mesmo idioma definido para a interface do usuário.

Obtendo Ajuda

O XClarity Orchestrator oferece várias maneiras para obter ajuda com a interface do usuário.

- Algumas páginas fornecem detalhes adicionais sobre um campo ou status específico usando os ícones **Ajuda** (). Passe o cursor sobre o ícone para exibir um pop-up com informações úteis.
- Para obter ajuda sobre como executar ações específicas na interface do usuário, clique no menu de ações do usuário (

) e, em seguida, clique em **Ajuda**.

Usando o aplicativo Lenovo XClarity Mobile

O Lenovo XClarity Administrator oferece um aplicativo móvel para dispositivos com Android e iOS. É possível usar o aplicativo Lenovo XClarity Mobile para monitorar com segurança sistemas físicos, obter notificações e alertas de status em tempo real e tomar medidas quanto a tarefas comuns de nível do

sistema. O aplicativo também pode se conectar diretamente por meio de uma porta USB habilitada a um servidor ThinkSystem e fornecer o recurso de LCD virtual.

Saiba mais:  Visão geral sobre o aplicativo Lenovo XClarity Mobile

Usando o aplicativo XClarity Mobile, é possível executar as atividades a seguir:
- Configurar definições de rede e propriedades
- Exibir o resumo de status de cada XClarity Administrator conectado.
- Exibir o resumo de status de todos os dispositivos gerenciados.
- Visualizar exibições gráficas (mapas) do chassi, servidores de rack e dispositivos de armazenamento.
- Exiba grupos de recursos que são definidos no XClarity Administrator.
- Exiba informações de portas de comutador de rack e altere o status da porta configurada.
- Monitorar o inventário e o status detalhado de cada dispositivo gerenciado.
- Monitorar eventos de auditoria, eventos de hardware e de gerenciamento, alertas e trabalhos.
- Ligar/desligar o LED de local em um dispositivo gerenciado.
- Ligar, desligar, reiniciar ou reposicionar um dispositivo gerenciado.
- Acionar a coleta de dados diagnósticos.
- Exibir status e informações sobre garantia de dispositivo
- Configurar uma notificação de problema automática por meio do Call Home.
- Exibir o resumo de tíquetes de serviço abertos e excluir tíquetes de serviço
- Enviar por push notificações de eventos para seu dispositivo móvel (consulte Encaminhamento de eventos à dispositivos móveis).
- Exibir o resumo de usuários ativos e uso de recursos do sistema
- Enviar comentários sobre esse aplicativo móvel para o Suporte Lenovo.
- Conecte o dispositivo móvel diretamente a um servidor ThinkSystem para gerenciar o servidor usando o aplicativo XClarity Mobile (para dispositivos que suportam compartilhamento USB).
- Baixe dados de serviço do Lenovo XClarity Controller quando o dispositivo móvel estiver conectado a um servidor ThinkSystem.

Também é possível conectar seu dispositivo móvel diretamente aos servidores ThinkSystem e, em seguida, iniciar o aplicativo XClarity Mobile e fazer login no Baseboard Management Controller do servidor usando as mesmas credenciais da Web e CLI. Um menu de informações adicionais e ações está disponível, incluindo:

- Serviço
  - Compartilhar informações de resumo usando e-mail ou outros meios fornecidos pelo dispositivo móvel
  - Limpar o log de auditoria e de eventos
  - Baixar o log de auditoria e de eventos para o armazenamento local do dispositivo móvel ou transmitir o log por outros meios fornecidos pelo dispositivo móvel
  - Baixar o arquivo de serviço BMC FFDC para o armazenamento local do dispositivo móvel ou transmitir o arquivo por outros meios fornecidos pelo dispositivo móvel
  - Exibir dados de gráfico de histórico de uso de energia, temperatura e sistema
  - Ativar o modo de serviço "Um Toque", que fornece um resumo imediato de alertas ativos e informações sobre o dispositivo crítico
- Instalação e configuração inicial
  - Gerenciar um novo dispositivo usando o XClarity Administrator selecionado
  - Configurar propriedades do servidor, como local e informações de contato para configuração inicial
  - Exibir e alterar as configurações de interface de rede do BMC IPv4 e IPv6
  - Especificar a ordem de inicialização e configurações de inicialização única
  - Alterar a atribuição da porta USB do painel frontal
  - Exibir o número de reinicializações do servidor e as horas totais em que ele ficou ligado
- Ações de Energia
  - Ligar ou desligar o servidor, reiniciando o servidor ou acionando o NMI
  - Redefinir o BMC

Dica: depois de abrir o aplicativo, você deve atualizá-lo para consultar o status atualizado, o inventário, eventos e trabalhos.

Pré-requisitos

- Tablets iOS são aceitos apenas na resolução de tela do iPhone. Tablets Android não são aceitos atualmente.
- Os sistemas operacionais móveis a seguir são aceitos:
  - Android 7 – 11
  - iOS 10 e posterior

    Notas:

    - O Android 5 é aceito apenas para XClarity Mobile 2.3.0 e anterior.
    - O reconhecimento facial que é usado em dispositivos iPhone X/XR/XS não é suportado.
- Garanta que uma conexão de rede esteja disponível no dispositivo móvel às instâncias do XClarity Administrator. Isso pode requerer o uso de uma solução de VPN. Consulte o administrador de rede para obter assistência.
- Importe o certificado da CA para cada instância do XClarity Administrator.

  Importante: Todas as conexões do XClarity Administrator usam HTTPS. Entretanto, deve haver uma cadeia de certificados válida para que a conexão seja considerada confiável e os dados possam ser transmitidos ao dispositivo móvel. Para criar uma cadeia de certificados confiáveis, você deverá importar a autoridade de certificação (CA) autoassinada do XClarity Administrator para o dispositivo móvel.

  Para importar o certificado da CA autoassinado de *cada instância do XClarity Administrator* para o dispositivo móvel, conclua as seguintes etapas.

  1. Baixe o certificado da CA para um sistema local:
     a. Conecte-se à instância do XClarity Administrator usando um navegador da Web no sistema local.
     b. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança** para exibir a página Segurança.
     c. Clique em **Autoridade de Certificação** na seção Gerenciamento de Certificados. A página Autoridade de Certificação é exibida.
     d. Clique em **Baixar Certificado Raiz da Autoridade de Certificação**.

        Atenção: Normalmente, não é necessário clicar em **Gerar Certificado Raiz da Autoridade de Certificação Novamente** para concluir esse processo. Isso pode interromper a comunicação com dispositivos gerenciados, a menos que o procedimento correto seja seguido. Para obter mais informações, consulte Trabalhando com certificados de segurança.
     e. Clique em **Salvar como der** ou **Salvar como pem** para salvar o certificado da CA como um arquivo DER ou PEM no sistema local. O formato PEM funciona na maioria dos casos.
  2. Transfira o arquivo de certificado da CA para o seu dispositivo móvel, por exemplo, utilizando um repositório de armazenamentos acessível (como Dropbox™), e-mail ou transferência de arquivos por um cabo conectado.
  3. Importe os certificados da CA confiáveis:
     - (Android) Em geral, isso é feito selecionando **Configurações → Segurança → Instalar** no armazenamento do telefone e depois selecionando o arquivo de certificado baixado.

       Importante: Se o certificado da CA instalado com êxito não for assinado por terceiros, a mensagem `A rede pode ser monitorada por um terceiro desconhecido` será exibida em dispositivos Android. Como o certificado da CA é gerado em seu ambiente de confiança, essa mensagem

pode ser ignorada com segurança. Certifique-se de que a mensagem seja para o certificado da CA do XClarity Administrator antes de ignorar a mensagem.

– (iOS) Abra o e-mail em seu dispositivo móvel e clique no link do documento no e-mail para importar o certificado da CA confiável.

Atenção: Para iOS 10.3 e posterior, os certificados importados não são confiáveis por padrão. Para confiar nos certificados, selecione **Configurações → Geral → Sobre → Configurações de Confiança do Certificado** e habilite a confiança do certificado.

Instalando e configurando

1. Baixe o aplicativo XClarity Mobile da iTunes App Store (iOS) ou da Google Play Store (Android).
2. Para instalar o aplicativo, siga as instruções no dispositivo móvel.

   Importante: É necessário um código de segurança do sistema operacional móvel para desbloquear a tela e usar o aplicativo XClarity Mobile. Se ainda não houver um configurado, configure um durante a instalação.
3. Clique em **Configurações** para adicionar ou editar as conexões em várias instâncias do XClarity Administrator usando a descoberta automática ou fornecendo um endereço IP e as credenciais do usuário, defina um código PIN para o aplicativo, altere as configurações do log de eventos e de auditoria e selecione o idioma preferencial.

Conectando diretamente a servidores ThinkSystem

Os servidores Lenovo Think System incluem uma porta USB no painel frontal que pode ser usada para conectar seu dispositivo móvel para fornecer recursos semelhantes que estavam disponíveis no painel de exibição LCD de informações do sistema em outros servidores Lenovo.

Para gerenciar um servidor ThinkSystem conectando diretamente ao servidor, conclua estas etapas.

1. Alterne o painel frontal USB do servidor de host para BMC realizando uma das seguintes etapas.
   a. Na CLI do controlador de gerenciamento, execute o comando `usbfp`
   b. Na interface da Web do controlador de gerenciamento, clique em **Configuração BMC → Rede → Gerenciamento da Porta USB do Painel Frontal**.
   c. No painel frontal, mantenha pressionado o LED de local de ID azul por pelo menos 3 segundos até que a luz pisque a cada dois segundos.
2. Conecte o cabo USB do telefone na porta USB do painel frontal no servidor ThinkSystem.
3. No dispositivo móvel, habilite o compartilhamento USB.
   a. Para iOS, clique em **Configurações → Celular → Hotspot Pessoal**.
   b. Para Android, clique em **Configurações → Hotspot móvel e compartilhamento → Compartilhamento USB**.
4. No dispositivo móvel, inicie o aplicativo XClarity Mobile.
5. Se a descoberta automática estiver desabilitada, clique em **Descoberta** na página Descoberta USB para conectar o controlador de gerenciamento do servidor e coletar informações, incluindo inventário, integridade, firmware, configuração de rede e uma lista dos eventos ativos mais recentes.

Dica:

- Use um cabo USB de alta qualidade que suporte dados e energia. Observe que alguns cabos fornecidos com dispositivos móveis servem apenas para fins de carregamento.

  Nota: Para conectar-se ao ThinkSystem SD530, use um cabo USB ou micro USB de alta qualidade ou adaptador.

- O servidor USB conectado deve estar ligado para relatar o conjunto completo de estatísticas de voltagem, temperatura e uso nos cartões de status resumido.
- Se o servidor USB conectado não tiver um LED/botão externo de "identificação azul" no painel frontal, use a interface da Web do controlador de gerenciamento ou a CLI para alterar a seleção de gerenciamento da porta USB do painel frontal, se necessário.
- As alterações feitas na interface de rede do controlador de gerenciamento no aplicativo XClarity Mobile têm efeito imediatamente sem exigir que o controlador de gerenciamento seja reiniciado. Por exemplo, se a interface IPv4 for alterada de um endereço estático para DHCP, a interface obtém imediatamente um endereço atribuído pelo DHCP.
- Na guia NewsFeed, o cartão "Eventos ativos mais recentes" exibe inicialmente até três eventos ativos listados na guia Eventos Ativos do controlador de gerenciamento. No aplicativo móvel, se você tocar nesse cartão, todos os eventos ativos, serão exibidos. Observe que esta é uma lista de eventos ativos e resolvidos, não uma lista completa de todos os eventos.

Usando o modo de demonstração

É possível ativar o **Modo de Demonstração** na página Configurações para preencher o aplicativo XClarity Mobile com dados da demonstração para as instâncias do XClarity Administrator, incluindo racks e chassis. Nesse modo, você pode exibir o resumo de status das instâncias do XClarity Administrator, exibir o status detalhado e o inventário dos dispositivos e monitorar eventos e alertas. Entretanto, as ações de gerenciamento, como ligar e desligar, não são aceitas.

Notas:

- É possível habilitar o modo de demonstração apenas quando não há conexões com as instâncias reais do XClarity Administrator.
- Não é possível adicionar conexões às instâncias reais do XClarity Administrator enquanto o modo de demonstração está habilitado.

Pesquisando

É possível usar o campo **Pesquisar** para exibir dispositivos gerenciados com um nome ou um status específico (Crítico, Aviso ou Normal). Por exemplo, se você procurar por "crit," apenas dispositivos gerenciados no status Crítico e com nomes que incluam "crit" serão exibidos.

Resolvendo problemas

Problemas de instalação:

- O aplicativo móvel Android é "assinado" com uma chave segura para melhorar a segurança. O tamanho da chave segura foi aumentado na nova versão. Como o aplicativo assinado não corresponde à assinatura de aplicativos anterior, o processo de segurança de instalação do Android impede a atualização automática.

  Para atualizar o aplicativo móvel, desinstale a versão atual do aplicativo móvel, baixe a versão mais recente do aplicativo Android na loja de aplicativos e reinstale o aplicativo. Na maioria dos dispositivos Android, o aplicativo pode ser desinstalado usando o item de menu **Configurações → Aplicativos → Gerenciador de Aplicativos**.

Problemas de conectividade:

- A função de compartilhamento USB no iOS 14, 14.0.1 e 14.0.2 não está funcionando corretamente e, portanto, a função de compartilhamento do aplicativo Lenovo XClarity Mobile não está disponível para essas versões do iOS. Isso afeta apenas o gerenciamento portátil conectado ao USB no datacenter. O gerenciamento remoto usando dispositivos móveis que oferecem suporte a comunicações celulares e Wi-Fi não é afetado e pode ser usado para conectar e coletar dados do XClarity Administrator e executar ações de gerenciamento em dispositivos gerenciados.

Se a função de gerenciamento portátil conectado ao USB for necessária, não faça a atualização para o iOS 14.

Esta notificação será atualizada quando a Apple resolver o problema com o iOS 14.

- O XClarity Mobile requer uma conexão de rede disponível do dispositivo móvel às instâncias do XClarity Administrator. Isso pode requerer o uso de uma solução de VPN. Consulte o administrador de rede para obter assistência.
- As conexões de seu dispositivo móvel com cada instância do XClarity Administrator requerem uma cadeia de certificados confiáveis. Consulte a documentação online para obter instruções para baixar e instalar os certificados confiáveis da CA em seu dispositivo móvel.

  Se o certificado da CA instalado com êxito não for assinado por terceiros, a mensagem `A rede pode ser monitorada por um terceiro desconhecido` será exibida. Como o certificado da CA é gerado em seu ambiente de confiança, essa mensagem pode ser ignorada com segurança. Certifique-se de que a mensagem seja para o certificado da CA do XClarity Administrator antes de ignorar a mensagem.
- Ao alternar entre seu dispositivo móvel a partir de uma rede privada virtual (VPN) e uma rede local ou vice versa, você poderá ver a mensagem `O gateway seguro rejeitou a tentativa de conexão. Uma nova tentativa de conexão com o gateway ou outro gateway seguro será necessária, o que exigirá uma nova autenticação.` Faça login no Lenovo XClarity Mobile para continuar a usar o aplicativo.

Problemas de segurança:

- Se você esquecer o código PIN, desinstale e reinstale o aplicativo XClarity Mobile. Em seguida, restabeleça todas as conexões.
- Se você limpar as credenciais em um dispositivo Android, a chave de criptografia será apagada. Você deve restabelecer todas as conexões.

Problemas de eventos:

- Por padrão, o log de eventos mostra os eventos de hardware e de gerenciamento que foram recebidos nas últimas 24 horas, e o log de auditoria mostra os eventos de auditoria recebidos nas últimas 2 horas. Se nenhum evento foi recebido durante os períodos selecionados, o log de eventos e de auditoria não serão mostrados na página Monitoramento no XClarity Mobile.
- Se você configurar o encaminhamento de evento no XClarity Administrator para enviar eventos para uma conta de e-mail, os links no e-mail poderão não funcionar em dispositivos Android. Certifique-se de que a versão do Android e o aplicativo de e-mail ofereçam suporte a hiperlinks. Se hiperlinks não forem aceitos, use outro aplicativo de e-mail.

Problemas do sistema de Ajuda:

- Em alguns dispositivos, o sistema de Ajuda não é dimensionado corretamente para o tamanho da tela. Use os controles de sistema de ajuda para maximizar e, em seguida, minimizar a página.

Capítulo 2. Administração de Lenovo XClarity Administrator

Várias tarefas de administração, como incluir usuários ou exibir trabalhos, estão disponíveis em Lenovo XClarity Administrator.

Gerenciando autenticação e autorização

O Lenovo XClarity Administrator fornece mecanismos de segurança para verificar as credenciais de um usuário e controlar o acesso a recursos e tarefas.

Gerenciando o servidor de autenticação

Por padrão, o Lenovo XClarity Administrator usa um servidor LDAP local para autenticar as credenciais do usuário.

Sobre esta tarefa

Servidores de autenticação suportados

O *servidor de autenticação* é um registro do usuário utilizado para autenticar as credenciais do usuário. O Lenovo XClarity Administrator oferece suporte aos seguintes tipos de servidores de autenticação.

- **Servidor de autenticação local**. Por padrão, o XClarity Administrator é configurado para usar o servidor LDAP integrado que reside no servidor de gerenciamento.
- **Servidor LDAP externo**. Atualmente, somente Microsoft Active Directory e OpenLDAP são aceitos. Este servidor deve residir em um servidor do Microsoft Windows externo conectado à rede de gerenciamento. Quando um servidor LDAP externo for usado, o servidor de autenticação local será desativado.

  Atenção: Para configurar o método de ligação do Active Directory para usar credenciais de login, o Baseboard Management Controller de cada servidor gerenciado deve estar executando o firmware de setembro de 2016 ou posterior.
- **Sistema externo de gerenciamento de identidade**. Atualmente, apenas o CyberArk é suportado.

  Se as contas de usuário de um servidor ThinkSystem ou ThinkAgile estiverem integradas ao CyberArk, você poderá escolher que o XClarity Administrator recupere credenciais do CyberArk para fazer login no servidor ao configurar inicialmente os servidores para gerenciamento (com autenticação gerenciada ou local). Para que as credenciais possam ser recuperadas do CyberArk, os caminhos do CyberArk devem ser definidos no XClarity Administrator e a confiança mútua deve ser estabelecida entre o CyberArk e o XClarity Administrator usando autenticação mútua TLS por meio de certificados de cliente.
- **SAML externo provedor de identidade**. Atualmente, apenas o Microsoft Active Directory Federation Services (AD FS) é suportado. Além de inserir um nome de usuário e senha, a autenticação de vários fatores pode ser configurada para ativar segurança adicional exigindo um código PIN, a leitura de um cartão inteligente e o certificado de cliente. Quando um provedor de identidade SAML for usado, o servidor de autenticação local não será desabilitado. As contas do usuário local são necessárias para fazer login diretamente a um chassi ou um servidor gerenciado (a menos que o Encapsulamento esteja habilitado nesse dispositivo), para autenticação PowerShell e API REST, e para recuperação se a autenticação externa não estiver disponível.

  Você pode escolher usar um servidor LDAP externo e um provedor de identidade externo. Se ambos estiverem habilitados, o servidor LDAP externo será usado para fazer login diretamente nos dispositivos gerenciados, e o provedor de identidade será usado para fazer login no servidor de gerenciamento.

Autenticação do dispositivo

Por padrão, os dispositivos são gerenciados usando a autenticação gerenciada do XClarity Administrator para fazer login nos dispositivos. Ao gerenciar servidores em rack e chassis da Lenovo, você pode optar por usar autenticação local ou autenticação gerenciada para fazer login nos dispositivos.

- Quando a *autenticação local* é usada para servidores em rack, chassi da Lenovo e comutadores de rack da Lenovo, o XClarity Administrator usa uma credencial armazenada para autenticar o dispositivo. A *credencial armazenada* pode ser uma conta do usuário ativa no dispositivo ou uma conta do usuário em um servidor do Active Directory.

  Você deve criar uma credencial armazenada no XClarity Administrator que corresponda a uma conta do usuário ativa no dispositivo ou uma conta do usuário em um servidor do Active Directory antes de gerenciar o dispositivo usando a autenticação local (consulte Gerenciando credenciais compartilhadas na documentação online do XClarity Administrator).

  Notas:

  – Dispositivos RackSwitch oferecem suporte apenas a credenciais armazenadas para autenticação. Não há suporte para as credenciais do usuário do XClarity Administrator.
- Usar a *autenticação gerenciada* permite gerenciar e monitorar vários dispositivos usando as credenciais no servidor de autenticação do XClarity Administrator em vez de credenciais locais. Quando a autenticação gerenciada é usada para um dispositivo (diferente de servidores ThinkServer, servidores System x M4 e comutadores), o XClarity Administrator configura o dispositivo e seus componentes instalados para usar o servidor de autenticação do XClarity Administrator para gerenciamento centralizado.

  – Quando a autenticação gerenciada estiver habilitada, você poderá gerenciar dispositivos usando credenciais armazenadas ou inseridas manualmente (consulte Gerenciando contas de usuário e na documentação online do XClarity Administrator).

    A credencial armazenada é usada somente até que o XClarity Administrator configure as definições LDAP no dispositivo. Depois disso, qualquer mudança nas credenciais armazenadas não tem impacto no gerenciamento ou no monitoramento desse dispositivo.

    Nota: Quando a autenticação gerenciada é ativada para um dispositivo, não é possível editar credenciais armazenadas para esse dispositivo usando o XClarity Administrator.

  – Se um servidor LDAP local ou externo for usado como servidor de autenticação do XClarity Administrator, as contas de usuário definidas no servidor de autenticação serão usadas para fazer login no XClarity Administrator, em CMMs e no Baseboard Management Controllers no domínio XClarity Administrator. As contas de usuário do CMM local e do controlador de gerenciamento são desativadas.

  – Se um provedor de identidade SAML 2.0 for usado como servidor de autenticação do XClarity Administrator, as contas de SAML não estarão acessíveis para dispositivos gerenciados. Entretanto, ao usar um provedor de identidade SAML e um servidor LDAP juntos, se o provedor de identidade usar contas existentes no servidor LDAP, as contas de usuário LDAP poderão ser usadas para fazer login nos dispositivos gerenciados, enquanto os métodos de autenticação mais avançados fornecidos por SAML 2.0 (como autenticação de vários fatores e logon único) podem ser usados para fazer login no XClarity Administrator.

  – O login único permite que um usuário já conectado ao XClarity Administrator faça login automaticamente no Baseboard Management Control. O login único é ativado por padrão quando um servidor ThinkSystem ou ThinkAgile é trazido para o gerenciamento pelo XClarity Administrator (a menos que o servidor seja gerenciado com senhas do CyberArk). É possível definir a configuração global para ativar ou desabilitar o login único para todos os servidores ThinkSystem e ThinkAgile gerenciados. Ativar o login único para um servidor ThinkSystem e ThinkAgile específico substitui a configuração global para todos os servidores ThinkSystem e ThinkAgile (consulte).

Nota: O logon único é desativado automaticamente ao usar o sistema de gerenciamento de identidade CyberArk para autenticação.

- Quando a autenticação gerenciada está ativada para servidores ThinkSystem SR635 e SR655:
  - O firmware do controlador de gerenciamento do baseboard oferece suporte a até cinco funções de usuário LDAP. O XClarity Administrator adiciona essas funções de usuário LDAP aos servidores durante o gerenciamento: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** e **lxc-os-admin**.

    Os usuários devem ser atribuídos a pelo menos uma das funções de usuário LDAP especificadas para se comunicar com os servidores ThinkSystem SR635 e SR655.
  - O firmware do controlador de gerenciamento não oferece suporte aos usuários LDAP com o mesmo nome do usuário local do servidor.
- Para servidores ThinkServer e System x M4, o servidor de autenticação do XClarity Administrator não é usado. Em vez disso, uma conta IPMI é criada no dispositivo com o prefixo "LXCA_" acompanhado por uma sequência aleatória. (As contas do usuário do IPMI local existente estão desabilitadas.) Quando você cancelar o gerenciamento de um servidor ThinkServer, a conta do usuário do "LXCA_" será desabilitada e o prefixo "LXCA_" será substituído por "DISABLED_". Para determinar se um servidor ThinkServer é gerenciado por outra instância, o XClarity Administrator verifica as contas de IPMI com o prefixo "LXCA_". Se você escolher forçar o gerenciamento de um servidor ThinkServer gerenciado, todas as contas de IPMI no dispositivo com o prefixo "LXCA_" serão desabilitadas e renomeadas. Considere apagar manualmente as contas de IPMI que não são mais usadas.

  Se você usar credenciais inseridas manualmente, o XClarity Administrator criará uma credencial armazenada automaticamente e usará essa credencial armazenada para gerenciar o dispositivo.

  Notas: Quando a autenticação gerenciada é ativada para um dispositivo, não é possível editar credenciais armazenadas para esse dispositivo usando o XClarity Administrator.

  - Cada vez que você gerencia um dispositivo usando credenciais inseridas manualmente, uma nova credencial armazenada é criada para o dispositivo, mesmo se outra credencial armazenada foi criada para o dispositivo durante um processo de gerenciamento anterior.
  - Quando você cancela o gerenciamento de um dispositivo, o XClarity Administrator não exclui credenciais armazenadas que foram criadas automaticamente para esse dispositivo durante o processo de gerenciamento.

Conta de recuperação

Se você especificar uma senha de recuperação, o XClarity Administrator desativará a conta do usuário do CMM local ou do controlador de gerenciamento e criará uma nova conta de usuário de recuperação (`RECOVERY_ID`) no dispositivo para futura autenticação. Se o servidor de gerenciamento falhar, será possível usar a conta `RECOVERY_ID` para fazer login no dispositivo e executar ações de recuperação a fim de restaurar as funções de gerenciamento de conta no dispositivo até que o nó de gerenciamento seja restaurado ou substituído.

Se você cancelar o gerenciamento de um dispositivo que tem uma conta de usuário `RECOVERY_ID` todas as contas do usuário do CMM local serão habilitadas, e a conta `RECOVERY_ID` será excluída.

- Se você alterar as contas do usuário local desabilitadas (por exemplo, se você alterar uma senha), as alterações não terão efeito na conta `RECOVERY_ID`. No modo de autenticação gerenciada, a conta `RECOVERY_ID` será a única a conta do usuário ativada e operacional.
- Use a conta `RECOVERY_ID` apenas em caso de emergência, por exemplo, se o servidor de gerenciamento falhar ou se um problema de rede impedir o dispositivo de se comunicar com o XClarity Administrator para autenticar os usuários.
- A senha de `RECOVERY_ID` é especificada quando você descobre o dispositivo. Certifique-se de gravar a senha para uso posterior.

Para obter informações sobre como recuperar o gerenciamento de um dispositivo, consulte "Recuperando o gerenciamento com um CMM após uma falha no servidor de gerenciamento" na página 227 e "Recuperando o gerenciamento do servidor em torre ou do rack após uma falha no servidor de gerenciamento" na página 279.

Configurando um servidor de autenticação LDAP externo

É possível usar um servidor de autenticação LDAP externo em vez do servidor de autenticação Lenovo XClarity Administrator local no nó de gerenciamento.

Antes de iniciar

A configuração inicial do XClarity Administrator deve ser concluída antes de configurar o servidor de autenticação externo.

Os servidores de autenticação externos a seguir são suportados:

- OpenLDAP
- Microsoft Active Directory. Deve residir em um servidor do Microsoft Windows externo conectado à rede de gerenciamento, à rede de dados ou a ambas

Garanta que todas as portas necessárias para o servidor de autenticação externo estejam abertas na rede e nos firewalls. Para obter informações sobre requisitos de porta, consulte Disponibilidade de porta na documentação online do XClarity Administrator.

Você deve criar ou renomear grupos de funções no servidor de autenticação local para fazer a correspondência dos grupos definidos no servidor de autenticação externo.

Certifique-se de que haja um ou mais usuários com autoridade **lxc-recovery** no servidor de autenticação local. É possível usar essa conta de usuário local para autenticar diretamente no XClarity Administrator quando ocorre um erro de comunicação com o servidor LDAP externo.

Nota: Quando o XClarity Administrator está configurado para usar um servidor de autenticação externo, a página Gerenciamento de Usuários na interface da Web do XClarity Administrator está desabilitada.

Atenção: No Active Directory, para configurar o método de ligação para usar credenciais de login, o Baseboard Management Controller de cada servidor gerenciado deve estar executando o firmware de setembro de 2016 ou posterior.

O XClarity Administrator executa uma verificação de conectividade cada 5 minutos para manter a conectividade com os servidores LDAP externos configurados. Ambientes com muitos servidores LDAP podem apresentar alto uso de CPU durante essa verificação de conectividade. Para obter melhor desempenho, garanta que a maioria ou todos os servidores LDAP no domínio estejam acessíveis ou defina o método de seleção de servidor de autenticação como **Usar Servidores Pré-configurados** e especifique apenas servidores LDAP conhecidos e acessíveis.

Procedimento

Para configurar o XClarity Administrator para usar um servidor de autenticação externo, conclua as seguintes etapas.

Etapa 1. Configure o método de autenticação de usuários para o Microsoft Active Directory ou OpenLDAP.

Se você optar por usar autenticação não segura, nenhuma configuração adicional será necessária. Os controladores de domínio do Windows Active Directory ou OpenLDAP usam autenticação LDAP não segura por padrão.

Se você optar por usar autenticação LDAP segura, deverá configurar os controladores de domínio para permitir a autenticação LDAP segura. Para obter mais informações sobre a configuração de autenticação LDAP segura no Active Directory, consulte o Artigo sobre LDAP over SSL (LDAPS) Certificate no site Microsoft TechNet.

Para verificar se os controladores de domínio do Active Directory estão configurados para usar autenticação LDAP segura:

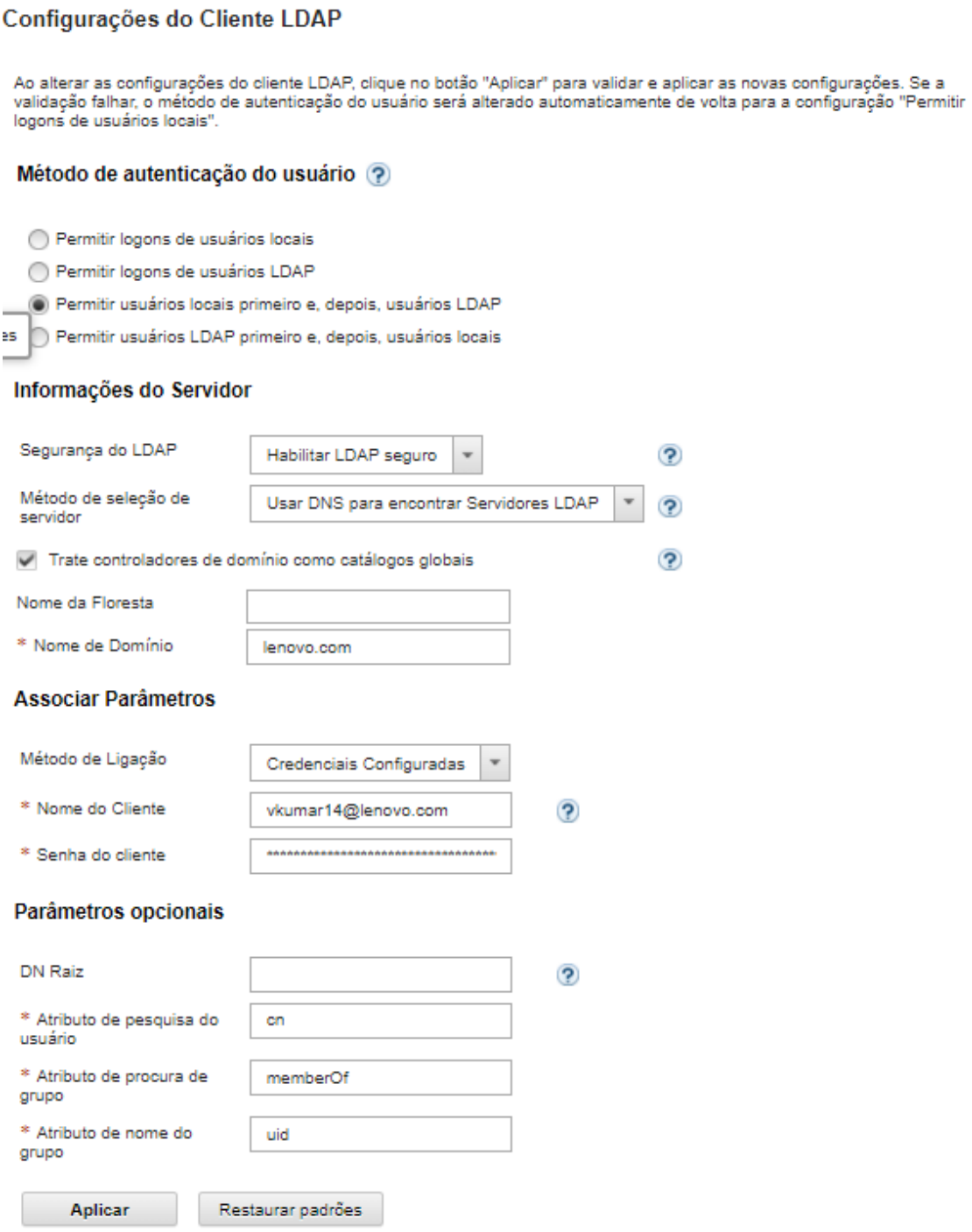
- Procure o evento `O protocolo LDAP sobre SSL agora está disponível` na janela do Visualizador de Eventos dos controladores de domínio.
- Use a ferramenta `ldp.exe` Windows para testar a conectividade LDAP segura com os controladores de domínio.

Etapa 2. Importe o certificado do servidor do Active Directory ou do OpenLDAP ou o certificado raiz da autoridade de certificação que assinou o certificado do servidor.

a. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.
b. Clique em **Certificados Confiáveis** na seção Gerenciamento de Certificados.
c. Clique no ícone **Criar** ( ) para adicionar um certificado.
d. Navegue para o arquivo ou cole o texto do certificado com formatação PEM.
e. Clique em **Criar**.

Etapa 3. Configure o cliente LDAP do XClarity Administrator:

a. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.
b. Clique no **Cliente LDAP** na seção Usuários e Grupos para exibir a caixa de diálogo Configurações do Cliente LDAP.



c. Preencha a caixa de diálogo com base nos critérios a seguir.

1. Selecione um destes métodos de autenticação do usuário:

   - **Permitir logons de usuários locais**. A autenticação é executada usando a autenticação local. Quando essa opção estiver selecionada, todas as contas de usuário existirão no servidor de autenticação local no nó de gerenciamento.
   - **Permitir logons de usuários LDAP**. A autenticação é executada por um servidor LDAP externo. Esse método permite o gerenciamento remoto de contas de usuário. Quando essa opção é selecionada, todas as contas de usuário existem remotamente em um servidor LDAP externo.

- **Permitir usuários locais primeiro, depois usuários LDAP**. O servidor de autenticação local executa a autenticação primeiro. Se isso falhar, um servidor LDAP externo executará a autenticação.
- **Permitir usuários LDAP primeiro, depois usuários locais**. Um servidor LDAP externo executará a autenticação primeiro. Se isso falhar, o servidor de autenticação local executará a autenticação.

2. Escolha entre habilitar ou desabilitar o LDAP seguro:
   - **Habilitar LDAP seguro**. O XClarity Administrator usa o protocolo LDAPS para se conectar com segurança ao servidor de autenticação externo. Quando essa opção for selecionada, você também deverá configurar certificados confiáveis para habilitar o suporte de LDAP seguro.
   - **Desabilitar LDAP seguro**. O XClarity Administrator usa um protocolo não seguro para se conectar ao servidor de autenticação externo. Se você escolher essa configuração, o hardware poderá ficar mais vulnerável a ataques à segurança.
3. Selecione um destes métodos de seleção de servidor:
   - **Usar Servidores Pré-configurados**. O XClarity Administrator usa os endereços IP e portas especificados para descobrir o servidor de autenticação externo.

     Se você selecionar essa opção, especifique até quatro endereços IP e portas pré-configurados do servidor. O cliente LDAP tenta autenticar usando o primeiro endereço do servidor. Se a autenticação falhar, o cliente LDAP tentará autenticar usando o próximo endereço IP do servidor.

     Se o número da porta de uma entrada *não for* explicitamente definido como `3268` ou `3269`, o sistema assumirá que a entrada identifica um controlador de domínio.

     Quando o número da porta estiver definido como `3268` ou `3269`, o sistema assumirá que a entrada identifica um catálogo global. O cliente LDAP tenta autenticar usando o controlador de domínio para o primeiro endereço IP do servidor configurado. Se isso falhar, o cliente LDAP tentará autenticar usando o controlador de domínio para o próximo endereço IP do servidor.

     Importante: Pelo menos um controlador de domínio deve ser especificado, mesmo se o catálogo global estiver especificado. A especificação apenas do catálogo global parece ter êxito, mas não é uma configuração válida.

     Quando o modo de criptografia estiver configurado como NIST-800-131A, XClarity Administrator poderá não ser capaz de se conectar a um servidor LDAP externo usando uma porta segura (por exemplo, usando LDAPS pela porta padrão 636) se o servidor LDAP não for capaz de estabelecer uma conexão Transport Layer Security (TLS) versão 1.2 com o cliente LDAP no XClarity Administrator.
   - **Usar DNS para encontrar Servidores LDAP**. O XClarity Administrator usa o nome de domínio especificado ou o nome de grupo para descobrir dinamicamente o servidor de autenticação externo. O nome de domínio e o nome de grupo são usados para obter uma lista de controladores de domínio, e o nome de grupo é usado para obter uma lista de servidores de catálogo global.

     Atenção: Ao usar DNS para encontrar servidores LDAP, certifique-se de que a conta do usuário a ser usada para autenticar no servidor de autenticação externo esteja hospedada em controladores de domínio especificados. Se a conta de usuário for hospedada em um controlador de domínio filho, inclua este controlador na lista de solicitações de serviço.
4. Selecione um destes métodos de vinculação:

- **Credenciais Configuradas**. Use esse método de vinculação para usar o nome do cliente e a senha para vincular o XClarity Administrator ao servidor de autenticação externo. Se essa vinculação falhar, o processo de autenticação também falhará.

  O nome do cliente pode ser qualquer nome ao qual o servidor LDAP oferecer suporte, incluindo um nome distinto, um AMAccountName, nome de NetBIOS ou um UserPrincipalName. O nome do cliente deve ser uma conta de usuário no domínio que tem pelo menos privilégios somente leitura. Exemplo:
  ```
  cn=username,cn=users,dc=example,dc=com
  domain\username
  username@domain.com
  username
  ```

  Atenção: Se você alterar a senha do cliente no servidor de autenticação externo, certifique-se de também atualizar a nova senha no XClarity Administrator. Para obter mais informações, consulte Não é possível fazer login no XClarity Administrator na documentação online XClarity Administrator.

- **Credenciais de Login**. Use esse método de ligação para usar um nome de usuário do Active Directory ou do OpenLDAP e senha para vincular o XClarity Administrator ao servidor de autenticação externo.

  O ID do usuário e a senha especificados são usados apenas para testar a conexão com o servidor de autenticação. Se for bem-sucedida, as configurações do cliente LDAP serão salvas, exceto as credenciais de login de teste que você especificou. Todas as vinculações futuras usarão o nome do usuário e a senha que você usou para fazer login no XClarity Administrator.

  Notas:

  – Você deve estar conectado ao XClarity Administrator usando um ID de usuário totalmente qualificado (por exemplo, `administrator@domain.com` ou `DOMAIN\admin`).

  – Você deve usar um nome de cliente de teste totalmente qualificado para o método de vinculação.

  Atenção: Para configurar o método de vinculação para usar credenciais de login, o controlador de gerenciamento de cada servidor gerenciado deve estar executando o firmware de setembro de 2016 ou posterior.

5. No campo **DN raiz**, recomenda-se não especificar um nome distinto raiz, especialmente para ambientes com vários domínios. Quando esse campo estiver em branco, o XClarity Administrator consultará o servidor de autenticação externo quanto aos contextos de nomenclatura. Se você usar DNS para descobrir o servidor de autenticação externo ou se você especificar vários servidores (por exemplo, `dc=example,dc=com`), será possível especificar uma entrada superior na árvore de diretórios LDAP. Nesse caso, as pesquisas são iniciadas com o nome distinto raiz especificado como base de procura.
6. Especifique o atributo a ser usado para procurar o nome do usuário.

   Quando o método de vinculação está definido como **Credenciais Configuradas**, a vinculação inicial com o servidor LDAP é seguida por uma solicitação de pesquisa que recupera informações específicas sobre o usuário, incluindo o DN do usuário, permissões de login e associação a grupos. Essa solicitação de procura deve especificar o nome do atributo que representa as IDs de usuário nesse servidor. Esse nome de atributo é configurado nesse campo. Se esse campo for deixado em branco, o padrão será **cn**.
7. Especifique o nome do atributo que é usado para identificar os grupos aos quais um usuário pertence. Se este campo ficar em branco, o nome do atributo no filtro será padronizado como **memberOf**.

8. Especifique o nome do atributo que é utilizado para identificar o nome do grupo configurado pelo servidor LDAP. Se esse campo for deixado em branco, o padrão será **uid**.

d. Clique em **Aplicar**.

O XClarity Administrator tenta testar a configuração para detectar erros comuns. Se o teste falhar, mensagens de erro serão exibidas indicando a origem de erros. Se o teste for bem-sucedido e as conexões com os servidores especificados forem concluídas com êxito, a autenticação do usuário ainda poderá falhar se:

- Não existe um usuário local com autoridade **lxc-recovery**.
- O nome distinto raiz estiver incorreto.
- O usuário não é um membro de, pelo menos, um grupo no servidor de autenticação externo que corresponde ao nome de um grupo de funções no servidor de autenticação do XClarity Administrator. O XClarity Administrator não pode detectar se o DN raiz está correto; entretanto, pode detectar se um usuário é membro de, pelo menos, um grupo. Se um usuário não for membro de, pelo menos, um grupo, será exibida uma mensagem de erro quando o usuário tentar fazer login no XClarity Administrator. Para obter mais informações sobre solução de problemas com os servidores de autenticação externos, consulte Problemas de conectividade na documentação online do XClarity Administrator.

Etapa 4. Crie uma conta de usuário externa que possa acessar o XClarity Administrator:

a. No servidor de autenticação externo, crie uma conta de usuário. Para obter instruções, consulte a documentação do Active Directory ou do OpenLDAP.

b. Crie um grupo global do Active Directory ou do OpenLDAP com o nome de um grupo predefinido e autorizado. O grupo deve existir dentro do contexto do nome distinto raiz definido no cliente LDAP.

c. Inclua o usuário do Active Directory ou do OpenLDAP como um membro do grupo de segurança criado anteriormente.

d. Faça login no XClarity Administrator usando o nome de usuário do Active Directory ou do OpenLDAP.

e. **Opcional:** defina e crie grupos adicionais. Você pode autorizar estes grupos e designar atribuições a eles a partir da página Usuários e Grupos.

f. Se o LDAP seguro estiver habilitado, importe certificados confiáveis para o servidor LDAP externo (consulte Instalando um certificado de servidor assinado externamente personalizado).

Resultados

O XClarity Administrator valida a conexão do servidor LDAP. Se a validação passar, a autenticação do usuário ocorrerá no servidor de autenticação externo quando você fizer login no XClarity Administrator, no CMM e no controlador de gerenciamento.

Se a validação falhar, o modo de autenticação será alterado automaticamente para a configuração **Permitir logons de usuários locais**, e uma mensagem que explica a causa da falha será exibida.

Nota: Os grupos de funções corretos devem ser configurados no XClarity Administrator, e contas de usuário devem ser definidas como membros de um dos grupos de funções no servidor do Active Directory. Caso contrário, a autenticação do usuário falhará.

Configurando um provedor de identidade SAML externo

É possível escolher usar um provedor de identidade SAML (Security Assertion Markup Language) 2.0 para executar autenticação e autorização do Lenovo XClarity Administrator.

Antes de iniciar

A configuração inicial do XClarity Administrator deve ser concluída antes de configurar o provedor de identidade.

O provedor de identidade deve se um AD FS (Active Directory Federated Service) da Microsoft e pode ser conectado à rede de gerenciamento, à rede de dados ou a ambas. Como a autenticação é realizada por meio do navegador da Web, seu navegador da Web deve ser capaz de acessar o XClarity Administrator e o servidor SAML.

É possível baixar metadados de IDP usando o seguinte URL: `https://<ADFS_IP_Address>/federationmetadata/2007-06/federationmetadata.xml`, em que *<ADFS_IP_Address>* é o endereço IP do AD FS (por exemplo, https://10.192.0.0/federationmetadata/2007-06/federationmetadata.xml).

Você deve criar ou renomear grupos de funções no servidor de autenticação local para fazer a correspondência dos grupos definidos no servidor de autenticação externo.

Para configurar um provedor de identidade SAML, você deverá ter feito login como um usuário que seja membro do grupo **lxc_admin** ou **lxc_supervisor**.

Sobre esta tarefa

O XClarity Administrator suporta o uso de um provedor de identidade SAML (Security Assertion Markup Language) 2.0 para autenticar e autorizar usuários. Além de inserir um nome do usuário e senha, o provedor de identidade pode ser configurado para requerer critérios adicionais para validar a identidade do usuário, como inserir um código PIN, ler um cartão inteligente e autenticar usando um certificado do cliente.

Quando o XClarity Administrator é configurado para usar o provedor de identidade, as solicitações interativas de login da interface da Web do XClarity Administrator estão redirecionadas para o provedor de identidade para autenticação. Após o usuário ser autenticado, o navegador da Web é redirecionado novamente para XClarity Administrator.

Nota: Se o provedor de identidade estiver ativado, será possível ignorar o provedor de identidade e fazer login no XClarity Administrator usando o servidor de autenticação LDAP local ou externo, abrindo seu navegador da Web na página de login do XClarity Administrator (por exemplo, `https://<ip_address>/ui/login.htm`).

Quando o XClarity Administrator está configurado para usar um perfil provedor de identidade, a página Gerenciamento de Usuários na interface da Web do XClarity Administrator não está desabilitada. As contas do usuário locais são necessárias para fazer login diretamente a um chassi ou um servidor gerenciado (exceto quando o Encapsulamento esteja habilitado nesse dispositivo) e para autenticação PowerShell e API REST, e para recuperação se a autenticação externa não estiver disponível.

Procedimento

Conclua as seguintes etapas para configurar um provedor de identidade SAML externo (AD FS).

Etapa 1. Crie uma conta do usuário de recuperação que possa ser usada para fazer login no XClarity Administrator se o provedor de identidade ficar indisponível (consulte Gerenciando contas de usuário).

Etapa 2. Recupere os metadados de provedor de identidade (IDP) do provedor de identidade e salve o arquivo no host XClarity Administrator.

Etapa 3. Configure o cliente SAML do XClarity Administrator.

a. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.

b. Clique em **Configurações de SAML** na seção Usuários e Grupos para exibir a caixa de diálogo Configurações de SAML.

c. Preencha os campos na página Configurações de SAML:
   1. Verifique se o ID da entidade corresponde ao endereço IP do servidor de gerenciamento do XClarity Administrator.
   2. Escolha se os metadados gerados serão assinados digitalmente.

3. Escolher se as solicitações de autenticação devem ser assinadas.
4. Escolher se as respostas de autenticação devem ser assinadas.
5. Escolha se as solicitações de resolução de artefato enviadas ao provedor de identidade remoto devem ser assinadas.
6. Cole os metadados de provedor de identidade (IDP) SAML que foram gerados pelo provedor de identidade e recuperados na etapa Etapa 2 3 na página 27 no campo **Metadados de IDP**.

d. Clique em **Aplicar** para aplicar as alterações e atualizar o texto no campo Metadados de SP.

Atenção: *Não* selecione **SAML Habilitado** neste momento. Você habilitará o SAML em uma etapa posterior para reiniciar o XClarity Administrator.

e. Copie e cole os dados do campo **Metadados de SP** em um arquivo e salve o arquivo com a extensão .XML (por exemplo, metadados_sp.xml). Copie esse arquivo para o host AD FS.

Etapa 4. Configure AD FS.

a. Abra a ferramenta de Gerenciamento AD FS.
b. Clique em **ADFS → Objetos de Confiança de Terceira Parte Confiável**.
c. Clique com o botão direito em **Objetos de Confiança de Terceira Parte Confiável** e, em seguida, em **Adicionar Objeto de Confiança de Terceira Parte Confiável** para exibir o assistente
d. Clique em **Iniciar**.
e. Na página Selecionar Origem de Dados, selecione **Importar dados sobre a terceira parte confiável de um arquivo** e, em seguida, selecione o arquivo de metadados de SP que você salvou na etapa 3e.
f. Digite um nome de exibição.
g. Clique em **Avançar** em todas as páginas para escolher os valores padrão.
h. Clique em **Concluir** para exibir a página Regras de Declaração
i. Deixe **Enviar Atributos LDAP como Declarações** como padrão e clique em **Avançar**.
j. Insira um nome da regra de declaração.
k. Selecione **Active Directory** para o armazenamento de atributo.
l. Adicione um mapeamento. Na lateral esquerda, selecione **SAM-Account-Name** e na lateral direita, selecione **ID de Nome** para o tipo de saída reivindicado.
m. Adicione outro mapeamento. Na lateral esquerda, selecione **Token-Groups-Unqualified Names** e na lateral direita, selecione **Grupo** para o tipo de saída reivindicado.
n. Clique em **OK**.
o. Localize o objeto de confiança que você acabou de criar na lista do **Objetos de Confiança de Terceira Parte Confiável**.
p. Clique com o botão direito no objeto de confiança e em **Selecionar propriedades**. A caixa de diálogo Propriedades de confiança é exibida.
q. Clique na guia **Avançado** e selecione `SHA-1` como o algoritmo hash seguro.

Etapa 5. Salve o certificado do servidor do AD FS.

a. Clique em **Console AD FS → Serviço → Certificados**.
b. Selecione **Certificado** em Token-assinatura.
c. Clique com o botão direito no certificado e em **Exibir certificado**.
d. Clique na guia **Detalhes**.

e. Clique em **Copiar em Arquivo** e salve o certificado como um arquivo DER codificado binário X.509 (.CER).

f. Copie o arquivo .CER do certificado do servidor para o host XClarity Administrator.

Etapa 6. Importe o certificado confiável AD FS para a interface da Web do XClarity Administrator.

a. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.

b. Clique em **Certificados Confiáveis** na seção Gerenciamento de Certificados.

c. Clique no ícone **Criar** ( ) para adicionar um certificado.

d. Selecione o arquivo .CER do certificado do servidor salvo na etapa anterior.

e. Clique em **Criar**.

Etapa 7. Clique em **Configurações de SAML** na seção Usuários e Grupos para exibir a caixa de diálogo Configurações de SAML.

Etapa 8. Selecione **SAML Habilitado** para habilitar o gerenciamento de contas do usuário usando um provedor de identidade externo. Quando essa opção é selecionada, todas as contas de usuário existem remotamente em um provedor de identidade.

Etapa 9. Clique em **Aplicar** para aplicar as alterações e reiniciar o servidor de gerenciamento.

Etapa 10. Aguarde alguns minutos para que o XClarity Administrator reinicie.

Atenção: Não reinicie o dispositivo virtual manualmente durante esse processo.

Etapa 11. Feche e abra novamente o navegador da Web.

Etapa 12. Faça login na interface da Web do XClarity Administrator a partir do provedor de identidade.

Resultados

O XClarity Administrator tenta testar a configuração para detectar erros comuns. Se o teste falhar, mensagens de erro serão exibidas indicando a origem de erros.

O XClarity Administrator valida conexão do provedor de identidade. Se a validação passar, a autenticação do usuário ocorre no provedor de identidade quando você fizer login no XClarity Administrator.

Configurando um sistema externo de gerenciamento de identidade

Um *sistema de gerenciamento de identidade* é um cofre de senhas externo que pode ser usado com o Lenovo XClarity Administrator para armazenar credenciais do XClarity Administrator e do XClarity Controller. Quando um sistema de gerenciamento de identidade é adicionado ao XClarity Administrator, o XClarity Administrator recupera as senhas do sistema de gerenciamento de identidade e não dos servidores de autenticação.

Sobre esta tarefa

O XClarity Administrator é compatível com o sistema de gerenciamento de identidade a seguir.

- CyberArk

Configurando um sistema externo de gerenciamento de identidade CyberArk

O CyberArk é um cofre de senhas externo que pode ser usado com o Lenovo XClarity Administrator para armazenar credenciais do XClarity Administrator e do Lenovo XClarity Controller. Depois que uma senha de conta é armazenada no CyberArk, ela é gerenciada pelo CyberArk

Sobre esta tarefa

O XClarity Administrator permite armazenar suas senhas do XCC em sistemas de gerenciamento de identidade fornecidos pelo CyberArk, um serviço de terceiros. A Lenovo não é responsável pelo serviço CyberArk, e você é responsável pelo seu relacionamento direto com a CyberArk.

Se as contas de usuário de um servidor ThinkSystem ou ThinkAgile estiverem integradas ao CyberArk, você poderá escolher que o XClarity Administrator recupere credenciais do CyberArk para fazer login no servidor ao configurar inicialmente os servidores para gerenciamento (com autenticação gerenciada ou local). Para que as credenciais possam ser recuperadas do CyberArk, os caminhos do CyberArk devem ser definidos no XClarity Administrator e a confiança mútua deve ser estabelecida entre o CyberArk e o XClarity Administrator usando autenticação mútua TLS por meio de certificados de cliente.

Procedimento

Para definir o XClarity Administrator para usar o CyberArk, conclua as etapas a seguir.

Etapa 1. Configure o CyberArk.

1. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.
2. Clique em **CyberArk** na seção Gerenciamento de identidade.
3. Clique em **Editar detalhes do servidor CyberArk** na barra de ferramentas.
4. Especifique o nome do host ou o endereço IP do CyberArk e o número da porta.
5. Clique em **Aplicar**.

Etapa 2. Importe o certificado de autenticação mútua do XClarity Administrator no CyberArk.

1. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.
2. Clique em **Certificado do Servidor** na seção Gerenciamento de Certificados.
3. Clique na guia **Certificado de Cliente**.
4. Selecione **CyberArk** como o tipo de servidor.
5. Clique em **Gerar certificado novamente** para gerar um novo certificado de autenticação mútua TLS para o CyberArk.

   Atenção: Se você gerar novamente o certificado de autenticação mútua TLS para CyberArk depois que uma conexão é estabelecida entre XClarity Administrator e o CyberArk, a conexão será perdida até que você importe o novo certificado no CyberArk.
6. Clique em **Fazer download do certificado** e, em seguida, clique em **Salvar como der** ou **Salvar como pem** para salvar o certificado como um arquivo no sistema local.
7. Importe o certificado baixado para o CyberArk.

Etapa 3. Importe o certificado da CA raiz do CyberArk para XClarity Administrator.

1. Faça download do certificado da CA raiz do CyberArk.
2. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.
3. Clique em **Certificados Confiáveis** na seção Gerenciamento de Certificados.
4. Clique no ícone **Criar** ( ) para adicionar um certificado.
5. Navegue para o arquivo ou cole o texto do certificado com formatação PEM.
6. Clique em **Criar**.

Etapa 4. Adicione caminhos que identifiquem a localização de contas de usuário integradas no CyberArk.

1. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.
2. Clique em **CyberArk** na seção Gerenciamento de identidade.
3. Clique na guia **Caminhos**.

4. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Criar caminho do CyberArk.

5. Opcionalmente, especifique o ID do aplicativo, o cofre e a pasta onde as contas de usuário são armazenadas no CyberArk.

   Se você especificar o ID do aplicativo, o cofre e opcionalmente a pasta, o XClarity Administrator tentará localizar a conta do usuário no local especificado.

   Se você especificar uma combinação de campos diferentes do ID do aplicativo e do cofre (por exemplo, se você especificar apenas o ID do aplicativo, apenas o cofre e a pasta ou apenas o ID do aplicativo e a pasta), o XClarity Administrator filtrará o caminho usando os valores especificados.

6. Clique em **Aplicar**.

Depois de concluir

- Modifique um caminho do CyberArk selecionado clicando no ícone **Editar** ( ).
- Exclua um caminho do CyberArk selecionado clicando no ícone **Excluir** ( ).

Determinando o tipo de método de autenticação que é usado pelo Lenovo XClarity Administrator

É possível determinar o tipo de método de autenticação que é usado atualmente nas guias **Cliente LDAP** e **Configurações de SAML** na página Segurança.

Sobre esta tarefa

O *servidor de autenticação* é um registro do usuário utilizado para autenticar as credenciais do usuário. O Lenovo XClarity Administrator oferece suporte aos seguintes tipos de servidores de autenticação.

- **Servidor de autenticação local**. Por padrão, o XClarity Administrator é configurado para usar o servidor LDAP integrado que reside no servidor de gerenciamento.
- **Servidor LDAP externo**. Atualmente, somente Microsoft Active Directory e OpenLDAP são aceitos. Este servidor deve residir em um servidor do Microsoft Windows externo conectado à rede de gerenciamento. Quando um servidor LDAP externo for usado, o servidor de autenticação local será desativado.

  Atenção: Para configurar o método de ligação do Active Directory para usar credenciais de login, o Baseboard Management Controller de cada servidor gerenciado deve estar executando o firmware de setembro de 2016 ou posterior.
- **Sistema externo de gerenciamento de identidade**. Atualmente, apenas o CyberArk é suportado.

Se as contas de usuário de um servidor ThinkSystem ou ThinkAgile estiverem integradas ao CyberArk, você poderá escolher que o XClarity Administrator recupere credenciais do CyberArk para fazer login no servidor ao configurar inicialmente os servidores para gerenciamento (com autenticação gerenciada ou local). Para que as credenciais possam ser recuperadas do CyberArk, os caminhos do CyberArk devem ser definidos no XClarity Administrator e a confiança mútua deve ser estabelecida entre o CyberArk e o XClarity Administrator usando autenticação mútua TLS por meio de certificados de cliente.

- **SAML externo provedor de identidade**. Atualmente, apenas o Microsoft Active Directory Federation Services (AD FS) é suportado. Além de inserir um nome de usuário e senha, a autenticação de vários fatores pode ser configurada para ativar segurança adicional exigindo um código PIN, a leitura de um cartão inteligente e o certificado de cliente. Quando um provedor de identidade SAML for usado, o servidor de autenticação local não será desabilitado. As contas do usuário local são necessárias para fazer login diretamente a um chassi ou um servidor gerenciado (a menos que o Encapsulamento esteja habilitado nesse dispositivo), para autenticação PowerShell e API REST, e para recuperação se a autenticação externa não estiver disponível.

  Você pode escolher usar um servidor LDAP externo e um provedor de identidade externo. Se ambos estiverem habilitados, o servidor LDAP externo será usado para fazer login diretamente nos dispositivos gerenciados, e o provedor de identidade será usado para fazer login no servidor de gerenciamento.

Procedimento

Para determinar o tipo de servidor de autenticação que está sendo usado pelo software de gerenciamento, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.

Etapa 2. Clique no **Cliente LDAP** na seção Usuários e Grupos para exibir a caixa de diálogo Configurações do Cliente LDAP.

Verifique se o método de autenticação do usuário está selecionado:

- **Permitir logons de usuários locais**. A autenticação é executada usando a autenticação local. Quando essa opção estiver selecionada, todas as contas de usuário existirão no servidor de autenticação local no nó de gerenciamento.
- **Permitir logons de usuários LDAP**. A autenticação é executada por um servidor LDAP externo. Esse método permite o gerenciamento remoto de contas de usuário. Quando essa opção é selecionada, todas as contas de usuário existem remotamente em um servidor LDAP externo.
- **Permitir usuários locais primeiro, depois usuários LDAP**. O servidor de autenticação local executa a autenticação primeiro. Se isso falhar, um servidor LDAP externo executará a autenticação.
- **Permitir usuários LDAP primeiro, depois usuários locais**. Um servidor LDAP externo executará a autenticação primeiro. Se isso falhar, o servidor de autenticação local executará a autenticação.

Etapa 3. Clique em **Configurações de SAML** na seção Usuários e Grupos para exibir a página Configurações de SAML.

Se **SAML Habilitado** for selecionado, um provedor de identidade será usado.

Acessando o Lenovo XClarity Administrator após uma falha do servidor LDAP externo

Se você estiver usando um servidor de autenticação LDAP e esse registro falhar ou não estiver disponível, use o procedimento a seguir para recuperar o acesso à interface da Web do Lenovo XClarity Administrator usando o servidor de autenticação local no nó de gerenciamento.

Procedimento

Para alterar a configuração do cliente LDAP, conclua as etapas a seguir.

Etapa 1. Faça login na interface da Web do XClarity Administrator usando uma conta de usuário com autoridade **lxc-recovery**. Para obter mais informações sobre o nome do domínio do cliente, consulte Configurando um servidor de autenticação LDAP externo.

Etapa 2. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.

Etapa 3. Clique no **Cliente LDAP** na seção Usuários e Grupos para exibir a caixa de diálogo Cliente LDAP.

Etapa 4. Selecione **Permitir logons de usuários locais** para que o método de autenticação de usuários permite o gerenciamento local de contas de usuário. Quando essa opção estiver selecionada, todas as contas de usuário existirão localmente no servidor de gerenciamento.

Etapa 5. Dê um clique em **Aplicar**.

Resultados

Agora você pode usar as contas de usuário no servidor de autenticação local para acessar o servidor de gerenciamento XClarity Administrator. Depois que seu servidor de autenticação externo for restaurado e estiver disponível para o servidor de gerenciamento, você poderá alterar a configuração do cliente LDAP de volta para o servidor de autenticação externo.

Acessando o Lenovo XClarity Administrator após uma falha do provedor de identidade SAML externo

Se você estiver usando um provedor de identidade SAML externo e esse registro falhar ou não estiver disponível, use o procedimento a seguir para recuperar o acesso à interface da Web do Lenovo XClarity Administrator usando o servidor de autenticação local XClarity Administrator.

Procedimento

Conclua as etapas a seguir para alterar a configuração do cliente SAML.

Etapa 1. Abra o navegador da Web da página de login XClarity Administrator (por exemplo, `https://<ip_address>/ui/login.html`).

Etapa 2. Faça login na interface da Web do XClarity Administrator usando uma conta do usuário de recuperação local criada ao configurar o provedor de identidade.

Etapa 3. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.

Etapa 4. Clique em **Configurações de SAML** na seção Usuários e Grupos para exibir a caixa de diálogo Configurações de SAML.

Etapa 5. Desmarque **Habilitar SAML** para desabilitar o SAML provedor de identidade. Quando essa opção estiver desmarcada, o servidor de autenticação local ou servidor LDAP externo (se configurado) são usados para autenticação.

Etapa 6. Dê um clique em **Aplicar**.

Resultados

Agora você pode usar as contas de usuário no servidor de autenticação local para acessar o servidor de gerenciamento XClarity Administrator. Após seu provedor de identidade externo ser restaurado e estar disponível para o servidor de gerenciamento, é possível alterar o método de autenticação para provedor de identidade.

Gerenciando contas de usuário

As contas de usuário são usadas para fazer login e gerenciar o Lenovo XClarity Administrator e todos os chassis e servidores gerenciados pelo XClarity Administrator. As contas de usuário do XClarity Administrator são sujeitadas a dois processos interdependentes: autenticação e autorização.

Sobre esta tarefa

Autenticação é o mecanismo de segurança pelo qual as credenciais do usuário são verificadas. O processo de autenticação usa as credenciais do usuário que estão armazenadas no servidor de autenticação configurado. Isso também impede que servidores de gerenciamento não autorizados ou aplicativos de sistema gerenciado desonestos acessem os recursos. Após a autenticação, um usuário pode acessar o XClarity Administrator. No entanto, para acessar um recurso específico ou executar uma tarefa específica, o usuário também deve ter a autorização apropriada.

A *autorização* verifica as permissões do usuário autenticado e controla o acesso aos recursos com base nas associações dos usuários em um grupo de funções. *Grupos de função* são usados para designar funções específicas a um conjunto de contas do usuário definidas e gerenciadas no servidor de autenticação. Por exemplo, se um usuário for um membro de um grupo de funções com permissões de Supervisor, esse usuário poderá criar, editar e excluir contas do usuário a partir do XClarity Administrator. Se um usuário tiver permissões de Operador, esse usuário só poderá exibir as informações da conta do usuário.

Nota: As contas de usuário SYSMGR_* e SYSRDR_* (em que * é um sufixo escolhido aleatoriamente entre os caracteres A a Z e 0 a 9) são geradas e usadas pelo XClarity Administrator como contas de usuário de serviço e são usadas em funções como autenticação gerenciada, implantação do SO e atualizações de firmware. As senhas SYSMGR_* e SYSRDR_* são alternadas sempre que o XClarity Administrator é inicializado e pouco antes do vencimento da senha.

Criando um usuário

As contas de usuário são usadas para gerenciar a autorização e o acesso a recursos.

Sobre esta tarefa

A primeira conta de usuário criada deve ter a função de Supervisor e estar ativada (habilitada).

Como uma medida de segurança adicional, crie pelo menos duas contas de usuário que tenham a função **Supervisor**. Certifique-se de gravar as senhas dessas contas de usuário e armazená-las em um local seguro para o caso de você precisar restaurar o Lenovo XClarity Administrator.

Procedimento

Para adicionar um usuário ao XClarity Administrator, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.

Etapa 2. Clique em **Usuários Locais** na seção Usuários e Grupos para exibir a página Gerenciamento de Usuários.

Etapa 3. Clique no ícone **Criar** ( ) para criar um usuário. A caixa de diálogo Criar Novo Usuário é exibida.

Etapa 4. Preencha as informações a seguir na caixa de diálogo.

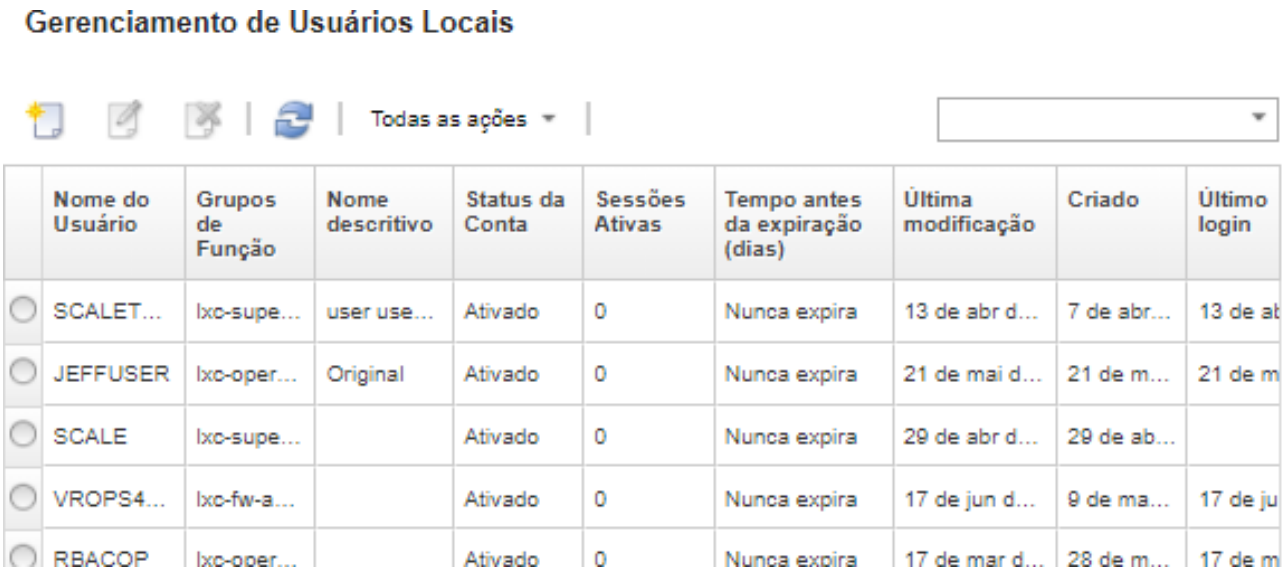
- Insira um nome de usuário e a descrição do usuário.
- Insira as senhas nova e de confirmação. As regras para as senhas se baseiam nas configurações atuais de segurança de conta.

- Selecione um ou mais grupos de função para autorizar o usuário a executar as tarefas apropriadas.Para obter informações sobre grupos de funções e como criar grupos de funções personalizados, consulte Criando um grupo de funções personalizado.
- (Opcional) Defina **Alterar senha no primeiro acesso** como `Yes` se desejar forçar o usuário a alterar a senha na primeira vez que ele fizer login no XClarity Administrator.

Etapa 5. Clique em **Criar**.

Depois de concluir

A conta de usuário é exibida na tabela Gerenciamento de Usuários. A tabela mostra os grupos de funções associados e o status da conta para cada conta de usuário.



Depois de criar uma conta de usuário, é possível executar as seguintes ações em uma conta de usuário selecionada:

- Modificar o nome de usuário, a descrição e a função de uma conta de usuário clicando no ícone **Editar** ( ).
- Excluir a conta de usuário clicando no ícone **Excluir** ( ).
- Redefinir a senha da conta do usuário (consulte Redefinindo a senha de um usuário).
- Desbloquear a conta (consulte Desbloqueando um usuário).
- Habilitar ou desabilitar uma conta de usuário (consulte Ativando ou desativando um usuário).

Ativando ou desativando um usuário

É possível habilitar ou desabilitar uma conta de usuário local no servidor de autenticação.

Procedimento

Para habilitar ou desabilitar uma conta de usuário, conclua as etapas a seguir.

- Se o servidor de autenticação local for usado:
  1. Na barra de título do Lenovo XClarity Administrator, clique em **Administração → Segurança**.
  2. Clique em **Usuários Locais** na seção Usuários e Grupos para exibir a página Gerenciamento de Usuários.
  3. Selecione uma conta de usuário.

4. Se a conta de usuário estiver habilitada, clique em **Todas as Ações → Desabilitar conta selecionada** para desabilitar o usuário. O status da conta na tabela muda para `Disabled`.
5. Se a conta de usuário estiver desabilitada, clique em **Todas as Ações → Habilitar conta selecionada** para habilitar o usuário. O status da conta na tabela muda para `Enabled`.

- Se um servidor LDAP externo for usado, habilite ou desabilite uma conta de usuário no Microsoft Active Directory.
- Se um servidor SAML externo provedor de identidade for usado, habilite ou desabilite uma conta de usuário no provedor de identidade.

Efetuando logoff de um usuário ativo

É possível efetuar logoff (encerrar a sessão) de um usuário ativo no Lenovo XClarity Administrator.

Você deve ser feito login no XClarity Administrator usando uma conta de usuário com autoridade **lxc-supervisor** ou **lxc-security-admin**.

Procedimento

Para efetuar logoff de um usuário ativo, conclua as etapas a seguir.

Etapa 1. Na barra de título do XClarity Administrator, clique em **Administração → Segurança**.

Etapa 2. Clique em **Sessões Ativas** na seção Usuários e Grupos para exibir a página Gerenciamento de Sessões Ativas.

Etapa 3. Selecione uma ou mais contas de usuário.

Etapa 4. Clique em **Efetuar Logoff de Usuário**.

Alterando a senha da conta do usuário

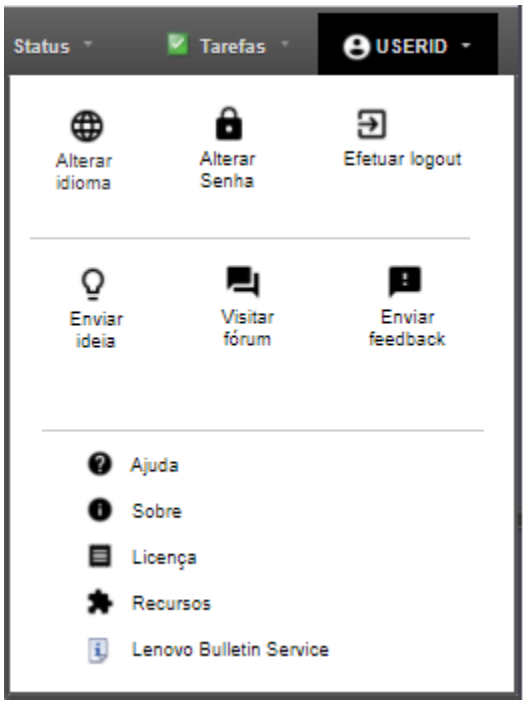
Você pode alterar a senha de sua conta de usuário.

Procedimento

Conclua as etapas a seguir para alterar a senha.

- Se o servidor de autenticação local for usado:
  1. Na barra de título do Lenovo XClarity Administrator, clique no menu de ações do usuário (

) e clique em **Alterar Senha**. A caixa de diálogo Alterar Senha é exibida.



2. Insira a senha atual.
3. Insira as senhas nova e de confirmação. As regras para as senhas se baseiam nas configurações atuais de segurança de conta.
4. Clique em **Alterar**.

- Se um servidor de autenticação externo for usado, altere sua senha no Microsoft Active Directory.

  Atenção: Se você atualizou o Microsoft Active Directory com uma nova senha para a conta de cliente usada para associar o XClarity Administrator ao servidor de autenticação externo, certifique-se de também atualizar a nova senha na interface da Web do XClarity Administrator (consulte Configurando um servidor de autenticação LDAP externo).
- Se o SAML externo provedor de identidade for usado, altere sua senha no provedor de identidade.

Redefinindo a senha de um usuário

Você pode redefinir a senha de qualquer conta de usuário.

Procedimento

Para redefinir uma senha, conclua as etapas a seguir.

- Se o servidor de autenticação local for usado, redefina a senha na interface da Web do Lenovo XClarity Administrator:
  1. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.
  2. Clique em **Usuários Locais** na seção Usuários e Grupos para exibir a página Gerenciamento de Usuários.
  3. Selecione uma conta de usuário na tabela.
  4. Se a conta de usuário estiver habilitada, clique em **Todas as Ações → Redefinir Senha para Usuário Selecionado**. A caixa de diálogo Redefinição de Senha é exibida.
     a. Insira as senhas nova e de confirmação. As regras para as senhas se baseiam nas configurações atuais de segurança de conta.

b. Como opção, defina **Alterar no primeiro acesso** como `Yes` se desejar forçar o usuário a alterar a senha na primeira vez que ele fizer login no XClarity Administrator.
c. Clique em **Redefinir**.

- Se um servidor LDAP externo for usado, redefina a senha no Microsoft Active Directory.
- Se um SAML externo provedor de identidade for usado, redefina a senha no provedor de identidade.
- Se não for possível fazer login no XClarity Administrator usando outra conta de supervisor ou se não houver outra conta de supervisor, você poderá redefinir a senha para um usuário local com autoridade de recuperação ou supervisor montando uma imagem ISO que contenha um arquivo de configuração com a nova senha. Para obter mais informações, consulte A senha de um usuário supervisor ou de recuperação local foi esquecida na documentação online do XClarity Administrator.

Desbloqueando um usuário

É possível desbloquear uma conta de usuário que esteja bloqueada no Lenovo XClarity Administrator. Uma conta de usuário poderá ficar temporariamente bloqueada se o usuário tentar muitos logins que não sejam válidos.

Sobre esta tarefa

As configurações de segurança de conta de usuário controlam o período de tempo que deve decorrer antes que um usuário que estava bloqueado possa tentar fazer login novamente. Se a configuração **Período de bloqueio após número máximo de falhas de login** estiver definida como `0`, a conta do usuário permanecerá bloqueada até o administrador a desbloquear explicitamente. Para obter mais informações sobre o período de bloqueio para número máximo de falhas de login, consulte Alterando as configurações de segurança de conta do usuário.

Também é possível desabilitar ou habilitar permanentemente uma conta de usuário. Para obter mais informações, consulte Ativando ou desativando um usuário.

Nota: Você deve ter autoridade de Supervisor para desbloquear uma conta de usuário.

Dica: É possível usar o XClarity Administrator para desbloquear as contas de usuário que são gerenciadas usando o servidor de autenticação local. Não é possível desbloquear contas de usuário em um servidor de autenticação externo usando o XClarity Administrator.

Procedimento

Para desbloquear uma conta do usuário, conclua as etapas a seguir.

- Se o servidor de autenticação local for usado:
  1. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.
  2. Clique em **Usuários Locais** na seção Usuários e Grupos para exibir a página Gerenciamento de Usuários.
  3. Selecione a conta de usuário na tabela.
  4. Clique em **Todas as Ações → Desbloquear Conta para Usuário Selecionado**.
- Se um servidor LDAP externo for usado, desbloqueie a conta do usuário no Microsoft Active Directory.
- Se um SAML externo provedor de identidade for usado, desbloqueie a conta do usuário no provedor de identidade.

Monitorando usuários ativos

É possível determinar quem fez login na interface da Web do Lenovo XClarity Administrator na página Painel.

Procedimento

- Você pode obter uma lista de usuários ativos e seus endereços IP clicando em **Painel** na barra de menus do XClarity Administrator.

  As sessões ativas de usuários são listadas na seção Atividade.

- É possível obter uma lista de todos os usuários ativos (além do usuário atual) e seus endereços IP clicando em **Administração → Segurança** na barra de menus do XClarity Administrator e, em seguida, clicando em **Sessões Ativas**.

  Nota: As sessões do usuário inativas por mais do que um período específico são desconectadas automaticamente. É possível configurar o período de inatividade clicando em **Administração → Segurança** na barra de menu do XClarity Administrator, clicando em Configurações de Segurança de Conta e, em seguida, ajustando o valor **Tempo limite da sessão de inatividade da web**. Observe que a alteração não afeta as sessões ativas do usuário. Ela afeta apenas as sessões do usuário que começam após a alteração da configuração.

Gerenciando credenciais compartilhadas

Credenciais armazenadas são usadas para gerenciar a autorização e o acesso ao chassi e a servidores gerenciados pelo Lenovo XClarity Administrator usando a autenticação local.

Antes de iniciar

Você deve ter autoridade **lxc-supervisor** ou **lxc-security-admin** para criar, modificar ou excluir as credenciais armazenadas.

Sobre esta tarefa

Uma credencial armazenada deve ser uma conta do usuário local em um dispositivo ou uma conta do usuário em um servidor do Active Directory.

Se você optar por gerenciar dispositivos usando a autenticação local em vez da autenticação gerenciada do XClarity Administrator, deverá selecionar uma conta de credenciais armazenadas durante o processo de gerenciamento.

Importante: O XClarity Administrator não valida o nome de usuário e a senha especificados para as credenciais armazenadas. É sua responsabilidade verificar se as informações especificadas correspondem a uma conta do usuário ativa no dispositivo local ou no Active Directory (se o dispositivo gerenciado estiver configurado para usar o Active Directory para autenticação).

Atenção: As credenciais armazenadas devem ter acesso de supervisor ou autoridade suficientes para fazer alterações de configuração no dispositivo. Se você tentar gerenciar um servidor com as credenciais armazenadas que não têm autoridade suficiente no dispositivo, o processo de gerenciamento poderá ser bem-sucedido, mas ações de inventário administrativas adicionais no dispositivo poderão falhar por causa de erros de acesso negado, o que pode resultar em problemas de conectividade observados no dispositivo.

Procedimento

Para adicionar uma credencial armazenada ao XClarity Administrator, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**. A página Segurança é exibida.

Etapa 2. Clique em **Credenciais Armazenadas** na seção Autenticação Gerenciada para exibir a página Credencial Armazenada.

Etapa 3. Clique no ícone **Criar** () para criar uma credencial armazenada. A caixa de diálogo Criar Novas Credenciais Armazenadas é exibida

Etapa 4. Preencha as informações a seguir na caixa de diálogo.
- Insira um nome de usuário e uma descrição opcional da credencial armazenada.
- Insira e, em seguida, confirme a senha para as credenciais armazenadas.
- Opcionalmente, insira e, em seguida, confirme a senha para as credenciais de recuperação armazenadas RECOVERY_ID.

Etapa 5. Clique em **Criar Credencial Armazenada**.

Depois de concluir

A conta da credencial armazenada é exibida na tabela Credencial Armazenada. A tabela mostra o ID associado e a descrição para cada conta de credencial armazenada.

Na página Credenciais Armazenadas, é possível executar as seguintes ações em uma conta de credencial armazenada selecionada:

- Modificar o nome de usuário, a senha e a descrição de uma conta de credencial armazenada, clicando no ícone **Editar** ( ).

  Nota: Se você gerenciar um dispositivo usando uma credencial armazenada e ativar a autenticação gerenciada, não poderá editar a credencial armazenada.

- Excluir a conta de credencial armazenada, clicando no ícone **Excluir** ( ).

Para resolver credenciais armazenadas que se tornaram expiradas ou inválidas, consulte Resolvendo credenciais armazenadas expiradas ou inválidas para um servidor.

Gerenciando funções e grupos de funções

Uma *função* é usada para controlar o acesso do usuário a recursos e limita as ações que os usuários podem executar nesses recursos. O *grupo de funções* é uma coleção de um ou mais funções e é usada para atribuir essas funções aos diversos usuários. As funções que você configura para um grupo de funções determinam o nível de acesso que é concedido a cada usuário que é um membro deste grupo de funções. Cada usuário do Lenovo XClarity Administrator deve ser membro de pelo menos um grupo de funções.

Criando uma função personalizada

Uma *função* é um conjunto de *privilégios* ou permissões para executar uma ação específica. O Lenovo XClarity Administrator inclui diversas funções predefinidas (padrão). Também é possível criar funções personalizadas que forcem um conjunto exclusivo de privilégios que os usuários possam executar.

Antes de iniciar

Você deve ter autoridade **lxc-supervisor** ou **lxc-security-admin** para executar essa tarefa.

Sobre esta tarefa

Para criar uma função personalizada, selecione uma ou mais funções predefinidas que estão mais próximas no escopo da função que você deseja criar e, em seguida, limpe os privilégios individuais que deseja restringir. Isso garante que você tenha todos os privilégios pretendidos e que a função seja construída corretamente com privilégios dependentes.

Alguns privilégios do XClarity Administrator dependem dos privilégios do módulo de gerenciamento correspondente para executar ações em dispositivos gerenciados (consulte Privilégios v1 de módulo de gerenciamento e Privilégios v2 de módulo de gerenciamento). Um privilégio do XClarity Administrator pode permitir que você solicite uma ação em um dispositivo gerenciado, mas o dispositivo negará a solicitação se você não tiver os privilégios correspondentes para o CMM, IMM ou XCC. Por exemplo, se você criar uma

função personalizada para executar ações de energia em dispositivos gerenciados, adicionará o privilégio **lxc-inventory-modify-device-power-state** e:

- Para um servidor ThinkSystem em um rack, adicione o privilégio **mm-power-and-restart-access-v1**.
- Para um chassi do Flex System inteiro (incluindo os dispositivos no chassi), adicione o privilégio **mm-power-and-restart-access-v1**.
- Para um servidor ThinkSystem em um chassi, adicione os privilégios **mm-power-and-restart-access-v1**, **mm-blade-operator-v2** e **mm-blade-#-scope-v2** que correspondam ao servidor de destino.

Todas as funções contêm privilégios de somente leitura. Nenhuma função personalizada pode ser mais restritiva que a função **lxc-operator**.

Se um usuário não tiver privilégios para executar ações específicas, itens de menu, ícones de barra de ferramentas e botões que executam essas ações serão desativados (esmaecidos).

O XClarity Administrator fornece um grupo de funções para cada função predefinida, usando o mesmo nome que a função. Considere a possibilidade de criar um grupo de funções para novas funções que você criar. Para obter mais informações sobre os grupos de função, consulte Criando um grupo de funções personalizado.

- **lxc-supervisor**. Usuários que atribuíram essa função pode acessar, configurar e executar todas as operações disponíveis no servidor de gerenciamento e todos os dispositivos gerenciados.Os usuários que são atribuídos a essa função sempre têm acesso a todos os dispositivos gerenciados. Você não pode restringir o acesso aos dispositivos para essa função.
- **lxc-admin**. Usuários que atribuíram essa função podem modificar configurações não relacionadas a segurança e realizar todas as operações não relacionadas à segurança no servidor de gerenciamento, incluindo a possibilidade de atualizar e reiniciar o servidor de gerenciador. Essa função também permite exibir todas as informações de configuração e status sobre o servidor de gerenciamento e dispositivos gerenciados.
- **lxc-security-admin**. Usuários atribuídos a esta função podem modificar as configurações de segurança e realizar operações relacionadas à segurança no servidor de gerenciamento e nos dispositivos gerenciados. Essa função também permite exibir todas as informações de configuração e status sobre o servidor de gerenciamento e dispositivos gerenciados.

  Os usuários que são atribuídos a essa função sempre têm acesso a todos os dispositivos gerenciados. Você não pode restringir o acesso aos dispositivos para essa função.
- **lxc-hw-admin**. Os usuários com essa função podem modificar configurações que não sejam segurança e realizar as operações não relacionadas a segurança nos dispositivos gerenciados, incluindo a possibilidade de atualizar e reiniciar os dispositivos gerenciados. Essa função também permite exibir todas as informações de configuração e status sobre o servidor de gerenciamento e todos os dispositivos gerenciados.
- **lxc-fw-admin**. Os usuários que são atribuídos a essa função podem criar políticas de firmware e implantar essas políticas em dispositivos gerenciados. Os usuários não atribuídos a essa função só podem ver informações de política.
- **lxc-os-admin**. Os usuários que recebem essa função podem baixar e implantar sistemas operacionais e atualizações de drivers de dispositivo em servidores gerenciados. Os usuários que não recebem essa função só podem ver informações do sistema operacional e dos drivers de dispositivo.
- **lxc-service-admin**. Os usuários que são atribuídos e essa função podem coletar e baixar arquivos de serviço para XClarity Administrator e dispositivos gerenciados. Os usuários que não são atribuídos a essa função podem coletar, mas não podem baixar os dados de serviço.
- **lxc-hw-manager**. Usuários que têm essa função podem descobrir novos dispositivos e colocá-los sob o controle de gerenciamento do XClarity Administrator. Essa função proíbe usuários de executar operações ou modificar configurações no servidor de gerenciamento e nos dispositivos gerenciados fora dessas operações que são necessárias para descobrir e gerenciar novos dispositivos.
- **lxc-operator**. Usuários que atribuíram esta função podem exibir todas as informações de configuração e status sobre o servidor de gerenciamento e dispositivos gerenciados. Essa função proíbe os usuários de

realizar operações ou modificar configurações no servidor de gerenciamento e em todos os dispositivos gerenciados.

- **lxc-recovery**. Usuários que atribuíram esta função podem modificar as configurações de segurança e realizar operações relacionadas à segurança no servidor de gerenciamento. Esses usuários também podem autenticar diretamente no XClarity Administrator mesmo se o método de autenticação estiver configurado como servidor LDAP externo. Essa função fornece um mecanismo de recuperação caso ocorra um erro de comunicação com o servidor LDAP externo que usa a configuração "Credenciais de Login".

  Os usuários que são atribuídos a essa função sempre têm acesso a todos os dispositivos gerenciados. Você não pode restringir o acesso aos dispositivos para essa função.

As seguintes funções predefinidas estão *reservadas* e não podem ser usadas para criar novos grupos de funções ou serem atribuídas a novos usuários.

- **lxc-sysrdr**
- **lxc-sysmgr**

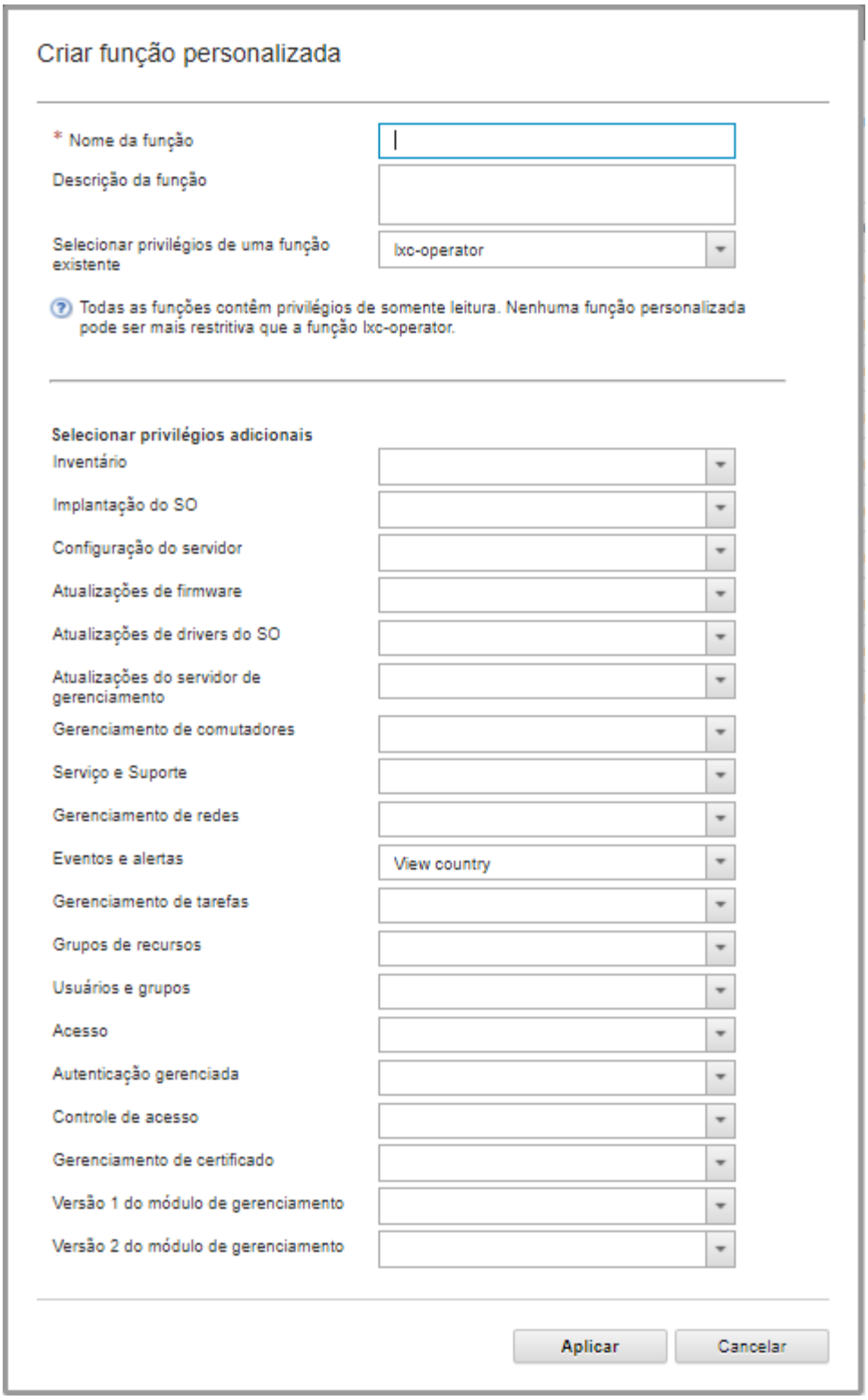
Procedimento

Para criar uma função personalizada, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.

Etapa 2. Clique em **Funções** na seção Usuários e Grupos para exibir a página Gerenciamento de Funções.

Etapa 3. Clique no ícone **Criar** ( ) para criar uma função. A caixa de diálogo Criar Função Personalizada é exibida.



Etapa 4. Insira um nome e descrição de função.

Etapa 5. Selecione uma função predefinida para ser usada como um ponto de partida para essa função personalizada.

Se você selecionar uma função existente, os privilégios que estão associados a essa função serão selecionados na caixa de diálogo.

Etapa 6. Modifique os privilégios para essa nova função, selecionando ou limpando os privilégios dos menus suspensos **Selecionar Privilégios Adicionais**.

Nota: Se você selecionar todos os privilégios de uma categoria específica e os privilégios forem adicionados a essa categoria quando você atualizar o XClarity Administrator, os novos privilégios serão adicionados automaticamente à função personalizada

Etapa 7. Clique em **Criar**. A nova função é adicionada à tabela na página Gerenciamento de Função.

Resultados

Também é possível executar as seguintes ações.

- Exiba os privilégios associados a uma função específica, selecionando a função e clicando no ícone **Exibir** ( ).
- Renomeie ou edite a função personalizada, clicando no ícone **Editar** ( ). Ao editar uma função personalizada, você pode alterar os privilégios selecionados, a descrição e a lista de usuários associados à função.

  Nota: Não é possível modificar uma função predefinida
- Exclua a função predefinida ou personalizada, clicando no ícone **Excluir** ( ).
- Adicione ou remova funções de um grupo de funções (consulte Adicionando e removendo vários usuários de um grupo de funções).
- Restaure todas as funções predefinidas que foram excluídas, clicando em **Todas as Ações → Restaurar Funções Padrão**.

Privilégios predefinidos

O Lenovo XClarity Administrator fornece um conjunto de *privilégios* (permissões) que permitem que um usuário execute uma ação específica. Os privilégios são organizados em categorias com base no tipo de ação.

Privilégios de acesso

Esses privilégios fornecem permissões para modificar os modos criptográfico e SSL/TLS.

Nome do privilégio	Descrição do privilégio	funções padrão
lxc-sec-apply-crypto-settings	Aplicar configurações de criptografia	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilégios de controle de acesso

Esses privilégios fornecem permissões para controlar o acesso a recursos.

Nome do privilégio	Descrição do privilégio	funções padrão
lxc-sec-modify-resource-access-control	Editar configurações de controle de acesso a recursos	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilégios de gerenciamento de certificados

Esses privilégios fornecem permissões para gerenciar certificados de segurança no Lenovo XClarity Administrator.

Nome do privilégio	Descrição do privilégio	Funções padrão
lxc-sec-add-external-certificates	Adicionar um certificado externo	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-add-trusted-certificates	Adicionar um certificado confiável	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-certificate-signing	Gerar solicitação de assinatura de certificado	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-external-certificates	Excluir um certificado externo existente	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-trusted-certificates	Excluir um certificado existente	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-ca	Baixar certificado raiz da autoridade de certificação	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-server-certificate	Baixar certificado do servidor	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-certificate-revocation-list	Modificar ou substituir lista de revogação de certificado	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-ca	Gerar certificado raiz da autoridade de certificação novamente	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-download-ca	Gerar certificado raiz da autoridade de certificação novamente	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-server-certificate	Gerar certificado de servidor novamente	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-resolve-untrusted-certificates	Resolver certificados não confiáveis	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-upload-server-certificate	Fazer upload do certificado do servidor	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc_sec_view_certpol_settings	Exibir configurações da política do certificado	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc_sec_apply_certpol_settings	Aplicar configurações da política do certificado	lxc-security-admin, lxc-supervisor

Monitoramento, eventos e privilégios

Esses privilégios fornecem permissões para gerenciar eventos e alertas.

Nome do privilégio	Descrição do privilégio	Funções padrão
lxc-event-audit	Gerenciar logs de eventos e de auditoria	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-create-edit-event-forwarders	Criar e modificar encaminhadores de evento	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-monitoring-create-edit-push-services	Criar e modificar serviços de push	lxc-admin, lxc-hw-admin, lxc-supervisor

Nome do privilégio	Descrição do privilégio	Funções padrão
lxc-monitoring-remove-event-forwarders	Excluir encaminhadores de evento	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-remove-push-services	Excluir serviços de push	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-set-event-thresholds	Definir limites de evento	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilégios de atualizações de firmware

Esses privilégios fornecem permissões para gerenciar e aplicar atualizações de firmware e UpdateXpress System Packs.

Nome do privilégio	Descrição do privilégio	funções padrão
lxc-fwUpdates-apply-assign-policy	Atribuir política de conformidade de firmware a dispositivos	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-apply-perform-updates	Executar atualizações de firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-create-policies	Criar, copiar, editar e importar políticas de conformidade de firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-delete-policies	Excluir políticas de conformidade	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-delete-packages	Excluir pacotes de atualização de firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-download-packages	Baixar e importar pacotes de atualização de firmware e atualizar o catálogo de pacotes de atualização de firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-export-packages	Exportar pacotes de atualização de firmware	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor

Privilégios do grupo de recursos

Esses privilégios fornecem permissões para usar grupos de recursos.

Nome do privilégio	Descrição do privilégio	Funções padrão
lxc-resource-create-edit-group	Criar e modificar grupos de recursos	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-resource-delete-group	Excluir grupos de recursos	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor

Privilégios de inventário

Esses privilégios fornecem permissões para descobrir e gerenciar dispositivos e exibir o inventário de dispositivos.

Nome do privilégio	Descrição do privilégio	funções padrão
lxc-dm-manage-device	Gerencie chassis, servidores, armazenamento e comutadores	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-dm-modify-ip-settings	Habilitar ou desabilitar a verificação de endereços IP duplicados na mesma sub-rede	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-power-state	Alterar o estado de energia de caixas, cmms, nós, armazenamento e comutadores	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-properties	Modificar propriedades de gabinetes, caixas, chassis, cmms, nós, armazenamento e de comutadores	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-node-pfa-config-settings	Modificar definições de configuração de alertas de falhas previstas (PFA)	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Privilégios de gerenciamento de trabalhos

Esses privilégios fornecem permissões para gerenciar trabalhos (tarefas).

Nome do privilégio	Descrição do privilégio	Funções padrão
lxc-tasks-remove-jobs	Excluir trabalhos	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-tasks-schedule-jobs	Planejar trabalhos	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Privilégios de autenticação gerenciada

Esses privilégios fornecem permissões para gerenciar a autenticação, incluindo credenciais armazenadas.

Nome do privilégio	Descrição do privilégio	funções padrão
lxc-sec-delete-stored-credentials	Excluir credenciais armazenadas	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-stored-credentials	Editar credenciais armazenadas existentes	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilégios v1 de módulo de gerenciamento

Esses privilégios estão associados aos bits de permissão LDAP (bitstrings) que são impostos pelos módulos de gerenciamento dos servidores em rack e do chassi do Flex System inteiro (incluindo todos os dispositivos nesse chassi).

O Lenovo XClarity Administrator não aplica essas permissões. As permissões serão impostas pelos dispositivos gerenciados que usam uma conta de usuário do XClarity Administrator.

Se o dispositivo for gerenciado usando *autenticação gerenciada* (com o servidor de autenticação local para autenticação), o servidor de autenticação local usará essas permissões para indicar aos dispositivos gerenciados quais permissões conceder ao usuário ao fazer login no dispositivo.

Você deve configurar essas mesmas permissões em um servidor LDAP externo. Ao usar um servidor LDAP externo com XClarity Administrator, certifique-se de incluir grupos no servidor LDAP externo com nomes que correspondam aos nomes do grupo de funções no XClarity Administrator e que os usuários LDAP externos sejam adicionados a um ou mais desses grupos. Usuários LDAP externos devem fazer parte de um grupo LDAP com um nome que corresponda a um grupo de funções XClarity Administrator que contenha

funções associadas às cadeias de bits do módulo de gerenciamento. XClarity Administrator usa esses grupos para vincular os usuários LDAP externos aos grupos de funções em XClarity Administrator e às cadeias de caracteres de bits que são aplicadas pelo módulo de gerenciamento. Em seguida, quando um usuário faz login em um dispositivo gerenciado usando uma conta de usuário LDAP externa, o módulo de gerenciamento sabe se deve conceder privilégios ao supervisor do usuário ou ao operador.

Nota: Os privilégios v1 do módulo de gerenciamento não são suportados para comutadores FlexSystem que não tenham IOM seguro habilitado, comutadores RackSwitch, dispositivos de armazenamento e servidores ThinkServer.

Para obter informações sobre os bits de permissão de LDAP para cada módulo de gerenciamento, consulte a documentação online.
- Configurando o LDAP na documentação online do CMM e CMM2
- Configurando o LDAP na documentação online do IMM e IMM2
- Configurando o LDAP na documentação online do XCC

Nome do privilégio	Descrição do privilégio	funções padrão
mm-advanced-adaptor-configuration-v1	Configuração de adaptador avançada	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-basic-configuration-v1	Configuração básica	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-clear-event-logs-v1	Limpar logs de evento	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v1	Negar sempre	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-networking-and-security-v1	Rede e segurança	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-power-and-restart-access-v1	Acesso de energia reinicialização para servidores e comutadores Flex	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-access-v1	Acesso de controle remoto para servidores	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-and-virtual-media-access-v1	Acesso ao console remoto e a mídias virtuais para servidores	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-supervisor-v1	Acesso de Supervisor	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-user-account-management-v1	Gerenciamento de usuários	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor

Privilégios v2 de módulo de gerenciamento

Esses privilégios estão associados aos bits de permissão LDAP (bitstrings) que são impostos pelos módulos de gerenciamento para dispositivos FlexSystem e ThinkSystem individuais em um chassi (chassis, servidores e comutadores com IOM seguro habilitado).

O Lenovo XClarity Administrator não aplica essas permissões. As permissões serão impostas pelos dispositivos gerenciados que usam uma conta de usuário do XClarity Administrator.

Se o dispositivo for gerenciado usando *autenticação gerenciada* (com o servidor de autenticação local para autenticação), o servidor de autenticação local usará essas permissões para indicar aos dispositivos gerenciados quais permissões conceder ao usuário ao fazer login no dispositivo.

Você deve configurar essas mesmas permissões em um servidor LDAP externo. Ao usar um servidor LDAP externo com XClarity Administrator, certifique-se de incluir grupos no servidor LDAP externo com nomes que correspondam aos nomes do grupo de funções no XClarity Administrator e que os usuários LDAP externos sejam adicionados a um ou mais desses grupos. Usuários LDAP externos devem fazer parte de um grupo LDAP com um nome que corresponda a um grupo de funções XClarity Administrator que contenha funções associadas às cadeias de bits do módulo de gerenciamento. XClarity Administrator usa esses grupos para vincular os usuários LDAP externos aos grupos de funções em XClarity Administrator e às cadeias de caracteres de bits que são aplicadas pelo módulo de gerenciamento. Em seguida, quando um usuário faz login em um dispositivo gerenciado usando uma conta de usuário LDAP externa, o módulo de gerenciamento sabe se deve conceder privilégios ao supervisor do usuário ou ao operador.

Notas:

- Você também deve especificar privilégios v1 do módulo de gerenciamento para o chassi inteiro (consulte Privilégios v1 de módulo de gerenciamento).
- Os privilégios v2 do módulo de gerenciamento não são suportados para comutadores FlexSystem que não têm IOM seguro habilitado.
- Para o chassi do Lenovo ThinkSystem, certifique-se de que o IMM2 seja configurado para permitir que a função personalizada tenha "Administração de nós." Se você deseja que a função personalizada tenha controle de todos os dispositivos no chassi do Lenovo ThinkSystem, certifique-se de que o IMM2 seja configurado para permitir que a função personalizada também tenha o "Escopo do nó X".

Para obter informações sobre os bits de permissão de LDAP para cada módulo de gerenciamento, consulte a documentação online.
- Configurando o LDAP na documentação online do CMM e CMM2
- Configurando o LDAP na documentação online do IMM e IMM2
- Configurando o LDAP na documentação online do XCC

Nome do privilégio	Descrição do privilégio	Funções padrão
mm-blade-1-scope-v2	Escopo do nó 1	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-2-scope-v2	Escopo do nó 2	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-3-scope-v2	Escopo do nó 3	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-4-scope-v2	Escopo do nó 4	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-5-scope-v2	Escopo do nó 5	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-6-scope-v2	Escopo do nó 6	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-7-scope-v2	Escopo do nó 7	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-8-scope-v2	Escopo do nó 8	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-9-scope-v2	Escopo do nó 9	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Nome do privilégio	Descrição do privilégio	Funções padrão
mm-blade-10-scope-v2	Escopo do nó 10	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-11-scope-v2	Escopo do nó 11	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-12-scope-v2	Escopo do nó 12	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-13-scope-v2	Escopo do nó 13	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-14-scope-v2	Escopo do nó 14	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-administration-v2	Administração de nó	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-configuration-v2	Configuração do nó	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-operator-v2	Operador do blade	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-remote-presence-v2	Presença remota do nó	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-administration-v2	Administração de chassi	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-configuration-v2	Configuração do chassi	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-log-management-v2	Gerenciamento de conta de log do chassi	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-operator-v2	Operador de chassi	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-chassis-scope-v2	Escopo do chassi	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-user-account-management-v2	Gerenciamento de usuários	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v2	Negar sempre	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-io-module-1-scope-v2	Escopo do módulo 1 de E/S	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-2-scope-v2	Escopo do módulo 2 de E/S	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-3-scope-v2	Escopo do módulo 3 de E/S	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-4-scope-v2	Escopo do módulo 4 de E/S	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Nome do privilégio	Descrição do privilégio	Funções padrão
mm-switch-administration-v2	Alternar administração	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-configuration-v2	Alternar configuração	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-operator-v2	Alternar operador	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-supervisor-v2	Acesso de Supervisor	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilégios do servidor de gerenciamento

Esses privilégios fornecem permissões para atualizar o servidor de gerenciamento.

Nome do privilégio	Descrição do privilégio	funções padrão
lxc-mgmtserverupdates-delete-updates	Excluir atualizações do servidor de gerenciamento	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-download-updates	Baixar e importar atualizações do servidor de gerenciamento e atualizar catálogo do servidor de gerenciamento	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-perform-updates	Realizar atualizações do servidor de gerenciamento	lxc-admin, lxc-fw-admin, lxc-supervisor

Privilégios de gerenciamento de rede

Esses privilégios fornecem permissões para definir configurações de rede.

Nome do privilégio	Descrição do privilégio	Funções padrão
lxc-network-edit	Modificar acesso à rede	lxc-admin, lxc-supervisor

Privilégios de implantação do SO

Esses privilégios fornecem permissões para gerenciar e implantar sistemas operacionais.

Nome do privilégio	Descrição do privilégio	Funções padrão
lxc-osdeploy-create-edit-remote-file-server	Criar e editar uma entrada de servidor de arquivos remoto	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-create-import-export-edit-os-files	Criar, importar, exportar e editar imagens do SO e arquivos personalizados	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-os-files	Excluir imagens do SO e arquivos personalizados	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-remote-file-server	Excluir uma entrada de servidor de arquivos remoto	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Nome do privilégio	Descrição do privilégio	Funções padrão
lxc-osdeploy-edit-global-settings	Editar informações na caixa de diálogo Configurações globais **Nota:** Alterar as configurações globais de atribuição de IP afeta as configurações de rede; portanto, para fazer alterações nas configurações globais de atribuição de IP, também é necessário ter privilégios **lxc-osdeploy-edit-settings-and-deploy-os-images**.	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-edit-settings-and-deploy-os-images	Modificar as configurações de implantação e implantar imagens do SO em um ou mais servidores	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Privilégios de atualização de driver de SO

Esses privilégios fornecem permissões para gerenciar e aplicar atualizações de driver de dispositivo do SO.

Nome do privilégio	Descrição do privilégio	funções padrão
lxc-osDriverUpdates-apply-assign-uxsp	Atribuir UXSP de drivers de dispositivos do SO a dispositivos	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-authentication	Verificar autenticação do SO	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-compliance	Verificar conformidade de driver de dispositivo de SO	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-perform-updates	Executar atualizações de drivers de dispositivo do SO	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-delete-packages	Excluir pacotes de atualização de drivers de dispositivo do SO	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-download-packages	Baixar e importar pacotes de atualização de drivers de dispositivos do SO e atualizar catálogo de UXSP de drivers de dispositivos do SO	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Privilégios de usuários e grupos

Esses privilégios fornecem permissões para gerenciar contas do usuário e grupos.

Nome do privilégio	Descrição do privilégio	funções padrão
lxc-sec-apply-saml-settings	Aplicar configurações de SAML	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-role-groups	Excluir um grupo de funções	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-roles	Excluir uma função	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-users	Excluir um usuário	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-edit-account-settings	Modificar configurações de segurança da conta	lxc-recovery, lxc-security-admin, lxc-supervisor

Nome do privilégio	Descrição do privilégio	funções padrão
lxc-sec-modify-ldap-settings	Aplicar configurações LDAP	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-role-groups	Modificar um grupo de funções	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-roles	Modificar uma função	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-users	Modificar um usuário	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilégios de configurações do servidor

Esses privilégios fornecem permissões para fornecer ou fornecer previamente servidores usando padrões de configuração.

Nome do privilégio	Descrição do privilégio	Funções padrão
lxc-cp-edit-management-ip	Modificar endereços IP de gerenciamento do chassi	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-edit-preferences	Definir preferências de padrões de configuração	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-address-pools	Gerenciar conjuntos de endereços	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-patterns	Gerenciar padrões	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-placeholders	Gerenciar marcadores	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-profiles	Implantar padrões, implantar marcador no chassi e gerenciar perfis	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-other-server-config	Redefinir o armazenamento local e aplicar a operação de segurança Intel Optane DCPMM	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilégios de serviço

Esses privilégios fornecem permissões para definir contatos de suporte para cada dispositivo gerenciado, coletar e enviar arquivos de serviço para o Suporte Lenovo, configurar a notificação automática para provedores de serviço quando ocorrerem certos eventos que permitem manutenção em dispositivos específicos, exibir o status do tíquete de serviço e informações sobre garantia e coletar e encaminhar dados de serviço.

Nome do privilégio	Descrição do privilégio	Funções padrão
lxc-ss-alter-backup-credentials	Modificar credenciais FFDC de backup	lxc-admin, lxc-hw-admin, lxc-service-admin, lxc-supervisor
lxc-ss-call-home	Realizar Call Home	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-change-service-recovery-password	Alterar a senha de recuperação de serviço	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-change-service-tickets	Modificar tíquetes de serviço	lxc-admin, lxc-hw-admin, lxc-supervisor

Nome do privilégio	Descrição do privilégio	Funções padrão
lxc-ss-remove-service-tickets	Excluir tíquetes de serviço	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-run-service-forwarders	Executar encaminhadores de serviço	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilégios de configuração de comutador

Esses privilégios fornecem permissões para configurar comutadores e fazer backup e restaurar dados de configuração do comutador.

Nome do privilégio	Descrição do privilégio	funções padrão
lxc-netcfg-template-management	Criar, modificar, excluir e implantar modelos de configuração do comutador e excluir uma implantação de configuração do comutador	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-config-management	Fazer backup, restaurar, excluir, exportar e importar arquivos de dados de configuração do comutador	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-port-management	Modificar status de porta do comutador	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Criando um grupo de funções personalizado

Um *grupo de funções* é um conjunto de funções e um conjunto de usuários que são membros do mesmo conjunto de funções. O nível de acesso que é concedido a cada usuário no grupo de funções é baseado nas funções que são atribuídas a esse grupo de funções. O XClarity Administrator fornece os seguintes grupos de funções predefinidos, que correspondem a cada uma das funções predefinidas. É possível também criar grupos de funções personalizados.

Sobre esta tarefa

Cada usuário do XClarity Administrator deve ser membro de pelo menos um grupo de funções.

Os grupos de função a seguir são predefinidos em XClarity Administrator.

- **LXC-SUPERVISOR**. Inclui a função **lxc-supervisor**.
- **LXC-ADMIN**. Inclui a função **lxca-admin**.
- **LXC-SECURITY-ADMIN**. Inclui a função **lxc-security-admin**.
- **LXC-HW-ADMIN**. Inclui a função **lxc-hw-admin**.
- **LXC-FW-ADMIN**. Inclui a função **lxc-fw-admin**.
- **LXC-OS-ADMIN**. Inclui a função **lxc-os-admin**.
- **LXC-SERVICE-ADMIN**. Inclui a função **lxc-service-admin**.
- **LXC-HW-MANAGER**. Inclui a função **lxc-hw-manager**.
- **LXC-OPERATOR**. Inclui a função **lxc-operator**.
- **LXC-RECOVERY**. Inclui a função **lxc-recovery**.

As seguintes funções predefinidas estão *reservadas* e não podem ser usadas para criar novos grupos de funções ou serem atribuídas a novos usuários.

- **lxc-sysrdr**

- **lxc-sysmgr**

Procedimento

Para criar um grupo de funções, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.

Etapa 2. Clique em **Grupos de Função** na seção Usuários e Grupos para exibir a página Configurações de Grupo.

Etapa 3. Clique no ícone **Criar** ( ) para criar um novo grupo de funções. A caixa de diálogo Criar Novo Grupo de Função é exibida.

Etapa 4. Insira um nome do grupo e descrição.

Nota: Dica: para o nome do grupo, é possível usar letras, números, espaços em branco, sublinhado, traços e pontos.

Etapa 5. Selecione uma ou mais funções para designar a este grupo de funções.

Etapa 6. Selecione um ou mais usuários como membros deste grupo de funções.

Etapa 7. Clique em **Criar**. O novo grupo de funções é adicionado à tabela na página Gerenciamento de Grupo.

Resultados

O grupo de funções é exibido na tabela Grupos de Função. A tabela mostra as funções de autorização associadas e os membros para cada grupo de função.

Gerenciamento de Grupo de Função

Um grupo de funções é uma coleção de uma ou mais funções. As operações que os usuários podem realizar são determinadas pelos grupos de função aos quais eles estão atribuídos. Saiba mais

Todas as ações

Nome do Grupo	Função	Lista de usuários	Predefinido
LXC-RECOVERY	lxc-recovery		Verdadeiro
LXC-FW-ADMIN	lxc-fw-admin		Verdadeiro
LXC-OPERATOR	lxc-operator		Verdadeiro
LXC-SECURITY-ADMIN	lxc-security-admin		Verdadeiro
LXC-HW-ADMIN	lxc-hw-admin		Verdadeiro
LXC-SERVICE-ADMIN	lxc-service-admin		Verdadeiro
LXC-ADMIN	lxc-admin		Verdadeiro
LXC-HW-MANAGER	lxc-hw-manager		Verdadeiro
LXC-OS-ADMIN	lxc-os-admin		Verdadeiro
LXC-SUPERVISOR	lxc-supervisor	USERID	Verdadeiro

Após criar uma grupo de funções, é possível executar as seguintes ações em um grupo de funções selecionado:

- Adicione ou remova funções atribuídas a este grupo de funções clicando no ícone **Editar** ( ).
- Adiciona ou remove os usuários membros do grupo de funções especificado (consulte "Adicionando e removendo vários usuários de um grupo de funções" na página 58).
- Exporta informações sobre grupos de função, incluindo permissões de acesso, clicando em **Todas as Ações → Exportar como CSV**.
- Exclui o grupo de funções, clicando no ícone **Excluir** ( ).Não é possível excluir os grupos de funções predefinidos.

Após um grupo de funções ser criado, editado ou excluído, a alteração é provisionada imediatamente para cada dispositivo gerenciado.

Adicionando e removendo vários usuários de um grupo de funções

É possível alterar a associação em um grupo de funções adicionando ou removendo diversos usuários.

Procedimento

Conclua as seguintes etapas para adicionar e remover usuários de um grupo de funções.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Segurança**.

Etapa 2. Clique em **Grupos de Função** na seção Usuários e Grupos para exibir a página Configurações de Grupo.

Etapa 3. Clique no ícone **Editar** ( ) para modificar o grupo de funções. A caixa de diálogo Editar Grupo de Funções é exibida.

Etapa 4. Clique na lista suspensa **Lista de usuários** e selecione os usuários a serem incluídos ou desmarque o usuário a ser excluído deste grupo de funções.

Etapa 5. Clique em **Salvar**. A coluna **Lista de Usuários** exibe a associação do usuário atual no grupo de funções.

Gerenciando o acesso a dispositivos

O controle de acesso a dispositivos é desabilitado por padrão e não têm efeito até você ativá-lo

Quando os dispositivos são gerenciados inicialmente pelo Lenovo XClarity Administrator, um conjunto predefinido de grupos de função tem permissão para acessar os dispositivos por padrão. Esse conjunto predefinido está vazio, por padrão, até ser configurado.

Altere os grupos de função que podem acessar dispositivos gerenciados específicos. Quando a permissão é fornecida a determinados grupos de função, apenas os usuários que são membros desses grupos de função podem ver e trabalhar nesses dispositivos específicos.

Controlando o acesso a dispositivos específicos

Quando os dispositivos são gerenciados inicialmente pelo Lenovo XClarity Administrator, um conjunto predefinido de grupos de função tem permissão para acessar os dispositivos por padrão. Altere os grupos de função que podem acessar dispositivos gerenciados específicos. Quando a permissão é fornecida a determinados grupos de função, apenas os usuários que são membros desses grupos de função podem ver e trabalhar nesses dispositivos específicos.

Antes de iniciar

Somente usuários com a autoridade **lxc-supervisor**, **lxc-security-admin** ou **lxc-recovery** podem executar essa ação.

Sobre esta tarefa

O controle de acesso é definido em dispositivos individuais. Ele não é definido para contêineres, como racks e grupos de recursos.

Para componentes em um chassi ou gabinete, os usuários devem ter, pelo menos, acesso somente leitura ao chassi ou ao gabinete para exibir componentes no chassi ou no gabinete. Se os usuários não tiverem, pelo menos, acesso somente leitura ao chassi ou ao gabinete, esses usuários poderão ver os componentes do chassi em algumas exibições, mas não há garantia de visualizá-los em todas elas.

Os usuários com autoridade **lxc-supervisor** podem visualizar e realizar ações em todos os recursos independentemente de estarem em um grupo de funções que tenha recebido acesso especificamente a esse recurso. Não é possível pode remover o acesso nenhum recurso para o grupo de funções **lxc-supervisor**.

Se um usuário não for membro de um grupo de funções que tenha acesso a um dispositivo gerenciado específico, o usuário não poderá ver ou trabalhar nesse dispositivo específico. Isso inclui iniciar a interface da Web do controlador de gerenciamento por meio do Lenovo XClarity Administrator. Para dispositivos Flex e System x, os usuários também não podem fazer login diretamente em um CMM nem no controlador de gerenciamento aos quais eles não tenham acesso.

As configurações de controle de acesso padrão são usadas para definir as permissões de acesso em dispositivos quando são gerenciados inicialmente pelo XClarity Administrator e ao redefinir permissões de acesso para um dispositivo específico como as configurações padrão. Alterar as configurações de controle de acesso padrão não altera automaticamente as permissões de acesso em dispositivos que já são gerenciados.

Importante:

- Se um usuário for membro de mais de um grupo de funções, e os grupos de funções forem atribuídos a dispositivos diferentes, as ações que o usuário tem permissão para realizar em cada dispositivo poderão ser diferentes. Por exemplo, se o usuário for membro dos grupos de função padrão LXC-FW-ADMIN e LXC-OS-ADMIN, e se LXC-FW-ADMIN receber acesso ao Servidor A, mas LXC-OS-ADMIN não receber acesso ao Servidor A, esse usuário poderá atualizar o firmware no Servidor A, mas não conseguirá implantar um sistema operacional para o Servidor A. Se LXC-OS-ADMIN receber acesso ao Servidor B, mas LXC-FW-ADMIN não receber acesso ao Servidor B, esse mesmo usuário poderá implantar um sistema operacional para o Servidor B, mas não poderá atualizar o firmware no Servidor B.
- Ao limitar o acesso a um dispositivo que tenha um recurso pai (como um servidor ou comutador em um chassi Flex), um usuário deve ter, pelo menos, permissões somente leitura para o recurso pai para interagir completamente com o dispositivo. Se um usuário tiver, pelo menos, acesso somente leitura para o dispositivo, mas não para o pai, ele não poderá consultar as exibições de inventário do dispositivo, mas talvez possa consultar sobre o dispositivo em algumas exibições, como trabalhos e eventos.

  Por exemplo, você pode criar um grupo de funções para o pai e atribuir esse grupo de funções para a função **lxc-operador**. Inclua todos os usuários que devem ter permissão de acesso a qualquer um dos filhos (como um servidor ou comutador em um chassi Flex), desse grupo de funções. Em seguida, inclua esse grupo de funções como um dos grupos que tenha acesso ao pai.

Procedimento

Execute os seguintes procedimentos para controlar o acesso a dispositivos específicos associando grupos de função a esses dispositivos.

Etapa 1. No menu principal Lenovo XClarity Administrator, clique em **Administração → Segurança**.

Etapa 2. No painel de navegação esquerdo, clique em **Exibição de Recursos**. A página Exibição de Recursos é exibida.

É possível classificar as colunas da tabela para facilitar a localização dos dispositivos específicos. Além disso, é possível selecionar um tipo de dispositivo no menu suspenso **Tipo de Recurso**, selecionar um grupo de funções no menu suspenso **Grupos de Função**, selecionar um grupo de recursos no menu suspenso **Grupos de Recursos** e inserir texto (como um nome ou tipo de recurso) no campo **Filtro** para listar apenas os dispositivos que atendem aos critérios selecionados.

Etapa 3. Selecione um ou mais dispositivos aos quais você deseja controlar o acesso.

Etapa 4. Clique no ícone **Editar** (). A caixa de diálogo Editar Recurso é exibida com os dispositivos de destino listados no campo **Nome do Recurso**.

Etapa 5. Na lista suspensa **Grupos de Função**, selecione os grupos de função para os quais você deseja permitir o acesso aos dispositivos de destino.

Nota: Se o dispositivo tiver um recurso pai (por exemplo, um servidor ou comutador em um chassi Flex), é possível especificar acesso para o dispositivo (coluna direita) e o recurso pai (coluna esquerda).

Etapa 6. Configure o **Acesso Público** a `No`. Isso significa que apenas os usuários que são membros dos grupos de função selecionados podem acessar os dispositivos de destino.

Etapa 7. Clique em **Salvar**.

Etapa 8. Depois de concluir a atribuição de permissões, clique no botão de alternância **Desabilitado** para alterar **Controle de Acesso de Recurso** para habilitado.

É possível habilitar o controle de acesso de recurso a qualquer momento antes ou depois de configurar o acesso a dispositivos específicos. Quando essa configuração é habilitada, a configuração exibida na tabela entra em vigor, incluindo a negação de acesso de usuários não supervisores aos dispositivos que não têm grupos configurados para acessá-los.

Depois de concluir

Você também pode controlar o acesso a dispositivos executando as seguintes ações:

- Altere as permissões para a configuração padrão de acesso público e grupos de função clicando no ícone **Editar** () e, em seguida, clicando em **Restaurar Padrões**.
- Altere a configuração padrão de acesso público e grupo de funções (consulte Alterando as permissões padrão).
- Desabilite o controle de acesso de recurso clicando no botão de alternância **Habilitado** para alterar **Controle de Acesso de Recurso** para desabilitado. Isso significa que todos os grupos de função podem acessar todos os dispositivos gerenciados.

Desabilitando o controle de acesso de recurso

Desabilite o controle de acesso para todos os dispositivos ou dispositivos específicos para que todos os usuários possam visualizar e trabalhar nesses dispositivos.

Sobre esta tarefa

Somente usuários com a autoridade **lxc-supervisor**, **lxc-security-admin** ou **lxc-recovery** podem executar essa ação.

Procedimento

Conclua as etapas a seguir para desabilitar o controle de acesso de recurso.

- Para todos os dispositivos gerenciados

1. No menu principal Lenovo XClarity Administrator, clique em **Administração → Segurança**.
2. No painel de navegação esquerdo, clique em **Exibição de Recursos**. A página Exibição de Recursos é exibida.
3. Clique no botão de alternância **Habilitado** para alterar **Controle de Acesso de Recurso** para desabilitado.

- Para dispositivos gerenciados específicos
  1. No menu principal XClarity Administrator, clique em **Administração → Segurança**.
  2. No painel de navegação esquerdo, clique em **Exibição de Recursos**. A página Exibição de Recursos é exibida.

     É possível classificar as colunas da tabela para facilitar a localização dos dispositivos específicos. Além disso, é possível selecionar um tipo de dispositivo no menu suspenso **Tipo de Recurso**, selecionar um grupo de funções no menu suspenso **Grupos de Função**, selecionar um grupo de recursos no menu suspenso **Grupos de Recursos** e inserir texto (como um nome ou tipo de recurso) no campo **Filtro** para listar apenas os dispositivos que atendem aos critérios selecionados.
  3. Selecione um ou mais dispositivos dos quais você deseja alterar o acesso.
  4. Clique no ícone **Editar** (). A caixa de diálogo Editar Recurso é exibida com os dispositivos selecionados listados no campo **Nome do Recurso**.
  5. Configure o **Acesso Público** a `Yes`. Isso significa que todos os grupos de função podem acessar os dispositivos de destino independentemente dos grupos de funções que estão listados na lista suspensa **Grupos de Função**.
  6. Clique em **Salvar**.

Alterando as permissões padrão

Há duas configurações que determinam se os grupos de função podem acessar dispositivos quando são gerenciados inicialmente pelo Lenovo XClarity Administrator: acesso público e grupos de função. A configuração de acesso público determina se todos ou apenas um conjunto específico de grupos de função pode acessar os dispositivos de destino. Por padrão, essa configuração é definida como `Yes`, o que significa que todos os grupos de função podem acessar os dispositivos de destino. Você pode alterar o comportamento padrão alterando a configuração de acesso público para `No` e, em seguida, selecionando o conjunto de grupos de função que pode acessar os dispositivos de destino

Sobre esta tarefa

Somente usuários com a autoridade **lxc-supervisor**, **lxc-security-admin** ou **lxc-recovery** podem executar essa ação.

Usuários com a autoridade **lxc-supervisor**, **lxc-security-admin** ou **lxc-recovery** podem acessar todos os dispositivos gerenciados. Não é possível remover o acesso a nenhum dispositivo destes grupos de funções.

As configurações de controle de acesso padrão são usadas para definir as permissões de acesso em dispositivos quando são gerenciados inicialmente pelo XClarity Administrator e ao redefinir permissões de acesso para um dispositivo específico como as configurações padrão. Alterar as configurações de controle de acesso padrão não altera automaticamente as permissões de acesso em dispositivos que já são gerenciados.

Procedimento

Execute os seguintes procedimentos para alterar os controles de acesso padrão.

Etapa 1. No menu principal XClarity Administrator, clique em **Administração → Segurança**.

Etapa 2. No painel de navegação esquerdo, clique em **Exibição de Recursos**. A página Exibição de Recursos é exibida.

É possível classificar as colunas da tabela para facilitar a localização dos dispositivos específicos. Além disso, é possível selecionar um tipo de dispositivo no menu suspenso **Tipo de Recurso**, selecionar um grupo de funções no menu suspenso **Grupos de Função**, selecionar um grupo de recursos no menu suspenso **Grupos de Recursos** e inserir texto (como um nome ou tipo de recurso) no campo **Filtro** para listar apenas os dispositivos que atendem aos critérios selecionados.

Etapa 3. Clique em **Todas as Ações → Editar Recursos Padrão**. A caixa de diálogo Editar Recursos Padrão é exibida.

Etapa 4. Na lista suspensa **Grupos de Função**, selecione os grupos de função que você deseja definir como conjunto padrão.

Etapa 5. Selecione a configuração **Acesso Público** padrão.

- **Sim**. Quando um dispositivo é gerenciado inicialmente, todos os grupos de função podem acessar esse dispositivo independentemente dos grupos de função que estão listados na lista suspensa **Grupos de Função**.
- **Não**. Quando um dispositivo é gerenciado inicialmente, somente os grupos de função que estão listados na lista suspensa **Grupos de Função** podem acessar esse dispositivo por padrão.

Etapa 6. Clique em **Salvar**.

Implementando um ambiente seguro

É importante avaliar os requisitos de segurança no seu ambiente, entender todos os riscos de segurança e minimizá-los. O Lenovo XClarity Administrator inclui diversos recursos que podem ajudar a proteger seu ambiente. Use as seguintes informações para ajudá-lo a implementar o plano de segurança para seu ambiente.

Sobre esta tarefa

Importante: Você é responsável pela avaliação, seleção e implementação dos recursos de segurança, procedimentos administrativos e controles apropriados para o ambiente do sistema. A implementação dos recursos de segurança que estão descritos nesta seção não protege seu ambiente completamente.

Considere as seguintes informações ao avaliar os requisitos de segurança para seu ambiente:

- A segurança física de seu ambiente é importante; limite o acesso a salas e racks onde o hardware de gerenciamento de sistemas é mantido.
- Use um firewall baseado em software para proteger seu hardware de rede e os dados contra ameaças de segurança conhecidas e emergentes, como vírus e acesso não autorizado.
- Não altere as configurações de segurança padrão para os comutadores de rede e módulos intermediários. As configurações padrão de fabricação para esses componentes desabilitam o uso de protocolos inseguros e habilitam o requisito de atualizações de firmware assinado.
- Os aplicativos de gerenciamento para os CMMs, Baseboard Management Controller, FSPs e comutadores permitem apenas pacotes de atualização de firmware assinados para esses componentes, para assegurar que apenas firmware confiável seja instalado.
- Apenas os usuários autorizados para atualizar componentes de firmware devem ter autoridade de atualização de firmware.
- No mínimo, certifique-se de que as atualização de firmware críticas foram instaladas. Depois de fazer mudanças, sempre faça backup da configuração.

- Certifique-se de que todas as atualizações relacionadas à segurança para servidores DNS foram instaladas imediatamente e mantidas atualizadas.
- Instrua os usuários a não aceitarem nenhum certificado não confiável. Para obter mais informações, consulte Trabalhando com certificados de segurança.
- Opções de violação evidente estão disponíveis para o hardware do Flex System. Se o hardware estiver instalado em um rack desbloqueado ou localizado numa área aberta, instale as opções de violação evidente para deter e identificar intrusões. Consulte a documentação fornecida com os produtos do Flex System para obter informações adicionais sobre opções de violação evidente.
- Sempre que possível e prático, coloque o hardware de gerenciamento de sistemas em uma sub-rede separada. Geralmente, apenas os administradores devem ter acesso ao hardware de gerenciamento de sistemas, e nenhum usuário básico deve receber acesso.
- Ao escolher as senhas, não use expressões fáceis de adivinhar, como "senha" ou nome de sua empresa. Mantenha as senhas em um local seguro e certifique-se de que o acesso às senhas esteja restrito. Implemente uma política de senha para sua empresa.

  Importante: Sempre altere o nome de usuário e a senha padrão. Regras de senha forte devem ser obrigatórias para todos os usuários.
- Estabeleça senhas de inicialização para os usuários como um meio de controlar quem tem acesso aos dados e programas de configuração nos servidores. Consulte a documentação fornecida com os servidores para obter mais informações sobre senhas de inicialização.
- Use os diversos níveis de autorização que estão disponíveis para diferentes usuários em seu ambiente. Não permita que todos os usuários trabalhem com o mesmo ID do usuário de supervisor.
- Assegure-se de que seu ambiente atenda aos seguintes critérios NIST 800-131A para suportar comunicações seguras:
  - Use o Secure Sockets Layer (SSL) sobre o protocolo TLS v1.2.
  - Use o SHA-256 ou as funções hash mais fortes para as assinaturas digitais e SHA-1 ou as funções hash mais fortes para os outros aplicativos.
  - Use o RSA-2048 ou mais forte ou o Elliptic Curves aprovado pelo NIST que têm 224 bits ou mais.
  - Use a criptografia simétrica aprovado pelo NIST com chaves com um mínimo de 128 bits de comprimento.
  - Use os geradores de números aleatórios aprovados pelo NIST.
  - Quando for possível, ofereça suporte aos mecanismos Diffie-Hellman ou Elliptic Curve Diffie-Hellman Key Exchange.

  Para obter mais informações sobre as configurações de criptografia, consulte Definindo configurações de criptografia no servidor de gerenciamento. Para obter mais informações sobre as configurações NIST, consulte Implementando a conformidade com NIST SP 800-131A.

Alterando as configurações de segurança de conta do usuário

As configurações de segurança de conta do usuário controlam a complexidade da senha, o bloqueio da conta e o tempo limite de inatividade da sessão. É possível alterar os valores das configurações.

Procedimento

Conclua as etapas a seguir para substituir as configurações de segurança de conta do usuário que estiverem definidas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.

Etapa 2. Clique em **Configurações de Segurança de Conta** na seção Usuários e Grupos para exibir a página Gerenciamento de Usuários.

Etapa 3. Para cada configuração a seguir que precisar de alteração, selecione o novo valor.

Tabela 1. Configurações de Segurança de Conta

Configuração de segurança	Descrição	Valores permitidos	Valores padrão
Período de Expiração da Senha	Período, em dias, durante o qual um usuário pode usar uma senha antes de precisar alterá-la. Com valores menores, os invasores têm menos tempo para adivinhar senhas Se for definido como **0**, as senhas nunca expirarão. **Nota:** Essa configuração é aplicável apenas quando as contas de usuário são gerenciadas com o servidor de autenticação local. Elas não são usadas quando o servidor de autenticação externo é usado.	**0 – 365**	**90**
Período de aviso de expiração da senha	O período, em dias, anterior à data de expiração da senha em que os usuários começam a receber avisos sobre a proximidade da expiração da senha. Se for definido como **0**, os usuários nunca serão avisados. **Nota:** Essa configuração é aplicável apenas quando as contas de usuário são gerenciadas com o servidor de autenticação local. Elas não são usadas quando o servidor de autenticação externo é usado.	**0 –** *configuração de expiração máxima de senha*	**5**
Ciclo mínimo de reutilização de senha	O número mínimo de vezes que o usuário deve inserir uma senha exclusiva ao alterar a senha antes de poder começar a repetir senhas. Se definido como **0**, os usuários poderão reutilizar as senhas imediatamente.	**0 – 10**	**5**
Intervalo mínimo de mudança de senha	O período mínimo, em horas, que deve decorrer antes que um usuário possa alterar uma senha novamente após já tê-la alterado. O valor especificado para essa configuração não pode ultrapassar o valor especificado para o período de expiração da senha. Se definido como **0**, os usuários poderão alterar as senhas imediatamente.	**0 – 1440**	**24**
Número máximo de falhas de login	O número máximo de vezes que o usuário pode tentar fazer login com uma senha incorreta antes que a conta do usuário seja bloqueada. O número especificado para o período de bloqueio após número máximo de falhas de login determina por quanto tempo a conta do usuário ficará bloqueada. As contas bloqueadas não podem ser usadas para obter acesso ao sistema, mesmo se uma senha válida for fornecida. Se for definido como **0**, as contas nunca serão bloqueadas. O contador de falhas de login é zerado depois de um login bem-sucedido.	**0 – 100**	**20**

Tabela 1. Configurações de Segurança de Conta (continuação)

Configuração de segurança	Descrição	Valores permitidos	Valores padrão
Período de bloqueio após número máximo de falhas de login	O período mínimo, em minutos, que deve decorrer antes que um usuário que estava bloqueado possa tentar fazer login novamente. Se for definido como **0**, a conta permanecerá bloqueada até ser explicitamente desbloqueada por um administrador. Uma configuração 0 pode tornar seu sistema mais exposto a ataques graves de negação de serviço, onde tentativas deliberadas de login com falha podem deixar contas permanentemente bloqueadas. **Dica:** Qualquer usuário com a função de Supervisor pode desbloquear uma conta de usuário. Para obter mais informações, consulte Desbloqueando um usuário. **Nota:** Essa configuração é aplicável apenas quando as contas de usuário são gerenciadas com o servidor de autenticação local. Elas não são usadas quando o servidor de autenticação externo é usado.	**0 – 2880**	**60**
Tempo limite da sessão de inatividade da web	O período, em minutos, que uma sessão estabelecida com o XClarity Administrator pode ficar inativa antes que o usuário seja desconectado Se definido como **0**, a sessão da Web nunca expirará. **Nota:** Ao alterar esse valor, as sessões somente do usuário que começam após a alteração da configuração serão afetadas.	**0 – 1440**	**1440**
Tamanho mínimo de senha	O número mínimo de caracteres que podem ser usados para especificar uma senha válida	**8 – 20**	**8**

Tabela 1. Configurações de Segurança de Conta (continuação)

Configuração de segurança	Descrição	Valores permitidos	Valores padrão
Número de regras de complexidade que devem ser seguidas ao criar uma nova senha	Número de regras de complexidade que devem ser seguidas ao criar uma nova senha As regras são aplicadas começando com a regra 1 e até o número de regras especificadas. Por exemplo, se a complexidade da senha for definida como 4, as regras 1, 2, 3 e 4 deverão ser seguidas. Se a complexidade da senha for definida como 2, as regras 1 e 2 deverão ser seguidas. O XClarity Administrator oferece suporte às seguintes regras de complexidade de senha. • (1) Deve conter pelo menos um caractere alfabético e não deve ter mais de dois caracteres sequenciais, incluindo sequências de caracteres alfabéticos, dígitos e teclas de teclado do QWERTY (por exemplo, "abc", "123" e "asd" não são permitidos). • (2) Deve conter pelo menos um número (0 a 9). • (3) Deve conter pelo menos *dois* dos caracteres a seguir. – Caracteres alfabéticos maiúsculos (A – Z) – Caracteres alfabéticos minúsculos (a – z) – Caracteres especiais ; @ _ ! ' $ & + • (4) Não deve repetir nem reverter o nome do usuário. • (5) Não deve conter mais de dois caracteres consecutivos (por exemplo, "aaa", "111" e "..." não são permitidos). Se for definido como **0**, as senhas não serão necessárias para cumprir as regras de complexidade.	**0 – 5**	**4**
Máximo de sessões ativas para um usuário específico	O número máximo de sessões ativas para um usuário específico que tem permissão a qualquer momento Se definido como **0**, o número de sessões ativas permitidas para um usuário específico é ilimitado.	**1 – 20**	**3**
Forçar o usuário a alterar senha no primeiro acesso	Indica se um usuário deve alterar a senha ao fazer login no XClarity Administrator pela primeira vez	**Sim** ou **Não**	**Sim**

Etapa 4. Clique em **Aplicar**.

Depois de concluir

Quando salvas com êxito, as novas configurações têm efeito imediatamente. Se você alterar a configuração de tempo-limite da sessão de inatividade da Web, as sessões ativas serão afetadas.

Se você alterar políticas de senha, essas políticas serão impostas na próxima vez que um usuário fizer login ou alterar a senha.

Definindo configurações de criptografia no servidor de gerenciamento

É possível configurar a versão SSL/TLS e a configuração de criptografia para o servidor de gerenciamento.

Antes de iniciar

Revise considerações de criptografia antes de modificar as configurações no servidor de gerenciamento (consulte Gerenciamento de criptografia na documentação online do XClarity Administrator).

Sobre esta tarefa

O *modo criptográfico* determina como as comunicações seguras são manipuladas entre XClarity Administrator e todos os sistemas gerenciados. Se as comunicações seguras forem implementadas, os comprimentos de chave de criptografia a serem usados serão definidos.

Nota: Independentemente do modo de criptografia selecionado, os geradores de bits digitais aleatórios aprovados pela NIST são usados sempre, e somente chaves com 128 bits ou mais são usadas para criptografia simétrica.

Para alterar a configuração de segurança para dispositivos gerenciados, consulte Definindo as configurações de segurança de um servidor gerenciado.

Procedimento

Para alterar as configurações de criptografia no servidor de gerenciamento, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança**.

Etapa 2. Escolha um dos seguintes modos criptográficos a ser usado para comunicações seguras:

- **Compatibilidade**. Este modo é o padrão. É compatível com versões de firmware, navegadores e outros clientes de rede mais antigos que não implementam padrões de segurança rígidos necessários para conformidade com o NIST SP 800-131A.
- **NIST SP 800-131A**. Este modo foi projetado para obedecer o padrão do NIST SP 800-131A. O XClarity Administrator foi projetado para sempre usar internamente uma criptografia forte e, sempre que disponível, usar conexões de rede com criptografia forte. Entretanto, sempre que estiver neste modo, as conexões de rede que estiverem usando criptografia não aprovada pelo NIST SP 800-131A não serão permitidas, incluindo a rejeição de certificados Transport Layer Security (TLS) que são assinados usando SHA-1 ou um hash mais vulnerável.

  Se selecionar esse modo:

  – Para todas as portas que não sejam a porta 8443, todas as cifras TLS CBC e todas as cifras incompatíveis com Perfect Forward Secrecy são desativadas.

  – As notificações de eventos podem não ser enviadas por push com sucesso a algumas assinaturas de dispositivo móvel (consulte Encaminhamento de eventos à dispositivos móveis). Os serviços externos, como Android e iOS, apresentam certificados assinados com SHA-1, que é um algoritmo que não está em conformidade com os requisitos mais rigorosos do modo NIST SP 800-131A. Como resultado, as conexões a estes serviços podem falhar com uma exceção de certificado ou falha de handshake.

  Para obter mais informações sobre a conformidade do NIST SP 800-131A, consulte Implementando a conformidade com NIST SP 800-131A.

Etapa 3. Escolha a versão mínima do protocolo TLS a ser usada para conexões de cliente com outros servidores (como servidor LDAP). É possível escolher a opção a seguir.

- **TLS1.2**. Impõe os protocolos de criptografia TLS v1.2.

- **TLS1.3**. Impõe os protocolos de criptografia TLS v1.3.

Etapa 4. Escolha a versão mínima do protocolo TLS a ser usada para conexões de servidor (como servidor da Web). É possível escolher a opção a seguir.

- **TLS1.2**. Impõe os protocolos de criptografia TLS v1.2.
- **TLS1.3**. Impõe os protocolos de criptografia TLS v1.3.

Etapa 5. Escolha a versão mínima do protocolo TLS a ser usada para a implantação do sistema operacional do XClarity Administrator e as atualizações de driver de dispositivo do SO. É possível escolher a opção a seguir.

- **TLS1.2**. Impõe os protocolos de criptografia TLS v1.2.
- **TLS1.3**. Impõe os protocolos de criptografia TLS v1.3.

Nota: Somente sistemas operacionais com um processo de instalação compatível com o algoritmo criptográfico selecionado ou forte podem ser implantados e atualizados por meio do XClarity Administrator.

Etapa 6. Selecione o comprimento da chave criptográfica e o algoritmo hash a ser usado para todas as partes do certificado, inclusive o certificado da CA raiz, o certificado do servidor e a CSR para certificados assinados externamente.

- **RSA 2048-bit / SHA-256** (padrão)

  Esse modo pode ser usado quando os dispositivos gerenciados estão no modo Compatibilidade, NIST SP 800-131A ou Segurança padrão. Esse modo *não pode* ser usado quando um ou mais dispositivos gerenciados estão no modo **Segurança corporativa estrita**.

- **RSA 3072-bit/SHA-384**

  Esse modo é necessário para quando dispositivos gerenciados estão no modo **Segurança corporativa estrita**.

  Importante: Somente servidores com XCC2 são compatíveis com assinaturas de certificado RSA-3072/SHA-384. Depois de configurar o XClarity Administrator com um certificado baseado em RSA-3072/SHA-384, os dispositivos não XCC2 não são gerenciados. Para gerenciar dispositivos não XCC2, é necessária uma instância separada do XClarity Administrator.

Etapa 7. Clique em **Aplicar**.

Etapa 8. Reinicie o XClarity Administrator (consulte Reiniciando o XClarity Administrator).

Etapa 9. Se você alterou o comprimento da chave criptográfica, gere novamente o certificado raiz da autoridade de certificação usando o comprimento da chave e o algoritmo hash corretos (consulte Gerar novamente ou restaurar o certificado de servidor autoassinado do Lenovo XClarity Administrator ou Implantando certificados de servidor personalizado em Lenovo XClarity Administrator).

Depois de concluir

Se você receber um alerta informando que o certificado do servidor não é confiável para um dispositivo gerenciado, consulte Resolvendo um certificado de servidor não confiável.

Definindo as configurações de segurança de um servidor gerenciado

É possível configurar a versão SSL/TLS e a configuração de criptografia para servidores gerenciados.

Sobre esta tarefa

Considere as seguintes implicações de alterar o modo criptográfico.

- A alteração do modo **Segurança de compatibilidade** ou **Segurança padrão** para **Segurança corporativa estrita** não é compatível.
- Se você atualizar do **Segurança de compatibilidade** para o modo **Segurança padrão**, será advertido se certificados importados ou chaves públicas SSH não forem compatíveis, mas você ainda poderá fazer a atualização para o modo **Segurança padrão**.
- Se você fizer downgrade do modo **Segurança corporativa estrita** para **Segurança de compatibilidade** ou **Segurança padrão**:
  - O servidor é reiniciado automaticamente para que o modo de segurança entre em vigor.
  - Se a chave FoD do modo estrito estiver ausente ou expirada no XCC2, e se o XCC2 usar um certificado TLS autoassinado, o XCC2 gerará novamente o certificado TLS autoassinado com base no algoritmo compatível com Estrito padrão. O XClarity Administrator mostra uma falha de conexão devido a um erro de certificado. Para resolver o erro de certificado não confiável, consulte Resolvendo um certificado de servidor não confiável na documentação online do XClarity Administrator. Se o XCC2 usar um certificado TLS personalizado, o XCC2 permitirá o downgrade e avisará que você precisa importar um certificado do servidor baseado na criptografia do modo **Segurança padrão**.
- O modo **NIST SP 800-131A** compatível com servidores com XCC2.
- O XClarity Administrator é definido como TLS v1.2 e se um servidor gerenciado que usa autenticação gerenciada tiver um modo de segurança definido como TLS v1.2, alterar o modo de segurança do servidor para TLS v1.3 usando XClarity Administrator ou XCC fará com que o servidor seja permanentemente offline.
- Se o modo criptográfico para XClarity Administrator for definido como TLS v1.2 e você tentar gerenciar um servidor com XCC que tenha seu modo de segurança definido como TLS v1.3, o servidor não poderá ser gerenciado usando autenticação gerenciada.

É possível alterar as configurações de segurança dos dispositivos a seguir.
- Servidores Lenovo ThinkSystem com processadores Intel ou AMD (exceto SR635/SR655)
- Servidores Lenovo ThinkSystem V2
- Servidores Lenovo ThinkSystem V3 com processadores Intel ou AMD
- Servidores Lenovo ThinkEdge SE350/SE450
- Servidores Lenovo System x

Procedimento

Para alterar as configurações de segurança de servidores gerenciados específicos, conclua as etapas a seguir.

Etapa 1. No menu XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados.

Etapa 2. Selecione um ou mais servidores.

Etapa 3. Configure o modo de segurança.

1. Clique em **Todas as Ações → Segurança → Definir modo de segurança** para exibir a caixa de diálogo Definir modo de segurança do sistema.

   A caixa de diálogo lista o número de servidores que podem ser definidos em cada modo. Passe o cursor sobre cada número para exibir uma caixa popup com uma lista de nomes de servidor aplicáveis.

2. Selecione o modo de segurança. Este pode ser um dos valores a seguir.

   - **Segurança de compatibilidade**. Selecione esse modo quando serviços e clientes requerem criptografia que não seja compatível com CNSA/FIPS. Este modo é compatível

com uma ampla gama de algoritmos criptográficos e permite que todos os serviços sejam habilitados.

- **NIST SP 800-131A**. Selecione esse modo para garantir a conformidade com o padrão NIST SP 800-131A. Isso inclui a restrição de chaves RSA a 2048 bits ou mais, a restrição de hashes usados para assinaturas digitais para SHA-256 ou mais e a garantia de que somente os algoritmos de criptografia simétricos aprovados pelo NIST sejam usados. Este modo requer a configuração do modo SSL/TLS como **TLS 1.2 Server Client**.

  Esse modo *não é* compatível com servidores com XCC2.

- **Segurança padrão**. (Apenas servidores com XCC2) Este é o modo de segurança padrão para servidores com XCC2. Selecione esse modo para garantir a conformidade com o padrão FIPS 140-3. Para que o XCC opere no modo validado FIPS 140-3, apenas serviços compatíveis com a criptografia de nível FIPS 140-3 podem ser habilitados. Os serviços não compatíveis com a criptografia de nível FIPS 140-2/140-3 são desativados por padrão, mas podem ser habilitados se necessário. Se qualquer serviço que usa criptografia de nível 140-3 não FIPS estiver habilitado, o XCC não poderá operar no modo validado fips 140-3. Esse modo requer certificados em nível de FIPs.
- **Segurança corporativa estrita**. (Apenas servidores com XCC2) Este é o modo mais seguro. Selecione esse modo para garantir a conformidade com o padrão CNSA. Somente serviços compatíveis com a criptografia de nível CNSA são permitidos. Os serviços não seguros são desabilitados por padrão e não podem ser habilitados. Esse modo requer certificados em nível de CNSA.

  O XClarity Administrator usa assinaturas de certificado RSA-3072/SHA-384 para servidores no modo **Segurança corporativa estrita**.

  Importante:

  – A chave XCC2 Feature On Demand deve ser instalada em cada um dos servidores com XCC2 selecionados para usar esse modo.

  – Nesse modo, se o XClarity Administrator usar certificado autoassinado, o XClarity Administrator deverá usar o certificado raiz e o certificado do servidor baseado em RSA3072/SHA384. Se o XClarity Administrator usar um certificado assinado externo, o XClarity Administrator deverá gerar uma CSR baseada em RSA3072/SHA384 e entrar em contato com a CA externa para assinar um novo certificado de servidor baseado em RSA3072/SHA384.

  – Quando o XClarity Administrator usar um certificado baseado em RSA3072/SHA384, o XClarity Administrator poderá desconectar dispositivos que não sejam o chassi do Flex System (CMMS) e servidores, servidores ThinkSystem, servidores ThinkServer, servidores System x M4 e M5, comutadores Lenovo ThinkSystem Série DB, Lenovo RackSwitch, comutadores Flex System, comutadores Mellanox, dispositivos de armazenamento ThinkSystem DE/DM, armazenamento da biblioteca de fita IBM e servidores ThinkSystem SR635/SR655 em flash com firmware anterior a 22C. Para continuar a gerenciar os dispositivos desconectados, configure outra instância do XClarity Administrator com um certificado baseado em RSA2048/SHA384.

3. Clique em **Aplicar**.

Etapa 4. Configure a versão mínima do TLS.

1. Clique em **Todas as Ações → Segurança → Definir versão de TLS do sistema** para exibir a caixa de diálogo Definir versão de TLS do sistema.
2. Selecione a versão mínima do protocolo TLS a ser usada para conexões de cliente a outros servidores (como as conexões de cliente LDAP a um servidor LDAP). O valor é configurado em dispositivos selecionados compatíveis com essa configuração. É possível escolher a opção a seguir.

- **TLS1.2**. Impõe os protocolos de criptografia TLS v1.2.
- **TLS1.3**. Impõe os protocolos de criptografia TLS v1.3.

Nota: Os dispositivos System x e CMM são compatíveis apenas com TLS v1.2.

3. Clique em **Aplicar**.

Trabalhando com certificados de segurança

Lenovo XClarity Administrator usa certificados SSL para estabelecer uma comunicação segura e confiável entre o XClarity Administrator e seus dispositivos gerenciados (como o chassi e processadores de serviços nos servidores System x), bem como a comunicação com o XClarity Administrator por usuários ou com diferentes serviços. Por padrão, o XClarity Administrator, CMMs e Baseboard Management Controllers usam certificados gerados pelo XClarity Administrator que são autoassinados e emitidos por uma autoridade de certificação interna.

Antes de iniciar

Esta seção é destinada a administradores que têm um entendimento básico do padrão SSL e dos certificados SSL, incluindo o que são e como gerenciá-los. Para obter informações gerais sobre certificados de chave pública, consulte Página da Web X.509 na Wikipédia e Página da Web Certificador de infraestrutura da chave pública X.509 da internet e Perfil da lista de revogação de certificados (CRL) (RFC5280).

Sobre esta tarefa

O certificado de servidor autoassinado padrão, produzido exclusivamente em cada instância do XClarity Administrator, fornece segurança adequada para muitos ambientes. É possível escolher se você quer deixar o XClarity Administrator gerenciar certificados, ou se você pode ter uma função mais ativa e personalizar ou substituir os certificados do servidor. O XClarity Administrator fornece opções para personalizar certificados para seu ambiente. Por exemplo, é possível optar por:

- Gere um novo par de chaves gerando novamente a autoridade de certificação interna e/ou o certificado do servidor final que usa valores específicos da sua organização.
- Gere uma Solicitação de Assinatura de Certificado (CSR) que pode ser enviada à autoridade de certificação de sua escolha para assinar um certificado padrão que pode, então, ser transferido por upload para o XClarity Administrator a ser usado como o certificado de servidor final para todos os seus serviços hospedados.
- Baixe o certificado de servidor para seu sistema local para poder importá-lo na lista do navegador da Web de certificados confiáveis.

O XClarity Administrator fornece diversos serviços que aceitam conexões SSL/TLS de entrada. Quando um cliente, como um dispositivo gerenciado ou um navegador da Web, se conecta a um desses serviços, o XClarity Administrator fornece o *certificado do servidor* a ser identificado pelo cliente que está tentando a conexão. O cliente deve manter uma lista de certificados confiáveis. Se o certificado do servidor do XClarity Administrator não estiver incluído na lista do cliente, o cliente se desconectará do XClarity Administrator para evitar a troca de qualquer informação confidencial de segurança com uma origem não confiável.

O XClarity Administrator age como um cliente ao se comunicar com dispositivos gerenciados e serviços externos. Quando o XClarity Administrator se conecta a um dispositivo ou serviço externo, o dispositivo ou o serviço externo fornece seu certificado do servidor a ser identificado pelo XClarity Administrator. O XClarity Administrator mantém uma lista de certificados confiáveis. Se o *certificado confiável* fornecido pelo dispositivo gerenciado ou serviço externo não estiver listado, o XClarity Administrator se desconectará do dispositivo gerenciado ou do serviço externo para evitar a troca de qualquer informação confidencial de segurança com uma origem não confiável.

A categoria de certificados a seguir é usada pelos serviços XClarity Administrator e deve ser confiável por qualquer cliente que se conecte a ele.

- **Certificado do Servidor**. Durante a primeira inicialização, uma chave exclusiva e o certificado autoassinado são gerados. Eles são usados como autoridade de certificação raiz padrão, que pode ser gerenciada na página Autoridade de Certificação nas configurações de segurança do XClarity Administrator. Não é necessário gerar novamente esse certificado raiz, a menos que a chave tenha sido comprometida ou se sua organização tiver uma política que obrigue a substituição periódica de todos os certificados (consulte Gerar novamente ou restaurar o certificado de servidor autoassinado do Lenovo XClarity Administrator).

  Também durante a configuração inicial, uma chave separada é gerada e um certificado de servidor é criado e assinado pela autoridade de certificação interna. Esse certificado é usado como o certificado do servidor padrão do XClarity Administrator. Ele é gerado de novo automaticamente sempre que o XClarity Administrator detecta que seus endereços de rede (endereços IP ou DNS) foram alterados para garantir que o certificado contenha os endereços corretos para o servidor. Ele pode ser personalizado e gerado sob demanda (consulte Gerar novamente ou restaurar o certificado de servidor autoassinado do Lenovo XClarity Administrator).

  É possível optar por usar um certificado de servidor assinado externamente em vez do certificado de servidor autoassinado padrão gerando uma solicitação de assinatura de certificado (CSR), solicitando que a CSR seja assinada por uma Autoridade de Certificação Raiz privada ou comercial e, em seguida, importando a cadeia de certificados completa para o XClarity Administrator (consulte Implantando certificados de servidor personalizado em Lenovo XClarity Administrator).

  Se você optar por usar o certificado de servidor autoassinado padrão, é recomendável importar o certificado de servidor no seu navegador da Web como uma autoridade raiz confiável para evitar mensagens de erro de certificado no seu navegador (consulte Importando o certificado da autoridade de certificação em um navegador da Web).
- **Certificado de implantação do SO**. Um certificado separado é usado pelo serviço de implantação do sistema operacional para assegurar que o instalador do sistema operacional possa se conectar com segurança ao serviço de implantação durante o processo de instalação do sistema operacional. Se a chave tiver sido comprometida, é possível gerá-la novamente reiniciando o servidor de gerenciamento.

A categoria a seguir (armazenamentos confiáveis) de certificados é usada pelos clientes do XClarity Administrator.

- **Certificados confiáveis**.

  Esse armazenamento confiável gerencia certificados usados para estabelecer uma conexão segura com os recursos locais quando o XClarity Administrator age como cliente. Exemplos de recursos locais são dispositivos gerenciados, software local ao encaminhar um evento e um servidor LDAP externo.
- **Certificados de serviço externos**. Esse armazenamento confiável gerencia certificados usados para estabelecer uma conexão segura com serviços externos quando o XClarity Administrator age como cliente. Exemplos de serviços externos são serviços online do Lenovo Support que são usados para recuperar informações de garantia ou criar tíquetes de serviço, software externo (como o Splunk) para o qual eventos podem ser encaminhados e servidores de notificação por push da Apple e da Google se as notificações por push do Lenovo XClarity Mobile estiverem habilitadas para um dispositivo iOS ou Android. Ele contém certificados confiáveis pré-configurados das Autoridades de Certificação Raiz de determinados provedores de autoridade de certificação geralmente confiáveis e conhecidos mundialmente, como o Digicert e o Globalsign).

  Ao configurar o XClarity Administrator para usar um recurso que exija uma conexão com outro serviço externo, consulte a documentação para determinar se você precisa adicionar manualmente um certificado a esse armazenamento confiável.

  Os certificados nesse armazenamento confiável não são confiáveis ao estabelecer conexões para outros serviços (como LDAP), a menos que você também os adicione ao armazenamento confiável principal de

certificados confiáveis. Remover certificados desse armazenamento confiável impede o funcionamento desses serviços.

O XClarity Administrator dá suporte a assinaturas de certificado RSA-3072/SHA-384, RSA-2048/SHA-256 e ECDSA p256/SHA-256. Outros algoritmos, como SHA-1 ou mais forte ou hashes SHA, podem ser compatíveis dependendo da sua configuração. Considere o modo criptográfico selecionado no XClarity Administrator (consulte Definindo configurações de criptografia no servidor de gerenciamento), as configurações de segurança selecionadas para servidores gerenciados (Definindo as configurações de segurança de um servidor gerenciado) e os recursos de outros softwares e dispositivos em seu ambiente. Os certificados ECDSA que são baseados em algumas curvas elípticas (incluindo p256), mas nem todas as curvas elípticas, são suportados na página Certificados confiáveis e na cadeia de assinatura do certificado XClarity Administrator, mas *não são* suportados atualmente para uso pelo certificado do servidor XClarity Administrator.

Nota: O XClarity Administrator usa assinaturas de certificado RSA-3072/SHA-384 para o servidores com XCC2 no modo estrito.

Instalando um certificado de servidor assinado externamente personalizado

É possível usar um certificado do servidor assinado por uma autoridade de certificação (CA) privada ou comercial.

Antes de iniciar

Verifique se a Autoridade de Certificação Raiz é gerada por sua organização e usada para assinar certificados dentro dessa organização ou uma geralmente confiável e conhecida mundialmente (consulte Página da Web Lista de certificados confiáveis).

Os algoritmos das chaves e assinaturas do certificado da CA raiz devem ser compatíveis. Apenas assinaturas RSA-3072/SHA-384 e RSA-2048/SHA-256 são compatíveis. Não há suporte para assinaturas RSA-PSS.

Assegure-se de que todos os dispositivos gerenciados tenham o firmware mais recente instalado antes de iniciar qualquer tarefa que possa afetar conexões entre dispositivos gerenciados. Para atualizar o firmware em dispositivos gerenciados, consulte Atualizando firmware em dispositivos gerenciados.

Verifique se o XClarity Administrator está se comunicando com êxito com todos os dispositivos gerenciados clicando em **Hardware** e, depois, no tipo de dispositivo (chassi ou servidor). É exibida uma página com uma exibição tabular de todos os dispositivos gerenciados desse tipo. Se algum dispositivo tiver o status "Offline", verifique se a conectividade de rede está funcionando entre o servidor de gerenciamento e o dispositivo, e resolva certificados de servidor não confiáveis se necessário (consulte Resolvendo um certificado de servidor não confiável).

Sobre esta tarefa

Ao instalar um certificado de servidor assinado externamente e personalizado no XClarity Administrator ou em um controlador de gerenciamento baseboard ou CMM, você deve fornecer o pacote de certificados que contém a cadeia de assinatura de CA inteira.

Ao instalar um certificado de servidor personalizado em um chassi ou servidor que não seja gerenciado pelo XClarity Administrator, instale o pacote de certificados no CMM antes de instalá-lo em todos os controladores de gerenciamento no CMM.

Ao instalar um certificado de servidor personalizado em um chassi gerenciado, primeiro adicione a cadeia de assinatura de CA ao armazenamento confiável do XClarity Administrator, instale o certificado do servidor em

cada controlador de gerenciamento e no CMM, em seguida, faça upload do certificado do servidor no XClarity Administrator. Isso pode ser facilmente ignorado confiando/adicionando todos os Certificados raiz da CA, mas não todas as cadeias de certificados de cada dispositivo gerenciado. O número de certificados importados deve ser igual ao número de certificados da CA raiz (certificados da CA raiz + todos os certificados da CA intermediários). Para obter mais informações, consulte Implantando certificados de servidor personalizado em dispositivos gerenciados.

Você deve adicionar o certificado raiz da CA e todos os certificados intermediários, um por vez, ao armazenamento confiável do XClarity Administrator. A ordem não importa. Cada certificado deve ser instalado uma vez. Assim, se todos os dispositivos usarem os mesmos certificados de CA e intermediários, o certificado da CA e cada certificado intermediário deverão ser instalados no armazenamento confiável do XClarity Administrator uma vez. Se mais de uma CA ou uma CA intermediária for usada, verifique se cada certificado raiz da CA ou certificado intermediário exclusivo usado na cadeia de assinatura de um dispositivo gerenciado seja importado segundo estas etapas.

Dica: se o novo certificado de servidor não tiver sido assinado por terceiros confiáveis, na próxima vez que você se conectar ao XClarity Administrator, o navegador exibirá uma mensagem de segurança e uma caixa de diálogo solicitando a aceitação do novo certificado no navegador. Para evitar mensagens de segurança, é possível importar um certificado do servidor baixado para a lista de certificados confiáveis do seu navegador da Web. Para obter mais informações sobre como importar certificados de servidor, consulte Importando o certificado da autoridade de certificação em um navegador da Web.

Implantando certificados de servidor personalizado em Lenovo XClarity Administrator

É possível optar por gerar uma solicitação de assinatura de certificado (CSR) a ser assinada pela autoridade de certificação da sua organização ou uma autoridade de certificação de terceiros. A CSR cria uma cadeia de certificados completa que você pode importar e usar no lugar de certificados exclusivos padrão assinados internamente.

Antes de iniciar

Verifique se os detalhes do certificado incluem os requisitos a seguir.

- O uso da chave deve conter
  - Contrato de chave
  - Assinatura digital
  - Criptografia de chave
- O uso da chave aprimorada deve conter
  - Servidor de autenticação (1.3.6.1.5.5.7.3.1)
  - Autenticação do cliente (1.3.6.1.5.5.7.3.2)

Sobre esta tarefa

Atenção: Se o NIST SP 800-131A estiver habilitado (consulte Implementando a conformidade com NIST SP 800-131A) e você estiver usando ou planeja usar certificados personalizados ou assinados externamente em um NIST, todos os certificados da cadeia deverão ser baseados em funções de hash SHA-256.

Quando o certificado do servidor é carregado, o XClarity Administrator tenta fornecer o novo certificado da CA a todos os dispositivos gerenciados. Se o processo de fornecimento for bem-sucedido, o XClarity Administrator começará a usar o novo certificado do servidor imediatamente. Se o processo falhar, mensagens de erro serão fornecidas instruindo você para corrigir os problemas manualmente antes de aplicar o certificado do servidor recém-importado. Após corrigir os erros, conclua a instalação do certificado anteriormente carregado.

Nota: Se o XClarity Administrator já usava um certificado assinado pela mesma autoridade raiz, a CA não precisará ser enviada para dispositivos, e XClarity Administrator começará a usar o certificado imediatamente.

Depois de carregar um certificado no XClarity Administrator v1.1.0 e anterior, o servidor da Web foi reiniciado e encerrou automaticamente todas as sessões do navegador. O XClarity Administrator v1.1.1 e posterior começa a usar o novo certificado sem encerrar as sessões existentes. As novas sessões são estabelecidas usando o novo certificado. Para ver o novo certificado em uso, reinicie seu navegador da Web.

Procedimento

Para gerar e implantar um certificado de servidor assinado externamente personalizado em Lenovo XClarity Administrator, conclua as seguintes etapas.

Etapa 1. Criar e baixar uma solicitação de assinatura de certificado (CSR) para XClarity Administrator.

a. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança** para exibir a página Segurança

b. Clique em **Certificado do Servidor** na seção Gerenciamento de Certificados para exibir a página Certificado do Servidor.

c. Clique na guia **Gerar Solicitação de Assinatura de Certificado (CSR)**.

d. Preencha os campos para a solicitação.
   - País ou Região
   - Estado
   - Cidade ou Localidade
   - Organização
   - Unidade Organizacional (opcional)
   - Nome Comum

   Atenção: Selecione um nome comum que corresponda ao endereço IP ou nome do host que o XClarity Administrator usa para conectar-se ao dispositivo gerenciado. Não selecionar o valor correto pode levar a conexões que não são confiáveis.

e. Personalize os nomes alternativos de assunto (SANs) que serão adicionados à extensão x.509 "subjectAltName" quando a CSR for gerada.

   Por padrão, XClarity Administrator define automaticamente os nomes alternativos de assunto (SANs) para a CSR com base no endereço IP e no nome do host que são descobertos pelas interfaces de rede do sistema operacional do convidado XClarity Administrator. Você pode personalizar, excluir ou adicionar esses valores de SAN.

   O nome que você especificar deve ser válido para o tipo selecionado:
   - **directoryName** (por exemplo, `cn=lxca-example,ou=dcg,dc=company,dc=com`)
   - **dNSName** (por exemplo, `lxca-example.dcg.company.com`)
   - **ipAddress** (por exemplo, `192.0.2.0`)
   - **registeredID** (por exemplo, `1.2.3.4.55.6.5.99`)
   - **rfc822Name** (por exemplo, `example@company.com`)
   - **uniformResourceIdentifier** (por exemplo, `https://lxca-dev.dcg.company.com/example`)

   Nota: Todos os SANs listados na tabela são validados, salvos e adicionados à CSR apenas depois que você gerar a CSR na próxima etapa.

f. Clique em **Gerar Arquivo CSR**. O certificado do servidor é exibido na caixa de diálogo Solicitação de Assinatura de Certificado.

g. Clique em **Salvar em Arquivo** para salvar o certificado do servidor do host.

Etapa 2. Forneça a CSR para uma autoridade de certificação (CA) confiável. A CA assina a CSR e responde com um certificado de servidor.

Etapa 3. Faça upload do certificado de servidor assinado externamente em XClarity Administrator. O conteúdo do certificado deve ser um pacote que contém o certificado raiz da CA, os certificados intermediários e o certificado do servidor.

a. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança** para exibir a página Segurança.

b. Clique em **Certificado do Servidor** na seção Gerenciamento de Certificados.

c. Clique na guia **Fazer upload de Certificado**.

d. Clique em **Fazer upload de Certificado** para exibir a caixa de diálogo Fazer upload de Certificado.

e. Especifique um pacote de certificados em formato PEM, DER ou PKCS7 ou cole o pacote de certificados em formato PEM.

f. Clique em **Fazer upload** para carregar o certificado do servidor e armazenar o certificado no armazenamento confiável do XClarity Administrator.

Implantando certificados de servidor personalizado em dispositivos gerenciados

É possível implantar certificados de servidor personalizado em dispositivos gerenciados fazendo upload e instalando o pacote de certificados assinados externamente usando o CMM e o controlador de gerenciamento para os dispositivos.

Antes de iniciar

Verifique se o firmware mais recente está instalado em todos os dispositivos gerenciados (consulte Atualizando firmware em dispositivos gerenciados).

Para gerar uma solicitação de assinatura de certificado (CSR) para certificados personalizados, selecione um nome comum que corresponda ao endereço IP ou nome do host utilizado para identificar o dispositivo. Não selecionar o valor correto pode levar a conexões que não são confiáveis.

Obtenha um pacote de certificados que contenha a cadeia de assinatura inteira, do certificado de servidor final ao certificado raiz (base) da CA confiável que pode ser usado para verificar a cadeia completa de certificados confiáveis.

Não altere o certificado do servidor do Lenovo XClarity Administrator quando um dispositivo gerenciado estiver "Offline." Você deve reparar a conexão antes de alterar Lenovo XClarity Administrator. Caso contrário, etapas adicionais podem ser necessárias para reparar os problemas de conectividade (consulte Resolvendo um certificado de servidor não confiável).

Sobre esta tarefa

Esta seção contém recomendações para assegurar a comunicação contínua entre o Lenovo XClarity Administrator e os dispositivos gerenciados. Para obter instruções detalhadas sobre como gerar uma CSR e importar um certificado assinado, consulte a documentação do dispositivo.

Se o Lenovo XClarity Administrator estiver gerenciando um ou mais chassis, servidores de rack e servidores em torre, e os certificados padrão assinados internamente do Lenovo XClarity Administrator estiverem instalados atualmente em Lenovo XClarity Administrator e nos dispositivos gerenciados, será possível implantar o certificado do servidor personalizado.

Se o certificado de servidor assinado externamente for instalado no dispositivo *antes* de você tentar gerenciar o dispositivo com Lenovo XClarity Administrator, nenhuma etapa adicional será necessária. Para

implantar um certificado de servidor personalizado em dispositivos que são gerenciados no gerenciamento de Lenovo XClarity Administrator, você deve executar uma destas etapas para assegurar conectividade contínua entre o servidor de gerenciamento e os dispositivos gerenciados.

Procedimento

Conclua uma das seguintes opções para implantar o certificado de servidor assinado externamente personalizado no chassi ou em servidores gerenciados.

- Se o Lenovo XClarity Administrator usar um certificado que seja assinado pela autoridade de certificação dos dispositivos gerenciados, execute as etapas Implantando certificados de servidor personalizado em Lenovo XClarity Administrator *antes* de instalar os certificados em dispositivos gerenciados. Instalar a cadeia de certificados de Lenovo XClarity Administrator da mesma CA primeiro garante que a cadeia de certificados esteja no armazenamento confiável do Lenovo XClarity Administrator e que Lenovo XClarity Administrator possa confiar nos dispositivos depois que os certificados assinados externamente forem instalados.
- Adicione os certificados assinados externamente nas cadeias de assinatura de CA no armazenamento confiável do Lenovo XClarity Administrator.

  Você deve adicionar o certificado raiz da CA e todos os certificados intermediários, um por vez, ao armazenamento confiável do Lenovo XClarity Administrator. A ordem não importa. Cada certificado deve ser instalado uma vez. Assim, se todos os dispositivos usarem os mesmos certificados de CA e intermediários, o certificado da CA e cada certificado intermediário deverão ser instalados no armazenamento confiável do Lenovo XClarity Administrator uma vez. Se mais de uma CA ou uma CA intermediária for usada, verifique se cada certificado raiz da CA ou certificado intermediário exclusivo usado na cadeia de assinatura de um dispositivo gerenciado seja importado segundo estas etapas.

  Nota: Não adicione certificados de servidor finais não de CA durante essas etapas.

  Execute as seguintes etapas para cada certificado no pacote.

  1. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Segurança** para exibir a página Segurança.
  2. Clique em **Certificados confiáveis** em Gerenciamento de Certificados na navegação esquerda.
  3. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Adicionar certificado.
  4. Especifique um arquivo de certificado em formato PEM ou DER, ou cole o certificado em formato PEM.
  5. Clique em **Criar** para criar o certificado.

  Após a instalação da cadeia de assinatura de CA, o Lenovo XClarity Administrator confia nas conexões com servidores CIM no CMM e no controlador de gerenciamento em que o certificado de servidor assinado externamente está instalado.
- Importe os certificados assinados externamente para os dispositivos gerenciados.

  Nota: Se os certificados necessários não estiverem presentes no armazenamento confiável do Lenovo XClarity Administrator, a conectividade entre Lenovo XClarity Administrator e o dispositivo gerenciado será perdida. Execute as etapas em Resolvendo um certificado de servidor não confiável para reparar a conexão.

  Importante: Essa opção envolve a perda temporária de conectividade; portanto, uma das opções anteriores é recomendada.

Gerar novamente ou restaurar o certificado de servidor autoassinado do Lenovo XClarity Administrator

Será possível gerar uma nova autoridade de certificação ou certificado do servidor para substituir os certificados autoassinados atuais ou para restabelecer um certificado gerado pelo Lenovo XClarity Administrator se o XClarity Administrator usar um certificado de servidor assinado externamente personalizado. O novo certificado de servidor autoassinado é então usado pelos servidores de autenticação, HTTPS e CIM no XClarity Administrator. Também é fornecido automaticamente para todos os dispositivos gerenciados.

Antes de iniciar

Ao gerar novamente ou fazer upload do certificado XClarity Administrator, XClarity Administrator será reiniciado.

Se um novo certificado da CA for gerado, o novo certificado da CA será implantado automaticamente no armazenamento confiável em cada CMM e no Baseboard Management Controller em todos os chassis, servidores em rack e servidores em torre gerenciados para manter conexões confiáveis do servidor de autenticação. Se ocorrer um erro ao implantar o certificado raiz da CA, baixe-o da página Autoridade de Certificação e importe-o manualmente para o armazenamento confiável de todos os dispositivos gerenciados que não o receberam antes de gerar um novo certificado do servidor.

Se você pretende gerar o certificado da CA novamente, reserve algum tempo para gerar a CA novamente, resolva os erros de fornecimento e gere novamente o certificado do servidor em um curto período.

Depois de gerar um novo certificado raiz da CA, erros de comunicação podem ocorrer ou talvez não seja possível fazer login em um dispositivo até que o certificado do servidor seja gerado novamente e assinado.

Importante: Para XClarity Administrator v1.1.1 e anterior, você deve importar o certificado raiz da CA para o armazenamento confiável de cada CMM e controlador de gerenciamento. Consulte a documentação do CMM e do controlador de gerenciamento para obter mais informações sobre como importar o certificado raiz da CA

Procedimento

Conclua as etapas a seguir para restaurar um certificado de servidor autoassinado no XClarity Administrator.

Nota: O certificado do servidor que está atualmente em uso no XClarity Administrator, autoassinado ou assinado externamente, permanecerá em uso até que o novo certificado do servidor seja gerado novamente e assinado.

Etapa 1. **Opcional:** gere um novo certificado raiz da CA.

a. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança** para exibir a página Segurança.

b. Clique em **Autoridade de Certificação** na seção Gerenciamento de Certificados.

c. Clique em **Gerar Certificado Raiz da Autoridade de Certificação Novamente**.

Se a chave e o certificado da CA forem gerados novamente, uma caixa de diálogo será exibida mostrando o status de trabalhos para fornecer esse certificado como um certificado confiável LDAP a todos os CMMs e controladores de gerenciamento (para servidores Converged, NeXtScale e System x). Essa caixa de diálogo e a página de monitoramento de trabalhos mostram o sucesso ou a falha de cada trabalho de fornecimento.

Se algum trabalho de fornecimento falhar, conclua as etapas a seguir para baixar o certificado raiz da CA e importe manualmente o certificado raiz como um certificado confiável LDAP em qualquer dispositivo para o qual o trabalho falhou.

Etapa 2. **Opcional:** baixe o certificado raiz da CA no sistema do host e importe-o para seu navegador da Web.

a. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança** para exibir a página Segurança.

b. Clique em **Autoridade de Certificação** na seção Gerenciamento de Certificados.

c. Clique em **Baixar Certificado Raiz da Autoridade de Certificação**. O atual certificado raiz da CA é exibido na caixa de diálogo Certificado Raiz da Autoridade de Certificação.

d. Clique em **Salvar em Arquivo** para salvar o certificado raiz da CA no sistema do host.

e. Siga as instruções do seu navegador da Web e do navegador de outros usuários que acessarão o XClarity Administrator para importar o certificado como uma autoridade raiz confiável.

Etapa 3. Gere novamente um novo certificado do servidor e assine o certificado com o novo certificado raiz da CA.

a. Na página Segurança, clique em **Certificado do Servidor** na seção Gerenciamento de Certificados.

b. Clique na guia **Gerar Certificado de Servidor Novamente**.

c. Preencha os campos na página Gerar Certificado de Servidor Novamente:
- País ou Região
- Estado
- Cidade ou Localidade
- Organização
- Unidade Organizacional
- Nome Comum
- Não válido antes da data
- Não válido antes da hora
- Não válido depois da data
- Não válido depois da hora

d. Clique em **Gerar Certificado Novamente**.

e. Se você estiver gerando novamente certificados autoassinados nos CMMs gerenciados e controladores de gerenciamento (para servidores Converged, NeXtScale, ThinkSystem e System x), depois de gerar novamente o certificado em cada dispositivo, importe o novo certificado do dispositivo para o armazenamento confiável do XClarity Administrator (consulte Resolvendo um certificado de servidor não confiável). Como alternativa, é possível baixar manualmente o certificado no dispositivo e importá-lo para o XClarity Administrator na página Certificados confiáveis.

Para XClarity Administrator v1.1.0 e anterior, o servidor da Web é reiniciado e encerra automaticamente todas as sessões do navegador após gerar novamente um certificado. Para XClarity Administrator v1.1.1 e posterior, o XClarity Administrator começa a usar o novo certificado sem encerrar as sessões existentes. As novas sessões são estabelecidas usando o novo certificado. Para ver o novo certificado em uso, reinicie seu navegador da Web.

Etapa 4. Se você estiver gerando novamente certificados autoassinados nos CMMs gerenciados e controladores de gerenciamento (para servidores Converged, NeXtScale, ThinkSystem e System x), depois de gerar novamente o certificado em cada dispositivo, importe o novo certificado do dispositivo para o armazenamento confiável do XClarity Administrator (consulte Resolvendo um certificado de servidor não confiável). Como alternativa, é possível baixar manualmente o certificado no dispositivo e importá-lo para o XClarity Administrator na página Certificados confiáveis.

Resolvendo um certificado de servidor não confiável

O certificado do servidor usado para estabelecer uma conexão segura com um dispositivo gerenciado pode se tornar não confiável. Se o problema ocorreu devido a uma versão anterior do certificado raiz da CA do dispositivo ou ao certificado autoassinado do dispositivo no armazenamento confiável do Lenovo XClarity Administrator, o XClarity Administrator pode solucionar o certificado de servidor não confiável.

Sobre esta tarefa

Se um dispositivo gerenciado passar a ser não confiável, o XClarity Administrator impedirá a comunicação com esse dispositivo, impedindo a execução de operações de gerenciamento ou inventário nesse dispositivo.

Procedimento

Para solucionar um certificado de servidor não confiável para um dispositivo gerenciado, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware** e, em seguida, clique no tipo de dispositivo (**Chassi**, **Servidor**, **Armazenamento** ou **Comutador**). É exibida uma página com uma exibição tabular de todos os dispositivos gerenciados desse tipo.

Etapa 2. Selecione um dispositivo específico no estado "Offline".

Etapa 3. Clique em **Todas as Ações → Segurança → Resolver Certificados Não Confiáveis**.

Etapa 4. Clique em **Instalar Certificado**.

O XClarity Administrator recupera o certificado atual do dispositivo de destino. Se esse certificado for diferente do certificado confiável do dispositivo no armazenamento confiável do XClarity Administrator, o novo certificado será colocado no armazenamento confiável do XClarity Administrator, substituindo o certificado anterior para esse dispositivo.

Se isso não resolver o problema, verifique se a conectividade de rede está funcionando entre XClarity Administrator e o dispositivo.

Baixando o certificado do servidor

É possível baixar uma cópia do certificado do servidor atual, em formato PEM ou DER, para seu sistema local. Você pode então importar o certificado para seu navegador da Web ou outros aplicativos (como Lenovo XClarity Mobile ou Lenovo XClarity Integrator).

Procedimento

Conclua as seguintes etapas para baixar o certificado do servidor.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Segurança** para exibir a página Segurança.

Etapa 2. Clique em **Certificado do Servidor** na seção Gerenciamento de Certificados. A página Certificado do Servidor é exibida.

Etapa 3. Clique na guia **Baixar Certificado**.

Etapa 4. Clique em **Baixar Certificado**.

Etapa 5. Clique em **Salvar como der** ou **Salvar como pem** para salvar o certificado do servidor como um arquivo DER ou PEM no sistema local.

Importando o certificado da autoridade de certificação em um navegador da Web

Para evitar mensagens de aviso de segurança do navegador da Web enquanto você acessa o Lenovo XClarity Administrator, é possível baixar uma cópia do certificado atual da autoridade de certificação (CA),

em formato PEM ou DER, no sistema local e depois importar esse certificado para a lista de certificados confiáveis do seu navegador da Web.

Sobre esta tarefa

O XClarity Administrator dá suporte a assinaturas de certificado RSA-3072/SHA-384, RSA-2048/SHA-256 e ECDSA p256/SHA-256. Outros algoritmos, como SHA-1 ou mais forte ou hashes SHA, podem ser compatíveis dependendo da sua configuração. Considere o modo criptográfico selecionado no XClarity Administrator (consulte Definindo configurações de criptografia no servidor de gerenciamento), as configurações de segurança selecionadas para servidores gerenciados (Definindo as configurações de segurança de um servidor gerenciado) e os recursos de outros softwares e dispositivos em seu ambiente. Os certificados ECDSA que são baseados em algumas curvas elípticas (incluindo p256), mas nem todas as curvas elípticas, são suportados na página Certificados confiáveis e na cadeia de assinatura do certificado XClarity Administrator, mas *não são* suportados atualmente para uso pelo certificado do servidor XClarity Administrator.

Nota: O XClarity Administrator usa assinaturas de certificado RSA-3072/SHA-384 para o servidores com XCC2 no modo estrito.

Procedimento

Para baixar o certificado do servidor, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Segurança** para exibir a página Segurança.

Etapa 2. Clique em **Autoridade de Certificação** na seção Gerenciamento de Certificados. A página Autoridade de Certificação é exibida.

Etapa 3. Clique em **Baixar Certificado Raiz da Autoridade de Certificação**.

Etapa 4. Clique em **Salvar como der** ou **Salvar como pem** para salvar o certificado do servidor como um arquivo DER ou PEM no sistema local.

Etapa 5. Importe o certificado baixado para a lista de certificados confiáveis de autoridade raiz para seu navegador.

- **Firefox:**
  1. Abra o navegador e clique em **Ferramentas → Opções → Avançado**.
  2. Clique na guia **Certificados**.
  3. Clique em **Exibir certificados**.
  4. Clique em **Importar** e vá até o local onde o certificado foi baixado.
  5. Selecione o certificado e clique em **Abrir**.
- **Internet Explorer:**
  1. Abra o navegador e clique em **Ferramentas → Opções de Internet → Conteúdo**.
  2. Clique em **Certificados** para ver uma lista de todos os certificados que atualmente são confiáveis.
  3. Clique em **Importar** para exibir o Assistente de Importação de Certificado.
  4. Conclua o assistente para importar o certificado.

Incluindo e substituindo uma lista de revogação de certificado

Uma *lista de revogação de certificado* é uma lista de certificados que foram revogados e não são mais confiáveis. Um certificado poderá ser revogado se tiver sido emitido incorretamente pela CA ou se a chave for comprometida, perdida ou roubada.

Procedimento

Conclua as seguintes etapas para incluir uma nova lista de revogação de certificado ou substituir uma lista de revogação de certificado existente.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Segurança** para exibir a página Segurança.

Etapa 2. Clique em **Listas de Revogação de Certificados** em Gerenciamento de Certificados na navegação esquerda. A página Listas de Revogação de Certificados é exibida com uma lista de todas as listas de revogação de certificado.

Etapa 3. Clique em **Adicionar/Substituir CLR** para incluir uma lista de revogação de certificado ou selecione uma lista de revogação de certificado e clique em **Adicionar/Substituir CLR** para substituir a CRL.

Etapa 4. Especifique um arquivo da lista de revogação de certificado, em formato PEM ou DER, ou cole o certificado em formato PEM.

Etapa 5. Clique em **Criar** para criar a lista de revogação de certificado.

Habilitando o encapsulamento

Ao gerenciar o chassi e os servidores Lenovo em Lenovo XClarity Administrator, é possível configurar Lenovo XClarity Administrator para modificar as regras de firewall para dispositivos para que as solicitações de entrada sejam aceitas apenas de Lenovo XClarity Administrator. Isso é referente ao *encapsulamento*. Também é possível habilitar ou desabilitar o encapsulamento no chassi e servidores que já são gerenciados pelo Lenovo XClarity Administrator.

Quando ativado nos dispositivos que suportam o encapsulamento, o Lenovo XClarity Administrator altera o modo de encapsulamento do dispositivo para "encapsulationLite" e modifica as regras de firewall no dispositivo para delimitar solicitações de entrada apenas desse Lenovo XClarity Administrator.

Quando desabilitado, o modo de encapsulamento está definido como "normal". Se o encapsulamento tiver sido ativado anteriormente em dispositivos, as regras de firewall de encapsulamento são removidas.

É possível habilitar ou desabilitar o encapsulamento globalmente para todos os dispositivos durante o processo de gerenciamento, selecionando a caixa de seleção **Habilitar encapsulamento em todos os dispositivos gerenciados futuros** na página Descobrir e Gerenciar Novos Dispositivos. O encapsulamento é desativado por padrão.

Pode-se também habilitar ou desabilitar o encapsulamento individualmente para dispositivos gerenciados específicos a qualquer momento, navegando até a página de resumo do dispositivo, selecionando-o e clicando em **Ações → Ativar encapsulamento** ou **Ações → Desabilitar Encapsulamento**.

Atenção: Se o encapsulamento estiver ativado e XClarity Administrator ficar indisponível antes que o gerenciamento de um dispositivo seja cancelado, as etapas necessárias deverão ser tomadas para desativar o encapsulamento e estabelecer comunicação com o dispositivo. Para procedimentos de recuperação, consulte o arquivo lenovoMgrAlert.mib e Recuperando o gerenciamento com um CMM após uma falha no servidor de gerenciamento.

Nota: O encapsulamento não é suportado em comutadores, dispositivos de armazenamento e, chassi e servidores que não são da Lenovo.

Implementando a conformidade com NIST SP 800-131A

Se precisar de conformidade com NIST SP 800-131A, é possível começar a funcionar em um ambiente totalmente compatível usando o Lenovo XClarity Administrator.

Sobre esta tarefa

O Special Publication 800-131A do National Institute of Standards and Technology (NIST SP 800-131A) especifica a maneira que as comunicações seguras devem ser manipuladas. O padrão reforça os algoritmos e aumenta os comprimentos da chave para melhorar a segurança. O padrão NIST SP 800-131A requer que os usuários sejam configurados para o cumprimento rigoroso do padrão.

Notas: Os seguintes componentes do Flex System não oferecem suporte ao NIST SP 800-131A atualmente. As comunicações entre o XClarity Administrator ou o CMM e estes componentes não são compatíveis:
- Comutador Escalável de 10 Gb EN4023 Flex System
- Comutador Ethernet de 40 Gb EN6131 Flex System
- Comutador SAN de 8 Gb FC3171 Flex System
- Comutador Escalável SAN de 16 Gb FC5022 Flex System
- Comutador InfiniBand IB6131 Flex System

Nota: Quando um provedor de identidade SAML é usado para autenticação, o XClarity Administrator usa o SHA-1 para efetuar a assinatura nos metadados. Usar o algoritmo SHA-1 para assinaturas digitais não é compatível com o NIST SP 800-131A.

Procedimento

Para implementar a conformidade com o NIST SP 800-131A, conclua as seguintes etapas.

Etapa 1. Certifique-se de que seus dispositivos atendam aos seguintes critérios:
- Use o Secure Sockets Layer (SSL) sobre o protocolo TLS v1.2.
- Use o SHA-256 ou as funções hash mais fortes para as assinaturas digitais e SHA-1 ou as funções hash mais fortes para os outros aplicativos.
- Use o RSA-2048 ou mais forte ou o Elliptic Curves aprovado pelo NIST que têm 224 bits ou mais.
- Use a criptografia simétrica aprovado pelo NIST com chaves com um mínimo de 128 bits de comprimento.
- Use os geradores de números aleatórios aprovados pelo NIST.
- Quando for possível, ofereça suporte aos mecanismos Diffie-Hellman ou Elliptic Curve Diffie-Hellman Key Exchange.

Etapa 2. Definido as configurações criptográficas no Lenovo XClarity Administrator. Há duas configurações relacionadas com a conformidade com o NIST SP 800-131A:
- O *Modo SSL/TLS* especifica os protocolos que devem ser usados para comunicações seguras. O XClarity Administrator oferece suporte a uma configuração de **Servidor e cliente TLS 1.2** para restringir o protocolo de criptografia a TLS 1.2 no XClarity Administrator e em todos os dispositivos gerenciados.
- Se as comunicações seguras forem implementadas, o *modo criptográfico* definirá os comprimentos de chave de criptografia a serem usados. É possível configurar o modo criptográfico como **NIST SP 800-131A**. Entretanto, você não pode implantar alguns sistemas operacionais por meio do XClarity Administrator porque alguns instaladores de sistema operacional não oferecem suporte às configurações restritas. Para oferecer suporte à implementação do sistema operacional, é possível optar por permitir uma exceção para implantação do sistema operacional.

  Ao modificar qualquer configuração de criptografia, o XClarity Administrator fornece as novas configurações para todos os dispositivos gerenciados e tenta resolver os novos certificados nesses dispositivos.

Nota: Você precisará reiniciar o XClarity Administrator depois de alterar as configurações de criptografia para que as alterações tenham efeito e para restaurar todos os serviços perdidos (consulte Reiniciando o XClarity Administrator).

Para obter mais informações sobre essas configurações, consulte Definindo configurações de criptografia no servidor de gerenciamento.

Etapa 3. Use um navegador da Web que ofereça suporte ao protocolo TLS1.2 e às funções hash SHA-256 e para habilite essas configurações em seu navegador.

Nota: Se você usa ou planeja usar certificados personalizados ou assinados externamente, todos os certificados da cadeia deverão ser baseados em funções de hash SHA-256.

Etapa 4. Use os protocolos criptografados para todas as comunicações. Não habilite os protocolos não criptografados, como Telnet, FTP e VNC, para comunicações remotas com dispositivos gerenciados XClarity Administrator.

Usando o VMware Tools

O pacote do VMware Tools é instalado no sistema operacional guest da máquina virtual quando você instala o Lenovo XClarity Administrator em ambientes baseados em VMware ESXi. Esse pacote fornece um subconjunto de ferramentas VMware que oferecem suporte a backup e migração otimizados de dispositivos virtuais enquanto preservam o status do aplicativo e a continuidade.

Para obter informações sobre como usar o VMware Tools, consulte Utilitário de configuração de ferramentas VMware no site da central de documentação do VMware vSphere.

Configurando o acesso à rede

Ao configurar inicialmente o Lenovo XClarity Administrator, você configura até duas interfaces de rede. Além disso, você precisa especificar qual dessas interfaces deve ser usada para implantar sistemas operacionais. Depois da configuração inicial, é possível modificar essas configurações.

Antes de iniciar

Atenção:

- Alterar o endereço IP do XClarity Administrator depois de gerenciar dispositivos pode fazer com que os dispositivos sejam colocados no estado offline no XClarity Administrator. Certifique-se de que o gerenciamento de todos os dispositivos seja cancelado antes de alterar o endereço IP.
- É possível habilitar ou desabilitar a verificação de endereços IP duplicados na mesma sub-rede clicando no botão de alternância **Verificação de endereço IP duplicado**. Ele está desabilitado por padrão. Quando habilitado, o XClarity Administrator gerará um alerta se você tentar gerenciar o endereço IP do XClarity Administrator ou gerenciar um dispositivo que esteja sendo gerenciado ou de outro dispositivo encontrado na mesma sub-rede.

  Nota: Quando habilitado, o XClarity Administrator realiza uma verificação ARP para encontrar dispositivos IPv4 ativos na mesma sub-rede. Para evitar a verificação ARP, desabilite a **Verificação de endereço IP duplicado**.
- Ao executar o XClarity Administrator como um dispositivo virtual, se a interface da rede de gerenciamento estiver configurada para usar DHCP, o endereço IP da interface de gerenciamento poderá ser alterado quando o arrendamento do DHCP expirar. Se o endereço IP for alterado, você deverá deixar de gerenciar o chassi, o rack e os servidores em torre e, em seguida, voltar a gerenciá-lo. Para evitar esse problema, altere a interface de gerenciamento para um endereço IP estático ou certifique-se de que a configuração do servidor DHCP esteja configurada para que o endereço do DHCP seja baseado em um endereço MAC ou que o arrendamento do DHCP não expire.

- Se você *não* pretende usar o XClarity Administrator para implantar o sistema operacional ou atualizar drivers de dispositivo do SO, é possível desativar servidores Samba e Apache alterando a interface de rede para usar a opção **descobrir e gerenciar somente hardware**. O servidor de gerenciamento é reiniciado depois de alterar a interface de rede.
- Ao executar o XClarity Administrator como um contêiner:
  - É possível habilitar ou desabilitar a verificação de endereço IP duplicada, modificar as funções da interface de rede e modificar configurações de proxy. Todas as outras configurações de rede (incluindo endereço IP, gateway e DNS) são definidas na configuração do contêiner.
  - Verifique se uma rede macvlan está configurada no sistema host.

Sobre esta tarefa

O XClarity Administrator tem duas interfaces de rede separadas que podem ser definidas para seu ambiente, dependendo da topologia de rede implementada. Para dispositivos virtuais, essas redes são chamadas de eth0 e eth1. Para contêineres, é possível escolher nomes personalizados.

- Quando somente uma interface de rede (eth0) estiver presente:
  - A interface deve ser configurada para oferecer suporte à descoberta e ao gerenciamento do dispositivo (como a configuração do servidor e atualizações de firmware). Ela deve conseguir se comunicar com os CMMs e os comutadores Flex em cada chassi gerenciado, no Baseboard Management Controller em cada servidor gerenciado e em cada comutador RackSwitch.
  - Caso você pretenda adquirir atualizações de firmware e de driver de dispositivo do SO usando o XClarity Administrator, pelo menos, uma das interfaces de rede deverá ser conectada à Internet, de preferência, por meio de um firewall. Caso contrário, você deve importar atualizações para o repositório.
  - Se você pretende coletar dados de serviço ou usar a notificação automática de problemas (incluindo Call Home e Recurso de Upload da Lenovo), pelo menos uma das interfaces de rede deve estar conectada à Internet, de preferência, por meio de um firewall.
  - Se você pretende implantar imagens do sistema operacional e atualizar drivers de dispositivo do SO, a interface deve ter conectividade de rede IP com a interface de rede do servidor que é usada para acessar o sistema operacional do host.

    Nota: Se implementar uma rede separada para implantação do SO e atualizações de driver do SO, você poderá configurar a segunda interface de rede para estabelecer conexão com essa rede em vez da rede de dados. No entanto, se o sistema operacional em cada servidor não tiver acesso à rede de dados, configure uma interface adicional nos servidores para fornecer conectividade, do sistema operacional do host para a rede de dados, para implantação do SO e atualizações de driver de dispositivo do SO, se necessário.
- Quando duas interfaces de rede (eth0 e eth1) estiverem presentes:
  - A primeira interface de rede (geralmente a interface Eth0) deve ser conectada à rede de gerenciamento e configurada para oferecer suporte à descoberta e ao gerenciamento do dispositivo (incluindo configuração do servidor e atualizações de firmware). Ela deve conseguir se comunicar com os CMMs e os comutadores Flex em cada chassi gerenciado, no controlador de gerenciamento em cada servidor gerenciado e em cada comutador RackSwitch.
  - A segunda interface de rede (geralmente, a interface eth1) pode ser configurada para se comunicar com uma rede de dados interna, rede de dados pública ou ambas.
  - Caso você pretenda adquirir atualizações de firmware e de driver de dispositivo do SO usando o XClarity Administrator, pelo menos, uma das interfaces de rede deverá ser conectada à Internet, de preferência, por meio de um firewall. Caso contrário, você deve importar atualizações para o repositório.

– Se você pretende coletar dados de serviço ou usar a notificação automática de problemas (incluindo Call Home e Recurso de Upload da Lenovo), pelo menos uma das interfaces de rede deve estar conectada à Internet, de preferência, por meio de um firewall.
– Se você pretende implantar imagens do sistema operacional e atualizar drivers de dispositivo, é possível usar a interface eth1 ou eth0. No entanto, a interface que você usar deve ter conectividade de rede IP com a interface de rede do servidor que é usada para acessar o sistema operacional do host.

  Nota: Se implementar uma rede separada para implantação do SO e atualizações de driver do SO, você poderá configurar a segunda interface de rede para estabelecer conexão com essa rede em vez da rede de dados. No entanto, se o sistema operacional em cada servidor não tiver acesso à rede de dados, configure uma interface adicional nos servidores para fornecer conectividade, do sistema operacional do host para a rede de dados, para implantação do SO e atualizações de driver de dispositivo do SO, se necessário.

A tabela a seguir mostra configurações possíveis para as interfaces de rede XClarity Administrator baseadas no tipo de topologia de rede que foi implementada em seu ambiente. Use esta tabela para determinar como configurar cada interface de rede.

Tabela 2. Função de cada interface de rede com base na topologia de rede

Topologia de rede	**Função da interface 1 (eth0)**	**Função da interface 2 (eth1)**
Rede convergida (gerenciamento e rede de dados com suporte para implantação do SO e atualizações de driver de dispositivo do SO)	Rede de gerenciamento • Descoberta e gerenciamento • Configuração do servidor • Atualizações de firmware • Coleta de dados de serviço • Notificação automática de problemas (como Call Home e Recurso de Upload da Lenovo) • Recuperação de dados de garantia • Implantação do SO • Atualizações de drivers de dispositivo do SO	Nenhum(a)
Rede de gerenciamento separada com suporte para implantação do SO, atualizações de driver de dispositivo do SO e rede de dados	Rede de gerenciamento • Descoberta e gerenciamento • Configuração do servidor • Atualizações de firmware • Coleta de dados de serviço • Notificação automática de problemas (como Call Home e Recurso de Upload da Lenovo) • Recuperação de dados de garantia • Implantação do SO • Atualizações de drivers de dispositivo do SO	Rede de dados • Nenhum(a)
Rede de gerenciamento e rede de dados separadas com suporte para implantação do SO e atualizações de driver de dispositivo do SO	Rede de gerenciamento • Descoberta e gerenciamento • Configuração do servidor • Atualizações de firmware • Coleta de dados de serviço • Notificação automática de problemas (como Call Home e Recurso de Upload da Lenovo) • Recuperação de dados de garantia	Rede de dados • Implantação do SO • Atualizações de drivers de dispositivo do SO

Tabela 2. Função de cada interface de rede com base na topologia de rede (continuação)

Topologia de rede	Função da interface 1 (eth0)	Função da interface 2 (eth1)
Rede de gerenciamento e rede de dados separadas sem suporte para implantação do SO e atualizações de driver de dispositivo do SO	Rede de gerenciamento • Descoberta e gerenciamento • Configuração do servidor • Atualizações de firmware • Coleta de dados de serviço • Notificação automática de problemas (como Call Home e Recurso de Upload da Lenovo) • Recuperação de dados de garantia	Rede de dados • Nenhum(a)
Somente rede de gerenciamento (não há suporte para implantação do SO e atualizações de driver de dispositivo do SO)	Rede de gerenciamento • Descoberta e gerenciamento • Configuração do servidor • Atualizações de firmware • Coleta de dados de serviço • Notificação automática de problemas (como Call Home e Recurso de Upload da Lenovo) • Recuperação de dados de garantia	Nenhum(a)

Para obter mais informações sobre interfaces de rede XClarity Administrator incluindo limitações de endereços IPv6, consulte Considerações de rede na documentação online do XClarity Administrator.

Procedimento

Para configurar o acesso de rede, conclua as etapas a seguir.

Etapa 1. Na barra de menus XClarity Administrator, clique em **Administração → Acesso à Rede**. As configurações de rede atuais são exibidas.

Etapa 2. É possível habilitar a verificação de endereços IP duplicados na mesma sub-rede clicando no botão de alternância **Verificação de endereço IP duplicado**.

Quando habilitado, o XClarity Administrator gerará um alerta se você tentar gerenciar o endereço IP do XClarity Administrator ou gerenciar um dispositivo que esteja sendo gerenciado ou de outro dispositivo encontrado na mesma sub-rede.

Etapa 3. Clique em **Editar Acesso à Rede** para exibir a página Editar Acesso à Rede.

Etapa 4. Se desejar implantar sistemas operacionais e atualizar drivers de dispositivo do SO usando o XClarity Administrator, escolha a interface de rede a ser usada para gerenciar os sistemas operacionais.

- Se apenas uma interface for definida para o XClarity Administrator, determine se essa interface deve ser usada para descobrir e gerenciar somente hardware ou se também deve ser usada para gerenciar sistemas operacionais.
- Se duas interfaces forem definidas para o XClarity Administrator (Eth0 e Eth1), determine qual interface deve ser usada para gerenciar sistemas operacionais. Se você escolher "Nenhum", *não* poderá implantar imagens do sistema operacional nem atualizar drivers de dispositivo do SO em servidores gerenciados do XClarity Administrator.

Etapa 5. (somente XClarity Administrator como um dispositivo virtual) Modifique as configurações de IP.

a. Para a primeira interface, especifique o endereço IPv4, o endereço IPv6 ou ambos.

- **IPv4**. Você deve atribuir um endereço IPv4 à interface. É possível usar um endereço IP designado estaticamente ou obter um endereço IP de um servidor DHCP.
- **IPv6**. Opcionalmente, é possível atribuir um endereço IPv6 à interface usando um destes métodos de atribuição:
  - Usar endereço IP atribuído estaticamente
  - Usar configuração de endereço com estado (DHCPv6)
  - Usar configuração automática de endereço sem estado

  Nota: Para obter informações sobre limitações do endereço IPv6, consulte Limitações de configuração IPv6 na documentação online do XClarity Administrator.

b. Se uma segunda interface estiver disponível, especifique o endereço IPv4, o endereço IPv6 ou ambos.

Nota: Os endereços IP atribuídos a essa interface devem estar em uma sub-rede diferente dos endereços IP atribuídos à primeira interface. Se você optar por usar DHCP para atribuir endereços IP às duas interfaces (Eth0 e Eth1), o servidor DHCP não deverá atribuir a mesma sub-rede dos endereços IP das duas interfaces.

- **IPv4**. É possível usar um endereço IP designado estaticamente ou obter um endereço IP de um servidor DHCP.
- **IPv6**. Opcionalmente, é possível atribuir um endereço IPv6 à interface usando um destes métodos de atribuição:
  – Usar endereço IP atribuído estaticamente
  – Usar configuração de endereço com estado (DHCPv6)
  – Usar configuração automática de endereço sem estado

c. Especifique o gateway padrão.

Se você especificar um gateway padrão, ele deverá ser um endereço IP válido e deverá usar a mesma máscara de rede (a mesma sub-rede) do endereço IP de uma das interfaces de rede (Eth0 ou Eth1). Se você usar uma única interface, o gateway padrão deverá estar na mesma sub-rede que a interface de rede.

Se uma das interfaces usar DHCP para obter um endereço IP, o gateway padrão também usará DHCP. Para inserir manualmente um endereço de gateway padrão que substitui o recebido do servidor DHCP, marque a caixa de seleção **Substituir Gateway**.

Dicas:

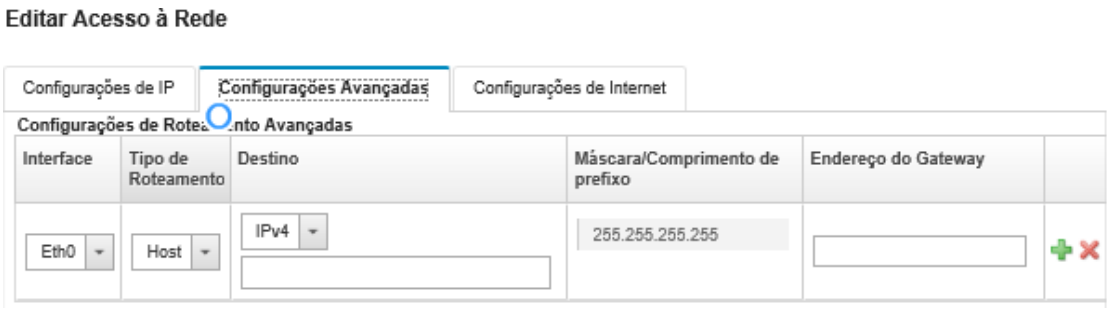
- Verifique se o gateway corresponde a uma sub-rede das interfaces de rede. O gateway padrão é definido automaticamente por meio dessa interface de rede.
- Para voltar a um gateway fornecido pelo DHCP, desmarque a caixa de seleção **Substituir Gateway**.

CUIDADO:
Se você optar por substituir o gateway, tome cuidado para inserir o endereço de gateway correto; caso contrário, esse servidor de gerenciamento ficará inacessível e não haverá como fazer login remotamente para corrigi-lo.

d. Clique em **Salvar configurações de IP**.

Etapa 6. (somente XClarity Administrator como um dispositivo virtual) Opcionalmente, modifique as configurações avançadas.

a. Clique na guia **Roteamento Avançado**.



b. Especifique uma ou mais entradas de rota na tabela **Configurações de Roteamento Avançadas** a ser usada por essa interface.

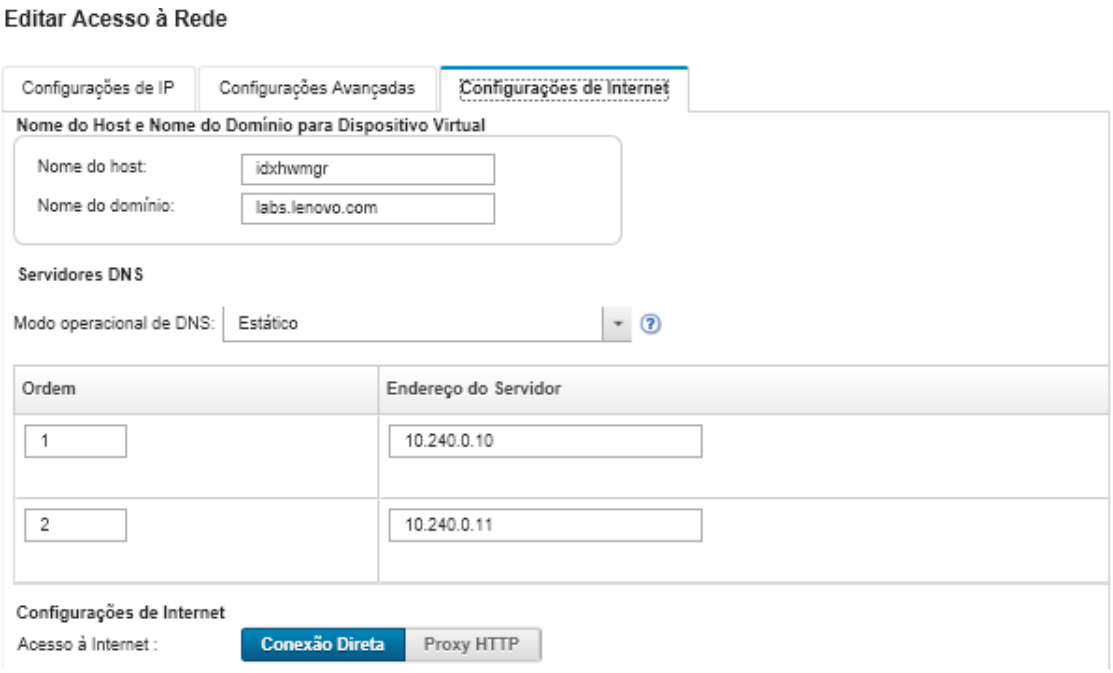
Para definir uma ou mais entradas de rota, conclua as etapas a seguir.
1. Escolha a interface.
2. Especifique o tipo de rota, que pode ser uma rota para outro host ou para uma rede.
3. Especifique o endereço de host ou rede de destino para o qual está direcionando a rota.
4. Especifique a máscara de sub-rede para o endereço de destino.
5. Especifique o endereço do gateway aos quais os pacotes devem ser endereçados.

c. Clique em **Salvar Roteamento Avançado**.

Etapa 7. Opcionalmente, modifique as configurações de DNS e proxy.

Quando o XClarity Administrator estiver configurado como um contêiner, somente as configurações de proxy poderão ser modificadas na interface da Web. As configurações de DNS são definidas no contêiner.

a. Clique na guia **DNS e Proxy**.



b. Especifique o nome do host e o nome de domínio a serem usados para XClarity Administrator.

c. Selecione o modo operacional de DNS. Pode ser **Estático** ou **DHCP**.

Atenção: Você deve reiniciar o servidor de gerenciamento ao alterar o modo operacional DNS.

Nota: Se você optar por usar um servidor DHCP para obter o endereço IP, as alterações feitas nos campos **Servidor DNS** serão substituídas na próxima vez que o XClarity Administrator renovar a autorização DHCP.

d. Especifique o endereço IP de um ou mais servidores de Sistema de Nomes de Domínio (DNS) a serem usados e a ordem de prioridade de cada.

e. Especifique se o acesso à Internet é feito com uma conexão direta ou um proxy HTTP (se o XClarity Administrator tiver acesso à Internet).

Notas: Se estiver usando um proxy HTTP, garanta que os seguintes requisitos sejam cumpridos.
- Assegure-se de que o servidor proxy esteja configurado para usar autenticação básica.
- Verifique se o servidor proxy está configurado como um proxy não encerrando.
- Verifique se o servidor proxy está configurado como um proxy de encaminhamento.
- Verifique se os balanceadores de carga estão configurados para manter sessões com um servidor proxy e alternar entre eles.

Se você optar por usar um proxy HTTP, preencha os campos obrigatórios:

1. Especifique o nome do host e a porta do servidor proxy.
2. Opte por usar autenticação e, se necessário, especifique o nome de usuário e a senha.
3. Especifique o URL do teste de proxy.
4. Clique em **Testar Proxy** para verificar se as configurações de proxy estão definidas e funcionando corretamente.

f. Clique em **Salvar DNS e Proxy**.

g. Envie o nome de domínio totalmente qualificado (FQDN) do servidor de gerenciamento do XClarity Administrator e informações DNS para servidores gerenciados com IMM2, XCC e XCC2 para que os servidores gerenciados possam encontrar o servidor de gerenciamento usando essas informações.

1. Clique em **Enviar FQDN/DNS para BMC**.
2. Escolha como manipular as entradas DNS existentes no Baseboard Management Controller.
   - Mantenha as entradas DNS existentes e anexe as entradas DNS do servidor de gerenciamento no próximo slot disponível.
   - Substitua todas as entradas DNS existentes por entradas DNS do servidor de gerenciamento.
3. Digite **SIM** no campo de edição.
4. Clique em **Aplicar**.

Um trabalho é criado para executar esta operação. É possível monitorar o andamento do trabalho no cartão **Monitoramento → Trabalhos**. Se o trabalho não foi concluído com êxito, clique no link do trabalho para exibir detalhes sobre o trabalho (consulte).

Também é possível remover as informações de FQDN e DNS do servidor de gerenciamento dos servidores gerenciados com IMM2, XCC e XCC2 clicando em **Remover FQDN/DNS do BMC**. É possível optar por manter outras entradas DNS existentes, remover todas as entradas DNS ou remover apenas entradas que corresponderem às informações do servidor de gerenciamento.

Etapa 8. Clique em **Reiniciar** para reiniciar o servidor de gerenciamento.

Etapa 9. Clique em **Testar Conexão** para verificar as configurações de rede.

Configurando data e hora

É possível configurar a data e hora a serem usadas para Lenovo XClarity Administrator.

Antes de iniciar

Deve-se usar pelo menos um (e até quatro) servidor Network Time Protocol (NTP) para sincronizar os registros de data e hora de todos os eventos recebidos dos dispositivos gerenciados com XClarity Administrator.

Dica: o servidor NTP deve estar acessível na rede de gerenciamento (geralmente a interface Eth0). Considere a possibilidade de configurar um servidor NTP no host em que XClarity Administrator está em execução.

Se você alterar a hora no servidor NTP, poderá levar alguns minutos para o XClarity Administrator ser sincronizado com a nova hora.

Atenção: O dispositivo virtual do XClarity Administrator e seu host devem ser configurados para sincronização com a mesma origem de horário para evitar a falta de sincronização de horário acidental entre

o XClarity Administrator e seu host. Normalmente, o host é configurado para que seus dispositivos virtuais tenham o horário sincronizado com ele. Se o XClarity Administrator estiver definido para sincronizar-se com uma origem diferente de seu host, você deverá desativar a sincronização de horário entre o dispositivo virtual XClarity Administrator e seu host.

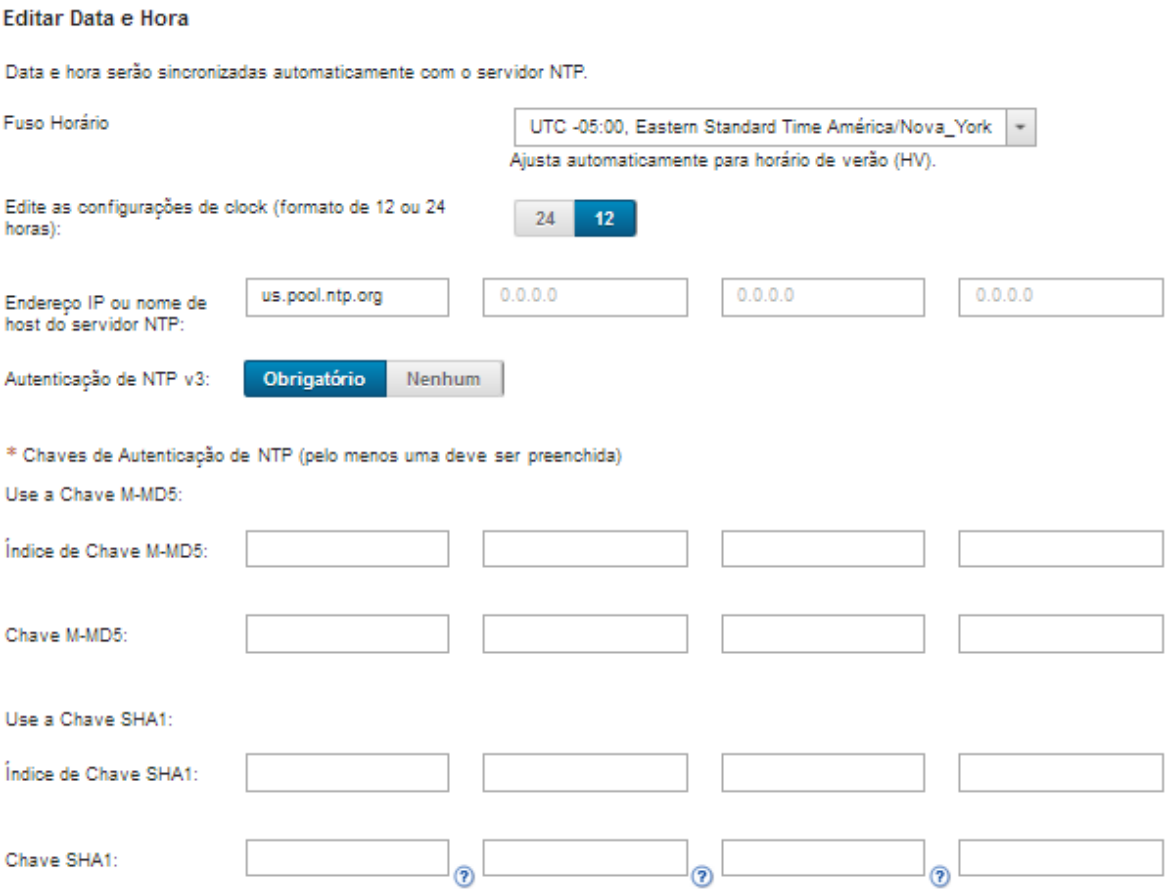
- Para o ESXi, seguindo as instruções no VMware – Página Desabilitar Sincronização de Tempo.
- Para o Hyper-V do Gerenciador Hyper-V, clique com o botão direito na máquina virtual XClarity Administrator e clique em **Configurações**. Na caixa de diálogo, clique em **Gerenciamento > Serviços de integração** no painel de navegação e, em seguida, limpe **Sincronização de horário**.

Procedimento

Conclua as seguintes etapas para definir data e hora para XClarity Administrator.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Data e Hora**. A página Data e Hora é exibida. Essa página mostra a data e hora atuais do XClarity Administrator.

Etapa 2. Clique em **Editar Data e Hora** para exibir a página Editar Data e Hora.



Etapa 3. Preencha a caixa de diálogo de data e hora.

1. Escolha o fuso horário onde o host para XClarity Administrator está localizado.

   Se o fuso horário selecionado estiver em horário de verão (DST), a hora será ajustada automaticamente para DST.
2. Opte por usar um relógio de 12 horas ou 24 horas.
3. Especifique o nome do host ou o endereço IP para cada servidor NTP na rede. Você pode definir até quatro servidores NTP.

4. Selecione **Obrigatório** para ativar a autenticação de NTP v3, ou selecione **Nenhum** para usar a autenticação NTP v1 entre o XClarity Administrator e os servidores NTP na rede.

   Você pode usar a autenticação v3 se os CMMs Flex System gerenciados e os Baseboard Management Controllers tiverem firmware que exija a autenticação v3 e se a autenticação de NTP v3 for necessária entre o XClarity Administrator e um ou mais servidores NTP na sua rede.

5. Se você habilitar a autenticação de NTP v3, defina a chave de autenticação e o índice de cada servidor NTP aplicável. É possível especificar uma chave M-MD5, uma chave SHA1 ou ambas. Se as chaves M-MD5 ou SHA1 forem especificadas, o XClarity Administrator enviará por push a chave M-MD5 ou SHA1 para os CMMs Flex System gerenciados e os controladores de gerenciamento que oferecem suporte a ele. O XClarity Administrator usa a chave para autenticar com o servidor NTP

   - Para a chave M-MD5, especifique uma string ASCII que inclua apenas letras maiúsculas e minúsculas (a-z, A-Z), dígitos (0 a 9) e os caracteres especiais @#.
   - Para a chave SHA1, especifique uma string ASCII de 40 caracteres, incluindo apenas 0-9 e a-f.
   - O índice de chave especificado e a chave de autenticação devem corresponder aos valores de ID da chave e senha configurados no servidor NTP. Por exemplo, se o índice de chave da chave SHA1 inserida no servidor NTP for 5, o índice de chave especificado da chave SHA1 do XClarity Administrator também será 5. Para obter informações sobre como configurar o ID de chave e a senha, consulte a documentação do servidor NTP.
   - Você deve especificar a chave para cada servidor NTP que usa a autenticação v3, mesmo se dois ou mais servidores NTP usarem a mesma chave.
   - Se você ativar a autenticação v3, mas não fornecer uma chave de autenticação e o índice de um servidor NTP, a autenticação v1 será usada por padrão.
   - Se você especificou vários servidores NTP, os servidores NTP deverão ser todos autenticados por v3 ou v1. Não há suporte para uma combinação de servidores NTP autenticados por v1 e v3.
   - Se você especificou vários servidores NTP com autenticação v3, o índice de chaves deverá ser exclusivo se as chaves não forem as mesmas. Por exemplo, o servidor NTP 1 e 2 não podem ter o índice de chaves SHA1 de 1 se as chaves SHA1 forem diferentes nos servidores NTP 1 e 2. Você deve reconfigurar um dos servidores NTP para aceitar a chave com um índice diferente do outro servidor NTP; caso contrário, a última chave definida que estava associada a um índice será configurada para todos os servidores NTP com o mesmo índice de chave.

Etapa 4. Clique em **Salvar**.

Definindo preferências de inventário

É possível definir as preferências de inventário para dispositivos gerenciados, incluindo a propriedade a ser usada para exibir o nome do dispositivo.

Procedimento

Conclua as etapas a seguir para definir as preferências de inventário para dispositivos gerenciados:

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Preferências de inventário**. A página Preferências de Inventário é exibida.

Etapa 2. Selecione a propriedade a ser usada para o nome do dispositivo exibido na interface do usuário do Lenovo XClarity Administrator. É possível selecionar uma das propriedades a seguir.
   - **Sequência predefinida (padrão)**

- **Nome definido pelo usuário**
- **Nome do host do DNS**
- **Nome do host**
- **Endereço IPv4**
- **Número de série**

Se a opção **Sequência predefinida** estiver selecionada, o nome do dispositivo que é exibido será escolhido com base na sequência de propriedades na lista anterior. Por exemplo, se um dispositivo tiver um nome definido pelo usuário, esse nome será exibido. Se um dispositivo não tiver um nome definido pelo usuário, o nome do host DNS será exibido. Se um dispositivo não tiver um nome definido pelo usuário ou o nome do host DNS, o nome do host será exibido.

Nota: A seleção de um valor diferente do padrão altera o nome exibido na interface do usuário do Lenovo XClarity Administrator para todos os dispositivos para a propriedade selecionada. O nome definido pelo usuário que é atribuído ao dispositivo não muda.

Etapa 3. Se preferir, clique em **Habilitar** para optar por classificar grades (tabelas) usando o valor selecionado para o nome do dispositivo.

Etapa 4. Selecione a preferência de ordem de numeração do rack, seja em ordem crescente (por exemplo, 1 – 52) ou decrescente (por exemplo, 52 – 1).

Nota: Alterar a preferência de ordem numérica não altera o local de um dispositivo no rack.

Etapa 5. Clique em **Aplicar**.

Depois de concluir

É possível configurar preferências de limite para gerar um alerta e um evento quando um determinado valor, como a vida útil de um SSD em um servidor ThinkSystem ou ThinkServer excede um nível crítico ou de aviso (consulte Configurando preferências de limite para gerar alertas e eventos).

Configurando preferências de limite para gerar alertas e eventos

É possível configurar preferências de limite para gerar um alerta e um evento quando um determinado valor, como a vida útil de um SSD em um servidor ThinkSystem ou ThinkServer excede um nível crítico ou de aviso.

Procedimento

Conclua as etapas a seguir para encaminhar arquivos de serviço específicos para o provedor de serviço.

Etapa 1. Na barra de menu Lenovo XClarity Administrator, clique em **Monitoramento → Alertas** para exibir a página Alertas.

Etapa 2. Clique no ícone **Configurações de limite** () para exibir a caixa de diálogo Configurações de limite.

Etapa 3. Modifique os limites de aviso ou críticos para a vida útil restante dos SSDs nos servidores ThinkSystem e ThinkServer.

A vida útil restante das SSDs é calculada utilizando medidores SMART do fornecedor. Os valores padrão são 30% para o limite de aviso e 20% para o limite crítico.

Etapa 4. Selecione o botão de alternância **Ativado** para gerar um alerta e um evento quando cada limite é atingido.

Etapa 5. Clique em **Aplicar**.

Configurando uma notificação de problema automática em Suporte da Lenovo (Call Home)

É possível criar um encaminhador de serviço que envie automaticamente dados de serviço para qualquer dispositivo gerenciado ao Suporte da Lenovo usando o Call Home quando determinados eventos que permitem manutenção são recebidos de dispositivos gerenciados específicos, como um erro de memória irrecuperável, para que o problema possa ser resolvido. Esse serviço encaminhado é chamado "Call Home Padrão."

A Lenovo está comprometida com a segurança. Quando ativado, Call Home Centro de Suporte da Lenovo quando um dispositivo relata uma falha de hardware ou quando você opta por iniciar um Call Home manual. Os dados de serviço que você costuma fazer upload manualmente para o suporte da Lenovo são enviados automaticamente para o Centro de Suporte da Lenovo via HTTPS usando TLS 1.2 ou posterior; seus dados corporativos nunca são transmitidos. O acesso aos dados de serviço no Centro de Suporte da Lenovo é restrito ao pessoal de serviço autorizado.

Antes de iniciar

Atenção: Você deve aceitar a Instrução de privacidade da Lenovo para poder transferir dados para o Suporte Lenovo.

Verifique se todas as portas que são necessárias para Lenovo XClarity Administrator (incluindo as portas necessárias para Call Home) estão disponíveis antes de ativar Call Home. Para obter mais informações sobre portas, consulte Disponibilidade de porta na documentação online do XClarity Administrator.

Verifique se existe uma conexão com os endereços da Internet exigidos pelo Call Home. Para obter informações sobre firewalls, consulte Firewalls e servidores proxy na documentação online do XClarity Administrator.

Se o XClarity Administrator acessa a Internet com um proxy HTTP, verifique se o servidor proxy está configurado para usar autenticação básica e configurado como um proxy não encerrando. Para obter mais informações sobre como configurar o proxy, consulte Configurando o acesso à redeConfigurando o acesso à rede na documentação online do XClarity Administrator.

Depois de configurar Call Home, o encaminhador de serviço **Call Home da Lenovo padrão** é adicionado à página Encaminhadores de Serviço. É possível editar esse encaminhador para definir configurações adicionais, incluindo quais dispositivos estão associados a esse encaminhador. Todos os dispositivos são compatíveis com o padrão. Se nenhum dispositivo for especificado, o Call Home *não* encaminhará notificações de problema ao Suporte Lenovo.

Sobre esta tarefa

Um *encaminhador de serviços* define informações sobre para onde enviar os arquivos de dados de serviço quando ocorrer um evento que permite manutenção. Você pode definir até 50 encaminhadores de serviço.

- **Se um encaminhador de serviços de Call Home não estiver configurado**, você poderá abrir manualmente um tíquete de serviço e enviar os arquivos de serviço ao Centro de Suporte da Lenovo seguindo as instruções no Nova página da Web de solicitação de serviço. Para obter informações sobre como coletar e baixar arquivos de dados de serviço, consulte Baixando arquivos de diagnóstico do XClarity Administrator e Coletando e baixando arquivos de diagnóstico de um dispositivo na documentação online do XClarity Administrator.
- **Se um encaminhador de serviços de Call Home estiver configurado, mas não habilitado**, você poderá abrir *manualmente* um tíquete de serviço usando a função Call Home para coletar e transferir

arquivos de dados de serviço ao Centro de Suporte da Lenovo a qualquer momento. Para obter mais informações, consulte Abrindo um tíquete de serviço na documentação online do XClarity Administrator.

- **Se um encaminhador de serviços de Call Home estiver configurado e habilitado**, o XClarity Administrator coletará dados de serviço *automaticamente*, abrirá um tíquete de serviço e transferirá os arquivos de serviço ao Centro de Suporte da Lenovo quando ocorrer um evento que permite manutenção para que o problema possa ser resolvido.

  Importante: Quando você habilita um encaminhador de serviços Call Home no Lenovo XClarity Administrator, o Call Home é desabilitado em todos os dispositivos gerenciados para evitar a criação de registros de problema duplicados. Se você pretende deixar de usar o XClarity Administrator para gerenciar dispositivos ou se pretende desativar Call Home em XClarity Administrator, poderá reativar Call Home em todos os dispositivos gerenciados no XClarity Administrator em vez de reativar Call Home para cada dispositivo individual posteriormente. Para obter informações sobre como reabilitar o Call Home em todos os dispositivos gerenciados quando o encaminhador de serviço do Call Home estiver desativado, consulte Reativando call home em todos os dispositivos gerenciados na documentação online do XClarity Administrator.Para servidores com XCC2, o XClarity Administrator salva dados de serviço em dois arquivos no repositório.

  - **Arquivo de serviço**. (.zip) Este arquivo contém informações de serviço e inventário em um formato acessível com facilidade. Esse arquivo é enviado automaticamente ao Centro de Suporte da Lenovo quando ocorre um evento que permite manutenção.
  - **Arquivo de depuração**. (.tzz) O arquivo contém todas as informações de serviço, inventário e logs de depuração para uso pelo Lenovo Support. É possível enviar esse arquivo manualmente ao Lenovo Support se forem necessárias informações adicionais para resolver um problema.

  Para outros dispositivos, o XClarity Administrator salva dados de serviço (por exemplo, informações de serviço, inventário e logs de depuração) em um único arquivo de serviço no repositório. Esse arquivo é enviado ao Centro de Suporte da Lenovo quando ocorre um evento que permite manutenção.

  Embora o XClarity Administrator ofereça suporte ao Call Home para dispositivos ThinkAgile e ThinkSystem, o Baseboard Management Controller para alguns dispositivos ThinkAgile e ThinkSystem não inclui suporte a Call Home. Portanto, não é possível ativar ou desativar o Call Home nesses dispositivos. O Call Home só pode ser habilitado para esses dispositivos no nível do XClarity Administrator.

  O call home será suprimido para eventos repetidos para qualquer dispositivo se um tíquete de serviço for aberto para esse evento nesse dispositivo. O call home também será suprimido para eventos semelhantes para qualquer dispositivo ThinkAgile e ThinkSystem se um tíquete de serviço for aberto para um evento nesse dispositivo. Os eventos ThinkAgile e ThinkSystem são strings de 16 caracteres no seguinte formato *xx<2_char_reading_type><2_char_sensor_type>xx<2_char_entity_ID>xxxxxx* (por exemplo, `806F010D0401FFFF`). Os eventos serão semelhantes se tiverem o mesmo tipo de leitura, tipo de sensor e ID de entidade. Por exemplo, se um tíquete de serviço for aberto para o evento 806F010D0401FFFF em um dispositivo ThinkAgile ou ThinkSystem específico, todos os eventos que ocorrerem nesse dispositivo com IDs de evento como *xx*`6F01`*xx*`04`*xxxxxx*, em que *x* é qualquer caractere alfanumérico, serão suprimidos.

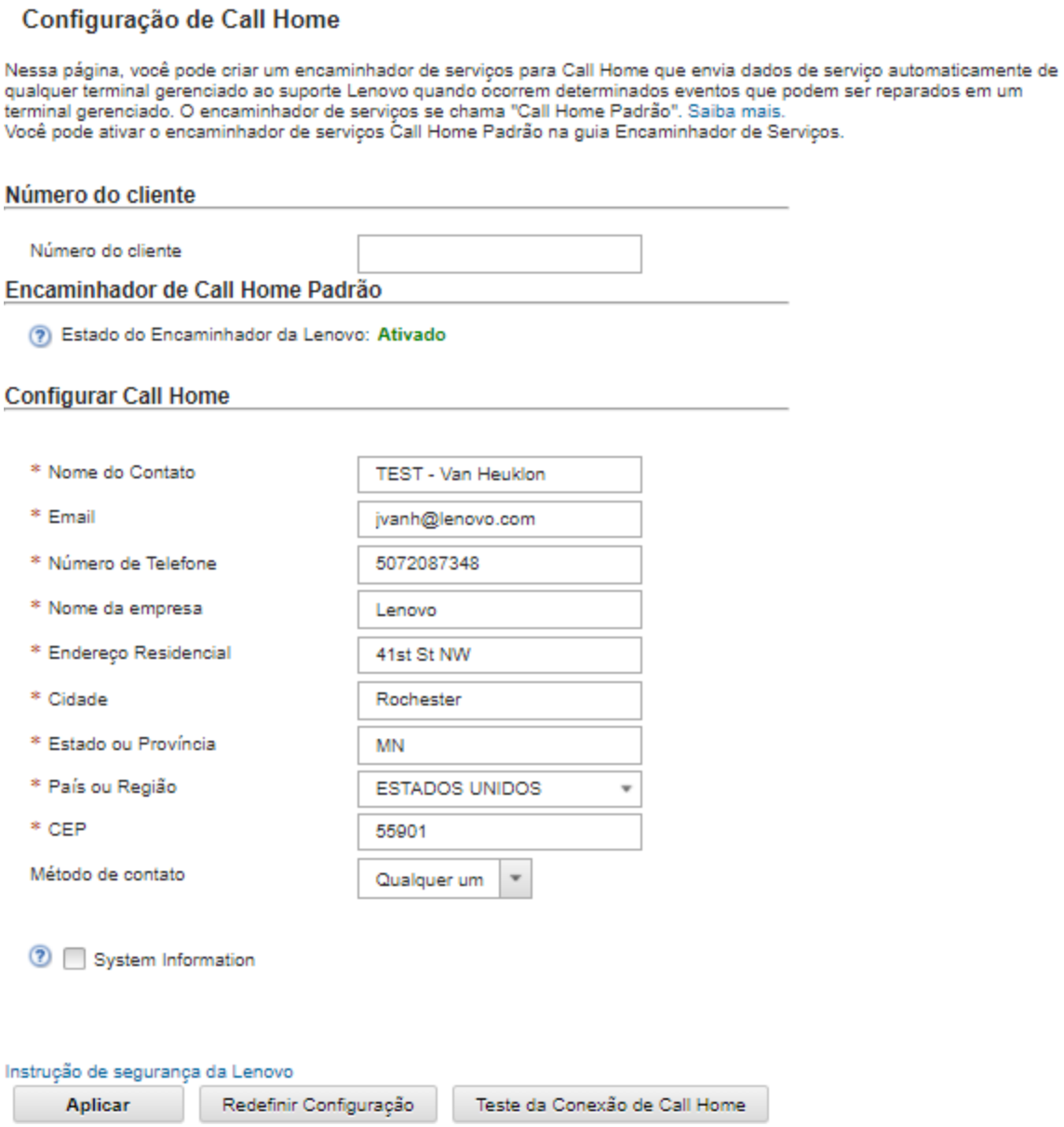
  Para obter informações sobre como exibir tíquetes de serviço que foram abertos automaticamente por um encaminhador de serviços de Call Home, consulte Exibindo tíquetes de serviço e o status na documentação online do XClarity Administrator.

Procedimento

Conclua as seguintes etapas para configurar um encaminhador de serviço para Call Home.

- Configure o Call Home para todos os dispositivos gerenciados (atuais e futuros):
  1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**.

2. Clique em **Configuração de Call Home** na navegação esquerda para exibir a página Configuração de Call Home.



3. (Opcional) Especifique o número do cliente Lenovo padrão a ser usado para relatar problemas com o XClarity Administrator.

   Dica: Você pode localizar o número do seu cliente no e-mail com a prova de direito recebido ao comprar o Lenovo XClarity Pro.
4. Preencha as informações de contato e local.
5. Selecione o método preferencial de contato pelo suporte da Lenovo.
6. (Opcional) Preencha as informações do sistema.
7. Clique em **Aplicar**.

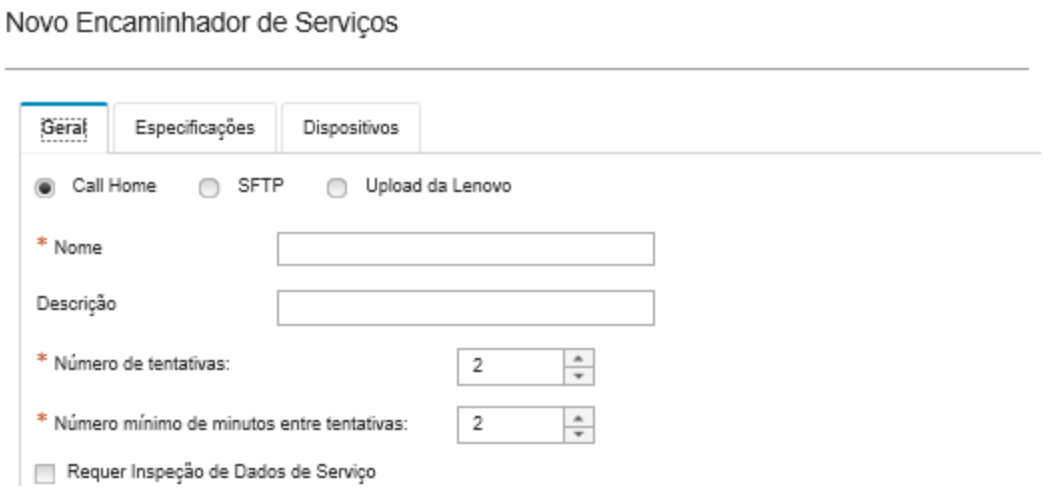
   Um encaminhador de serviço do Call Home chamado "Call Home Padrão" é criado para todos os dispositivos gerenciados usando as informações de contato especificadas.
8. Ative e teste o encaminhador de serviço "Call Home Padrão".

a. Clique em **Encaminhador de Serviços** na navegação esquerda para exibir a página Encaminhadores de Serviços.
b. Selecione **Ativar** na coluna **Status** do encaminhador de serviço "Call Home Padrão".
c. Selecione o encaminhador de serviço "Call Home Padrão" e clique em **Testar Encaminhadores de Serviço** para gerar um evento de teste para o encaminhador de serviço e verifique se o XClarity Administrator pode se comunicar com o Suporte Lenovo Center.

   Você pode monitorar o progresso do teste clicando em **Monitoramento → Trabalhos** na barra de menu do XClarity Administrator.

   Nota: O encaminhador de serviço deve ser habilitado antes de ser testado

- Configure o Call Home para dispositivos gerenciados específicos:
  1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**.
  2. Clique em **Encaminhadores de Serviços** na navegação esquerda para exibir a página Encaminhadores de Serviços.
  3. Clique no ícone **Criar Encaminhador de Serviço** ( ) para exibir a caixa de diálogo Novo Encaminhador de Serviço.
  4. Clique na guia **Geral**.



     a. Selecione **Call Home** como o encaminhador de serviço:
     b. Insira o nome de encaminhador de serviços e uma descrição.
     c. Especifique o número de novas tentativas de notificação automática. O padrão é 2.
     d. Especifique o número mínimo de minutos entre tentativas. O padrão é 2.
     e. (Opcional) Clique em **Requer Inspeção de Dados de Serviço** se desejar examinar os arquivos de dados de serviço antes que sejam transferidos e, opcionalmente, especifique o endereço de e-mail do contato que será notificado quando os arquivos de dados de serviço precisarem ser inspecionados.
  5. Clique na guia **Específico** e preencha as informações de contato e do sistema.

     Dica: Para usar as mesmas informações de contato e local configuradas na página Configuração de call home, selecione **Configuração Geral** no menu suspenso **Configuração**.
  6. Clique na guia **Dispositivos** e selecione os dispositivos gerenciados e os grupos de recursos para os quais esse encaminhador de serviços deve encaminhar arquivos de serviço.

Dica: Para encaminhar arquivos de serviço para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Corresponder todos os dispositivos**.

7. Clique em **Criar**. O encaminhador de serviço é incluído na página Serviço e Suporte.
8. Na página Encaminhadores de Serviços, selecione **Habilitar** na coluna **Status** para habilitar o encaminhador de serviços.
9. Selecione o encaminhador de serviço e clique em **Testar Encaminhadores de Serviço** para gerar um evento de teste para o encaminhador de serviço e verifique se o XClarity Administrator pode se comunicar com o Suporte Lenovo Center.

   Você pode monitorar o progresso do teste clicando em **Monitoramento → Trabalhos** na barra de menu do XClarity Administrator.

   Nota: O encaminhador de serviços deve ser ativado antes de ser testado.

Depois de concluir

Na página Serviço e Suporte, também é possível executar as ações a seguir:

- Se **Requer Inspeção de Dados de Serviço** for selecionado e um evento que permite manutenção tiver sido recebido de um dos dispositivos gerenciados associados ao encaminhador de serviço, você deverá inspecionar os arquivos de serviço antes que sejam encaminhados para o provedor de serviço. Para obter mais informações, consulte Transferindo arquivos de diagnóstico para o Suporte Lenovo na documentação online do XClarity Administrator.
- Determine se o Call Home está habilitado ou desabilitado em um dispositivo gerenciado clicando em **Ações de terminal** na navegação esquerda e verificando o estado na coluna Status do **Call Home**.

  Dica: Se "Estado Desconhecido" for exibido na coluna **Call Home Status**, atualize o navegador da Web para exibir o status correto.
- Defina as informações de contato e o local do suporte para um dispositivo gerenciado específico clicando em **Ações de terminal** na navegação esquerda, selecionando o dispositivo e, em seguida, clicando no ícone **Criar perfil de contato** ( ) ou no ícone **Editar perfil de contato** ( ). As informações de contato e local para o dispositivo gerenciado estão incluídas no tíquete de serviço que o Call Home envia para o Centro de Suporte da Lenovo. Se informações exclusivas de contato e local forem especificadas para um dispositivo gerenciado, essas informações serão incluídas no tíquete de serviço. Caso contrário, as informações gerais que são especificadas para a configuração do XClarity Administrator Call Home (na página **Call Home Configuração** ou na página **Encaminhadores de Serviços**) serão usadas. Para obter mais informações, consulte Centro de Suporte da Lenovo. Para obter mais informações, consulte Definindo os contatos de suporte de um dispositivo na documentação online do XClarity Administrator.
- Exiba tíquetes de serviço que foram enviados para o Centro de Suporte da Lenovo clicando em **Status do Tíquete de Serviço** na navegação esquerda. Esta página lista os tíquetes de serviço que foram abertos automática ou manualmente por um encaminhador de serviços de Call Home, o status e os arquivos de serviço transmitidos para o Centro de Suporte da Lenovo. Para obter mais informações, consulte Exibindo tíquetes de serviço e o status na documentação online do XClarity Administrator.
- Colete dados de serviço para um dispositivo específico clicando em **Ações de terminal** na navegação esquerda, selecionando o dispositivo e, em seguida, clicando no ícone **Coletar Dados de Serviço** ( ). Para obter mais informações, consulte Coletando e baixando arquivos de diagnóstico de um dispositivo na documentação online do XClarity Administrator.
- Abra manualmente um tíquete de serviço no Centro de Suporte da Lenovo, colete dados de serviço para um dispositivo específico e envie os arquivos para o Centro de Suporte da Lenovo clicando em **Ações de terminal** na navegação esquerda, selecionando o dispositivo e clicando em **Todas as Ações → Realizar ManualCall Home**.Se o Centro de Suporte da Lenovo solicitar dados adicionais, o Suporte da Lenovo poderá instruir você a coletar novamente dados de serviço para esse ou outro dispositivo.

Para obter mais informações, consulte Abrindo um tíquete de serviço na documentação online do XClarity Administrator.

- Reabilite o Call Home em todos os dispositivos gerenciados clicando em **Ações de terminal** na navegação esquerda e, em seguida, clicando em **Todas as Ações → Habilitar Call Home em todos os dispositivos**.

  Quando você habilita um encaminhador de serviços Call Home no Lenovo XClarity Administrator, o Call Home é desabilitado em todos os dispositivos gerenciados para evitar a criação de registros de problema duplicados. Se você pretende deixar de usar o XClarity Administrator para gerenciar dispositivos ou se pretende desativar Call Home em XClarity Administrator, poderá reativar Call Home em todos os dispositivos gerenciados no XClarity Administrator em vez de reativar Call Home para cada dispositivo individual posteriormente.

  Para obter mais informações, consulte Reativando call home em todos os dispositivos gerenciados na documentação online do XClarity Administrator.

Configurando a notificação de problema automática em um provedor de serviços preferencial

É possível configurar Lenovo XClarity Administrator para enviar automaticamente arquivos de diagnóstico para um conjunto específico de dispositivos gerenciados ao provedor de serviços preferencial (incluindo o Suporte Lenovo utilizando Call Home) quando determinados eventos são recebidos de dispositivos gerenciados (como um erro de memória irrecuperável) para que o problema possa ser resolvido.

Antes de iniciar

Atenção: Você deve aceitar a Instrução de privacidade da Lenovo para poder transferir dados para o Suporte Lenovo.

Verifique se todas as portas que são necessárias para XClarity Administrator (incluindo as portas necessárias para call home) estão disponíveis antes de configurar um encaminhador de serviços. Para obter mais informações sobre portas, consulte Disponibilidade de porta na documentação online do XClarity Administrator.

Verifique se existe uma conexão com os endereços da Internet exigidos pelo provedor de serviço.

Se você optar por usar o Suporte da Lenovo, verifique se existe uma conexão com os endereços da Internet exigidos pelo Call Home. Para obter informações sobre firewalls, consulte Firewalls e servidores proxy na documentação online do XClarity Administrator.

Se o XClarity Administrator acessa a Internet com um proxy HTTP, verifique se o servidor proxy está configurado como um proxy não encerrando. Para obter mais informações sobre como configurar o proxy, consulte Configurando o acesso à redeConfigurando o acesso à rede na documentação online do XClarity Administrator.

Sobre esta tarefa

Um *encaminhador de serviços* define informações sobre para onde enviar os arquivos de dados de serviço quando ocorrer um evento que permite manutenção. Você pode definir até 50 encaminhadores de serviço.

Para cada encaminhador de serviço, é possível transferir automaticamente dados de serviço ao Suporte Lenovo (denominado *Call Home*), ao Recurso de Upload da Lenovo ou a outro provedor de serviço usando o SFTP. Para obter informações sobre a configuração de um encaminhador de serviço para o Call Home, consulte Configurando uma notificação de problema automática em Suporte da Lenovo (Call Home) e Configurando a notificação de problema automática em um provedor de serviços preferencial. Para obter

informações sobre a configuração de um encaminhador de serviço para o Recurso de Upload da Lenovo, consulte Configurando a notificação automática de problemas para o Recurso de Upload da Lenovo na documentação online do XClarity Administrator.

Se um encaminhador de serviço estiver configurado e ativado para SFTP, o XClarity Administrator coletará *automaticamente* os dados de serviço e transferirá os arquivos de serviço ao site de SFTP especificado do provedor de serviço preferencial.

Para servidores com XCC2, o XClarity Administrator salva dados de serviço em dois arquivos no repositório.

- **Arquivo de serviço**. (.zip) Este arquivo contém informações de serviço e inventário em um formato acessível com facilidade. Esse arquivo é enviado automaticamente ao provedor de serviço preferencial quando ocorre um evento que permita manutenção.
- **Arquivo de depuração**. (.tzz) O arquivo contém todas as informações de serviço, inventário e logs de depuração para uso pelo Lenovo Support. É possível enviar esse arquivo manualmente ao Lenovo Support se forem necessárias informações adicionais para resolver um problema.

Para outros dispositivos, o XClarity Administrator salva dados de serviço (por exemplo, informações de serviço, inventário e logs de depuração) em um único arquivo de serviço no repositório. Esse arquivo é enviado ao provedor de serviço preferencial quando ocorre um evento que permita manutenção.

Nota: Se vários encaminhadores de serviço SFTP forem configurados para o mesmo dispositivo, somente um deles transferirá dados de serviço. O endereço e a porta usados dependem do encaminhador de serviço que é acionado primeiro.

Procedimento

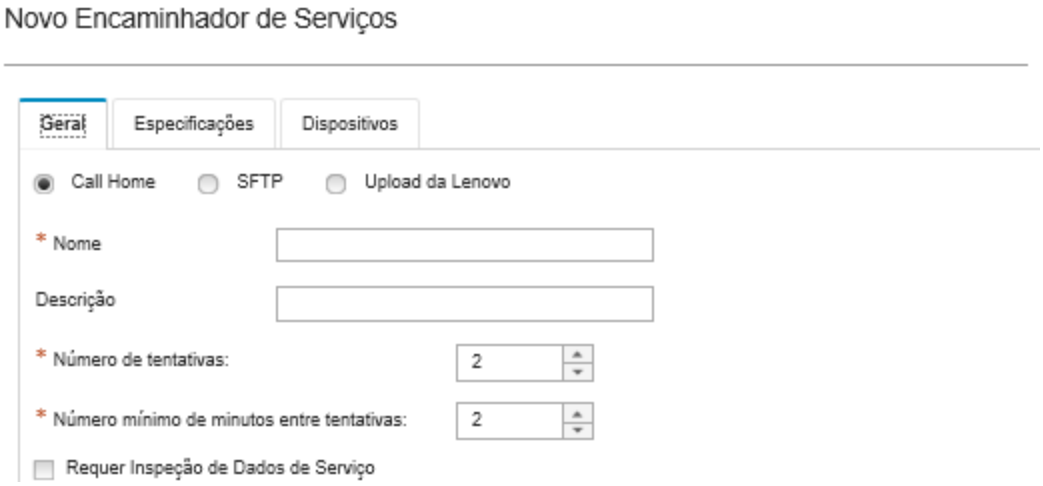
Conclua as seguintes etapas para configurar e ativar um encaminhador de serviços.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.

Etapa 2. Clique em **Encaminhadores de Serviços** na navegação esquerda para exibir a página Encaminhadores de Serviços.

Etapa 3. Clique no ícone **Criar Encaminhador de Serviço** ( ) para exibir a caixa de diálogo Novo Encaminhador de Serviço.

Etapa 4. Clique na guia **Geral**.



1. Selecione **SFTP** para o encaminhador de serviço:
2. Insira o nome de encaminhador de serviços e uma descrição.

3. Especifique o número de novas tentativas de notificação automática. O padrão é 2.
4. Especifique o número mínimo de minutos entre tentativas. O padrão é 2.
5. (Opcional) Clique em **Requer Inspeção de Dados de Serviço** se desejar examinar os arquivos de serviço antes que eles sejam transferidos e, opcionalmente, especifique o endereço de e-mail do contato que será notificado quando os arquivos de serviço precisarem ser inspecionados.

Etapa 5. Clique na guia **Específico** e preencha as seguintes informações:
- Endereço IP e número da porta do servidor SFTP
- ID do usuário e senha para autenticação no servidor SFTP

Etapa 6. Clique na guia **Dispositivo** e selecione os dispositivos gerenciados e os grupos de recursos para os quais esse encaminhador de serviços deve encaminhar dados de serviço.

Dica: Para encaminhar dados de serviço para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Corresponder todos os dispositivos**.

Etapa 7. Clique em **Criar**. O encaminhador de serviço é incluído na página Serviço e Suporte

Etapa 8. Na página Serviço e Suporte, selecione **Ativar** na coluna **Status** para ativar o encaminhador de serviços.

Etapa 9. Para evitar que os eventos que permitem manutenção que estão na lista de eventos excluídos abram relatórios de problemas automaticamente, selecione **Não** ao lado da pergunta **Deseja que os eventos excluídos abram relatórios de problemas?**.

Etapa 10. Selecione o encaminhador de serviço e clique em **Testar Encaminhadores de Serviço** para gerar um evento de teste para o encaminhador de serviço e verifique se XClarity Administrator pode se comunicar com cada provedor de serviço.

Nota: O encaminhador de serviços deve ser ativado antes de ser testado.

Depois de concluir

Na página Serviço e Suporte, também é possível executar as ações a seguir:

- Se **Requer Inspeção de Dados de Serviço** for selecionado e um evento que permite manutenção tiver sido recebido de um dos dispositivos gerenciados associados ao encaminhador de serviço, você deverá inspecionar os arquivos de serviço antes que sejam encaminhados para o provedor de serviço. Para obter mais informações, consulte Inspecionando arquivos de diagnóstico na documentação online do XClarity Administrator.
- Modifique as informações do encaminhador de serviços clicando em **Encaminhadores de Serviço** na navegação esquerda e clicando no ícone **Editar Encaminhador de Serviço** ( ).
- Habilite ou desabilite um provedor de serviço, clicando em **Encaminhadores de Serviços** e selecionando **Habilitar** ou **Desabilitar** na coluna **Status**.
- Exclua o provedor de serviço clicando em **Encaminhadores de Serviços** e clicando no ícone **Excluir Encaminhador de Serviço** ( ).
- Defina as informações de contato e o local do suporte para um dispositivo gerenciado específico clicando em **Ações de terminal** na navegação esquerda, selecionando o dispositivo e, em seguida, clicando no ícone **Criar perfil de contato** ( ) ou no ícone **Editar perfil de contato** ( ). As informações de contato e local para o dispositivo gerenciado estão incluídas no registro de problemas criado por call home no Centro de Suporte da Lenovo. Se informações exclusivas de contato e local forem especificadas para um dispositivo gerenciado, essas informações serão incluídas no registro de problemas. Caso contrário, as informações gerais especificadas para a configuração de call home do XClarity Administrator (na página **Configuração de Call Home** ou na página **Encaminhadores de Serviço**) serão usadas. Para obter mais

informações, consulte Definindo os contatos de suporte de um dispositivo na documentação online do XClarity Administrator.

- Colete dados de serviço para um dispositivo específico clicando em **Ações de terminal**, selecionando o dispositivo e, em seguida, clicando no ícone **Coletar Dados de Serviço** (). Para obter mais informações, consulte Coletando e baixando arquivos de diagnóstico de um dispositivo na documentação online do XClarity Administrator.

Para obter mais informações sobre essas tarefas de serviço e suporte, consulte Trabalhando com serviço e suporte na documentação online do XClarity Administrator.

Conectando o XClarity Administrator como um hub ao portal TruScale

É possível conectar o Lenovo XClarity Administrator como um hub de gerenciamento ao portal Lenovo TruScale.

Antes de iniciar

Atenção: Estas etapas de configuração são destinadas apenas a representantes do Serviço Lenovo.

Procedimento

Para conectar o XClarity Administrator ao portal TruScale, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Administração → Configuração do hub** para exibir a página Configuração do hub.

Etapa 2. Crie uma chave de registro clicando em **Gerar solicitação de registro**. A caixa de diálogo Gerar solicitação de registro é exibida.

Etapa 3. Clique em **Copiar para área de transferência** para copiar a chave de registro e, em seguida, feche a caixa de diálogo.

Etapa 4. Clique em **Instalar chave de registro** para exibir a caixa de diálogo Instalar chave de registro.

Etapa 5. Cole a chave de registro no campo **Chave de registro**.

Etapa 6. Clique em **Enviar**.

Depois de concluir

É possível desinstalar a chave de registro clicando em **Redefinir Configuração**.

Fazer backup, restaurar e migrar dados e configurações do sistema

É possível usar o Lenovo XClarity Administrator para fazer backup e restaurar dados e configurações do sistema e os arquivos importados como imagens do sistema operacional, firmware é atualizado e drivers de dispositivo do SO.

Fazendo backup do Lenovo XClarity Administrator

Se você já possui procedimentos de backup para hosts virtuais, assegure-se de que seus procedimentos incluam o Lenovo XClarity Administrator.

Antes de iniciar

Atenção: Certifique-se de notificar todos os usuários ativos antes de iniciar o procedimento de backup. O XClarity Administrator é desativado durante o procedimento para evitar que os dados sejam modificados.

Portanto, não é possível acessar o XClarity Administrator enquanto o procedimento de backup está em execução.

O certificado da Autoridade de Certificação deve ser baixado do dispositivo virtual XClarity Administrator e importado para o seu navegador da Web (consulte Importando o certificado da autoridade de certificação em um navegador da Web).

Certifique-se de que todos os trabalhos em execução sejam concluídos e não haja nenhum trabalho pendente. Se houver trabalhos em execução, será possível interrompê-los e continuar a criar o backup.

Certifique-se também de que os servidores DNS estejam configurados corretamente. Caso contrário, SMTP e NTP talvez não funcionem corretamente depois da restauração do backup.

Certifique-se de que haja espaço em disco suficiente disponível no servidor de gerenciamento para o backup. Se não houver, libere espaço em disco excluindo recursos do XClarity Administrator, incluindo backups anteriores, que não são mais necessários (consulte Gerenciando espaço em disco) ou crie um novo backup sem incluir imagens do sistema operacional, atualização de firmware e drivers de dispositivo do SO.

Verifique se a implantação do SO está configurada na interface de rede apropriada, eth1 ou eth0, se você deseja fazer backup de imagens do SO (consulte Configurando o acesso à rede).

Sobre esta tarefa

Sempre faça backup do XClarity Administrator após o processo de configuração inicial e depois de fazer alterações significativas de configuração, incluindo:
- Antes de atualizar o XClarity Administrator
- Ao gerenciar um novo chassi ou servidores de rack
- Ao adicionar usuários a XClarity Administrator
- Quando você cria e implementa novos padrões de configuração

Faça backup do XClarity Administrator regularmente.

É recomendável fazer o download de backups para seu sistema local. Se o sistema operacional do host desligar inesperadamente, não será possível autenticar com XClarity Administrator após o sistema operacional do host ser reiniciado. Para resolver esse problema, restaure XClarity Administrator do backup mais recente no sistema local (consulte Restaurando o Lenovo XClarity Administrator).

Procedimento

Conclua as etapas a seguir para fazer backup do XClarity Administrator.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Backup e restauração de dados**. A página de Backup e restauração dos dados é exibida.

Etapa 2. Clique no ícone **Backup** (). A caixa de diálogo Backup de dados e configurações será exibida.

Etapa 3. Forneça uma descrição para este backup.

Etapa 4. Escolha o local onde você deseja criar o backup. Pode ser o repositório local ou um compartilhamento remoto.

O backup é criado no repositório local por padrão. É possível copiar um backup do repositório local em um compartilhamento remoto clicando no ícone **Copiar backup** ().

Se você escolher um compartilhamento remoto, o backup será criado primeiro no repositório local. Em seguida, o backup será copiado no compartilhamento remoto selecionado, e a cópia

local será excluída. Para obter mais informações, consulte Gerenciando o compartilhamentos remotos.

Etapa 5. Como opção, selecione para incluir imagens do sistema operacional, atualizações de firmware e drivers de dispositivo do SO.

Etapa 6. Especifique a senha de criptografia para o backup.

Atenção: Registre a senha de criptografia. A senha é necessária para restaurar o backup para essa ou outra instância do XClarity Administrator. Se você esquecer a senha, não é possível recuperá-lo.

Etapa 7. Clique em **Backup** para fazer backup dos dados e das configurações imediatamente ou clique em **Programação** para programar este backup para ser executado posteriormente.

Atenção: Se você optar por fazer backup imediatamente, não feche nem atualize a guia do navegador da Web nem a janela antes que o backup seja concluído. Caso contrário, o backup não poderá ser gerado.

Gerar o backup pode levar alguns minutos. Uma barra de progresso mostra o status do trabalho.

Se você tiver optado por criar o backup em um compartilhamento remoto, poderá monitorar o andamento na página Trabalhos (consulte Monitorando trabalhos).

Se você programar um backup, o servidor de gerenciamento será desligado temporariamente durante o processo de backup. Depois que o servidor de gerenciamento voltar a ficar online, você poderá monitorar o status do processo de backup na página Trabalhos.

Etapa 8. Faça login no XClarity Administrator para continuar a gerenciar dispositivos.

Depois de concluir

Na página Backup e restauração dos dados, você pode realizar as seguintes ações:

- Copie os backups do XClarity Administrator de ou em um compartilhamento remoto clicando no ícone **Copiar backup** ( ).
- Exclua backups selecionados do repositório local ou compartilhamentos remotos que não são mais necessários, clicando no ícone **Excluir Backup** ( ).
- Restaurar dados e configurações de sistema para este servidor de gerenciamento (consulte Restaurando o Lenovo XClarity Administrator).
- Importar ou exportar backups do sistema local, clicando no ícone **Importar backup** ( ) ou **Exportar backup** ( ), respectivamente.
- Move o backup selecionado para uma nova instância do XClarity Administrator (consulte Migrar dados e configurações do sistema para outra instância do XClarity Administrator).

Restaurando o Lenovo XClarity Administrator

É possível usar dados de backup e configurações para restaurar o Lenovo XClarity Administratorpara um estado anterior.

Antes de iniciar

Atenção: Certifique-se de notificar todos os usuários ativos antes de iniciar o procedimento de backup. O XClarity Administrator é desativado durante o procedimento para evitar que os dados sejam modificados.

Portanto, não é possível acessar o XClarity Administrator enquanto o procedimento de backup está em execução.

Baixe o certificado da Autoridade de Certificação do dispositivo virtual do XClarity Administrator e importe o certificado para o seu navegador da Web (consulte Importando o certificado da autoridade de certificação em um navegador da Web).

Certifique-se de que todos os trabalhos em execução sejam concluídos e não haja nenhum trabalho pendente.

É possível restaurar um backup apenas na mesma versão do XClarity Administrator que foi utilizada para criar o backup.

Sobre esta tarefa

Atenção:

- Todas as alterações desde quando o backup foi criado serão perdidas.
- Para restaurar dados, o dispositivo virtual é redefinido como seu estado original limpo. Todas as configurações atuais, inventário do dispositivo e arquivos (imagens do sistema operacional, as atualizações de firmware e drivers de dispositivo do SO) são excluídos antes de restauração de dados no backup. Dados e as configurações no backup não são misturar com o dispositivo virtual dados atuais e as configurações. Se você optar por não restaurar inventário do dispositivo, imagens do sistema operacional, as atualizações de firmware e drivers de dispositivo do SO, apenas os dados XClarity Administrator padrão estão presentes após a conclusão da operação de restauração.

Restaurar um backup não excluir backups na instância XClarity Administrator.

Restaurar um backup não mudarão dados ou configurações nos dispositivos gerenciados. Por exemplo, se você cancelar o gerenciamento de um dispositivo e, em seguida, restaurar um backup anterior quando o dispositivo ainda seja gerenciado no XClarity Administrator, você pode ter problemas de conectividade com o dispositivo após a conclusão da operação de restauração. Da mesma forma, se você gerenciar um dispositivo e, em seguida, restaurar um backup anterior quando o dispositivo ainda não for gerenciado, talvez seja necessário modificar manualmente a configuração do dispositivo para desfazer o status gerenciado ou usar a opção **Forçar** ao tentar gerenciá-lo no XClarity Administrator novamente.

Procedimento

Conclua as etapas a seguir para restaurar o XClarity Administrator.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Administração → Backup e restauração de dados**. A página de Backup e restauração dos dados é exibida.

Etapa 2. Se você exportado o pacote de backup para seu sistema local e excluídos-lo do XClarity Administrator, conclua as seguintes etapas.

a. Na página Backup e restauração de dados, clique no ícone **Importar backup** () para exibir a caixa de diálogo Importar backup.

b. Clique em **Procurar** para obter o backup exportado da fonte uma instância XClarity Administrator.

c. Clique em **Importar** para fazer upload do backup no XClarity Administrator.

Importar o backup pode levar alguns minutos. Uma barra de progresso mostra o status do trabalho.

Atenção: Se você fechar ou atualizar a guia do navegador da Web ou a janela antes que a carga seja concluída, o processo poderá falhar.

d. Quando a importação for concluída, especifique a passphrase de criptografia para o backup.

Nota: Se você não tiver a senha de criptografia, será necessário criar um novo backup na fonte de XClarity Administrator (consulte Fazendo backup do Lenovo XClarity Administrator).

Etapa 3. Selecione o backup a ser restaurado e clique no ícone **Restaurar Backup** (). A caixa de diálogo Restore Data é exibida.

Etapa 4. Especifique a senha de criptografia para o backup.

Etapa 5. Clique em **Confirmar**.

Etapa 6. Na caixa de diálogo Confirm Data Restore, verifique se todas as informações na caixa de diálogo estão corretas.

Etapa 7. Na caixa de diálogo Restore Options, é possível optar por importar imagens do sistema operacional, atualizações de firmware, Drivers do dispositivo do SO, configurações de rede e inventário de dispositivo.

Atenção: Certifique-se de ter lido cuidadosamente todos aviso que são exibidos na caixa de diálogo.

Etapa 8. Clique em **Confirmar** para começar a restauração de dados.

Restaurar as configurações e dados pode levar alguns minutos. Uma barra de progresso mostra o status do trabalho.

Quando o processo de restauração de dados for concluído, você está redirecionadas para a página de login.

Atenção: Se você fechar ou atualizar a guia do navegador da Web ou a janela antes que o processo seja concluído, o processo poderá falhar.

Etapa 9. Faça login no XClarity Administrator para continuar a gerenciar dispositivos.

Migrar dados e configurações do sistema para outra instância do XClarity Administrator

Você pode migrar os dados armazenados em backup do sistema e as configurações para um novo Lenovo XClarity Administrator que esteja na mesma ou em outra rede.

Antes de iniciar

O servidor de gerenciamento de destino deve ser uma *nova* instância do XClarity Administrator com a mesma versão do servidor de gerenciamento que foi usado para criar o backup e deve estar no Assistente de configuração inicial, sem nenhuma etapa concluída. Para obter mais informações, consulte Instalando e configurando o XClarity Administrator na documentação online do XClarity Administrator.

Certifique-se de notificar todos os usuários ativos antes de iniciar o procedimento de backup. O XClarity Administrator é desativado durante o procedimento para evitar que os dados sejam modificados. Portanto, não é possível acessar o XClarity Administrator enquanto o procedimento de backup está em execução.

Baixe o certificado da Autoridade de Certificação do XClarity Administrator e importe o certificado para o seu navegador da Web (consulte Gerenciando espaço em disco na documentação online do XClarity Administrator).

Backups do repositório de backup do servidor de gerenciamento de origem não são migrados para o servidor de gerenciamento de destino. Antes de migrar dados e configurações, exporte os backups necessários para seu sistema local.

Sobre esta tarefa

As alterações para o servidor de gerenciamento de origem depois que o backup foi criado não são migradas para o servidor de gerenciamento de destino.

Restaurar um backup não mudarão dados ou configurações nos dispositivos gerenciados. Por exemplo, se você cancelar o gerenciamento de um dispositivo e, em seguida, restaurar um backup anterior quando o dispositivo ainda seja gerenciado no XClarity Administrator, você pode ter problemas de conectividade com o dispositivo após a conclusão da operação de restauração. Da mesma forma, se você gerenciar um dispositivo e, em seguida, restaurar um backup anterior quando o dispositivo ainda não for gerenciado, talvez seja necessário modificar manualmente a configuração do dispositivo para desfazer o status gerenciado ou usar a opção **Forçar** ao tentar gerenciá-lo no XClarity Administrator novamente.

Notas: Ao executar o XClarity Administrator como um contêiner, os volumes que foram criados no host para um contêiner podem ser usados como volumes por outro contêiner. Depois que os volumes forem vinculados ao novo contêiner (destino), eles não poderão mais ser usados pelo contêiner inicial (de origem).

1. Configurando o arquivo `docker-compose.yml` para que o contêiner de destino use o mesmo endereço IP e o nome do contêiner de origem.
2. Pare o contêiner de origem usando o comando a seguir.
   `docker-compose -p ${CONTAINER_NAME} down`
3. Inicie o contêiner de destino usando o comando a seguir, em que <*env_filename*> é o nome do arquivo de variáveis do ambiente. Quando o contêiner de destino for iniciado, os volumes serão vinculados ao contêiner de destino do XClarity Administrator e o XClarity Administrator usará dados do sistema e as configurações desses volumes.
   COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file` <*ENV_FILENAME*> `up -d`

Procedimento

Conclua as etapas a seguir para restaurar o XClarity Administrator.

Etapa 1. Se origem e destino de XClarity Administrator estiverem na mesma rede, conclua as seguintes etapas.

a. Na barra de menu do XClarity Administrator, clique em **Administração → Backup e restauração de dados**. A página de Backup e restauração dos dados é exibida.

b. Clique no ícone **Enviar Backup** () para exibir a caixa de diálogo Enviar dados.

c. Especifique o endereço IP atual do destino de XClarity Administrator.

d. Clique em **Continuar** para fazer upload de backup para o XClarity Administrator de destino.

Carregar o backup pode levar alguns minutos. Uma barra de progresso mostra o status do trabalho.

Atenção: Se você fechar ou atualizar a guia do navegador da Web ou a janela antes que a carga seja concluída, o pacote não poderá ser carregado.

Etapa 2. Se origem e destino XClarity Administrator *não estão* na mesma rede, conclua as seguintes etapas.

a. Na barra de menu da origem XClarity Administrator, clique em **Administration → Back Up e Restore Data**. Na página Backup e restauração de dados, clique no ícone **Exportar backup** () para exportar o backup para o sistema local.

Exportar o backup pode levar alguns minutos.

b. Copie o backup exportado do servidor de gerenciamento de origem para um sistema na mesma rede que o servidor de gerenciamento de destino

c. Na página do assistente do destino XClarity Administrator, clique no ícone **Importar backup** () para exibir a caixa de diálogo Importar pacote de dados.

d. Clique em **Procurar** para obter o backup exportado da fonte de XClarity Administrator.

e. Clique em **Upload** para importar o backup para o destino XClarity Administrator.

Importar o backup pode levar alguns minutos. Uma barra de progresso mostra o status do trabalho.

Atenção: Se você fechar ou atualizar a guia do navegador da Web ou a janela antes que a carga seja concluída, o processo poderá falhar.

Etapa 3. Quando a importação for concluída, especifique a passphrase de criptografia para o backup.

Nota: Se você não tiver a senha de criptografia, será necessário criar um novo backup na fonte de XClarity Administrator (consulte Fazendo backup do Lenovo XClarity Administrator.

Etapa 4. Na caixa de diálogo Confirm Data Restore, verifique se todas as informações estão corretas.

Etapa 5. Clique em **Confirmar** para iniciar o carregamento de dados do sistema e as configurações.

Etapa 6. Na caixa de diálogo Restore Options, é possível optar por importar imagens do sistema operacional, atualizações de firmware, Drivers do dispositivo do SO, configurações de rede e inventário de dispositivo.

Atenção: Certifique-se de ter lido cuidadosamente todos aviso que são exibidos na caixa de diálogo.

Etapa 7. Se você escolheu importar configurações de rede ou inventário do dispositivo, desligue o servidor de gerenciamento de origem da fonte de XClarity Administratorclicando em **Administration → Shutdown Management Server → Shutdown** .

Confirme se o dispositivo virtual de origem foi desligado antes de continuar.

Etapa 8. No XClarity Administrator de destino, clique em **Confirmar** para iniciar o carregamento de dados e as configurações do pacote

Se você escolheu importar configurações de rede, após a migração os endereços IP da fonte de XClarity Administratorreatribuído no destino de XClarity Administrator.

Atenção: Se a fonte de XClarity Administratorusa DHCP, você deve ligar o destino de XClarity Administratorendereços MAC para a fonte de correspondente XClarity Administratorendereços IP no servidor DHCP. Aguarde pelo menos 15 minutos após o servidor DHCP é alterado antes de continuar.

Etapa 9. Aguarde até a carga de dados e as configurações da barra de progresso do pacote para ser concluída.

Quando o processo de migração de dados for concluído, você está redirecionadas para a página de login.

Atenção: Se você fechar ou atualizar a guia do navegador da Web ou a janela antes que a carga seja concluída, o processo poderá falhar.

Etapa 10. Faça login no destino XClarity Administratorpara continuar a gerenciar dispositivos.

Gerenciando espaço em disco

É possível gerenciar a quantidade de espaço em disco usada pelo Lenovo XClarity Administrator movendo arquivos de dados grandes que não são necessários imediatamente para um compartilhamento remoto ou excluindo recursos que não são mais necessários.

Sobre esta tarefa

Para determinar quanto espaço em disco está sendo utilizado atualmente, clique em **Painel** na barra de menu do XClarity Administrator. O uso de espaço em disco no repositório e compartilhamentos remotos está listado na seção XClarity Administrator Atividade.

Procedimento

Conclua uma ou mais das etapas a seguir para liberar espaço em disco movendo arquivos para um compartilhamento remoto e excluindo recursos desnecessários.

- **Excluir recursos desnecessários**

  É possível excluir rapidamente arquivos do repositório local que não são mais necessários concluindo as etapas a seguir.

  1. Na barra de menu do XClarity Administrator, clique em **Administração → Limpeza de disco** para exibir a página Limpeza de Disco.
  2. Selecione os arquivos que deseja excluir. O cabeçalho da seção identifica a quantidade de espaço que será liberada quando os arquivos forem excluídos.
     - **Arquivos relacionados do sistema operacional**

       É possível excluir imagens do SO, arquivos de opção de inicialização e arquivos de software.
     - **Atualizações de firmware**

       É possível excluir arquivos de carga útil para todos os drivers de dispositivo do SO associados aos UpdateXpress System Packs (UXSPs) e drivers de dispositivo individuais que estão no estado Baixado.

       É possível excluir arquivos de carga útil para atualizações de firmware individuais que estão no estado Baixado e não são usadas em uma política de conformidade de firmware.

       É possível excluir arquivos de carga útil para atualizações do servidor de gerenciamento que estão no estado Baixado.

       Nota: Quando o repositório das atualizações de firmware está localizado em um compartilhamento remoto, não é possível usar a função de limpeza de disco para excluir atualizações de firmware individuais e UXSPs.
     - **Arquivos de dados de serviço**

       Quando ocorre um evento de serviço em um dispositivo, os dados de serviço são coletados automaticamente para esse dispositivo. Os dados de serviço são capturados automaticamente para o servidor de gerenciamento sempre que ocorre uma exceção no XClarity Administrator. É recomendável excluir periodicamente esses arquivos se o XClarity Administrator e os dispositivos gerenciados estiver funcionando sem problemas.

       Quando as atualizações do servidor de gerenciamento são aplicadas com êxito, os arquivos de atualização são removidos automaticamente do repositório.
  3. Clique em **Excluir Selecionado**.
  4. Revise a lista de arquivos selecionados e clique em **Excluir**.

- **Mova os pacotes de atualização de firmware para um repositório remoto**

  Por padrão, o Lenovo XClarity Administrator usa um repositório local (interno) para armazenar atualizações de firmware. É possível liberar o espaço em disco que está disponível para o repositório local do XClarity Administrator usando um compartilhamento remoto montado no SSH File System (SSHFS) como repositório remoto. É possível então usar arquivos de atualização de firmware diretamente do repositório remoto para manter a conformidade de firmware em seus dispositivos. Para obter mais informações, consulte Usando um repositório remoto para atualizações de firmware.

  Ao alterar o local do repositório de atualizações de firmware, é possível optar por copiar todas as atualizações de firmware do repositório original no novo repositório.

  Os arquivos de atualização de firmware no repositório original *não* são limpos automaticamente depois de alternar locais.

  Dica: O repositório de atualizações remotas pode ser compartilhado por vários servidores de gerenciamento do XClarity Administrator.

  Para mover atualizações de firmware para um repositório de atualizações de firmware remotas, conclua as etapas a seguir.

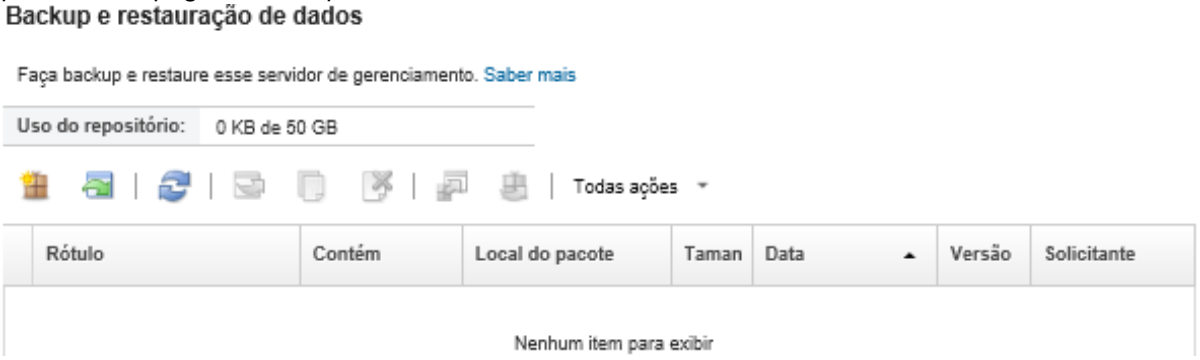
  1. Adicione um compartilhamento remoto XClarity Administrator (consulte Gerenciando o compartilhamentos remotos).
  2. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Repositório**. A página Repositório das Atualizações de Firmware é exibida.
  3. Clique em **Todas as Ações → Alternar local do repositório** para exibir a caixa de diálogo Alternar Local do Repositório.
  4. Selecione o compartilhamento remoto que você acabou de criar na lista suspensa **Local do repositório**.
  5. Selecione **Copiar pacotes de atualização do repositório atual no novo repositório** para copiar arquivos de atualização de firmware para o novo local do repositório antes de alternar o local do repositório.
  6. Clique em **OK**.

     Um trabalho é criado para copiar pacotes de atualização de firmware para o novo repositório. Você pode monitorar o andamento do trabalho clicando em **Monitoramento → Trabalhos** na barra de menus do XClarity Administrator.
  7. Limpe os arquivos de atualização de firmware no repositório local.
     a. Alterne o local para o repositório local clicando em **Todas as Ações → Alternar local do repositório**, selecione o **Repositório Local** para o local do repositório e, em seguida, clique em **OK**.
     b. Clique na guia **Atualizações Individuais**, clique na caixa de seleção select-all na tabela para selecionar todas as atualizações de firmware e, em seguida, clique no ícone **Excluir pacotes de atualização completas** ()
     c. Clique na guia **UpdateXpress System Pack (UXSP)**, clique na caixa de seleção select-all na tabela para selecionar todos os UXSPs e, em seguida, clique no ícone **Excluir UXSP e política associada** ()
     d. Alterne o local de volta para o repositório remoto clicando em **Todas as Ações → Alternar local do repositório**, selecione o novo repositório remoto para o local do repositório e, em seguida, clique em **OK**.
- **Mover XClarity Administrator backups para um compartilhamento remoto**

É possível liberar espaço em disco que está disponível para o repositório local do XClarity Administrator movendo backups do XClarity Administrator para um compartilhamento remoto. No entanto, não é possível usar os arquivos diretamente no compartilhamento remoto. Para usar os arquivos, você deverá movê-los de volta para o repositório local XClarity Administrator. Para obter mais informações sobre compartilhamentos remotos, consulte Gerenciando o compartilhamentos remotos.

Importante: É recomendável fazer download de backups para seu sistema local ou copiar os backups em um compartilhamento remoto antes de excluir os backups em XClarity Administrator.

1. Na barra de menu XClarity Administrator, clique em **Administration → Back Up and Restore Data** para exibir a página Back Up and Restore Data.



   A coluna **Local do pacote** identifica se o backup está armazenado localmente no repositório local do XClarity Administrator ou em um compartilhamento remoto.

2. Selecione o backup e clique no ícone **Copiar backup** ( ) para exibir a caixa de diálogo Copiar backup.
3. Escolha o compartilhamento remotopara armazenar o backup.
4. Clique em **Copiar**.
5. Monitore o andamento da cópia na página Trabalhos. Quando a cópia for concluída, selecione o backup novamente e clique no ícone **Excluir backup** ( ) para exibir a caixa de diálogo Excluir backup.
6. Selecione "Local" para o local.
7. Clique em **Excluir**.

Gerenciando o compartilhamentos remotos

É possível montar compartilhamentos remotos e mover arquivos de dados grandes, como backups e atualizações de firmware do Lenovo XClarity Administrator, do repositório local para o compartilhamento remoto a fim de gerenciar o espaço em disco que está disponível para o servidor de gerenciamento.

Antes de iniciar

Ao executar o XClarity Administrator como um contêiner, os compartilhamentos remotos são montados no contêiner usando o arquivo yml durante a instalação (consulte Instalando o XClarity Administrator em ambientes baseados em VMware ESXi na documentação online do XClarity Administrator).

Ao executar o XClarity Administrator como um dispositivo virtual, você deve ter autoridade de **lxc-supervisor** para montar ou desmontar um compartilhamento remoto.

Verifique se você tem uma rede estável e de alta velocidade entre o servidor de arquivos e o XClarity Administrator.

As ações remotas não são suportadas ao executar o XClarity Administrator como um contêiner.

Sobre esta tarefa

Você deve usar compartilhamentos remotos separados para armazenar backups e atualizações de firmware do XClarity Administrator.

Não é possível usar os arquivos de backup do XClarity Administrator diretamente do compartilhamento remoto. Para usar os arquivos de backup, é necessário movê-los de volta para o repositório local.

Atualmente, apenas o SSHFS é suportado.

Procedimento

Para adicionar um compartilhamento remoto ao executar o XClarity Administrator como um dispositivo virtual, execute as etapas a seguir.

1. Na barra de menu do XClarity Administrator, clique em **Administração → Compartilhamento remoto**. A página Compartilhamento remoto é exibida.
2. Clique no ícone **Criar** ( ) para criar um compartilhamento remoto. A caixa de diálogo Criar compartilhamento remoto é exibida.
3. Especifique o endereço IP do servidor de arquivos que hospeda o compartilhamento remoto.
4. Especifique as credenciais armazenadas a serem usadas para acessar o compartilhamento remoto.

   Dica: Para criar uma credencial armazenada, consulte Gerenciando credenciais compartilhadas.
5. Especifique o ponto de montagem (diretório local) no servidor de gerenciamento a ser usado para montar o compartilhamento remoto.

   Importante: O caminho deve começar com "/mnt".
6. Especifique o diretório compartilhado (caminho do servidor remoto) a ser montado como o compartilhamento remoto no servidor de gerenciamento.
7. Clique em **Criar**.

Depois de concluir

- Desmonte o compartilhamento remoto selecionando-o e clicando no ícone **Excluir** ( ).
- Mova os arquivos de backup do XClarity Administrator para e de um compartilhamento remoto (consulte Gerenciando espaço em disco).
- Configure o XClarity Administrator para usar um compartilhamento remoto como o repositório das atualizações de firmware (consulte Usando um repositório remoto para atualizações de firmware).

Alterando o idioma da interface do usuário

Você pode alterar o idioma da interface do usuário depois de se conectar.

Procedimento

Na barra de título do Lenovo XClarity Administrator, clique no menu de ações do usuário (ADMIN_USER) e clique em **Alterar idioma**. Selecione o idioma que você deseja exibir e, em seguida, clique em **Fechar**.

Nota: O sistema de ajuda é exibido no mesmo idioma definido para a interface do usuário.

Desligando o XClarity Administrator

Quando o Lenovo XClarity Administrator é desligado, a conectividade com o Lenovo XClarity Administrator é perdida.

Antes de iniciar

Você deve ter autoridade **lxc-supervisor** ou **lxc-admin** para desligar um dispositivo virtual do XClarity Administrator.

Certifique-se de que não haja nenhum trabalho em execução no momento. Os trabalhos em execução são cancelados durante o processo de desligamento. Para exibir o log de trabalhos, consulte Monitorando trabalhos.

Procedimento

Conclua as etapas a seguir para desligar o Lenovo XClarity Administrator.

- **Contêineres**

  Execute os comandos a seguir para parar o contêiner.
  ```
  docker-compose -p ${CONTAINER_NAME} down
  ```
- **Dispositivos virtuais**
  1. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Desligar Servidor de Gerenciamento**.

     Uma caixa de diálogo de confirmação é exibida com uma lista de trabalhos que estão em execução. Quando você desliga o XClarity Administrator, os trabalhos são cancelados.
  2. Clique em **Desligar**.

Depois de concluir

Para reiniciar o XClarity Administrator após um desligamento, consulte Reiniciando o XClarity Administrator.

Reiniciando o XClarity Administrator

É possível reiniciar o Lenovo XClarity Administrator a partir da interface da Web ou do hipervisor após um desligamento.

Antes de iniciar

Você deve ter autoridade **lxc-supervisor** ou **lxc-admin** para reiniciar o XClarity Administrator.

Certifique-se de que não haja nenhum trabalho em execução no momento. Os trabalhos em execução são cancelados durante o processo de reinicialização. Para exibir o log de trabalhos, consulte Monitorando trabalhos.

Sobre esta tarefa

Há situações em que é necessário reiniciar o Lenovo XClarity Administrator:
- Ao gerar um novo certificado de servidor
- Ao fazer upload de um novo certificado de servidor

Procedimento

Conclua um dos procedimentos a seguir para reiniciar o Lenovo XClarity Administrator.

- **Contêineres**

  Execute os comandos a seguir para parar e, em seguida, iniciar o contêiner, em que <*env_filename*> é o nome do arquivo de variáveis do ambiente.
  ```
  docker-compose -p ${CONTAINER_NAME} down
  COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
  ```

- **Dispositivos virtuais**
  - Reiniciar o Lenovo XClarity Administrator a partir da interface da Web:
    1. Na barra de menus do Lenovo XClarity Administrator, clique em **Administração → Desligar Servidor de Gerenciamento**.

       Uma caixa de diálogo de confirmação é exibida com uma lista de trabalhos que estão em execução. Quando você reinicia o Lenovo XClarity Administrator, os trabalhos são cancelados.
    2. Clique em **Reiniciar**.

       Quando o Lenovo XClarity Administrator é desligado, a conectividade com o Lenovo XClarity Administrator é perdida.
    3. Aguarde alguns minutos para o Lenovo XClarity Administrator ser reiniciado e faça login novamente.
  - Reiniciar o hipervisor do Lenovo XClarity Administrator após um desligamento:
    - Microsoft Hyper-V
      1. No painel do Server Manager, clique em **Hyper-V**.
      2. Clique com o botão direito no servidor e clique em **Gerenciador Hyper-V**.
      3. Clique com o botão direito na máquina virtual e clique em **Iniciar**. Quando a máquina virtual é iniciada, os endereços IPv4 e IPv6 são listados para cada interface, conforme mostrado no exemplo a seguir.

         A porta de gerenciamento eth0 do XClarity Administrator usa um endereço IP de DHCP por padrão. No final do processo de inicialização do XClarity Administrator, é possível optar por definir um endereço IP estático para a porta de gerenciamento eth0 inserindo 1 quando solicitado, conforme mostrado no exemplo a seguir. O prompt fica disponível por 150 segundos, até o prompt de login ser exibido. Para continuar para o prompt de login sem atraso, digite x no prompt.

         Importante:

         - Ao alterar as configurações de endereço IP estáticas, você pode ter no máximo 60 segundos para inserir as novas configurações. Certifique-se de que você tenha as informações de IP necessárias antes de continuar.
           - Para as configurações de IPv4, você deve ter o endereço IP, a máscara de sub-rede e o endereço IP do gateway
           - Para as configurações de IPv6, você deve ter o comprimento de prefixo e de endereço IP
         - Se você não estiver usando um servidor DHCP, também poderá usar um arquivo de configuração para especificar as configurações de IP para a porta de gerenciamento eth0 do XClarity Administrator que deseja usar para acessar o XClarity Administrator. Para obter mais informações, consulte a seção "O que fazer a seguir" abaixo.
         - Se você alterar as configurações de endereço IP do console, o XClarity Administrator será reiniciado para aplicar as novas configurações.

- Nenhuma ação é necessária para fazer login. Ignore a mensagem de login do console. A interface do console não é para uso do cliente.
- Você poderá consultar a mensagem `TCP: eth0: Driver tem implementação GRO suspeita, o desempenho do TCP pode ser comprometido` no console do. O desempenho da máquina virtual não é afetado, e você pode ignorar esta aviso.

Atenção: Alterar o endereço IP da porta de gerenciamento do XClarity Administrator depois de gerenciar dispositivos pode fazer com que os dispositivos sejam colocados no estado offline no XClarity Administrator. Se você optar por alterar o endereço IP após a inicialização do XClarity Administrator, certifique-se de que o gerenciamento de todos os dispositivos seja cancelado antes de alterar o endereço IP.

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  ... ...
```

4. Faça login no Lenovo XClarity Administrator (consulte Efetuando login no XClarity Administrator).

– VMware ESXi

1. Conecte-se ao host por meio do VMware vSphere Client.
2. Clique com o botão direito na máquina virtual e clique em **Energia → Ligar**.
3. Clique na guia **Console**. Quando a máquina virtual é iniciada, os endereços IPv4 e IPv6 são listados para cada interface, conforme mostrado no exemplo a seguir.

   A porta de gerenciamento eth0 do XClarity Administrator usa um endereço IP de DHCP por padrão. No final do processo de inicialização do XClarity Administrator, é possível optar por definir um endereço IP estático para a porta de gerenciamento eth0 inserindo 1 quando solicitado, conforme mostrado no exemplo a seguir. O prompt fica disponível por 150 segundos, até o prompt de login ser exibido. Para continuar para o prompt de login sem atraso, digite x no prompt.

   Importante:

   - Ao alterar as configurações de endereço IP estáticas, você pode ter no máximo 60 segundos para inserir as novas configurações. Certifique-se de que você tenha as informações de IP necessárias antes de continuar.
     – Para as configurações de IPv4, você deve ter o endereço IP, a máscara de sub-rede e o endereço IP do gateway
     – Para as configurações de IPv6, você deve ter o comprimento de prefixo e de endereço IP

- Se você não estiver usando um servidor DHCP, também poderá usar um arquivo de configuração para especificar as configurações de IP para a porta de gerenciamento eth0 do XClarity Administrator que deseja usar para acessar o XClarity Administrator. Para obter mais informações, consulte a seção "O que fazer a seguir" abaixo.
- Se você alterar as configurações de endereço IP do console, o XClarity Administrator será reiniciado para aplicar as novas configurações.
- Nenhuma ação é necessária para fazer login. Ignore a mensagem de login do console. A interface do console não é para uso do cliente.
- Você poderá consultar a mensagem `TCP: eth0: Driver tem implementação GRO suspeita, o desempenho do TCP pode ser comprometido` no console do. O desempenho da máquina virtual não é afetado, e você pode ignorar esta aviso.

Atenção: Alterar o endereço IP da porta de gerenciamento do XClarity Administrator depois de gerenciar dispositivos pode fazer com que os dispositivos sejam colocados no estado offline no XClarity Administrator. Se você optar por alterar o endereço IP após a inicialização do XClarity Administrator, certifique-se de que o gerenciamento de todos os dispositivos seja cancelado antes de alterar o endereço IP.

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  ... ...
```

4. Faça login no Lenovo XClarity Administrator (consulte Efetuando login no XClarity Administrator).

Depois de concluir

Quando o Lenovo XClarity Administrator é reiniciado, ele coleta novamente o inventário de cada dispositivo gerenciado. Aguarde cerca de 30 a 45 minutos, dependendo do número de dispositivos gerenciados, antes de tentar atualizações de firmware, implantações de padrão de configuração ou implantações do sistema operacional.

Capítulo 3. Monitoramento de dispositivos e atividades

É possível monitorar seus dispositivos e atividades pelo painel, alertas, logs de auditoria e de trabalhos.

Exibindo um resumo do ambiente

O Painel exibe o status de todos os dispositivos gerenciados, uma visão geral de todas as tarefas relacionadas a fornecimento, uma informações sobre recursos e atividades do Lenovo XClarity Administrator.

Saiba mais:  XClarity Administrator: monitoramento

Procedimento

Etapa 1. Na barra de menus XClarity Administrator, clique em **Painel**.

Etapa 2. Expanda o status de hardware, o status de fornecimento ou a seção de atividades de administrador para obter mais informações sobre cada uma dessas áreas.

Exibindo um resumo do status de hardware

A área Status de hardware exibe o status de todos os dispositivos gerenciados.

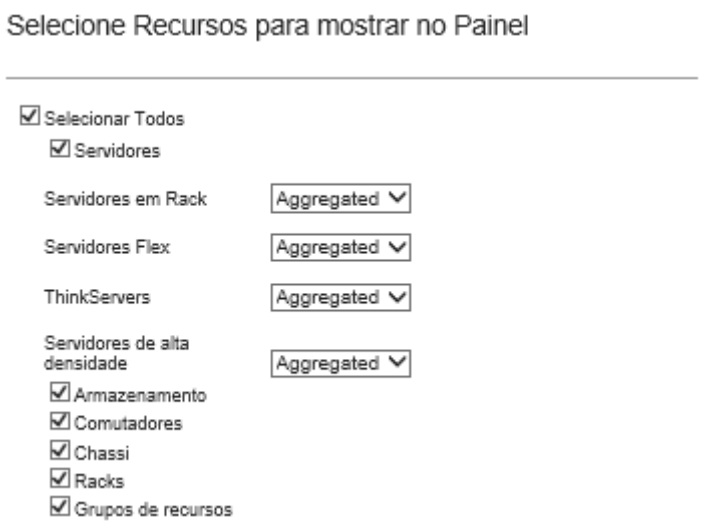
Procedimento

Para obter mais informações sobre todos os dispositivos desse tipo, clique no número listado abaixo do tipo de dispositivo.

Para exibir mais informações apenas sobre esses dispositivos desse tipo e status, clique no ícone ou no número ao lado de cada ícone de status.

- **Servidores**. Exibe o número total de servidores (nós de cálculo, servidores do rack e servidores em torre) que o XClarity Administrator gerencia, e o número de servidores com status normal, de aviso e crítico. Para obter mais informações, consulte Visualizando o status de um servidor gerenciado.
- **Armazenamento**. Exibe o número total de dispositivos de armazenamento que o XClarity Administrator gerencia, e o número de dispositivos de armazenamento com o status normal, de aviso e crítico. Para obter mais informações, consulte Exibindo o status dos dispositivos de armazenamento.
- **Comutadores**. Exibe o número total de RackSwitch e comutadores Flex System que o XClarity Administrator gerencia, bem como o número de comutadores com o status normal, de aviso e crítico. Para obter informações adicionais, veja Exibindo o status de comutadores
- **Chassi**. Exibe o número total de chassis Flex que o XClarity Administrator gerencia, e o número de chassis Flex com o status normal, de aviso e crítico. Para obter mais informações, consulte Visualizando o status de um chassi gerenciado.
- **Racks**. Exibe o número de racks criados no XClarity Administrator e o número de racks com dispositivos que têm o status normal, de aviso e crítico como seu status mais elevado. Para obter mais informações, consulte Exibindo status dos dispositivos em um rack.
- **Grupos de recursos**. Exibe o número de grupos de recursos que o XClarity Administrator gerencia e o número de grupos de recursos com dispositivos que têm normal, aviso e crítico como os status mais altos. Para obter mais informações, consulte Exibindo o status dos dispositivos em um grupo de recursos.

Para personalizar os recursos de hardware exibidos no painel, clique no ícone **Personalizar** (). É possível escolher os tipos de dispositivo que você deseja mostrar ou ocultar. É possível também escolher se deseja agregar servidores em um único resumo, exibir resumos separados para cada tipo de servidor (servidores em rack e em torre, Flex System, ThinkServer e NeXtScale) ou omitir tipos específicos de servidores.



Exibindo um resumo do status de fornecimento

A área Status de Fornecimento fornece um resumo de todas as tarefas associadas a dispositivos de fornecimento.

Procedimento

- **Padrões de Configuração**. Exibe detalhes sobre o número de servidores que têm perfis, incluindo as estatísticas a seguir.

Nota: Quando o servidor de gerenciamento não é compatível com licença, todos os valores são 0 (consulte Instalando a licença de habilitação com funcionalidade completa na documentação online do XClarity Administrator).

- O número de servidores que estão em conformidade com o perfil de servidor. É possível clicar no número para exibir a página Padrões de Configuração: Perfis de Servidor com uma lista de servidores compatíveis.
- O número de servidores que não estão em conformidade com o perfil de servidor. É possível clicar no número para exibir a página Padrões de Configuração: Perfis de Servidor com uma lista de servidores não compatíveis.
- O número de dispositivos para os quais o status de conformidade é desconhecido. É possível clicar no número para exibir a página Padrões de Configuração: Perfis de Servidor com uma lista de servidores com conformidade desconhecida.

  Nota: O status de conformidade é desconhecido, geralmente após uma implantação de perfil parcial, quando o Lenovo XClarity Administrator não coletou as informações de configuração do servidor. Atualize o inventário do servidor ou revisite a página de detalhes do perfil do servidor para forçar a coleta de informações de configuração do servidor.
- O número de servidores que estão atribuídos a um perfil de servidor. É possível clicar no número para exibir a página Padrões de Configuração: Perfis de Servidor com uma lista de servidores com perfis.
- O número de servidores que não estão atribuídos a um perfil de servidor. É possível clicar no número para exibir a página Padrões de Configuração: Padrões de Servidor com uma lista de padrões de servidor que podem ser implantados em servidores sem perfis.
- O número de padrões de servidor que estão sendo implantados.

Para exibir dados de tendência de padrões de configuração, clique em **Exibir dados de tendência** (consulte Monitorando tendências no status de fornecimento).

Para obter mais informações sobre padrões de configuração e perfis de servidor, consulte Configurando servidores com padrões de configuração.

- **Imagens do sistema operacional**. Exibe detalhes sobre implantações do sistema operacional, incluindo as estatísticas a seguir.

  Nota: Quando o servidor de gerenciamento não é compatível com licença, todos os valores são 0 (consulte Instalando a licença de habilitação com funcionalidade completa na documentação online do XClarity Administrator).

  - O número de imagens do SO no repositório. É possível clicar no número para exibir a página Implantar sistemas operacionais: gerenciar imagens de SO com uma lista de sistemas operacionais.
  - O número de implantações atuais do SO que estão em andamento. É possível clicar no número para exibir a página Implantar sistemas operacionais: implantar imagens de SO com uma lista de dispositivos para os quais um sistema operacional está sendo instalado.
- **Atualizações de firmware**. Exibe detalhes sobre atualizações de firmware, incluindo as estatísticas a seguir.
  - O número de dispositivos compatíveis. É possível clicar no número para exibir a página Atualizações de firmware: Aplicar/Ativar com uma lista de dispositivos compatíveis.
  - O número de dispositivos que não são compatíveis. É possível clicar no número para exibir a página Atualizações de firmware: Aplicar/Ativar com uma lista de dispositivos não compatíveis.
  - O número de dispositivos que não têm uma política de conformidade de firmware atribuída. É possível clicar no número para exibir a página Atualizações de firmware: Aplicar/Ativar com uma lista de dispositivos sem uma política de conformidade.

Nessa página, é possível atribuir a cada dispositivo uma política de conformidade de firmware selecionando uma política na coluna **Política de conformidade atribuída**.

- O número de dispositivos para os quais as atualizações não são permitidas. É possível clicar no número para exibir a página Atualizações de Firmware: Aplicar/Ativar com uma lista de dispositivos para os quais as atualizações não são permitidas.
- O número de atualizações que estão em andamento.
- O número de dispositivos com firmware pendente. É possível clicar no número para exibir a página Atualizações de Firmware: Aplicar/Ativar com uma lista de dispositivos para os quais as atualizações estão com ativação pendente.

Para exibir dados de tendência de atualizações de firmware, clique em **Exibir dados de tendência** (consulte Monitorando tendências no status de fornecimento).

Para obter mais informações sobre atualizações de firmware e políticas de conformidade, consulte Atualizando firmware em dispositivos gerenciados.

Exibindo um resumo da atividade do Lenovo XClarity Administrator

A área Atividade do XClarity Administrator exibe informações sobre trabalhos ativos, sessões ativas e recursos do sistema no XClarity Administrator.

Procedimento

- **Trabalhos**. Exibe o número de trabalhos ativos que estão atualmente em andamento. Para obter informações adicionais sobre trabalhos, consulte Monitorando trabalhos.
- **Sessões Ativas**. Exibe o ID do usuário e o endereço IP de cada sessão ativa do XClarity Administrator. Para obter mais informações sobre usuários, consulte Gerenciando contas de usuário.
- **Uso de recursos**. Exibe o uso do processador, o uso da memória e a capacidade do disco no sistema host e nos compartilhamentos de arquivos remotos. Para obter mais informações sobre os recursos do sistema, consulte Monitorando os recursos do sistema.

Monitorando os recursos do sistema

É possível determinar no Painel o uso do processador, o uso de memória e a capacidade do disco no sistema host.

Antes de iniciar

Os seguintes *requisitos mínimos* devem ser atendidos para XClarity Administrator. Dependendo do tamanho do ambiente e o uso do Padrões de Configuração, recursos adicionais podem ser necessários para obter o desempenho ideal.

- Dois microprocessadores virtuais
- 8 GB de memória
- 192 GB de armazenamento para uso do XClarity Administrator dispositivo virtual.
- Exibir com uma resolução mínima de 1024 pixels de largura (XGA)

A tabela a seguir lista as configurações mínimas recomendadas para determinado número de dispositivos. Lembre-se de que se executar a configuração mínima, você poderá ter tempos de conclusão mais longos que o esperado para tarefas de gerenciamento. Para tarefas de provisionamento, como implantação do sistema operacional, atualizações de firmware e configuração do servidor, você precisará aumentar os recursos de VM temporariamente.

Número de Dispositivos Gerenciados	CPU Virtual/Configuração de Memória
0 - 100 dispositivos	2 vCPUs, 8 GB de RAM
100 - 200 dispositivos	4 vCPUs, 10 GB de RAM
200 - 400 dispositivos	6 vCPUs, 12 GB de RAM
400 - 600 dispositivos	8 vCPUs, 16 GB de RAM
600 - 800 dispositivos	10 vCPUs, 20 GB de RAM
800 - 1.000 dispositivos	12 vCPUs, 24 GB de RAM

Notas:

- Uma instância XClarity Administrator única pode oferecer suporte a no máximo 1.000 dispositivos.
- Para as recomendações mais recentes e as considerações sobre desempenho adicionais, consulte o XClarity Administrator: Guia de desempenho (White paper).
- Dependendo do tamanho de seu ambiente gerenciado e do padrão de uso em sua instalação, você precisará adicionar recursos para manter o desempenho aceitável. Se você observa com frequência o uso de processadores no painel de recursos do sistema exibindo valores altos ou muito altos, considere adicionar um a dois núcleos de processador virtual. Se o uso de memória persistir acima de 80% em estado ocioso, considere adicionar 1 a 2 GB de RAM. Se o sistema estiver respondendo a uma configuração conforme definido na tabela, considere operar a VM por um período maior, para avaliar o desempenho do sistema.
- Para obter informações sobre como liberar espaço em disco excluindo os recursos XClarity Administrator que não são mais necessários, consulte Gerenciando espaço em disco.

Procedimento

Na barra de menu do Lenovo XClarity Administrator, clique em **Painel**.

O uso de recursos do sistema host é listado na seção XClarity Administrator Atividade.

Processador

A medida de uso indica o número de processos do XClarity Administrator que estão acessando simultaneamente os processadores no host.

Dica: a medida de uso pode ocasionalmente atingir o nível Alto ou Muito Alto. Se o uso continuar nesses níveis por mais de 30 minutos, verifique o log de trabalhos para ver se trabalhos de execução longa estão em andamento (consulte Monitorando trabalhos).

A medida de capacidade total indica o número de processadores que estão disponíveis no host.

Memória

A medida de uso indica a quantidade de memória que está atualmente sendo usada pelo XClarity Administrator.

A medida de capacidade total indica a quantidade total de memória disponível no host.

Dados do usuário

A medida de uso indica a quantidade de espaço em disco que está atualmente sendo usada pelo XClarity Administrator no sistema host.

A medida de capacidade total indica a quantidade total de espaço (e não usado) que é alocado para dados do usuário, como atualizações de firmware e sistemas operacionais.

Para obter mais informações sobre como gerenciar o espaço em disco, consulte Gerenciando espaço em disco.

Atenção: Se os recursos alocados não forem suficientes para manipular o número atual de dispositivos gerenciados com bom desempenho, considere aumentar a alocação de recurso. Para obter mais informações sobre os requisitos de hardware recomendados com base no número de dispositivos gerenciados em seu ambiente, consulte Sistemas de host compatíveis na documentação online do XClarity Administrator.

Monitorando tendências no status de fornecimento

O Lenovo XClarity Administrator coleta o status de fornecimento regularmente, incluindo trabalhos ativos e de conformidade para atualizações de firmware e padrões de configuração, para todos os dispositivos gerenciados para que você possa monitorar tendências durante um período.

Sobre esta tarefa

Você deve ter autoridade **lxc_admin** ou **lxc-supervisor** para exibir dados de tendência.

Os seguintes dados são coletados:

- **Atualizações de firmware**
  - **Dispositivos compatíveis**. O número de dispositivos que são compatíveis com sua política de conformidade de firmware atribuída
  - **Dispositivos não compatíveis**. O número de dispositivos que não são compatíveis com sua política de conformidade de firmware atribuída
  - **Dispositivos sem política**. O número de dispositivos que não têm uma política de conformidade de firmware atribuída
  - **Dispositivos não suportados para atualizações**. O número de dispositivos para os quais as atualizações de firmware não são permitidas
  - **Atualizações em andamento**. O número de dispositivos para os quais as atualizações de firmware estão em andamento
- **Padrões de configuração**
  - **Servidores com perfis**. Número de dispositivos que têm um perfil de servidor atribuído
  - **Servidores sem perfis**. Número de dispositivos que não têm um perfil de servidor atribuído
  - **Servidores compatíveis**. Número de dispositivos que estão em conformidade com o perfil de servidor atribuído
  - **Servidores não compatíveis**. Número de dispositivos que não estão em conformidade com o perfil de servidor atribuído
  - **Padrões de servidor em andamento**. O número de dispositivos para os quais as atualizações de padrão de configuração estão em andamento

Procedimento

Execute as etapas a seguir para visualizar tendências no status de fornecimento.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Painel** para exibir a página Painel.

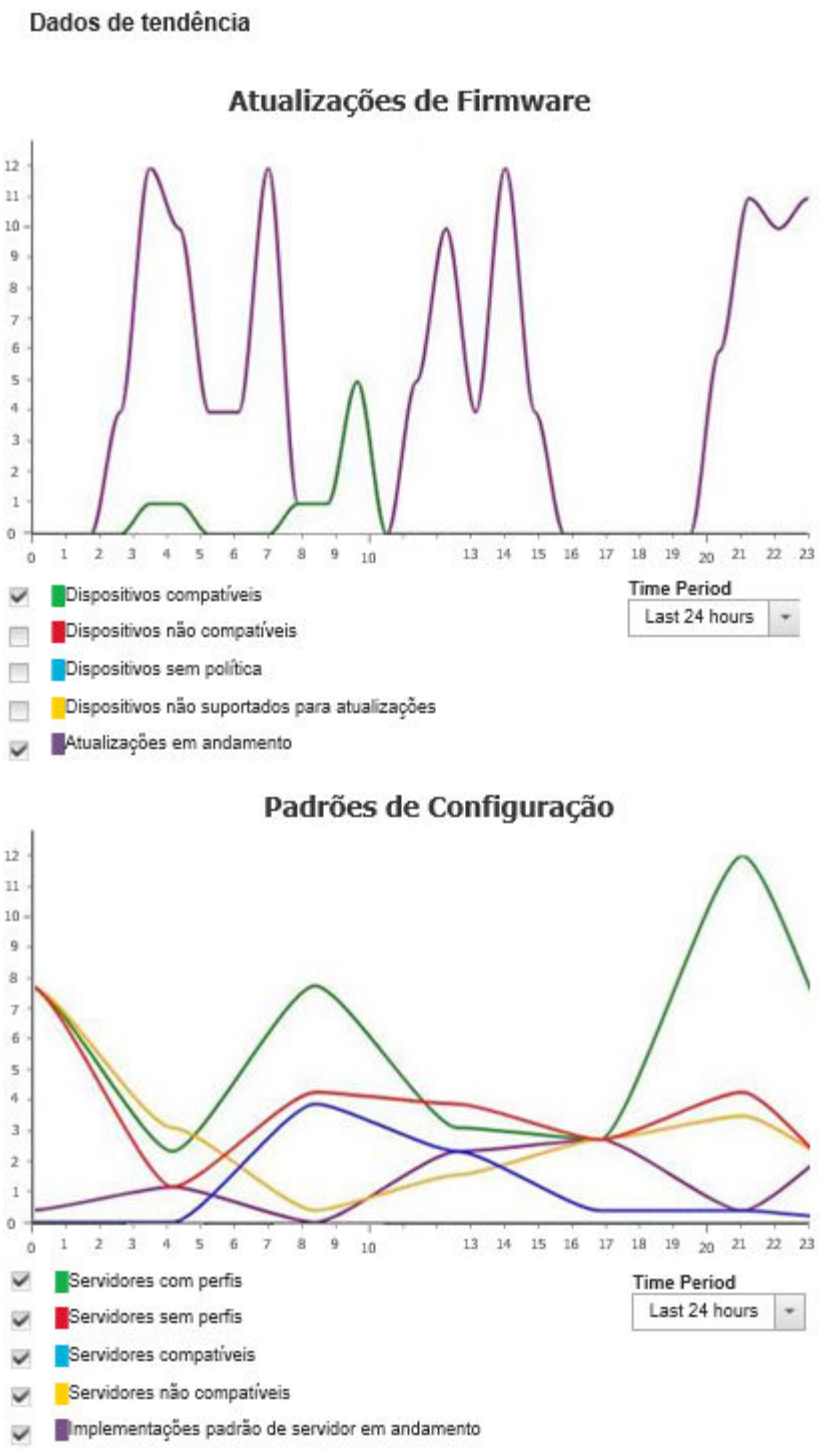
Etapa 2. Clique no link **Dados de tendência** para exibir a caixa de diálogo Configurações de limite.

Etapa 3. Limpe ou selecione os dados que você deseja exibir.

Etapa 4. Selecione o período que você deseja exibir.

- **24 horas**. Exibe os dados para últimas 24 horas. Cada ponto de dados é uma média durante um período de 1 hora.
- **1 mês**. Exibe os dados para últimas 30 dias. Cada ponto de dados é uma média durante um período de 24 hora.

Os dados de tendência são mostrados como um gráfico do período selecionado.



Monitorando métricas históricas

O Lenovo XClarity Administrator coleta regularmente dados de métricas para dispositivos ThinkSystem e ThinkAgile gerenciados, para que você possa analisar o estado atual do seu ambiente.

Antes de iniciar

As métricas históricas são compatíveis apenas com servidores ThinkSystem (exceto SR635, SR645, SR655 e SR665).

Apenas SSDs nos servidores ThinkAgile e ThinkSystem (exceto SR635 e SR655) executando o firmware XCC lançado após abril de 2019 são suportados.

Os drivers Onboard SATA não são suportados.

As unidades NVMe devem suportar a especificação NVMe Management Interface (NVMe-MI).

Sobre esta tarefa

As seguintes métricas são coletadas.

- **Monitoramento de SSD** Este boletim inclui as seguintes estatísticas e gráficos.
  - O número total de SSDs nos dispositivos gerenciados (com base no escopo).
  - O número de SSDs analisados
  - O número de SSDs não elegíveis para análise
  - Um gráfico circular que mostra o número de dispositivos com SSDs que têm vida útil restante em uma faixa específica.
    - Vida útil restante <= 10%. Número de SSDs com 10% ou menos de vida útil restante
    - Vida útil restante 11 – 50%. Número de SSDs com 11 – 50% de vida útil restante
    - Vida útil restante 51 – 100%. Número de SSDs com mais de 50% de vida útil restante
- **Utilização do sistema** Este boletim inclui as seguintes estatísticas e gráficos.
  - O uso atual do processador, como porcentagem
  - O uso atual da memória, como porcentagem
  - Um gráfico de linhas que mostra o uso do processador e da memória ao longo do tempo
- **Consumo de energia** Este boletim inclui as seguintes estatísticas e gráficos.
  - A entrada de energia total atual para todas as fontes de alimentação, em watts
  - Um gráfico de linhas que mostra a entrada de energia total ao longo do tempo
- **Temperatura do dispositivo** Este boletim inclui as seguintes estatísticas e gráficos.
  - A temperatura máxima atual do ar de entrada, em Celsius
  - Um gráfico de linhas que mostra a temperatura máxima ao longo do tempo

Você pode passar o mouse sobre cada linha colorida do gráfico circular, em cada ponto no gráfico de linhas ou no número próximo a cada métrica para obter mais informações sobre a métrica. Você pode mostrar ou ocultar métricas no gráfico clicando no ícone colorido na legenda. Você também pode clicar em qualquer número vinculado ou na opção no ícone **Configurações** () no canto superior direito do cartão para exibir uma lista de todos os dispositivos que têm métricas que satisfazem os critérios selecionados.

Procedimento

Conclua as etapas a seguir para visualizar o diagrama de fluxo para uma atividade específica.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Métricas históricas** para exibir a página Métricas históricas com boletins para cada tipo de métrica.

Etapa 2. Defina o escopo para todos ou um grupo específico de dispositivos.

Colocando dispositivos no modo de manutenção

Quando um dispositivo está no modo de manutenção, o Lenovo XClarity Administrator exclui todos os eventos e alertas para esse dispositivo de todas as páginas em que os eventos e alertas são exibidos. Os alertas excluídos ainda são registrados em log, mas são ocultos na exibição.

Sobre esta tarefa

Apenas eventos e alertas gerados para um dispositivo enquanto o dispositivo estiver no modo de manutenção são excluídos. Os eventos e alertas gerados antes do dispositivo ser colocado no modo de manutenção, são exibidos.

Colocar um dispositivo gerenciado em manutenção e, em seguida, de volta ao serviço pode fazer com que o inventário desse dispositivo fique desatualizado. Se você vir anormalidades, atualize manualmente o inventário na página do dispositivo selecionando o dispositivo e clicando em **Todas as Ações → Inventário → Atualizar Inventário**.

Procedimento

Conclua uma das etapas a seguir para colocar os dispositivos no modo de manutenção.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Serviço e Suporte**. A página Serviço e Suporte é exibida.

Etapa 2. Clique em **Ações de Terminal** na navegação esquerda para exibir a página Ações de Terminal.

Etapa 3. Selecione um ou mais dispositivos para colocar no modo de manutenção.

Etapa 4. Clique em **Ações → Manutenção** para exibir a caixa de diálogo Mono de manutenção.

Etapa 5. Selecione a data e hora para tirar o dispositivo do modo de manutenção e coloque-o de volta em serviço.

Selecione **Indefinidamente** se não desejar que o dispositivo seja colocado novamente em serviço.

Etapa 6. Clique em **Confirmar**. A coluna de manutenção na tabela muda para Sim para esse dispositivo.

Depois de concluir

Quando você tiver concluído a manutenção no dispositivo, poderá colocar o dispositivo novamente em serviço selecionando o dispositivo e clicando em **Ações → Manutenção** e, em seguida, clicando em **Desativar manutenção** na caixa de diálogo. Se você não colocar manualmente o dispositivo novamente no modo de serviço, ele será colocado no modo de serviço automaticamente depois que a data e a hora de término especificadas expirarem.

Trabalhando com alertas

Alertas são condições de hardware ou de gerenciamento que requerem análise e ação do usuário. O Lenovo XClarity Administrator sonda os dispositivos gerenciados assincronicamente e exibe os alertas que são recebidos desses dispositivos.

Saiba mais: XClarity Administrator: monitoramento

Sobre esta tarefa

Normalmente, quando um alerta é recebido, um evento correspondente é armazenado no log de eventos. É possível ter um alerta sem um evento correspondente no log de eventos (mesmo se o log for fechado). Por exemplo, os eventos que ocorrem antes de gerenciar um chassi não são exibidos no log de eventos. Entretanto, os alertas do chassi são exibidos no log de alertas porque o Lenovo XClarity Administrator sonda o CMM após o chassi ser gerenciado.

Visualizando alertas ativos

É possível exibir uma lista de todos os alertas ativos de hardware e de gerenciamento.

Sobre esta tarefa

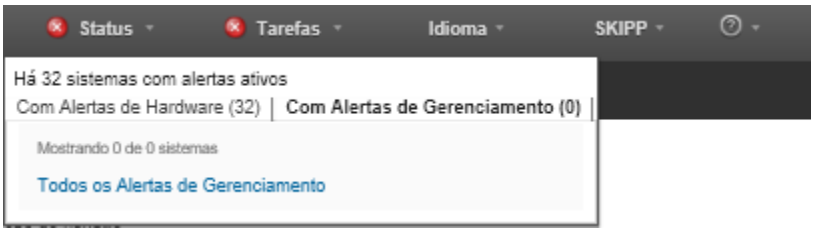
Nota: Os alertas de dispositivos Lenovo Storage são apresentados apenas em inglês, mesmo quando o local de Lenovo XClarity Administrator é configurado em outro idioma. Use um sistema externo de tradução para traduzir manualmente as mensagens, se necessário.

Procedimento

Conclua um desses procedimentos para exibir os alertas ativos.

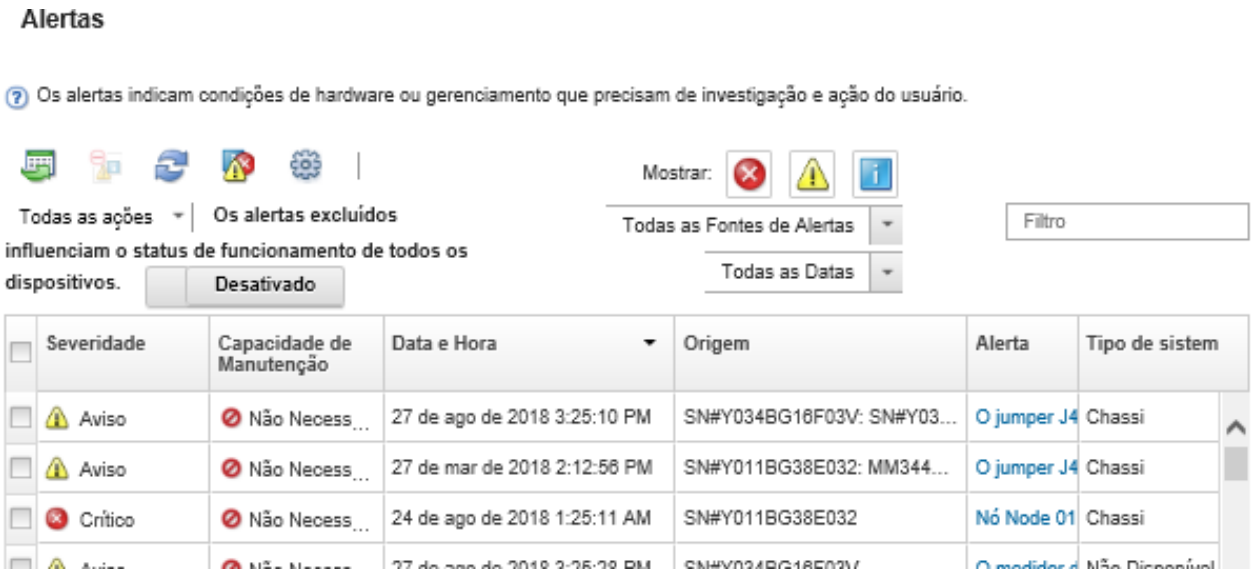
- Para exibir apenas alertas de dispositivos gerenciados (conhecidos como *alertas de hardware*):
  1. Na barra de título do XClarity Administrator, clique no menu suspenso **Status** para exibir um resumo dos alertas de hardware e de gerenciamento.
  2. Clique na guia **Com Alertas de Hardware** para ver um resumo de alertas para cada dispositivo gerenciado.

  3. Passe o cursor sobre um dispositivo que esteja listado nessa guia para exibir uma lista de alertas desse dispositivo.
  4. Clique no link **Todos os Alertas de Hardware** para exibir a página Alertas com uma lista filtrada de todos os alertas de hardware.
- Para exibir apenas alertas do XClarity Administrator (conhecidos como *alertas de gerenciamento*):
  1. Na barra de título do XClarity Administrator, clique no menu suspenso **Status** para exibir um resumo dos alertas de hardware e de gerenciamento.
  2. Clique na guia **Com Alertas de Gerenciamento** para ver um resumo de todos os alertas do CMM e do XClarity Administrator.



3. Passe o cursor sobre um dispositivo que esteja listado nessa guia para exibir uma lista de alertas desse dispositivo.
4. Clique no link **Todos os Alertas de Gerenciamento** para exibir a página Alertas com uma lista filtrada de todos os alertas do CMM e do XClarity Administrator.

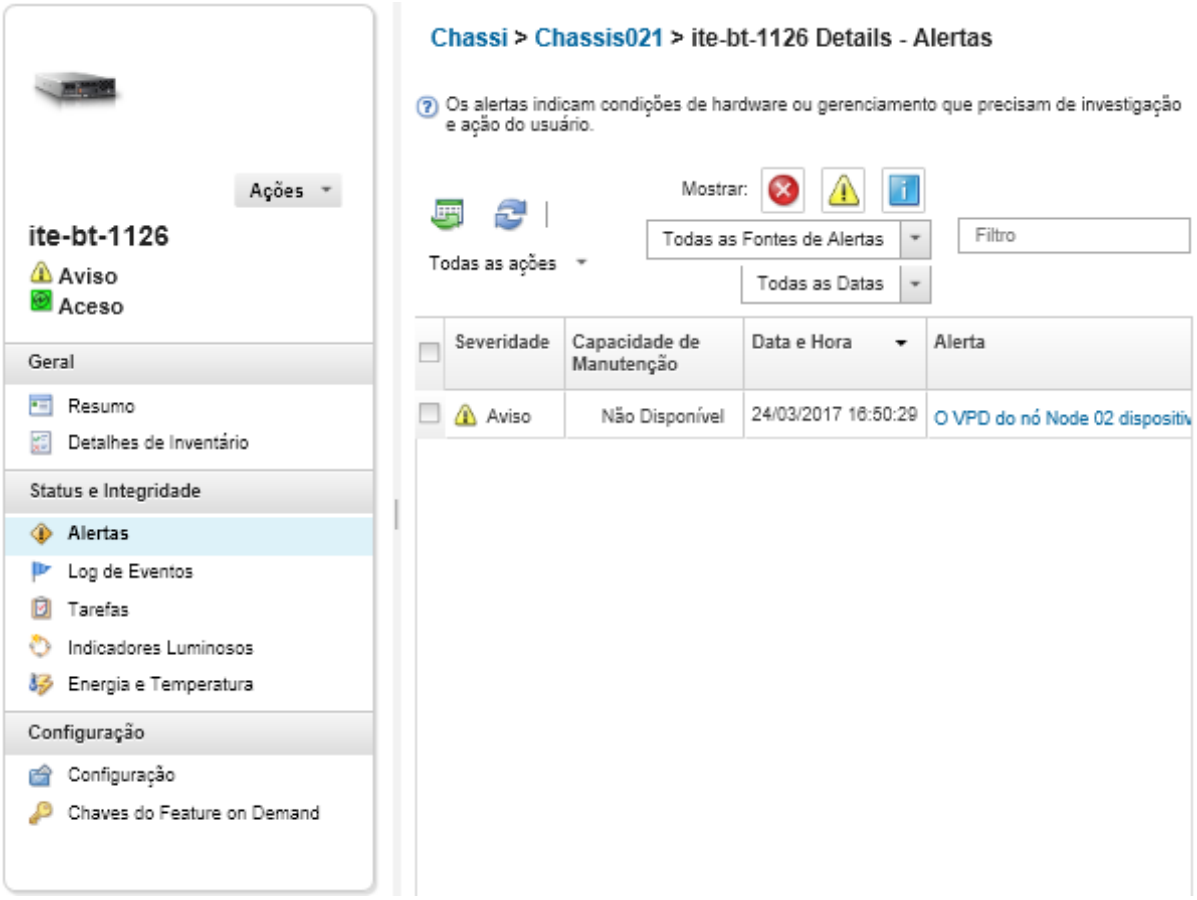
- Para exibir todas os alertas no XClarity Administrator, clique em **Monitoramento → Alertas** na barra de menu do XClarity Administrator. A página Alertas é exibida com uma lista de todos os alertas ativos.



- Para exibir alertas de um dispositivo específico:
  1. Na barra de menu do XClarity Administrator, clique em **Hardware** e clique em um tipo de dispositivo. É exibida uma página com uma exibição tabular de todos os dispositivos gerenciados desse tipo. Por exemplo, clique em **Hardware → Servidores** para exibir a página Servidores.
  2. Clique em um dispositivo específico para exibir a página Resumo do dispositivo.
  3. Em Status e Funcionamento, clique em **Alertas** para exibir uma lista de todos os alertas associados a esse dispositivo.

     Notas: A coluna Capacidade de Manutenção poderá mostrar "Não Disponível" se:

     – O alerta no dispositivo ocorrer antes de XClarity Administrator iniciar o gerenciamento
     – O log de eventos tiver sido encapsulado e o evento associado a esse alerta não estiver mais no log de eventos.



Resultados

Na página Alertas, é possível executar as ações a seguir:

- Atualizar a lista de alertas clicando no ícone **Atualizar** ( ).

  Dica: se novos alertas forem detectados, o log de alertas será atualizado automaticamente a cada 30 segundos.
- Visualize informações sobre um alerta específico (incluindo uma explicação e uma ação do usuário) e sobre o dispositivo que é a origem do alerta (como o identificador exclusivo universalmente) clicando no link na coluna **Alerta**. Uma caixa de diálogo com informações sobre as propriedades e detalhes de alerta é exibida.

  Nota: Se a explicação e as ações de recuperação de um alerta não forem exibidas na guia **Detalhes**, vá até Documentação online do Lenovo Flex System e procure o ID do alerta (por exemplo, `FQXHMSE0004G`). O website sempre fornece as informações mais atualizadas.
- Por padrão, os alertas excluídos não influenciam o status de integridade dos dispositivos gerenciados. Você pode permitir que os alertas excluídos influenciem o status de funcionamento de dispositivos gerenciados na página Alertas clicando em Alternar para ativar **Alertas excluídos influenciam o status de funcionamento de todos os dispositivos**.
- É possível configurar preferências de limite para gerar um alerta e um evento quando um determinado valor, como a vida útil de um SSD em um servidor ThinkSystem ou ThinkServer excede um nível crítico ou de aviso (consulte Configurando preferências de limite para gerar alertas e eventos).
- Exportar o log de alertas clicando no ícone **Exportar como CSV** ( ).

Nota: Os registros de data e hora no log exportado usam a hora local que é especificada pelo navegador da Web.

- Excluir alertas específicos de todas as páginas em que eles são exibidos (consulte Excluindo alertas).
- Refinar a lista de alertas que são exibidos na página atual:
  - Mostrar ou ocultar alertas de uma determinada gravidade clicando nos seguintes ícones:
    - Ícone **Alertas críticos** ()
    - Ícone **Alertas de avisos** ()
    - Ícone **Alertas informativos** ()
  - Mostrar alertas somente de origens específicas. É possível escolher uma das opções a seguir na lista suspensa:
    - Todas as Fontes de Alertas
    - Eventos de Hardware
    - Eventos de Gerenciamento
    - Eventos do Centro de Manutenção
    - Eventos com Possibilidade de Manutenção pelo Cliente
    - Eventos que não permitem manutenção
  - Mostrar apenas alertas com uma data e hora específicas. É possível escolher uma das opções a seguir na lista suspensa:
    - Todas as Datas
    - Duas horas anteriores
    - 24 horas anteriores
    - Semana Passada
    - Mês Passado
  - Listar apenas alertas que contêm o texto específico inserindo o texto no campo **Filtro**.
  - Classificar os alertas por coluna clicando em um título de coluna.

Excluindo alertas

Se houver alertas específicos que não são de seu interesse, será possível excluí-los de todas as páginas em que os alertas são exibidos. Os alertas excluídos ainda estão no log, mas são ocultos em todas as páginas em que alertas são exibidos, incluindo visualizações de log e status do dispositivo.

Sobre esta tarefa

Os alertas excluídos são ocultos para todos os usuários, não apenas para o usuário que define a configuração.

É possível colocar os dispositivos no modo de manutenção para que todos os eventos e alertas para esses dispositivos sejam excluídos (consulte Colocando dispositivos no modo de manutenção).

Restrição: Apenas usuários com autoridade de administrador podem restaurar ou excluir alertas.

Importante: Se você excluir alertas de status, o status do dispositivo no resumo e as páginas detalhadas não mudarão.

Procedimento

Complete as etapas a seguir para excluir alertas do log de alertas.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Alertas**. A página Alertas é exibida.

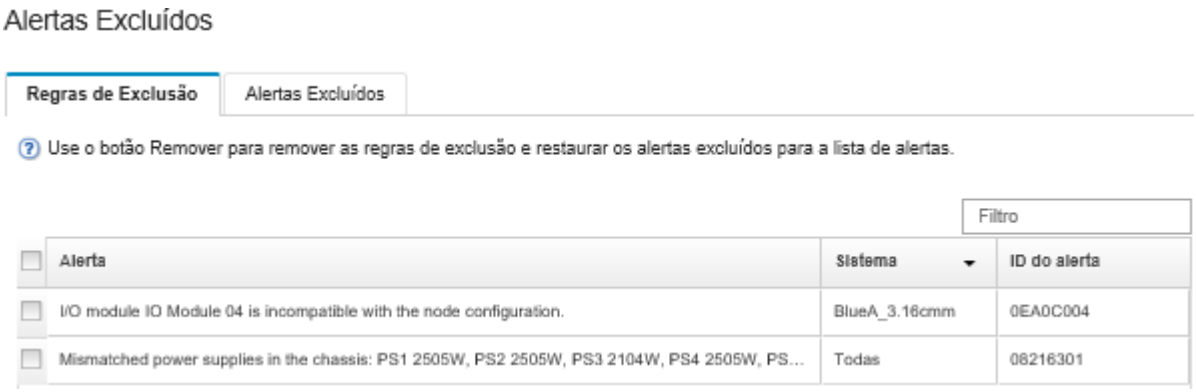
Etapa 2. Selecione os alertas a serem excluídos, e clique no ícone **Excluir alertas** (). A caixa de diálogo de Excluir alertas é exibida.

Etapa 3. Selecione uma das opções a seguir:
- **Excluir alertas selecionados de todos os sistemas**. Exclui os alertas selecionados de todos os dispositivos gerenciados.
- **Excluir alertas somente de sistemas no escopo da instância selecionada**. Exclui os alertas selecionados dos dispositivos gerenciados aos quais os alertas selecionados se aplicam.

Etapa 4. Clique em **Salvar**.

Depois de concluir

Quando você exclui alertas, o Lenovo XClarity Administrator cria regras de exclusão baseadas nas informações fornecidas. É possível exibir uma lista de regras de exclusão e de alertas excluídos na página Alertas clicando no ícone **Mostrar alertas excluídos/confirmados** (). Na caixa de diálogo Alertas excluídos/confirmados, clique na guia **Regras de exclusão** para exibir a lista de regras de exclusão ou clique na guia **Alertas excluídos** para exibir a lista de alertas excluídos.



Por padrão, os alertas excluídos não influenciam o status de integridade dos dispositivos gerenciados. Você pode permitir que os alertas excluídos influenciem o status de funcionamento de dispositivos gerenciados na página Alertas clicando em Alternar para ativar **Mostrar alertas excluídos/confirmados**.

É possível restaurar os alertas que foram excluídos no log de alertas removendo a regra de exclusão apropriada. Para remover uma regra de exclusão, clique no ícone **Mostrar Alertas Excluídos** () para exibir a caixa de diálogo Alertas Excluídos, selecione as regras de exclusão ou o alerta excluído a serem restaurados e clique em **Remover**.

Resolvendo um alerta

O Lenovo XClarity Administrator fornece informações sobre as ações apropriadas a serem executadas para resolver um alerta.

Procedimento

Conclua as seguintes etapas para resolver um alerta.

Etapa 1. Na barra de menu Lenovo XClarity Administrator, clique em **Monitoramento → Alertas** para exibir a página Alertas.

Etapa 2. Localize o alerta no log de alertas.

Etapa 3. Clique no link na coluna **Alerta** para exibir informações sobre o alerta (incluindo uma explicação e ações de recuperação) e as propriedades do dispositivo que é a origem de alerta (como o identificador exclusivo universalmente).

Etapa 4. Conclua as ações de recuperação listadas na guia **Detalhes** para resolver o alerta. O exemplo a seguir ilustra ações de recuperação para um evento.

Altere a configuração de política de segurança no chassi gerenciado referenciado para corresponder à política de segurança atual no servidor de gerenciamento.

Para alterar a política de segurança no chassi, abra uma sessão da interface da linha de comandos no Chassis Management Module (CMM) e execute um dos seguintes comandos:

- Para alterar o nível de política de segurança para `Secure`:
  `security -p secure -T mm[p]`
- Para alterar o nível de política de segurança para `Legacy`:
  `security -p legacy -T mm[p]`

Nota: Se a explicação e as ações de recuperação de um alerta não forem exibidas na guia **Detalhes**, vá até Documentação online do Lenovo Flex System e procure o ID do alerta (por exemplo, `FQXHMSE0004G`). O website sempre fornece as informações mais atualizadas.

Se você seguir as ações recomendadas e o problema persistir, entre em contato com Suporte da Lenovo.

Confirmando alertas

Quando um alerta ativo é confirmado, ele é listado em páginas em que os alertas são exibidos, mas não afeta o status de gravidade do dispositivo aplicável.

Procedimento

Conclua as etapas a seguir para confirmar um alerta.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Alertas**. A página Alertas é exibida.

Etapa 2. Selecione os alertas a serem confirmados.

Etapa 3. Clique no ícone **Confirmar alertas** ( ).

Depois de concluir

- É possível exibir uma lista de alertas confirmados na página Alerts (Alertas) clicando no ícone **Mostrar alertas excluídos/confirmados** ( ) para exibir a caixa de diálogo Excluded/Acknowledged Alerts (Alertas excluídos/confirmados) e, em seguida, clicando na guia **Alertas confirmados**.
- É possível remover a confirmação de um alerta ativo clicando no ícone **Mostrar alertas excluídos/confirmados** ( ) para exibir a caixa de diálogo Alertas excluídos/confirmados e, em seguida, clicando na guia **Alertas confirmados**, selecione os alertas e clique no ícone **Remover confirmação** ( ).

Trabalhando com eventos

No Lenovo XClarity Administrator, você terá acesso a um log de eventos e um log de auditoria.

Saiba mais: XClarity Administrator: monitoramento

Sobre esta tarefa

O *log de evento* fornece uma lista histórica de todos os hardwares e eventos gerenciados.

O *log de auditoria* fornece um registro histórico das ações do usuário, como fazer login no Lenovo XClarity Administrator, criar um novo usuário e alterar uma senha de usuário. É possível usar o log de auditoria para acompanhar e documentar a autenticação e controles nos sistemas de TI.

Monitorando eventos no log de eventos

O *log de evento* fornece uma lista histórica de todos os hardwares e eventos gerenciados.

Sobre esta tarefa

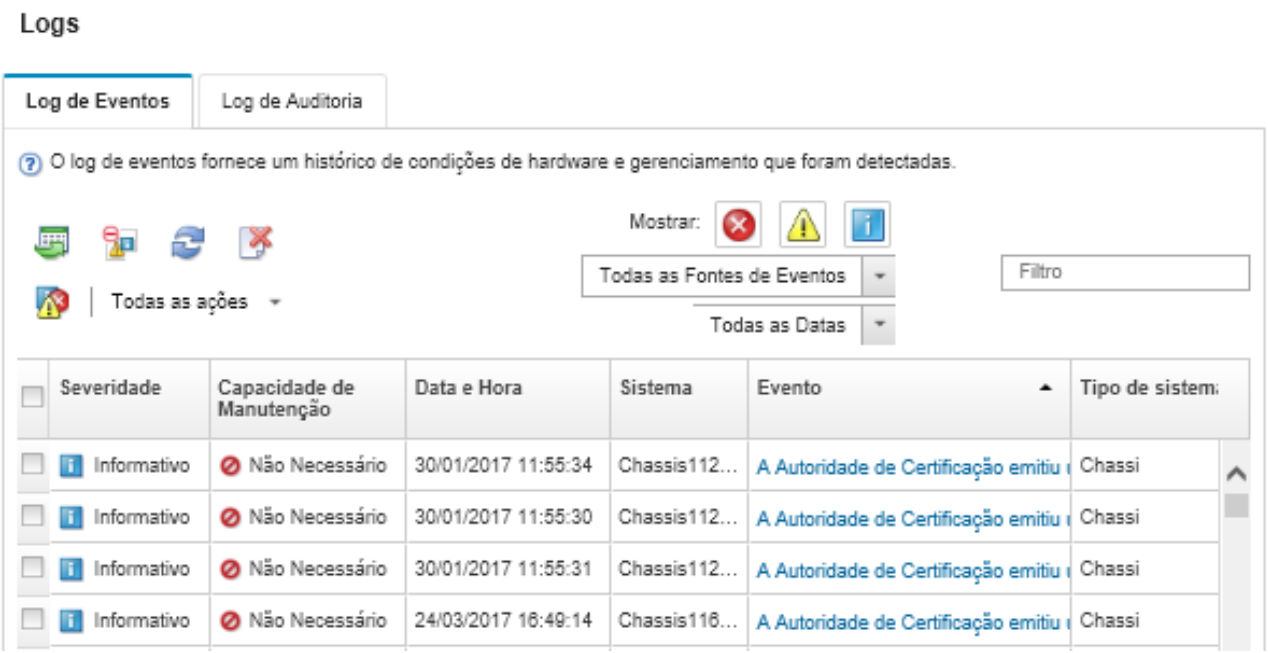
O log de evento contém eventos informativos e não informativos. O número de cada um destes eventos variam até, no máximo, 50.000 eventos ser atingido no log de eventos. Nesse ponto, há um máximo de 25.000 eventos informativos e 25.000não informativos sem informações e eventos informativos. Por exemplo, há 0 eventos no log de eventos inicialmente. Suponha que os eventos são recebidos e que 20.000 eventos informativos e 30.000 eventos não informativos são recebidos. Quando o evento seguinte é recebido, o evento informativo mais antigo será descartado se um evento não informativo for mais antigo. Finalmente, o log equilibra para que haja 25.000 de cada tipo de evento.

O Lenovo XClarity Administrator envia um evento quando o log de evento atinge 80% de seu tamanho mínimo e outro evento quando a soma de logs de evento e auditoria atingem 100% de seu tamanho máximo.

Dica: você pode exportar o log de evento para certificar-se de ter um registro completo de todos os hardwares e eventos de gerenciamento. Para exportar o log de evento, clique no ícone **Exportar como CSV** ( ).

Procedimento

Para exibir o log de evento, clique em **Monitoramento → Logs de Evento** na barra de menu do Lenovo XClarity Administrator e clique na guia **Log de Evento**. A página Log de Eventos é exibida.



A coluna **Capacidade de Manutenção** identifica se o dispositivo requer o serviço. Esta coluna pode conter um dos seguintes valores:

- **Não necessário**. O evento é informativo e não requer o serviço.
- **Usuário**. Toma ação de recuperação apropriada para resolver o problema.

Para exibir informações sobre um evento específico, clique no link na coluna **Evento**. Uma caixa de diálogo é exibida com informações sobre as propriedades do dispositivo que enviou o evento, detalhes sobre o evento e as ações de recuperação.

- **Suporte**. Se o Call Home é habilitado no Lenovo XClarity Administrator, o evento é enviado geralmente ao Centro de Suporte da Lenovo, a menos que já exista um tíquete de serviço aberto para o mesmo ID do evento para o dispositivo.

  Se o Call Home não estiver ativado, é recomendável abrir manualmente um tíquete de serviço para resolver o problema (consulte Abrindo um tíquete de serviço na documentação online do Lenovo XClarity Administrator).

Resultados

Na página Log de Evento, é possível executar as ações a seguir:

- Exibir a origem do evento, clicando no link na coluna **Fonte**.
- Atualizar a lista de eventos clicando no ícone **Atualizar** ( ).

  Dica: O log de evento será atualizado automaticamente a cada 30 segundos se novos eventos forem detectados.
- Limpar todos os eventos no log de eventos, selecionando **Todas as Ações → Limpar o log de eventos**.
- Exibir detalhes sobre um evento específico, clicando no link na coluna **Evento** e clicando na guia **Detalhes**.
- Exportar o log de evento clicando no ícone **Exportar como CSV** ( ).

  Nota: Os registros de data e hora no log exportado usam a hora local que é especificada pelo navegador da Web.
- Excluir eventos específicos de todas as páginas em que os eventos são exibidos (consulte Excluindo eventos).
- Refinar a lista de hardwares e eventos de gerenciamento que são exibidos na página atual:
  - Mostrar ou ocultar eventos de uma determinada gravidade clicando nos seguintes ícones na lista suspensa:
    - Ícone **Eventos críticos** ( )
    - Ícone **Eventos de avisos** ( )
    - Ícone **Eventos informativos** ( )
  - Mostrar eventos somente de origens específicas. É possível escolher uma das opções a seguir na lista suspensa:
    - Todas as Fontes de Alertas
    - Eventos de Hardware
    - Eventos de Gerenciamento
    - Eventos que Permitem Manutenção
    - Eventos com Possibilidade de Manutenção pelo Cliente
    - Eventos que não permitem manutenção
  - Mostrar apenas eventos com uma data e hora específicas. É possível escolher uma das opções a seguir:
    - Todas as Datas
    - 2 horas anteriores
    - 24 horas anteriores
    - Semana Passada
    - Mês Passado
    - Custom

Se você selecionar **Personalizar**, poderá filtrar os eventos de hardware e de gerenciamento que foram gerados entre uma data de início personalizada e a data atual.

- Listar apenas eventos que contêm o texto específico inserindo o texto no campo **Filtro**.
- Classificar os eventos por coluna clicando em um título de coluna.

Monitorando eventos no log de auditoria

O *log de auditoria* fornece um registro histórico das ações do usuário, como fazer login no Lenovo XClarity Administrator, criar um novo usuário e alterar uma senha de usuário. É possível usar o log de auditoria para acompanhar e documentar a autenticação e controles nos sistemas de TI.

Sobre esta tarefa

O log de auditoria pode conter um máximo de 50.000 eventos. Quando o tamanho máximo for atingido, o evento mais antigo em log será descartado e um novo evento será incluído no log.

O XClarity Administrator envia um evento quando o log de auditoria atinge 80% de seu tamanho máximo e outro evento quando a soma de logs de evento e auditoria atingem 100% de seu tamanho máximo.

Dica: você pode exportar o log de auditoria para certificar-se de ter um registro completo de todos os eventos de auditoria. Para exportar o log de auditoria, clique no ícone **Exportar como CSV** ( ).

Procedimento

Para exibir o log de auditoria, clique em **Monitoramento → Logs de Evento** na barra de menu do XClarity Administrator e clique na guia **Log de Auditoria**. A página Log de Auditoria é exibida.

Para exibir informações sobre um evento de auditoria específico, clique no link na coluna **Evento**. Uma caixa de diálogo é exibida com informações sobre as propriedades do dispositivo que enviou o evento, detalhes sobre o evento e as ações de recuperação.

Resultados

Nesta página, é possível executar as ações a seguir:

- Exibir a origem do evento de auditoria, clicando no link coluna **Fonte**.

- Atualizar a lista de eventos de auditoria, clicando no ícone **Atualizar** ().

  Dica: O log de evento será atualizado automaticamente a cada 30 segundos se novos eventos forem detectados.
- Exibir detalhes sobre um evento de auditoria específico, clicando no link na coluna **Evento** e, em seguida, clicando na guia **Detalhes**.
- Exportar o log de auditoria clicando no ícone **Exportar como CSV** ().

  Nota: Os registros de data e hora no log exportado usam a hora local que é especificada pelo navegador da Web.
- Excluir eventos de auditoria específicos de todas as páginas em que os eventos são exibidos (consulte Excluindo eventos).
- Refinar a lista de eventos de auditoria que são exibidos na página atual:
  - Mostrar ou ocultar eventos de uma determinada gravidade clicando nos seguintes ícones:
    - Ícone **Eventos críticos** ()
    - Ícone **Eventos de avisos** ()
    - Ícone **Eventos informativos** ()
  - Mostrar apenas eventos com uma data e hora específicas. É possível escolher uma das opções a seguir na lista suspensa:
    - Todas as Datas
    - 2 horas anteriores
    - 24 horas anteriores
    - Semana Passada
    - Mês Passado
    - Custom

    Se você selecionar **Personalizar**, poderá filtrar os eventos de hardware e de gerenciamento que foram gerados entre uma data de início personalizada e a data atual.
  - Listar apenas eventos que contêm o texto específico inserindo o texto no campo **Filtro**.
  - Classificar os eventos por coluna clicando em um título de coluna.

Resolvendo um evento

O Lenovo XClarity Administrator fornece informações sobre as ações apropriadas a serem executadas para resolver um evento.

Procedimento

Conclua as seguintes etapas para resolver um evento.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Logs de Eventos** para exibir a página Logs.

Etapa 2. Clique na guia **Log de Eventos**.

Etapa 3. Localize o evento no log de eventos.

Etapa 4. Clique no link na coluna **Evento** para exibir informações sobre esse evento (incluindo uma explicação e ações de recuperação) e sobre o dispositivo que é a origem do evento.

Etapa 5. Clique na guia **Detalhes**.

Etapa 6. Conclua as ações de recuperação no guia **Detalhes** para resolver o evento.

Nota: Se uma explicação e ação de recuperação para um evento não forem exibidas, acesse Documentação online do Lenovo Flex System e procure pelo título do evento. O website sempre fornece as informações mais atualizadas.

Se você seguir as ações recomendadas e o problema persistir, entre em contato com Suporte da Lenovo.

Excluindo eventos

Se houver eventos específicos que não são de seu interesse, será possível excluí-los de todas as páginas as quais os eventos são exibidos. Eventos excluídos continuam no log, mas são ocultos das páginas as quais os eventos são exibidos.

Sobre esta tarefa

Os eventos excluídos são ocultos para todos os usuários, não apenas para o usuário que define a configuração.

É possível colocar os dispositivos no modo de manutenção para que todos os eventos e alertas para esses dispositivos sejam excluídos (consulte Colocando dispositivos no modo de manutenção).

Restrição: apenas usuários com autoridade de administrador podem restaurar ou excluir eventos.

Procedimento

Complete as etapas a seguir para excluir eventos dos logs de eventos:

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Logs de Eventos** e clique na guia **Log de Eventos**. Os Logs de Eventos são exibidos.

Etapa 2. Selecione os eventos a serem excluídos, e clique no ícone **Excluir eventos** ( ). A caixa de diálogo de Excluir Eventos é exibida.

Etapa 3. Selecione uma das opções a seguir:
- **Excluir eventos selecionados de todos os sistemas**. Exclui os eventos selecionados de todos os dispositivos gerenciados.
- **Excluir eventos somente de sistemas no escopo da instância selecionada**. Exclui os eventos selecionados dos dispositivos gerenciados os quais eventos selecionados se aplicam.

Etapa 4. Clique em **Salvar**.

Depois de concluir

Quando você exclui eventos, o Lenovo XClarity Administrator cria regras de exclusão baseadas em informações fornecidas.

- Exiba uma lista de regras de exclusão e de eventos excluídos na página de Logs, clicando no ícone **Mostrar Eventos Excluídos** ( ). Na caixa de diálogo Eventos excluídos, clique na guia **Regras de Exclusão** para exibir as regras de exclusão ou clique na guia **Eventos Excluídos** para exibir os eventos excluídos.

- Restaure os eventos que foram excluídos no log de eventos removendo a regra de exclusão apropriada.

  Para remover uma regra de exclusão, clique no ícone **Mostrar Eventos Excluídos** ( ) para exibir a caixa de diálogo Eventos Excluídos, selecione as regras de exclusão a serem restauradas e clique em **Remover Exclusões**.
- Impeça os eventos que permitem manutenção que estão na lista de eventos excluídos de abrir relatórios de problemas automaticamente clicando em **Administração → Serviço e Suporte** na barra de menu do Lenovo XClarity Administrator, clicando na guia **Encaminhadores de Serviço** e selecionando **Não** ao lado da pergunta **Deseja que os eventos excluídos abram relatórios de problemas?**.

Encaminhamento de eventos

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos para dispositivos móveis e aplicativos conectados instalados no seu ambiente para agregar e monitorar o status e o tempo de execução de hardware para seu ambiente de hardware.

Saiba mais: XClarity Administrator: monitoramento

Encaminhando eventos para o syslog, gerenciador SNMP remoto, e-mail e outros serviços de evento

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos para aplicativos conectados instalados no seu ambiente para agregar e monitorar o status e o tempo de execução de hardware para seu ambiente de hardware. É possível definir o escopo de eventos para que sejam encaminhados com base no dispositivo, classe do evento, gravidade do evento e componente.

Sobre esta tarefa

O Lenovo XClarity Administrator pode encaminhar eventos para um ou mais dispositivos. Para eventos de auditoria, será possível escolher encaminhar todos os eventos de auditoria ou nenhum. Não é possível encaminhar eventos específicos de auditoria. Para eventos de hardware e de gerenciamento, é possível escolher encaminhar os eventos para uma ou mais severidades (crítico, aviso e informativo) e para um ou mais componentes (tais como unidades de disco, processadores e adaptadores).

O Lenovo XClarity Administrator usa encaminhadores de eventos para encaminhar eventos. Um *encaminhador de evento* inclui informações sobre o protocolo a ser usado, o destinatário, os dispositivos a serem monitorados e os eventos a serem encaminhados. Depois de criar e habilitar um encaminhador de evento, o Lenovo XClarity Administrator inicia o monitoramento para eventos recebidos com base em critérios de filtro. Quando uma correspondência é encontrada, o protocolo associado é usado para encaminhar o evento.

Os seguintes protocolos são suportados:

- **Análise de Log do Azure**. O Lenovo XClarity Administrator encaminha os eventos monitorados pela rede para o Microsoft Azure Log Analytics.
- **E-mail**. O Lenovo XClarity Administrator encaminha os eventos monitorados para um ou mais endereços de e-mail usando SMTP. O e-mail contém informações sobre o evento, nome de host do dispositivo de origem e vinculá-lo a interface da Web Lenovo XClarity Administrator e ao aplicativo Lenovo XClarity Mobile.
- **FTP**. Encaminha os eventos monitorados pela rede para um servidor FTP.
- **REST**. O Lenovo XClarity Administrator encaminha os eventos monitorados pela rede para um serviço da Web REST.
- **SNMP**. O Lenovo XClarity Administrator encaminha os eventos monitorados na rede para um gerenciador SNMP remoto. Os traps SNMPv1 e SNMPv3 são suportados.

  Para obter informações sobre o arquivo MIB (Management Information Base) que descreve os traps SNMP que o Lenovo XClarity Administrator gera, consulte arquivo lenovoMgrAlert.mibarquivo lenovoMgrAlert.mib na documentação online do Lenovo XClarity Administrator.
- **Syslog**. O Lenovo XClarity Administrator encaminha os eventos monitorados na rede para um servidor de log central onde ferramentas nativas podem ser usadas para monitorar o syslog.

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Nota: Os eventos não são entregues se, por exemplo, a conectividade entre Lenovo XClarity Administrator e o encaminhador de evento está inativa ou a porta está bloqueada.

Configurando o encaminhamento de evento para o Análise de Log do Azure

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos específicos ao Análise de Log do Azure.

Sobre esta tarefa

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Nota: Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Procedimento

Conclua as etapas a seguir para criar um encaminhador de evento para o Análise de Log do Azure.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Evento é exibida.

Etapa 2. Clique na guia **Encaminhamento de eventos**.

Etapa 3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Encaminhador de Evento é exibida.

Etapa 4. Selecione **Análise de Log Azure** como o tipo de encaminhador de evento e preencha as informações específicas do protocolo:

- Digite o nome e a descrição opcional para o encaminhador de evento.
- Insira a chave primária para a interface do Análise de Log do Azure.
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.
- **Opcional**: Se a autenticação for necessária, selecione um dos tipos de autenticação a seguir:
  - **Básico**. Autentica ao servidor especificado usando o ID do usuário e senha especificados.
  - **Nenhum**. Nenhuma autenticação é usada.

Etapa 5. Clique em **Formato de saída** para escolher o formato de saída dos dados de evento a serem encaminhados. As informações variam para cada tipo de encaminhador de evento.

O formato de saída de exemplo a seguir é o formato padrão para destinatários do Análise de Log do Azure. Todas as palavras entre colchetes duplos são as variáveis que são substituídas por valores reais quando um evento é encaminhado. As variáveis disponíveis para destinatários do Análise de Log do Azure estão listadas na caixa de diálogo Formato de Saída.

```
{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",\"Serialnum\":
\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",\"Flags\":
\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",\"LocalLogID\":
\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",\"SystemName\":
\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",\"FailFRUs\":
\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",\"SourceID\":
\"[[EventSourceUUID]]\",\"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
\"FailSNs\":\"[[EventFailSerialNumbers]]\",\"FailFRUUUIDs\":
\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",\"ComponentID\":
\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",\"MsgID\":
\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":
\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],\"Service\":
\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",\"EventDate\":
\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",\"DeviceSerialNumber\":
\"[[DeviceSerialNumber]]\",\"DeviceIPAddress\":\"[[DeviceIPAddress]]\",
\"LXCA\":\"[[LXCA_IP]]\"}
```

É possível clicar em **Redefinir para padrões** para alterar o formato de saída novamente para os campos padrão.

Etapa 6. Clique no botão de alternância **Permitir Eventos Excluídos** para permitir ou impedir que o evento excluído seja encaminhado.

Etapa 7. Selecione **Habilitar este encaminhador** para ativar o encaminhamento de eventos para esse encaminhador.

Etapa 8. Clique em **Avançar** para exibir a guia **Dispositivos**.

Etapa 9. Selecione os dispositivos e os grupos que deseja monitorar para este encaminhador de evento.

Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um

DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.

Etapa 10. Clique em **Avançar** para exibir a guia **Eventos**.

Etapa 11. Selecione os filtros a serem usados para este encaminhador de evento.

- **Fazer a correspondência por categoria de evento**.
  1. Para encaminhar todos os eventos de auditoria independentemente do nível de status, selecione **Inclui todos os eventos de Auditoria**.
  2. Para encaminhar todos os eventos de garantia, selecione **Inclui eventos de Garantia**.
  3. Para encaminhar todos os eventos de alteração de status de funcionamento, selecione **Incluir eventos de alteração de status**.
  4. Para encaminhar todos os eventos de atualização de status de funcionamento, selecione **Incluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja encaminhar.
  6. Insira os IDs para um ou mais eventos que você deseja que o encaminhamento seja excluído. Separe os IDs usando uma vírgula (por exemplo, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Faça a correspondência por código de evento**. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe diversos IDs usando uma vírgula.
- **Excluir por categoria de evento**.
  1. Para excluir todos os eventos de auditoria independentemente do nível de status, selecione **Excluir todos os eventos de Auditoria**.
  2. Para excluir todos os eventos de garantia, selecione **Excluir eventos de Garantia**.
  3. Para excluir todos os eventos de alteração de status de funcionamento, selecione **Excluir eventos de alteração de status**.
  4. Para excluir todos os eventos de atualização de status de funcionamento, selecione **Excluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja excluir.
  6. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe os IDs usando uma vírgula.
- **Exclua por código de evento**. Insira os IDs de um ou mais eventos que você deseja excluir. Separe diversos IDs usando uma vírgula.

Etapa 12. Decida se deve incluir determinados tipos de eventos.

- **Incluir Todos os Eventos de Auditoria**. Envia notificações sobre eventos de auditoria, com base nas classes de eventos e gravidades selecionadas.
- **Incluir eventos de Garantia**. Envia notificações sobre garantias.
- **Incluir eventos de alteração de status**. Envia notificações sobre alterações no status.
- **Incluir eventos de atualização de status**. Enviou notificações sobre novos alertas.
- **Incluir eventos do boletim**. Envia notificação sobre novos boletins.

Etapa 13. Selecione os tipos de eventos e as gravidades sobre os quais deseja ser notificado.

Etapa 14. Selecione se deve filtrar eventos por capacidade de manutenção.

Etapa 15. Clique em **Avançar** para exibir a guia **Planejador**.

Etapa 16. **Opcional:** Defina a hora e os dias em que deseja que os eventos especificados sejam encaminhados para este encaminhador de evento. Apenas eventos que ocorrem durante o slot de tempo especificado são encaminhados.

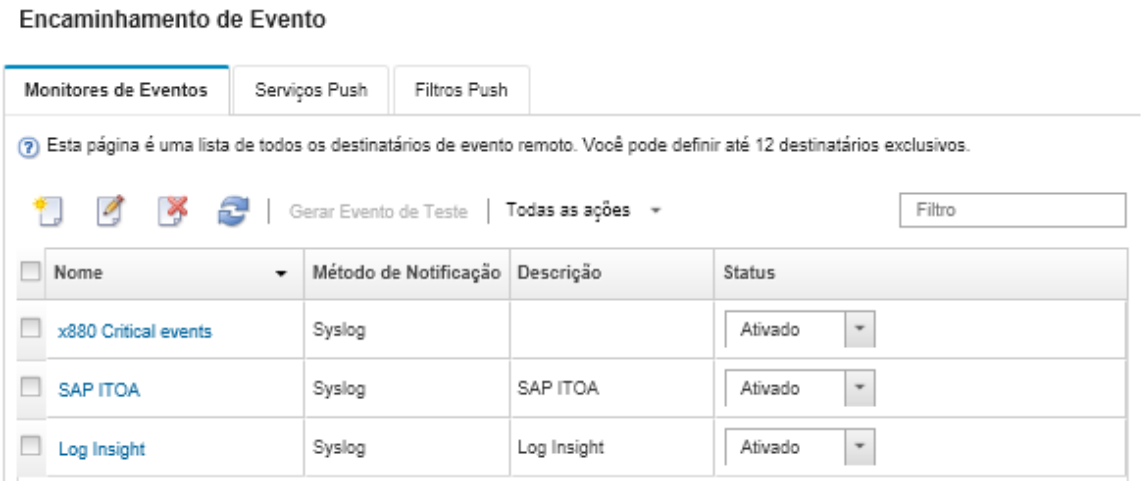
Se você não criar um planejamento para o encaminhador de evento, os eventos serão encaminhados 24h por dia/7 dias por semana.

1. Use o ícone **Rolar para a esquerda** (◀) e o ícone **Rolar para a direita** (▶), e os botões **Dia**, **Semana** e **Mês** para localizar o dia e a hora em que você deseja iniciar o planejamento.
2. Clique duas vezes no slot de tempo para abrir a caixa de diálogo Novo Período de Tempo.
3. Preencha as informações necessárias, incluindo a data e a hora de início e encerramento, e se está planejado para ocorrer novamente.
4. Clique em **Criar** para salvar o planejamento e fechar a caixa de diálogo. O novo planejamento é incluído no calendário.

Dica:
- É possível alterar o período arrastando a entrada de programação para outro período no calendário.
- É possível alterar a duração selecionando o início ou o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar o horário de encerramento selecionando o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar uma programação clicando duas vezes na entrada da programação no calendário e clicando em **Editar Entrada**.
- É possível exibir um resumo de todas as entradas da programação selecionando **Mostrar Resumo do Planejador**. O resumo inclui o período de cada entrada e quais entradas são repetíveis.
- É possível excluir uma entrada da programação do calendário ou do resumo planejador selecionando a entrada e clicando em **Excluir Entrada**.

Etapa 17. Clique em **Criar**.

O encaminhador de evento está listado na tabela Encaminhamento de Evento.



Etapa 18. Selecione o novo encaminhador de evento, clique em **Gerar Evento de Teste** e verifique se os eventos foram encaminhados corretamente para o servidor do Análise de Log do Azure apropriado.

Depois de concluir

Na página Encaminhamento de Evento, é possível executar as seguintes ações em um encaminhador de evento selecionado:

- Atualizar a lista de encaminhadores de evento clicando no ícone **Atualizar** ( ).
- Exibir detalhes sobre um encaminhador de evento específico, clicando no link na coluna **Nome**.
- Alterar as propriedades do encaminhador de evento e filtrar os critérios clicando no nome do encaminhador de evento na coluna **Nome**.
- Excluir o encaminhador de evento clicando no ícone **Excluir** ( ).
- Suspender o encaminhamento de evento (consulte Suspendendo o encaminhamento de evento).

Configurando o encaminhamento de evento em um serviço de e-mail usando SMTP

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos específicos para um serviço de e-mail usando SMTP.

Antes de iniciar

Para encaminhar o e-mail para um serviço e-mail baseado na Web (como Gmail, Hotmail ou Yahoo), o servidor SMTP deve dar suporte ao encaminhamento do e-mail da Web.

Antes de configurar um encaminhador de eventos para um serviço da Web Gmail, revise as informações em Configurando o encaminhamento de eventos para um serviço SMTP do GmailConfigurando o encaminhamento de evento para o syslog, gerenciador SNMP remoto ou e-mail na documentação online do Lenovo XClarity Administrator.

Sobre esta tarefa

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Nota: Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Procedimento

Conclua as etapas a seguir para criar um encaminhador de evento para e-mail usando SMTP.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Evento é exibida.

Etapa 2. Clique na guia **Encaminhamento de eventos**.

Etapa 3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Encaminhador de Evento é exibida.

Etapa 4. Selecione **E-mail** como o tipo de encaminhador de evento e preencha as informações específicas do protocolo:

- Digite o nome, o host de destino e a descrição opcional para o encaminhador do evento.
- Insira a porta a ser usada para o encaminhamento de eventos. O padrão é 25.

- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.
- Insira o endereço de e-mail para cada destinatário. Separe diversos endereços de e-mail usando uma vírgula.

  Para enviar o e-mail do contato de suporte atribuído para o dispositivo, selecione **Usar e-mail (s) do contato de suporte** (consulte Definindo os contatos de suporte de um dispositivo na documentação online do XClarity Administrator).
- **Opcional:** Insira o endereço de e-mail do remetente do e-mail (por exemplo, `john@company.com`).

  Se você não especificar um endereço de e-mail, o endereço do remetente será `LXCA.`*<source_identifier>*`@`*<smtp_host>* por padrão.

  Se você especificar apenas o domínio do remetente, o formato do endereço do remetente será *<LXCA_host_name>*`@`*<sender_domain>* (por exemplo, XClarity1@company.com).

  Notas:

  – Se você configurou o servidor SMTP para requerer um nome do host para encaminhar e-mails e não configurou um nome do host para XClarity Administrator, é possível que o servidor SMTP descarte os eventos encaminhados. Se o XClarity Administrator não tiver um nome do host, o evento será encaminhado com o endereço IP. Se o endereço IP não pode ser obtido, o "localhost" é enviado no seu lugar, o que pode fazer com que o servidor SMTP descarte o evento.

  – Se você especificar o domínio do remetente, a origem não identificará o endereço do remetente. Ao invés disso, as informações sobre a origem do evento serão incluídas no corpo do e-mail, incluindo o nome do sistema, endereço IP, tipo/modelo e o número de série.

  – Se o servidor SMTP só aceita e-mails que foram enviados por um usuário registrado, o endereço padrão do remetente (`LXCA.`*<source_identifier>*`@`*<smtp_host>*) é rejeitado. Nesse caso, você deve especificar pelo menos um nome de domínio no campo **Do endereço**.
- **Opcional:** Para estabelecer uma conexão segura com o servidor SMTP, selecione os tipos de conexão a seguir:
  – **SSL**. Usam o protocolo SSL durante a comunicação.
  – **STARTTLS**. Usa TLS para formar uma comunicação segura em um canal não seguro.

  Se um destes tipos de conexão for selecionado, o LXCA tentará baixar e importar o certificado do servidor SMTP para seu armazenamento confiável. Você é solicitado a aceitar a adição desse certificado ao armazenamento confiável.
- **Opcional:** Se a autenticação for necessária, selecione um dos tipos de autenticação a seguir:
  – **Regular**. Autentica ao servidor SMTP especificado usando o ID do usuário e senha especificados.
  – **NTLM**. Usa o protocolo NT LAN Manager (NTLM) para autenticação ao servidor SMTP especificado usando o ID do usuário, senha e nome de domínio especificados.
  – **OAUTH2**. Usa protocolo SASL (Simple Authentication and Security Layer) para autenticar o servidor SMTP especificado usando o nome de usuário e o token de segurança especificados. Normalmente, o nome do usuário é o seu endereço de e-mail.

    Atenção: O token de segurança expira após um curto período de tempo. É sua responsabilidade atualizar o token de segurança.
  – **Nenhum**. Nenhuma autenticação é usada.

Etapa 5. Clique em **Formato de saída** para escolher o formato de saída dos dados do evento a serem encaminhados no corpo do e-mail e o formato do assunto do e-mail. As informações variam para cada tipo de encaminhador de evento.

O formato de saída de exemplo a seguir é o formato padrão para destinatários do e-mail. Todas as palavras entre colchetes duplos são as variáveis que são substituídas por valores reais quando um evento é encaminhado. As variáveis disponíveis para destinatários do e-mail estão listadas na caixa de diálogo Formato de Saída.

Assunto do e-mail

```
[[DeviceName]]-[[EventMessage]]
```

Corpo do e-mail

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
  iOS link         : [[iOSLink]]\n
  Android link     : [[AndroidLink]]\n
  System Name      : [[DeviceFullPathName]]\n
```

É possível clicar em **Redefinir para padrões** para alterar o formato de saída novamente para os campos padrão.

Etapa 6. Clique no botão de alternância **Permitir Eventos Excluídos** para permitir ou impedir que o evento excluído seja encaminhado.

Etapa 7. Selecione **Habilitar este encaminhador** para ativar o encaminhamento de eventos para esse encaminhador.

Etapa 8. Clique em **Avançar** para exibir a guia **Dispositivos**.

Etapa 9. Selecione os dispositivos e os grupos que deseja monitorar para este encaminhador de evento.

Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de

gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.

Etapa 10. Clique em **Avançar** para exibir a guia **Eventos**.

Etapa 11. Selecione os filtros a serem usados para este encaminhador de evento.

- **Fazer a correspondência por categoria de evento**.
  1. Para encaminhar todos os eventos de auditoria independentemente do nível de status, selecione **Inclui todos os eventos de Auditoria**.
  2. Para encaminhar todos os eventos de garantia, selecione **Inclui eventos de Garantia**.
  3. Para encaminhar todos os eventos de alteração de status de funcionamento, selecione **Incluir eventos de alteração de status**.
  4. Para encaminhar todos os eventos de atualização de status de funcionamento, selecione **Incluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja encaminhar.
  6. Insira os IDs para um ou mais eventos que você deseja que o encaminhamento seja excluído. Separe os IDs usando uma vírgula (por exemplo, `FQXHMEM0214I,FQXHMEM0214I`).
- **Faça a correspondência por código de evento**. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe diversos IDs usando uma vírgula.
- **Excluir por categoria de evento**.
  1. Para excluir todos os eventos de auditoria independentemente do nível de status, selecione **Excluir todos os eventos de Auditoria**.
  2. Para excluir todos os eventos de garantia, selecione **Excluir eventos de Garantia**.
  3. Para excluir todos os eventos de alteração de status de funcionamento, selecione **Excluir eventos de alteração de status**.
  4. Para excluir todos os eventos de atualização de status de funcionamento, selecione **Excluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja excluir.
  6. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe os IDs usando uma vírgula.
- **Exclua por código de evento**. Insira os IDs de um ou mais eventos que você deseja excluir. Separe diversos IDs usando uma vírgula.

Etapa 12. Decida se deve incluir determinados tipos de eventos.

- **Incluir Todos os Eventos de Auditoria**. Envia notificações sobre eventos de auditoria, com base nas classes de eventos e gravidades selecionadas.
- **Incluir eventos de Garantia**. Envia notificações sobre garantias.
- **Incluir eventos de alteração de status**. Envia notificações sobre alterações no status.
- **Incluir eventos de atualização de status**. Enviou notificações sobre novos alertas.
- **Incluir eventos do boletim**. Envia notificação sobre novos boletins.

Etapa 13. Selecione os tipos de eventos e as gravidades sobre os quais deseja ser notificado.

Etapa 14. Selecione se deve filtrar eventos por capacidade de manutenção.

Etapa 15. Clique em **Avançar** para exibir a guia **Planejador**.

Etapa 16. **Opcional:** Defina a hora e os dias em que deseja que os eventos especificados sejam encaminhados para este encaminhador de evento. Apenas eventos que ocorrem durante o slot de tempo especificado são encaminhados.

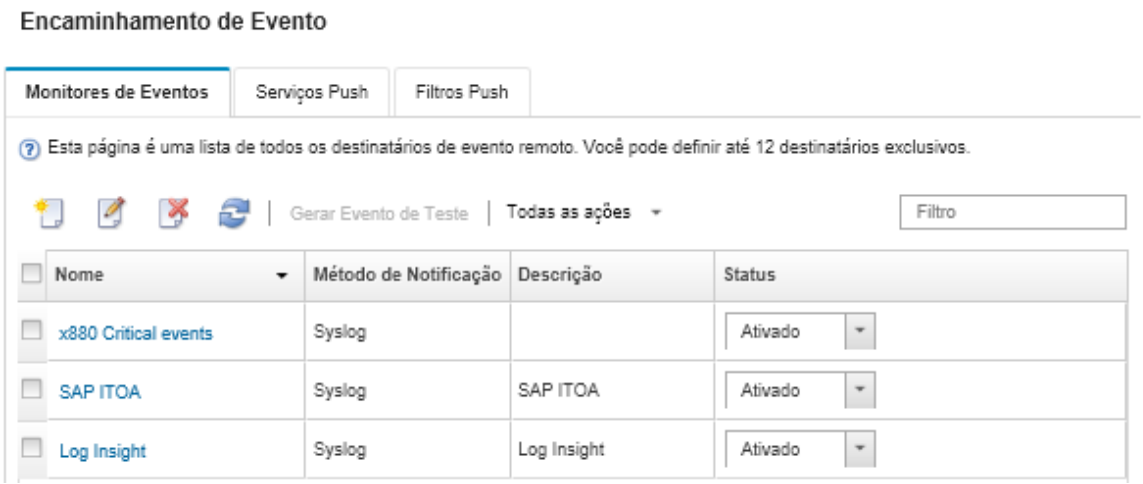
Se você não criar um planejamento para o encaminhador de evento, os eventos serão encaminhados 24h por dia/7 dias por semana.

1. Use o ícone **Rolar para a esquerda** (◀) e o ícone **Rolar para a direita** (▶), e os botões **Dia**, **Semana** e **Mês** para localizar o dia e a hora em que você deseja iniciar o planejamento.
2. Clique duas vezes no slot de tempo para abrir a caixa de diálogo Novo Período de Tempo.
3. Preencha as informações necessárias, incluindo a data e a hora de início e encerramento, e se está planejado para ocorrer novamente.
4. Clique em **Criar** para salvar o planejamento e fechar a caixa de diálogo. O novo planejamento é incluído no calendário.

Dica:
- É possível alterar o período arrastando a entrada de programação para outro período no calendário.
- É possível alterar a duração selecionando o início ou o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar o horário de encerramento selecionando o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar uma programação clicando duas vezes na entrada da programação no calendário e clicando em **Editar Entrada**.
- É possível exibir um resumo de todas as entradas da programação selecionando **Mostrar Resumo do Planejador**. O resumo inclui o período de cada entrada e quais entradas são repetíveis.
- É possível excluir uma entrada da programação do calendário ou do resumo planejador selecionando a entrada e clicando em **Excluir Entrada**.

Etapa 17. Clique em **Criar**.

O encaminhador de evento está listado na tabela Encaminhamento de Evento.



Etapa 18. Selecione o novo encaminhador de evento, clique em **Gerar Evento de Teste** e verifique se os eventos foram encaminhados corretamente para o serviço de e-mail apropriado.

Depois de concluir

Na página Encaminhamento de Evento, é possível executar as seguintes ações em um encaminhador de evento selecionado:

- Atualizar a lista de encaminhadores de evento clicando no ícone **Atualizar** ().
- Exibir detalhes sobre um encaminhador de evento específico, clicando no link na coluna **Nome**.
- Alterar as propriedades do encaminhador de evento e filtrar os critérios clicando no nome do encaminhador de evento na coluna **Nome**.
- Excluir o encaminhador de evento clicando no ícone **Excluir** ().
- Suspender o encaminhamento de evento (consulte Suspendendo o encaminhamento de evento).

Configurando o encaminhamento de evento em um serviço SMTP do Gmail

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos monitorados para um serviço de e-mail baseado na web, como Gmail.

Use os seguintes exemplos de configuração para ajudá-lo a configurar seu encaminhador de evento para usar o serviço Gmail SMTP.

Nota: Gmail recomenda o usar o método de autenticação OAUTH2 para comunicação mais seguro. Se você optar por usar autenticação regular, você receberá um e-mail indicando que um aplicativo tentou usar sua conta sem usar os padrões de segurança mais recente. O e-mail inclui instruções para configurar sua conta de e-mail para aceitar esses tipos de aplicativos.

Para obter informações sobre como configurar um servidor SMTP Gmail, consulte https://support.google.com/a/answer/176600?hl=en.

Autenticação normal usando SSL na porta 465

Este exemplo comunica-se com o servidor SMTP Gmail usando o protocolo SSL na porta 465 e autentica-o usando uma conta de usuário e senha do Gmail válidos.

Parâmetro	Valor
Host	smtp.gmail.com
Porta	465
SSL	Selecionar
STARTTLS	Limpar
Autenticação	Regular
Usuário	Endereço de e-mail do Gmail válido
Senha	Senha de autenticação do Gmail
Do endereço	(opcional)

Autenticação normal usando TLS na porta 587

Este exemplo comunica-se com o servidor SMTP Gmail usando o protocolo TLS na porta 587 e autentica-o usando uma conta de usuário e senha do Gmail válidos.

Parâmetro	Valor
Host	smtp.gmail.com
Porta	587
SSL	Limpar

Parâmetro	Valor
STARTTLS	Selecionar
Autenticação	Regular
Usuário	Endereço de e-mail do Gmail válido
Senha	Senha de autenticação do Gmail
Do endereço	(opcional)

Autenticação OAUTH2 usando TLS na porta 587

Este exemplo comunica-se com o servidor SMTP Gmail usando o protocolo TLS na porta 587 e autentica-o usando uma conta de usuário e token de segurança do Gmail válidos.

Use o seguinte procedimento de amostra para obter o token de segurança.

1. Crie um projeto no Console dos Desenvolvedores do Google e recupere o ID e o segredo do cliente. Para obter mais informações, consulte o website Página Google Sign-In for Websites.
   a. Em um navegador da Web, abra o Página Google APIs.
   b. Clique em **Selecione um projeto → Crie um projeto** no menu nesta página da Web. A caixa de diálogo Novo Projeto é exibida.
   c. Digite um nome, selecione **Sim** para concordar o contrato de licença e clique em **Criar**.
   d. Na guia **Visão Geral**, use o campo de pesquisa para procurar por "Gmail."
   e. Clique em **API DO GMAIL** nos resultados da pesquisa.
   f. Clique em **Habilitar**.
   g. Clique na guia **Credenciais do Usuário**.
   h. Clique em **Tela do acordo de OAuth**.
   i. Digite um nome no campo **Nome do produto mostrado aos usuários** e clique em **Salvar**.
   j. Clique em **Criar credenciais → ID do cliente OAuth**.
   k. Selecione **Outro** e insira um nome.
   l. Clique em **Criar**. A caixa de diálogo OAuth client é exibida com seu ID do cliente e cliente em segredo.
   m. Registre o ID do e o segredo do cliente para uso posterior.
   n. Clique em **OK** para fechar a caixa de diálogo.
2. Use o script do Python oauth2.py para gerar e autorizar um token de segurança, inserindo o ID e o segredo do cliente que foi gerado quando você criou o projeto.

   Nota: O Python 2.7 é necessário para concluir esta etapa. É possível baixar e instalar o Python 2.7 a partir do Site do Python).
   a. Em um navegador da Web, abra o Página gmail-oauth2-tools.
   b. Clique em **Bruto** e, em seguida, salve o conteúdo como um nome de arquivo `oauth2.py` no sistema local.
   c. Execute o seguinte comando no terminal (Linux) ou uma linha de comandos (Windows):
      ```
      py oauth2.py --user=<your_email> --client_id=<client_id>
         --client_secret=<client_secret> --generate_oauth2_token
      ```
      Exemplo
      ```
      py oauth2.py --user=jon@gmail.com
         --client_id=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
      ```

```
--client_secret=3tnyXgEiBIbT2mOOzqnlTszk --generate_oauth2_token
```

Esse comando retorna uma URL que você deve usar para autorizar o token e para recuperar um código de verificação do website do Google, por exemplo:

```
To authorize token, visit this url and follow the directions:

https://accounts.google.com/o/oauth2/auth?client_id=884243132302
-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&amp;redirect_uri=
urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&amp;response_type=code&amp;scope=https%3A%2F%2Fmail.
google.com%2F

Enter verification code:
```

d. Em um navegador da Web, abra a URL que foi retornada na etapa anterior.

e. Clique em **Permitir** para concordar com este serviço. Um código de verificação a ser retornado.

f. Insira o código de verificação no comando `oauth2.py`.

O comando retorna o token de segurança e atualiza o token, por exemplo:

```
Refresh Token: 1/K8lPGx6UQQajj7tQGYKq8mVG8lVvGIVzHqzxFIMeYEQMEudVrK5jSpoR3OzcRFq6
Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
Access Token Expiration Seconds: 3600
```

Importante: O token de segurança expira após um período de tempo. Você pode usar o script do Python oauth2.py e o token atualizado para gerar um novo token de segurança. É sua responsabilidade gerar um novo token de segurança e o atualizar o encaminhador de evento no Lenovo XClarity Administrator com o novo token.

3. Na interface da Web Lenovo XClarity Administrator, configure o encaminhador de evento por e-mail usando os seguintes atributos:

Parâmetro	Valor
Host	smtp.gmail.com
Porta	587
SSL	Limpar
STARTTLS	Selecionar
Autenticação	OAUTH2
Usuário	Endereço de e-mail do Gmail válido
Token	Token de segurança
Do endereço	(opcional)

Configurando o encaminhamento de evento em um servidor FTP

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos específicos a um servidor FTP.

Sobre esta tarefa

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Nota: Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Procedimento

Conclua as etapas a seguir para criar um encaminhador de evento para um servidor FTP.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Evento é exibida.

Etapa 2. Clique na guia **Encaminhamento de eventos**.

Etapa 3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Encaminhador de Evento é exibida.

Etapa 4. Selecione **FTP** como o tipo de encaminhador de evento e preencha as informações específicas do protocolo:

- Digite o nome, o host de destino e a descrição opcional para os encaminhadores do evento.
- Insira a porta a ser usada para o encaminhamento de eventos. O padrão é 21.
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.
- **Opcional:** especificar a sequência de caracteres a ser removido do conteúdo do arquivo.
- Insira o formato do nome do arquivo a ser usado pelo arquivo que contém o evento encaminhado. O formato padrão é `event_[[EventSequenceID]].txt`.

  Nota: Cada arquivo contém informações para um único evento.
- Insira o caminho no servidor FTP remoto onde o arquivo deve ser carregado.
- Escolha a codificação de caracteres **UTF 8** ou **Big5**. O padrão é UTF-8.
- Selecione o tipo de autenticação. Este pode ser um dos valores a seguir.
  - **Anônimo**. (padrão) Nenhuma autenticação é usada
  - **Básico**. Autentica ao servidor FTP usando o ID e senha do usuário especificado.

Etapa 5. Clique em **Formato de saída** para escolher o formato de saída dos dados de evento a serem encaminhados. As informações variam para cada tipo de encaminhadores de evento.

O formato de saída de exemplo a seguir é o formato padrão para destinatários do FTP. Todas as palavras entre colchetes duplos são as variáveis que são substituídas por valores reais quando um evento é encaminhado. As variáveis disponíveis para destinatários do FTP estão listadas na caixa de diálogo Formato de Saída.

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
```

```
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
  iOS link         : [[iOSLink]]\n
  Android link     : [[AndroidLink]]\n
  System Name      : [[DeviceFullPathName]]\n"
```

É possível clicar em **Redefinir para padrões** para alterar o formato de saída novamente para os campos padrão.

Etapa 6. Clique no botão de alternância **Permitir Eventos Excluídos** para permitir ou impedir que o evento excluído seja encaminhado.

Etapa 7. Selecione **Habilitar este encaminhador** para ativar o encaminhamento de eventos para esse encaminhador.

Etapa 8. Clique em **Avançar** para exibir a guia **Dispositivos**.

Etapa 9. Selecione os dispositivos e os grupos que deseja monitorar para este encaminhador de evento.

Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.

Etapa 10. Clique em **Avançar** para exibir a guia **Eventos**.

Etapa 11. Selecione os filtros a serem usados para este encaminhador de evento.

- **Fazer a correspondência por categoria de evento**.
  1. Para encaminhar todos os eventos de auditoria independentemente do nível de status, selecione **Inclui todos os eventos de Auditoria**.
  2. Para encaminhar todos os eventos de garantia, selecione **Inclui eventos de Garantia**.
  3. Para encaminhar todos os eventos de alteração de status de funcionamento, selecione **Incluir eventos de alteração de status**.
  4. Para encaminhar todos os eventos de atualização de status de funcionamento, selecione **Incluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja encaminhar.
  6. Insira os IDs para um ou mais eventos que você deseja que o encaminhamento seja excluído. Separe os IDs usando uma vírgula (por exemplo, `FQXHMEM0214I,FQXHMEM0214I`).
- **Faça a correspondência por código de evento**. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe diversos IDs usando uma vírgula.

- **Excluir por categoria de evento**.
    1. Para excluir todos os eventos de auditoria independentemente do nível de status, selecione **Excluir todos os eventos de Auditoria**.
    2. Para excluir todos os eventos de garantia, selecione **Excluir eventos de Garantia**.
    3. Para excluir todos os eventos de alteração de status de funcionamento, selecione **Excluir eventos de alteração de status**.
    4. Para excluir todos os eventos de atualização de status de funcionamento, selecione **Excluir eventos de atualização de status**.
    5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja excluir.
    6. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe os IDs usando uma vírgula.
- **Exclua por código de evento**. Insira os IDs de um ou mais eventos que você deseja excluir. Separe diversos IDs usando uma vírgula.

Etapa 12. Decida se deve incluir determinados tipos de eventos.

- **Incluir Todos os Eventos de Auditoria**. Envia notificações sobre eventos de auditoria, com base nas classes de eventos e gravidades selecionadas.
- **Incluir eventos de Garantia**. Envia notificações sobre garantias.
- **Incluir eventos de alteração de status**. Envia notificações sobre alterações no status.
- **Incluir eventos de atualização de status**. Enviou notificações sobre novos alertas.
- **Incluir eventos do boletim**. Envia notificação sobre novos boletins.

Etapa 13. Selecione os tipos de eventos e as gravidades sobre os quais deseja ser notificado.

Etapa 14. Selecione se deve filtrar eventos por capacidade de manutenção.

Etapa 15. Clique em **Avançar** para exibir a guia **Planejador**.

Etapa 16. **Opcional:** Defina a hora e os dias em que deseja que os eventos especificados sejam encaminhados para este encaminhador de evento. Apenas eventos que ocorrem durante o slot de tempo especificado são encaminhados.

Se você não criar um planejamento para o encaminhador de evento, os eventos serão encaminhados 24h por dia/7 dias por semana.

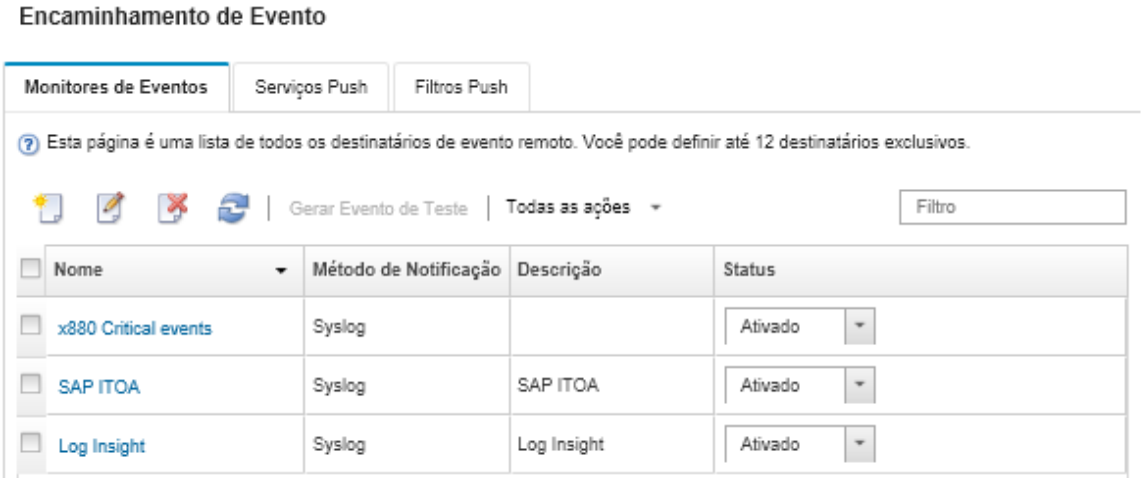
1. Use o ícone **Rolar para a esquerda** (◀) e o ícone **Rolar para a direita** (▶), e os botões **Dia**, **Semana** e **Mês** para localizar o dia e a hora em que você deseja iniciar o planejamento.
2. Clique duas vezes no slot de tempo para abrir a caixa de diálogo Novo Período de Tempo.
3. Preencha as informações necessárias, incluindo a data e a hora de início e encerramento, e se está planejado para ocorrer novamente.
4. Clique em **Criar** para salvar o planejamento e fechar a caixa de diálogo. O novo planejamento é incluído no calendário.

Dica:
- É possível alterar o período arrastando a entrada de programação para outro período no calendário.
- É possível alterar a duração selecionando o início ou o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar o horário de encerramento selecionando o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar uma programação clicando duas vezes na entrada da programação no calendário e clicando em **Editar Entrada**.

- É possível exibir um resumo de todas as entradas da programação selecionando **Mostrar Resumo do Planejador**. O resumo inclui o período de cada entrada e quais entradas são repetíveis.
- É possível excluir uma entrada da programação do calendário ou do resumo planejador selecionando a entrada e clicando em **Excluir Entrada**.

Etapa 17. Clique em **Criar**.

O encaminhador de evento está listado na tabela Encaminhamento de Evento.



Etapa 18. Selecione o novo encaminhador de evento, clique em **Gerar Evento de Teste** e verifique se os eventos foram encaminhados corretamente para o servidor FTP apropriado.

Depois de concluir

Na página Encaminhamento de Evento, é possível executar as seguintes ações em um encaminhador de evento selecionado:

- Atualizar a lista de encaminhadores de evento clicando no ícone **Atualizar** ( ).
- Exibir detalhes sobre um encaminhador de evento específico, clicando no link na coluna **Nome**.
- Alterar as propriedades do encaminhador de evento e filtrar os critérios clicando no nome do encaminhador de evento na coluna **Nome**.
- Excluir o encaminhador de evento clicando no ícone **Excluir** ( ).
- Suspender o encaminhamento de evento (consulte Suspendendo o encaminhamento de evento).

Configurando o encaminhamento de evento em um serviço Web REST

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos específicos a um serviço da Web REST.

Sobre esta tarefa

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Nota: Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou

para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Procedimento

Conclua as etapas a seguir para criar um encaminhador de evento para um serviço Web REST.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Evento é exibida.

Etapa 2. Clique na guia **Encaminhamento de eventos**.

Etapa 3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Encaminhador de Evento é exibida.

Etapa 4. Selecione **REST** como o tipo de encaminhador de evento e preencha as informações específicas do protocolo:

- Insira o caminho do recurso em que o encaminhador deve publicar os eventos (por exemplo, /rest/test).
- Selecione o protocolo a ser usado para o encaminhamento de eventos. Este pode ser um dos valores a seguir.
  - **HTTP**
  - **HTTPS**
- Selecione o método REST. Este pode ser um dos valores a seguir.
  - **PUT**
  - **POST**
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.
- **Opcional:** Se a autenticação for necessária, selecione um dos tipos de autenticação a seguir:
  - **Básico**. Autentica ao servidor especificado usando o ID do usuário e senha especificados.
  - **Nenhum**. Nenhuma autenticação é usada.

Etapa 5. Clique em **Formato de saída** para escolher o formato de saída dos dados de evento a serem encaminhados. As informações variam para cada tipo de encaminhador de evento.

O formato de saída de exemplo a seguir é o formato padrão para destinatários do serviço Web REST. Todas as palavras entre colchetes duplos são as variáveis que são substituídas por valores reais quando um evento é encaminhado. As variáveis disponíveis para destinatários do serviço Web REST estão listadas na caixa de diálogo Formato de Saída.

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

É possível clicar em **Redefinir para padrões** para alterar o formato de saída novamente para os campos padrão.

Etapa 6. Clique no botão de alternância **Permitir Eventos Excluídos** para permitir ou impedir que o evento excluído seja encaminhado.

Etapa 7. Selecione **Habilitar este encaminhador** para ativar o encaminhamento de eventos para esse encaminhador.

Etapa 8. Clique em **Avançar** para exibir a guia **Dispositivos**.

Etapa 9. Selecione os dispositivos e os grupos que deseja monitorar para este encaminhador de evento.

Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.

Etapa 10. Clique em **Avançar** para exibir a guia **Eventos**.

Etapa 11. Selecione os filtros a serem usados para este encaminhador de evento.

- **Fazer a correspondência por categoria de evento**.
  1. Para encaminhar todos os eventos de auditoria independentemente do nível de status, selecione **Inclui todos os eventos de Auditoria**.
  2. Para encaminhar todos os eventos de garantia, selecione **Inclui eventos de Garantia**.
  3. Para encaminhar todos os eventos de alteração de status de funcionamento, selecione **Incluir eventos de alteração de status**.
  4. Para encaminhar todos os eventos de atualização de status de funcionamento, selecione **Incluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja encaminhar.
  6. Insira os IDs para um ou mais eventos que você deseja que o encaminhamento seja excluído. Separe os IDs usando uma vírgula (por exemplo, `FQXHMEM0214I,FQXHMEM0214I`).
- **Faça a correspondência por código de evento**. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe diversos IDs usando uma vírgula.
- **Excluir por categoria de evento**.
  1. Para excluir todos os eventos de auditoria independentemente do nível de status, selecione **Excluir todos os eventos de Auditoria**.
  2. Para excluir todos os eventos de garantia, selecione **Excluir eventos de Garantia**.
  3. Para excluir todos os eventos de alteração de status de funcionamento, selecione **Excluir eventos de alteração de status**.
  4. Para excluir todos os eventos de atualização de status de funcionamento, selecione **Excluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja excluir.
  6. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe os IDs usando uma vírgula.
- **Exclua por código de evento**. Insira os IDs de um ou mais eventos que você deseja excluir. Separe diversos IDs usando uma vírgula.

Etapa 12. Decida se deve incluir determinados tipos de eventos.

- **Incluir Todos os Eventos de Auditoria**. Envia notificações sobre eventos de auditoria, com base nas classes de eventos e gravidades selecionadas.
- **Incluir eventos de Garantia**. Envia notificações sobre garantias.
- **Incluir eventos de alteração de status**. Envia notificações sobre alterações no status.
- **Incluir eventos de atualização de status**. Enviou notificações sobre novos alertas.
- **Incluir eventos do boletim**. Envia notificação sobre novos boletins.

Etapa 13. Selecione os tipos de eventos e as gravidades sobre os quais deseja ser notificado.

Etapa 14. Selecione se deve filtrar eventos por capacidade de manutenção.

Etapa 15. Clique em **Avançar** para exibir a guia **Planejador**.

Etapa 16. **Opcional:** Defina a hora e os dias em que deseja que os eventos especificados sejam encaminhados para este encaminhador de evento. Apenas eventos que ocorrem durante o slot de tempo especificado são encaminhados.

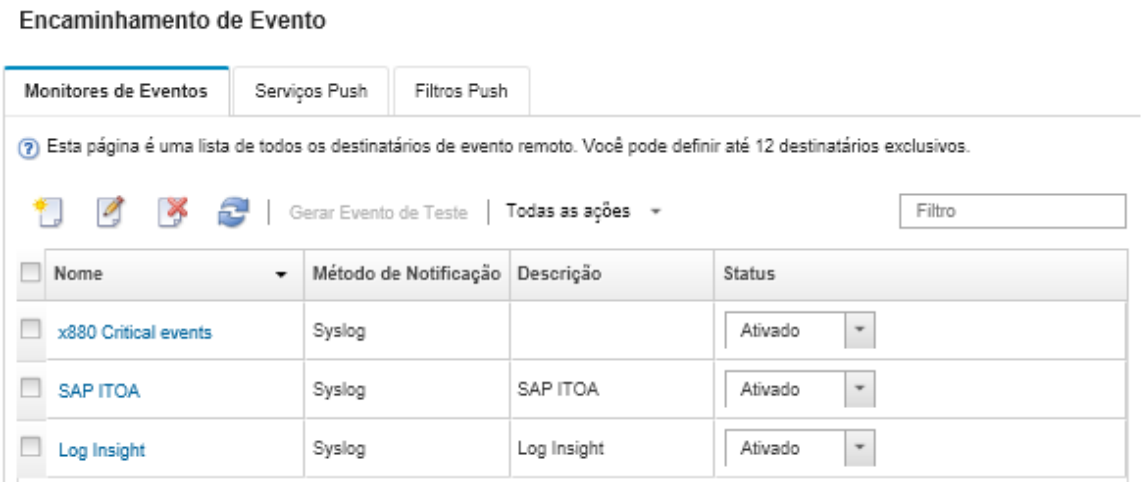
Se você não criar um planejamento para o encaminhador de evento, os eventos serão encaminhados 24h por dia/7 dias por semana.

1. Use o ícone **Rolar para a esquerda** (◀) e o ícone **Rolar para a direita** (▶), e os botões **Dia**, **Semana** e **Mês** para localizar o dia e a hora em que você deseja iniciar o planejamento.
2. Clique duas vezes no slot de tempo para abrir a caixa de diálogo Novo Período de Tempo.
3. Preencha as informações necessárias, incluindo a data e a hora de início e encerramento, e se está planejado para ocorrer novamente.
4. Clique em **Criar** para salvar o planejamento e fechar a caixa de diálogo. O novo planejamento é incluído no calendário.

Dica:
- É possível alterar o período arrastando a entrada de programação para outro período no calendário.
- É possível alterar a duração selecionando o início ou o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar o horário de encerramento selecionando o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar uma programação clicando duas vezes na entrada da programação no calendário e clicando em **Editar Entrada**.
- É possível exibir um resumo de todas as entradas da programação selecionando **Mostrar Resumo do Planejador**. O resumo inclui o período de cada entrada e quais entradas são repetíveis.
- É possível excluir uma entrada da programação do calendário ou do resumo planejador selecionando a entrada e clicando em **Excluir Entrada**.

Etapa 17. Clique em **Criar**.

O encaminhador de evento está listado na tabela Encaminhamento de Evento.



Etapa 18. Selecione o novo encaminhador de evento, clique em **Gerar Evento de Teste** e verifique se os eventos foram encaminhados corretamente para o serviço Web REST apropriado.

Depois de concluir

Na página Encaminhamento de Evento, é possível executar as seguintes ações em um encaminhador de evento selecionado:

- Atualizar a lista de encaminhadores de evento clicando no ícone **Atualizar** ( ).
- Exibir detalhes sobre um encaminhador de evento específico, clicando no link na coluna **Nome**.
- Alterar as propriedades do encaminhador de evento e filtrar os critérios clicando no nome do encaminhador de evento na coluna **Nome**.
- Excluir o encaminhador de evento clicando no ícone **Excluir** ( ).
- Suspender o encaminhamento de evento (consulte Suspendendo o encaminhamento de evento).

Configurando o encaminhamento de eventos para um gerenciador remoto de SNMPv1 ou de SNMPv3

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos específicos para um gerenciador remoto de SNMPv1 ou de SNMPv3.

Sobre esta tarefa

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Nota: Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Para obter informações sobre o XClarity Administrator MIB, consulte arquivo lenovoMgrAlert.mib.

Procedimento

Conclua as seguintes etapas para criar um encaminhador de evento para um gerenciador remoto de SNMPv1 ou de SNMPv3.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Evento é exibida.

Etapa 2. Clique na guia **Encaminhamento de eventos**.

Etapa 3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Encaminhador de Evento é exibida.

Etapa 4. Selecione **SNMPv1** ou **SNMPv3** como o tipo de encaminhador de evento e preencha as informações específicas do protocolo:

- Digite o nome e o host de destino para o encaminhador do evento.
- Insira a porta a ser usada para o encaminhamento de eventos. O padrão é `162`.
- **Opcional:** insira informações adicionais, incluindo a descrição, nome de contato e local.
- Selecione a versão do SNMP. Este pode ser um dos valores a seguir.
  - **SNMPv1**. Se essa versão estiver selecionada, especifique a senha da comunidade enviada com cada solicitação de SNMP ao dispositivo.
  - **SNMPv3**. Esta é a versão padrão e é recomendada para segurança aprimorada. Se SNMPv3 estiver selecionado, opcionalmente, especifique o ID do usuário, o tipo de autenticação e senha, e o tipo e senha de privacidade.

    Se o receptor do trap SNMPv3 precisar do ID do mecanismo para a instância do XClarity Administrator, é possível localizá-lo executando as seguintes etapas:

    1. Certifique-se de que os parâmetros de conexão (nome de usuário, authProtocol, authPassword, privProtocol, privPassword) correspondam aos parâmetros configurados em XClarity Administrator.
    2. Usando o software preferencial (como o snmpwalk), execute uma solicitação GET do SNMP no servidor do XClarity Administrator usando um dos OIDs a seguir:
       - EngineID: 1.3.6.1.6.3.10.2.1.1.0
       - EngineBoots: 1.3.6.1.6.3.10.2.1.2.0

       Use a seguinte sintaxe para o comando `snmpget`. Observe que o tipo de autenticação do encaminhador pode ser SHA ou em branco (sem autenticação).
       ```
       snmpget -v 3 -u <FORWARDER_USER_ID> -l authPriv -a <FORWARDER_AUTH_TYPE> -A <FORWARDER_A
       ```

       Por exemplo, se o endereço IP do XClarity Administrator for 192.0.1.0, o tipo de autenticação for SHA e o tipo de privacidade for AES, o comando a seguir exibirá o engineID.
       ```
       snmpget -v 3 -u someUserID -l authPriv -a SHA -A someUserIDPassword_1 -x AES -X somePrivacyPassword_1
       ```

       A resposta de exemplo a seguir é retornada. Neste exemplo, o engineID é 0x80001370017F00000134C27E12.
       ```
       iso.3.6.1.6.3.10.2.1.1.0 = Hex-STRING: 80 00 13 70 01 7F 00 00 01 34 C2 7E 12
       ```
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.
- **Opcional**: se a autenticação do trap for necessária, insira o ID do usuário e a senha de autenticação. O mesmo ID do usuário e a mesma senha devem ser inseridos no gerenciador de SNMP remoto para o qual os traps são encaminhados.
- Selecione o protocolo de autenticação usado pelo gerenciador de SNMP remoto para verificar o remetente do trap. Este pode ser um dos valores a seguir
  - **SHA**. Usa o protocolo SHA para autenticação ao servidor SNMP especificado usando o ID do usuário, senha e nome de domínio especificados.
  - **Nenhum**. Nenhuma autenticação é usada

- Se a criptografia do trap for necessária, insira o tipo de privacidade (protocolo de criptografia) e a senha. Este pode ser um dos valores a seguir. O mesmo protocolo e a mesma senha devem ser inseridos no gerenciador de SNMP remoto para o qual os traps são encaminhados.
  - **AES**
  - **DES**
  - **Nenhum**

Etapa 5. Clique no botão de alternância **Permitir Eventos Excluídos** para permitir ou impedir que o evento excluído seja encaminhado.

Etapa 6. Selecione **Habilitar este encaminhador** para ativar o encaminhamento de eventos para esse encaminhador.

Etapa 7. Clique em **Avançar** para exibir a guia **Dispositivos**.

Etapa 8. Selecione os dispositivos e os grupos que deseja monitorar para este encaminhador de evento.

Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.

Etapa 9. Clique em **Avançar** para exibir a guia **Eventos**.

Etapa 10. Selecione os filtros a serem usados para este encaminhador de evento.

- **Fazer a correspondência por categoria de evento**.
  1. Para encaminhar todos os eventos de auditoria independentemente do nível de status, selecione **Inclui todos os eventos de Auditoria**.
  2. Para encaminhar todos os eventos de garantia, selecione **Inclui eventos de Garantia**.
  3. Para encaminhar todos os eventos de alteração de status de funcionamento, selecione **Incluir eventos de alteração de status**.
  4. Para encaminhar todos os eventos de atualização de status de funcionamento, selecione **Incluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja encaminhar.
  6. Insira os IDs para um ou mais eventos que você deseja que o encaminhamento seja excluído. Separe os IDs usando uma vírgula (por exemplo, `FQXHMEM0214I,FQXHMEM0214I`).
- **Faça a correspondência por código de evento**. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe diversos IDs usando uma vírgula.
- **Excluir por categoria de evento**.
  1. Para excluir todos os eventos de auditoria independentemente do nível de status, selecione **Excluir todos os eventos de Auditoria**.
  2. Para excluir todos os eventos de garantia, selecione **Excluir eventos de Garantia**.
  3. Para excluir todos os eventos de alteração de status de funcionamento, selecione **Excluir eventos de alteração de status**.
  4. Para excluir todos os eventos de atualização de status de funcionamento, selecione **Excluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja excluir.

6. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe os IDs usando uma vírgula.

- **Exclua por código de evento**. Insira os IDs de um ou mais eventos que você deseja excluir. Separe diversos IDs usando uma vírgula.

Etapa 11. Decida se deve incluir determinados tipos de eventos.

- **Incluir Todos os Eventos de Auditoria**. Envia notificações sobre eventos de auditoria, com base nas classes de eventos e gravidades selecionadas.
- **Incluir eventos de Garantia**. Envia notificações sobre garantias.
- **Incluir eventos de alteração de status**. Envia notificações sobre alterações no status.
- **Incluir eventos de atualização de status**. Enviou notificações sobre novos alertas.
- **Incluir eventos do boletim**. Envia notificação sobre novos boletins.

Etapa 12. Selecione os tipos de eventos e as gravidades sobre os quais deseja ser notificado.

Etapa 13. Selecione se deve filtrar eventos por capacidade de manutenção.

Etapa 14. Clique em **Avançar** para exibir a guia **Planejador**.

Etapa 15. **Opcional:** Defina a hora e os dias em que deseja que os eventos especificados sejam encaminhados para este encaminhador de evento. Apenas eventos que ocorrem durante o slot de tempo especificado são encaminhados.

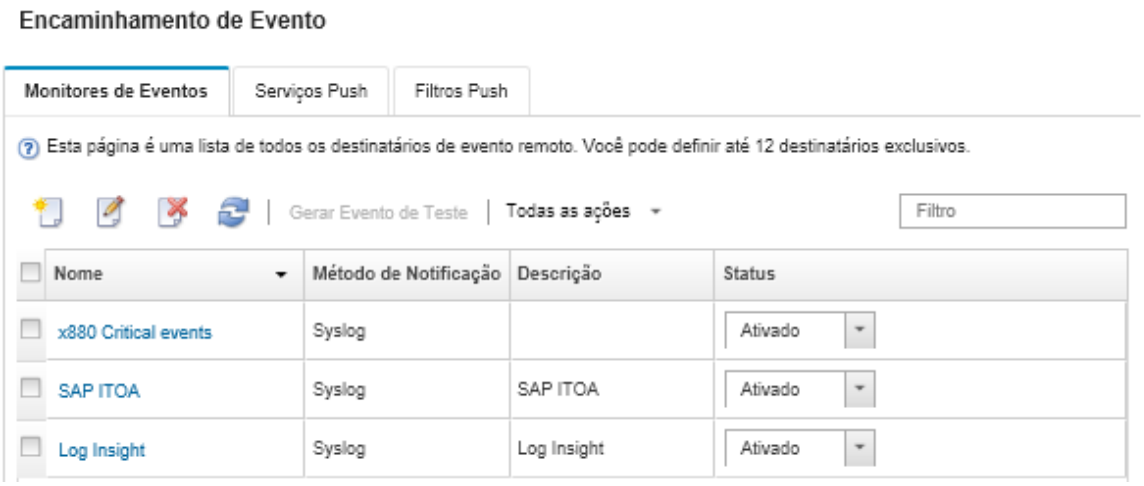
Se você não criar um planejamento para o encaminhador de evento, os eventos serão encaminhados 24h por dia/7 dias por semana.

1. Use o ícone **Rolar para a esquerda** (◀) e o ícone **Rolar para a direita** (▶), e os botões **Dia**, **Semana** e **Mês** para localizar o dia e a hora em que você deseja iniciar o planejamento.
2. Clique duas vezes no slot de tempo para abrir a caixa de diálogo Novo Período de Tempo.
3. Preencha as informações necessárias, incluindo a data e a hora de início e encerramento, e se está planejado para ocorrer novamente.
4. Clique em **Criar** para salvar o planejamento e fechar a caixa de diálogo. O novo planejamento é incluído no calendário.

Dica:
- É possível alterar o período arrastando a entrada de programação para outro período no calendário.
- É possível alterar a duração selecionando o início ou o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar o horário de encerramento selecionando o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar uma programação clicando duas vezes na entrada da programação no calendário e clicando em **Editar Entrada**.
- É possível exibir um resumo de todas as entradas da programação selecionando **Mostrar Resumo do Planejador**. O resumo inclui o período de cada entrada e quais entradas são repetíveis.
- É possível excluir uma entrada da programação do calendário ou do resumo planejador selecionando a entrada e clicando em **Excluir Entrada**.

Etapa 16. Clique em **Criar**.

O encaminhador de evento está listado na tabela Encaminhamento de Evento.



Etapa 17. Selecione o novo encaminhador de evento, clique em **Gerar Evento de Teste** e verifique se os eventos foram encaminhados corretamente para o gerenciador de SNMP remoto apropriado.

Depois de concluir

Na página Encaminhamento de Evento, é possível executar as seguintes ações em um encaminhador de evento selecionado:

- Atualizar a lista de encaminhadores de evento clicando no ícone **Atualizar** ( ).
- Exibir detalhes sobre um encaminhador de evento específico, clicando no link na coluna **Nome**.
- Alterar as propriedades do encaminhador de evento e filtrar os critérios clicando no nome do encaminhador de evento na coluna **Nome**.
- Excluir o encaminhador de evento clicando no ícone **Excluir** ( ).
- Suspender o encaminhamento de evento (consulte Suspendendo o encaminhamento de evento).
- Baixe o arquivo MIB que contém informações sobre traps SNMP clicando no ícone **Criar** ( ) e, em seguida, clique em **Baixar Arquivo MIB** na guia Geral da caixa de diálogo Novo Encaminhamento de Evento

arquivo lenovoMgrAlert.mib

Este arquivo MIB (Management Information Base) descreve os traps SNMP que o Lenovo XClarity Administrator gera, inclusive alertas que foram emitidos pelo XClarity Administrator e dispositivos gerenciados. Você pode compilar este arquivo MIB em qualquer gerenciador de trap SNMP, para que os traps SNMP enviados ao XClarity Administrator possam ser renderizados significativamente.

É possível baixar o arquivo MIB a partir da interface da Web clicando em **Monitoramento → Encaminhamento de Evento** na barra de menus, clicando no ícone **Criar** ( ), selecionando **SNMP** para o tipo do encaminhador de evento. Em seguida, clique em **Baixar Arquivo MIB** na parte inferior da caixa de diálogo.

Os seguintes objetos são incluídos em todos os traps SNMP de saída. Objetos adicionais podem ser incluídos em alguns traps SNMP. Todos os objetos são descritos no arquivo MIB. As informações de recuperação não estão incluídas no trap.

Nota: Essa lista pode ser diferente de uma versão do XClarity Administrator para outra.
- **mgrTrapAppId**. Este é o "Lenovo Event Manager".
- **mgrTrapCommonEvtID**. ID de evento comum
- **mgrTrapDateTime**. Data e hora locais em que o evento foi gerado

- **mgrTrapEventClass**. A origem do evento. Isso pode ser Auditoria, Resfriamento, Energia, Discos, Memória, Processadores, Sistema, Teste, Adaptador, Expansão, IOModule ou Blade.
- **mgrTrapEvtID**. O identificador exclusivo do evento
- **mgrTrapFailFRUs**. Uma lista dos UUIDs de FRU com falha separados por vírgula, se aplicável
- **mgrTrapFailSNs**. Uma lista de dos números de série separados por vírgula de FRUs com falha, se aplicável.
- **mgrTrapFullyQualifiedDomainName**. O nome de domínio totalmente qualificado: o nome do host e o nome do domínio
- **mgrTrapID**. ID do trap
- **mgrTrapMsgText**. Texto de mensagem (apenas em inglês)
- **mgrTrapMsgID**. Identificador de mensagem
- **mgrTrapMtm**. Modelo e tipo do dispositivo que gerou o evento
- **mgrTrapService**. Indicador de capacidade de manutenção. Pode ser 000 (Desconhecido), 100 (Nenhum), 200 (Centro de Manutenção) ou 300 (Cliente)
- **mgrTrapSeverity**. Indicador de gravidade. Pode ser Informativo, Aviso, Menor, Grave ou Crítico
- **mgrTrapSN**. Número de série do dispositivo que gerou o evento
- **mgrTrapSrcIP**. Endereço IP do dispositivo do qual o evento gerado foi recebido
- **mgrTrapSrcLoc**. Local do dispositivo que gerou o evento, apenas em inglês (por exemplo, Slot#xx)
- **mgrTrapSrcName**. Nome do host ou nome de exibição do dispositivo que gerou o evento
- **mgrTrapSysContact**. ID de contato configurado pelo usuário
- **mgrTrapSysLocation**. Informações de local do dispositivo configurado pelo usuário
- **mgrTrapSystemName**. Nome do dispositivo, nome do componente e local do slot
- **mgrTrapTxtId**. Nome do host ou endereço IP do servidor do Lenovo Event Manager que gerou o trap
- **mgrTrapUserid**. ID do usuário associado ao evento (se o evento for interno e a classe de eventos for Auditoria)
- **mgrTrapUuid**. UUID do dispositivo que gerou o evento

Configurando o encaminhamento de evento em um syslog

É possível configurar o Lenovo XClarity Administrator para encaminhar eventos específicos a um syslog.

Sobre esta tarefa

É possível criar e habilitar até 20 encaminhadores de evento para enviar eventos a destinatários específicos.

Se o XClarity Administrator for reinicializado após os encaminhadores de evento serem configurados, você deverá aguardar o servidor de gerenciamento para gerar novamente dados internos antes que os eventos sejam encaminhados corretamente.

Nota: Para XClarity Administrator v1.2.0 e posterior, os **Comutadores** são incluído na guia **Eventos** nas caixas de diálogo Novo Encaminhador de Eventos e Alterar Encaminhador de Eventos. Se você atualizou para 1.2.0 ou posterior de uma versão anterior, lembre-se de atualizar seus encaminhadores de evento para incluir ou excluir os eventos de RackSwitch conforme apropriado. Isso será necessário mesmo se você tiver marcado a caixa de seleção **Todos os Sistemas** para selecionar todos os dispositivos.

Procedimento

Conclua as etapas a seguir para criar um encaminhador de evento para um syslog.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Evento é exibida.

Etapa 2. Clique na guia **Encaminhamento de eventos**.

Etapa 3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Encaminhador de Evento é exibida.

Etapa 4. Selecione **Syslog** como o tipo de encaminhador de evento e preencha as informações específicas do protocolo:

- Digite o nome, o host de destino e a descrição opcional para o encaminhador do evento.
- Insira a porta a ser usada para o encaminhamento de eventos. O padrão é `514`.
- Selecione o protocolo a ser usado para o encaminhamento de eventos. Este pode ser um dos valores a seguir.
  - **UDP**
  - **TCP**
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.
- Opcionalmente, selecione o formato do carimbo de data/hora no syslog. Este pode ser um dos valores a seguir.
  - **Hora local**. O formato padrão, por exemplo `Fri Mar 31 05:57:18 EDT 2017`.
  - **Horário GMT**. Padrão internacional (ISO8601) para data e hora, por exemplo `2017-03-31T05:58:20-04:00`.

Etapa 5. Clique em **Formato de saída** para escolher o formato de saída dos dados de evento a serem encaminhados. As informações variam para cada tipo de encaminhador de evento.

O formato de saída de exemplo a seguir é o formato padrão para destinatários do sylog. Todas as palavras entre colchetes duplos são as variáveis que são substituídas por valores reais quando um evento é encaminhado. As variáveis disponíveis para destinatários do syslog estão listadas na caixa de diálogo Formato de Saída.

```
<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]] severity=[[EventSeverity]]
class=[[EventClass]] appladdr=[[LXCA_IP]] user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]] systemName=[[DeviceFullPathName]]
seq=[[EventSequenceID]] EventID=[[EventID]] CommonEventID=[[CommonEventID]]
```

É possível clicar em **Redefinir para padrões** para alterar o formato de saída novamente para os campos padrão.

Etapa 6. Clique no botão de alternância **Permitir Eventos Excluídos** para permitir ou impedir que o evento excluído seja encaminhado.

Etapa 7. Selecione **Habilitar este encaminhador** para ativar o encaminhamento de eventos para esse encaminhador.

Etapa 8. Clique em **Avançar** para exibir a guia **Dispositivos**.

Etapa 9. Selecione os dispositivos e os grupos que deseja monitorar para este encaminhador de evento.

Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.

Etapa 10. Clique em **Avançar** para exibir a guia **Eventos**.

Etapa 11. Selecione os filtros a serem usados para este encaminhador de evento.

- **Fazer a correspondência por categoria de evento**.
  1. Para encaminhar todos os eventos de auditoria independentemente do nível de status, selecione **Inclui todos os eventos de Auditoria**.

2. Para encaminhar todos os eventos de garantia, selecione **Inclui eventos de Garantia**.
3. Para encaminhar todos os eventos de alteração de status de funcionamento, selecione **Incluir eventos de alteração de status**.
4. Para encaminhar todos os eventos de atualização de status de funcionamento, selecione **Incluir eventos de atualização de status**.
5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja encaminhar.
6. Insira os IDs para um ou mais eventos que você deseja que o encaminhamento seja excluído. Separe os IDs usando uma vírgula (por exemplo, `FQXHMEM0214I,FQXHMEM0214I`).

- **Faça a correspondência por código de evento**. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe diversos IDs usando uma vírgula.
- **Excluir por categoria de evento**.
  1. Para excluir todos os eventos de auditoria independentemente do nível de status, selecione **Excluir todos os eventos de Auditoria**.
  2. Para excluir todos os eventos de garantia, selecione **Excluir eventos de Garantia**.
  3. Para excluir todos os eventos de alteração de status de funcionamento, selecione **Excluir eventos de alteração de status**.
  4. Para excluir todos os eventos de atualização de status de funcionamento, selecione **Excluir eventos de atualização de status**.
  5. Selecione o nível de classes e capacidade de manutenção de evento que você deseja excluir.
  6. Insira os IDs de um ou mais eventos que você deseja encaminhar. Separe os IDs usando uma vírgula.
- **Exclua por código de evento**. Insira os IDs de um ou mais eventos que você deseja excluir. Separe diversos IDs usando uma vírgula.

Etapa 12. Decida se deve incluir determinados tipos de eventos.

- **Incluir Todos os Eventos de Auditoria**. Envia notificações sobre eventos de auditoria, com base nas classes de eventos e gravidades selecionadas.
- **Incluir eventos de Garantia**. Envia notificações sobre garantias.
- **Incluir eventos de alteração de status**. Envia notificações sobre alterações no status.
- **Incluir eventos de atualização de status**. Enviou notificações sobre novos alertas.
- **Incluir eventos do boletim**. Envia notificação sobre novos boletins.

Etapa 13. Selecione os tipos de eventos e as gravidades sobre os quais deseja ser notificado.

Etapa 14. Selecione se deve filtrar eventos por capacidade de manutenção.

Etapa 15. Clique em **Avançar** para exibir a guia **Planejador**.

Etapa 16. **Opcional:** Defina a hora e os dias em que deseja que os eventos especificados sejam encaminhados para este encaminhador de evento. Apenas eventos que ocorrem durante o slot de tempo especificado são encaminhados.

Se você não criar um planejamento para o encaminhador de evento, os eventos serão encaminhados 24h por dia/7 dias por semana.

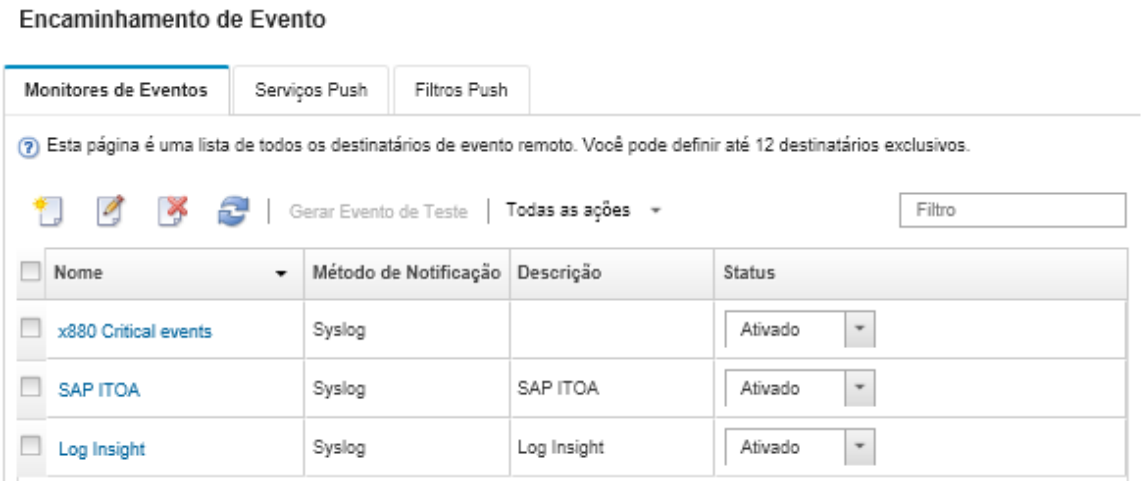
1. Use o ícone **Rolar para a esquerda** (◀) e o ícone **Rolar para a direita** (▶), e os botões **Dia**, **Semana** e **Mês** para localizar o dia e a hora em que você deseja iniciar o planejamento.
2. Clique duas vezes no slot de tempo para abrir a caixa de diálogo Novo Período de Tempo.

3. Preencha as informações necessárias, incluindo a data e a hora de início e encerramento, e se está planejado para ocorrer novamente.
4. Clique em **Criar** para salvar o planejamento e fechar a caixa de diálogo. O novo planejamento é incluído no calendário.

Dica:
- É possível alterar o período arrastando a entrada de programação para outro período no calendário.
- É possível alterar a duração selecionando o início ou o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar o horário de encerramento selecionando o fim da entrada da programação e arrastando para o novo horário no calendário.
- É possível alterar uma programação clicando duas vezes na entrada da programação no calendário e clicando em **Editar Entrada**.
- É possível exibir um resumo de todas as entradas da programação selecionando **Mostrar Resumo do Planejador**. O resumo inclui o período de cada entrada e quais entradas são repetíveis.
- É possível excluir uma entrada da programação do calendário ou do resumo planejador selecionando a entrada e clicando em **Excluir Entrada**.

Etapa 17. Clique em **Criar**.

O encaminhador de evento está listado na tabela Encaminhamento de Evento.



Etapa 18. Selecione o novo encaminhador de evento, clique em **Gerar Evento de Teste** e verifique se os eventos foram encaminhados corretamente para o syslog apropriado.

Depois de concluir

Na página Encaminhamento de Evento, é possível executar as seguintes ações em um encaminhador de evento selecionado:

- Atualizar a lista de encaminhadores de evento clicando no ícone **Atualizar** ( ).
- Exibir detalhes sobre um encaminhador de evento específico, clicando no link na coluna **Nome**.
- Alterar as propriedades do encaminhador de evento e filtrar os critérios clicando no nome do encaminhador de evento na coluna **Nome**.
- Excluir o encaminhador de evento clicando no ícone **Excluir** ( ).
- Suspender o encaminhamento de evento (consulte Suspendendo o encaminhamento de evento).

Suspendendo o encaminhamento de evento

É possível suspender o encaminhamento de evento, desabilitando o encaminhador de evento. Suspendendo o encaminhamento de evento, o monitoramento de eventos recebidos é interrompido. Os eventos recebidos enquanto o monitoramento está suspenso não são encaminhados.

Sobre esta tarefa

O estado desabilitado não é persistente. Se o nó de gerenciamento for reiniciado, todos os encaminhadores de evento serão habilitados.

Procedimento

Conclua as seguintes etapas para desabilitar o encaminhamento de eventos.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Encaminhamento de Eventos**. A página Encaminhamento de Eventos é exibida.

Etapa 2. Selecione **Desabilitar** na coluna **Status** para cada encaminhador de evento que você deseja suspender.

Encaminhamento de eventos à dispositivos móveis

É possível configurar o Lenovo XClarity Administrator para enviar notificações de evento por push à dispositivos móveis

Antes de iniciar

Os requisitos a seguir devem ser atendidos para encaminhar eventos à dispositivos móveis:

- Certifique-se de que um servidor DNS válido esteja configurado para permitir que o Lenovo XClarity Administrator se conecte aos servidores push da Apple ou do Google. Isso pode ser configurado clicando em **Administração → Acesso à Internet → Editar Acesso à Rede** e, em seguida, clique na guia **Configurações de Internet** (consulte Configurando o acesso à rede).
- Certifique-se de que todas as portas necessárias para o gerenciamento de evento estão abertas na rede e no firewall. Para obter informações sobre requisitos de porta, consulte Disponibilidade de porta na documentação online do Lenovo XClarity Administrator.

Sobre esta tarefa

Quando o aplicativo do Lenovo XClarity Mobile está pré-instalado em um dispositivo móvel, é possível habilitar cada instância do Lenovo XClarity Administrator conectada para enviar notificações de eventos por push para esse dispositivo móvel. Quando as notificações por push estão habilitadas para uma instância específica, é criada uma assinatura no Lenovo XClarity Administrator para esse dispositivo móvel.

É possível definir os eventos que são enviados por push para o dispositivo móvel, atribuindo filtros de evento global predefinidos ou personalizados para cada instância do Lenovo XClarity Administrator. Os filtros de evento global predefinidos são habilitados por padrão. O Lenovo XClarity Administrator inicia o monitoramento para eventos recebidos com base em critérios de filtro. Quando uma correspondência é encontrada, o evento é encaminhado ao dispositivo móvel.

Para obter mais informações sobre o Lenovo XClarity Mobile e os dispositivos móveis suportados, consulte Usando o aplicativo Lenovo XClarity Mobile.

Procedimento

Para configurar as notificações por push nesse dispositivo móvel, conclua as etapas a seguir no aplicativo do Lenovo XClarity Mobile no seu dispositivo móvel.

Etapa 1. Habilite notificações por push:

- É possível habilitar notificações por push ao criar uma conexão para uma instância do Lenovo XClarity Administrator. As notificações por push são ativadas por padrão.
- É possível ativar as notificações por push em conexões existentes ativando um ou mais filtros de evento

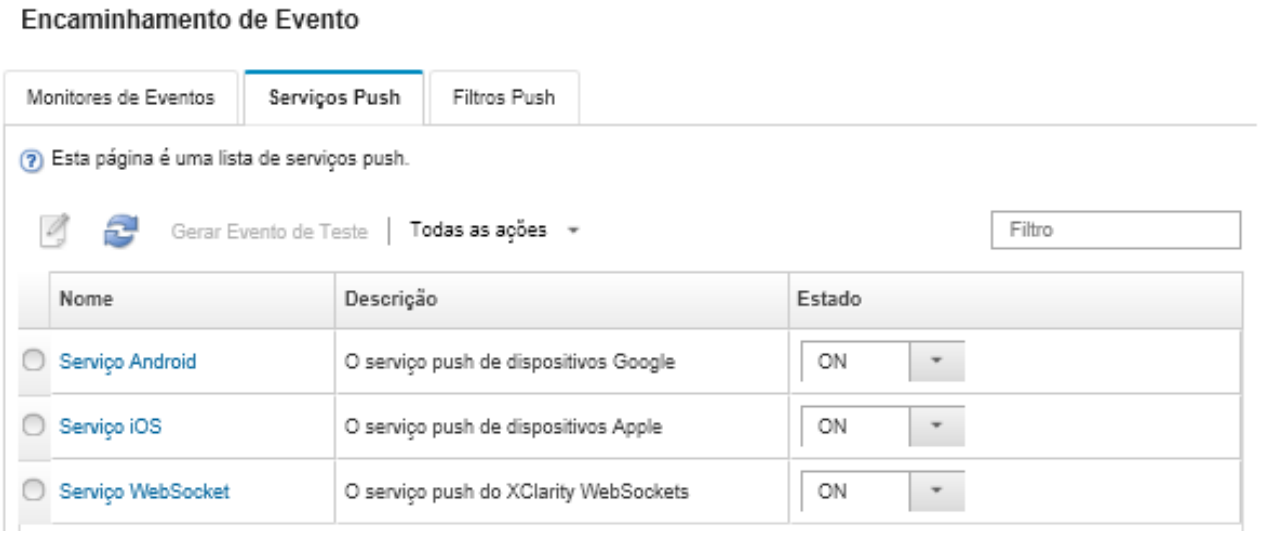
Etapa 2. Atribua filtros de evento global para especificar quais eventos devem ser encaminhados ao dispositivo móvel:

Nota: É possível incluir ou remover filtros globais de assinaturas apenas pelo aplicativo do Lenovo XClarity Mobile. É possível criar filtros globais apenas a partir da interface da Web do Lenovo XClarity Administrator. Para obter informações sobre como criar filtros de evento global personalizados, consulte Criando filtros de evento para dispositivos móveis e WebSockets.

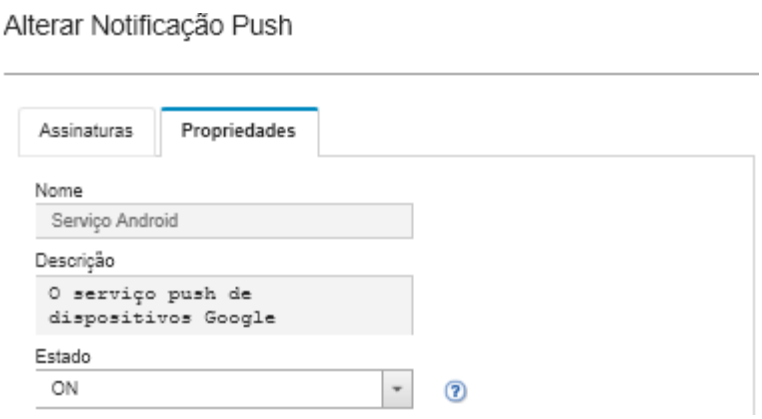
1. Toque em **Configurações → Notificações por Push**. Uma lista de conexões do Lenovo XClarity Administrator é exibida.
2. Toque na instância do Lenovo XClarity Administrator para exibir uma lista de filtros de push.
3. Habilite os filtros de evento para os eventos que você deseja que sejam enviados por push ao dispositivo móvel para a instância do Lenovo XClarity Administrator.
4. Toque em **Toque para gerar notificação por push teste** para verificar se as notificações de evento foram enviadas por push corretamente.

Resultados

É possível gerenciar assinaturas a partir da página de Encaminhamento de Evento na interface da Web do Lenovo XClarity Administrator. Clique em **Monitoramento → Encaminhamento de Eventos** para exibir a página de Encaminhamento de Eventos.



- É possível alterar propriedades do serviço de notificação do dispositivo na guia **Serviço de Push** na página de Encaminhamento de Evento. Para isso, clique no link para o serviço de notificação por push (Google ou Apple) ou na coluna **Nome** para exibir a caixa de diálogo Alterar Notificação por Push e, em seguida, clique na guia **Propriedades**.



- Você pode habilitar e desabilitar as assinaturas:
  - Habilite ou desabilite todas as assinaturas para um serviço de notificação de um dispositivo específico na guia **Serviço de Push** na página de Encaminhamento de Evento selecionando o estado **ATIVADO** ou **DESATIVADO** na tabela para o serviço de notificação do dispositivo.
  - Habilite ou desabilite todas as assinaturas de um dispositivo específico a partir do aplicativo do Lenovo XClarity Mobile tocando em **Configurações → Notificação por push** e, em seguida, habilitando ou desabilitando as notificação por push.
  - Habilite ou desabilite uma assinatura específica a partir do aplicativo do Lenovo XClarity Mobile tocando em **Configurações → Notificação por push**, tocando em uma conexão de Lenovo XClarity Administrator e habilitando pelo menos um filtro de evento ou desabilitando todos os filtros de eventos.
- É possível gerar um evento de teste para todas as assinaturas para um serviço móvel específico na guia **Serviço de Push** na página Encaminhamento de Evento selecionando o serviço móvel e clicando em **Gerar Evento de Teste**.
- É possível exibir uma lista de assinaturas atuais. Na guia **Serviço de Push** na página de Encaminhamento de Evento, clique no link para o serviço de notificação do dispositivo aplicável (Android ou iOS) na coluna **Nome** para exibir a caixa de diálogo Alterar Notificação por Push e, em seguida, clique na guia **Assinaturas**. O ID do dispositivo identifica cada assinatura.

  Dicas:

  - O ID do dispositivo são os 6 primeiros e últimos dígitos do ID de registro de push. É possível localizar o ID de registro de push a partir do aplicativo Lenovo XClarity Mobile, tocando em **Configurações → Sobre → ID de registro de push**.
  - Se tiver feito login como usuário com uma das seguintes funções, todas as assinaturas serão exibidas; caso contrário, apenas as assinaturas para o usuário conectado serão exibidas.
    - **lxc-admin**
    - **lxc-supervisor**
    - **lxc-security-admin**
    - **lxc-sysmgr**
- É possível exibir a lista de filtros de evento atribuída à assinatura na guia **Assinaturas** na caixa de diálogo Alterar Notificação por Push, expandindo a **Lista de filtros** na coluna **Filtros de Evento** da assinatura.

- É possível criar filtros de evento para uma assinatura específica na guia **Assinaturas** na caixa de diálogo Alterar Notificação por Push, selecionando a assinatura e clicando no ícone **Criar** ( ).

  Nota: Esses filtros de evento se aplicam apenas a uma assinatura específica e não podem ser usados por outras assinaturas.

  Também é possível editar ou remover um filtro de evento, selecionando o filtro de evento e clicando no ícone **Editar** ( ) ou no ícone **Remover** ( ), respectivamente.
- É possível determinar o status da última tentativa por push para uma assinatura específica na guia **Assinaturas** na caixa de diálogo Alterar Notificação por Push. A coluna **Registro de data e hora** indica a data e hora do push mais recente. O **Status** indica se a notificação por push foi bem-sucedida no envio ao serviço de push. Nenhum status está disponível quanto à entrega bem-sucedida da notificação por push ao dispositivo pelo serviço. Se a entrega para o serviço de push tiver falhado, a coluna Status fornecerá informações adicionais sobre a falha.
- É possível gerar um evento de teste para uma assinatura específica na guia **Assinaturas** na caixa de diálogo Alterar Notificação por Push, selecionando a assinatura e clicando em **Gerar Evento de Teste**.
- É possível remover uma assinatura na guia **Assinaturas** na caixa de diálogo Alterar Notificação por Push, selecionando a assinatura e clicando no ícone **Remover** ( ).

Encaminhamento de eventos para serviços WebSocket

É possível configurar o Lenovo XClarity Administrator para enviar notificações de evento por push aos serviços WebSocket.

Sobre esta tarefa

As assinaturas do WebSocket não são armazenadas persistentemente em Lenovo XClarity Administrator. Quando o Lenovo XClarity Administrator é reinicializado, os assinantes do WebSocket devem assiná-lo novamente.

Procedimento

Para enviar por push a notificação de evento para um serviço WebSocket, conclua as seguintes etapas.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Eventos é exibida.

Etapa 2. Clique na guia **Serviços de Push**.

Etapa 3. Clique no link do **Serviço WebSocket** na coluna **Nome**. A caixa de diálogo Alterar Notificação por Push é exibida.

Etapa 4. Clique na guia **Assinaturas**.

Etapa 5. Clique no ícone **Criar** ( ).

Etapa 6. Insira o endereço IP do host de destino.

Etapa 7. Clique em **Criar**.

Etapa 8. Selecione a nova assinatura, clique em **Gerar Evento de Teste** e, em seguida, verifique se os eventos foram encaminhados corretamente ao serviço WebSocket.

Resultados

Na guia **Assinaturas**, na caixa de diálogo Alterar Notificação por Push, é possível executar as seguintes ações em uma assinatura do WebSocket selecionada:

- Atualizar a lista de serviços WebSocket clicando no ícone **Atualizar** ( ).
- Exclua as assinaturas, selecionando-as e clicando no ícone **Excluir** ( ).
- Determine o status da última tentativa de push de uma assinatura específica, visualizando o conteúdo da coluna **Status**. Se a tentativa falhar, esta coluna irá conter uma mensagem que descreverá o erro.

Na guia **Propriedades**, na caixa de diálogo Alterar Notificação por Push, é possível executar as seguintes ações:

- Altere as propriedades do serviço WebSocket, incluindo tempo de inatividade de conexão, o tamanho máximo de buffer, o número máximo de assinantes e o período limite para se registrar.
- É possível redefinir o serviço WebSocket às configurações padrão, clicando em **Restaurar Padrões**.
- Suspenda o enviar por push de notificações de evento a todas as assinaturas para o serviço WebSocket, configurando o **Estado** como Desligado.

Na guia **Serviço de Push** na página Encaminhamento de Evento, é possível gerar um evento de teste para todas as assinaturas do WebSocket, selecionando o serviço WebSocket e clicando em **Gerar Evento de Teste**.

Criando filtros de evento para dispositivos móveis e WebSockets

É possível criar filtros de eventos globais que podem ser usados em uma ou várias assinaturas para dispositivos móveis e WebSockets. Também é possível criar filtros de evento que são exclusivos a uma assinatura.

Antes de iniciar

Você deve ter autoridade de supervisor para criar filtros de evento.

É possível criar até 20 filtros de evento global.

Sobre esta tarefa

Os seguintes filtros de evento global são predefinidos:

- **Corresponda a Todos Alertas Críticos**. Este filtro corresponde a todos os eventos críticos gerados por qualquer dispositivo gerenciado ou pelo XClarity Administrator.
- **Corresponda a Todos os Avisos**. Este filtro corresponde a todos os eventos de aviso gerados por qualquer dispositivo gerenciado ou pelo XClarity Administrator.

Procedimento

Para criar um filtro de evento global, conclua as etapas a seguir.

- Crie um filtro de evento global que pode ser usado por qualquer assinatura.
  1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Encaminhamento de Eventos é exibida.
  2. Clique na guia **Filtros de Push**.
  3. Clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Filtro de Push é exibida.
  4. Especifique a descrição de nome e a opção para este novo filtro de evento.
  5. Clique em **Avançar** para exibir a guia **Sistemas**.
  6. Selecione os dispositivos que você deseja monitorar.

     Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.
  7. Clique em **Avançar** para exibir a guia **Eventos**.
  8. Selecione os componentes e as severidades para qual deseja que os eventos sejam encaminhados.

     Dica:
     - Para encaminhar todos os eventos de hardware, selecione **Corresponder todos os eventos**.
     - Para encaminhar eventos de auditoria, selecione **Incluir Todos os Eventos de Auditoria**.
     - Para encaminhar eventos de garantia, selecione **Inclui eventos de Garantia**.
  9. Clique em **Criar**.
- Crie um filtro de evento para uma assinatura específica:
  1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Encaminhamento de Evento**. A página Novo Encaminhamento de Eventos é exibida.
  2. Clique na guia **Filtros de Push**.
  3. Selecione o link para o tipo de dispositivo móvel (Android ou iOS) na coluna Nome da tabela. A caixa de diálogo Alterar Notificação por Push é exibida.
  4. Clique na guia **Assinaturas** para exibir uma lista de assinaturas ativas.
  5. Selecione a assinatura e clique no ícone **Criar** ( ). A guia **Geral** da caixa de diálogo Novo Filtro de Evento é exibida.
  6. Especifique a descrição de nome e a opção para este novo filtro de evento.
  7. Clique em **Avançar** para exibir a guia **Sistemas**.
  8. Selecione os dispositivos que você deseja monitorar.

     Dica para encaminhar eventos para todos os dispositivos gerenciados (atuais e futuros), marque a caixa de seleção **Combinar todos os sistemas**.Se você não marcar a caixa de seleção **Combinar todos os sistemas**, certifique-se que os dispositivos selecionados não tenham um DUMMY-UUID na coluna UUID. Um Dummy-UUID é atribuído para dispositivos que ainda não se recuperaram após uma reinicialização ou não foram totalmente descobertos pelo servidor de gerenciamento. Se você selecionar um dispositivo com um Dummy-UUID, o encaminhamento de evento funcionará para este

dispositivo até o ponto quando o dispositivo for descoberto ou recuperado, e o Dummy-UUID é alterado para o UUID real.

9. Clique em **Avançar** para exibir a guia **Eventos**.
10. Selecione os componentes e as severidades para qual deseja que os eventos sejam encaminhados.

    Dica:
    - Para encaminhar todos os eventos de hardware, selecione **Corresponder todos os eventos**.
    - Para encaminhar eventos de auditoria, selecione **Incluir Todos os Eventos de Auditoria**.
    - Para encaminhar eventos de garantia, selecione **Inclui eventos de Garantia**.
11. Clique em **Criar**.

Depois de concluir

Na guia Filtros de Push, na página de Encaminhamento de Evento, é possível executar as seguintes ações em um filtro de evento selecionado:

- Atualizar a lista de filtros de evento, clicando no ícone **Atualizar** ().
- Exibir detalhes sobre um filtro de evento específico, clicando no link na coluna **Nome**.
- Alterar as propriedades do filtro de evento e os critérios do filtro, clicando no ícone **Editar** ().

Excluir os filtros de evento, clicando no ícone **Excluir** ().

Trabalhando com trabalhos

Trabalhos são tarefas de execução mais longa que são executadas em um ou mais dispositivos. Você pode programar alguns trabalhos para serem executados apenas uma vez (imediatamente ou mais tarde), de maneira recorrente, ou quando ocorre um evento específico.

Trabalhos executados em segundo plano. É possível ver o status de cada tarefa no log de trabalhos.

Monitorando trabalhos

É possível exibir um log de todos os trabalhos que são iniciados pelo Lenovo XClarity Administrator. O log de trabalhos inclui os trabalhos que estão em execução, que foram concluídos ou têm erros.

Sobre esta tarefa

Trabalhos são tarefas de execução mais longa que são executadas em um ou mais dispositivos. Por exemplo, se você implantar um sistema operacional em diversos servidores, cada implantação de servidor será listada como um trabalho separado.

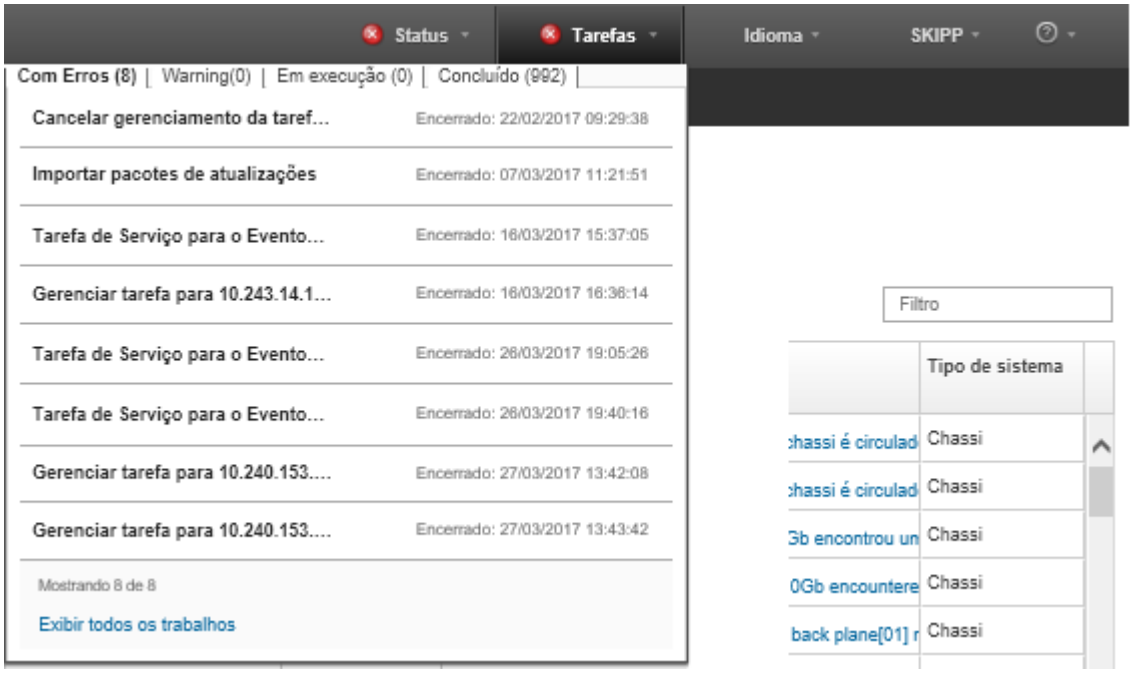
Trabalhos executados em segundo plano. É possível ver o status de cada tarefa no log de trabalhos.

O log de trabalhos contém informações sobre cada trabalho. O log pode conter no máximo 1000 trabalhos ou 1 GB. Quando o tamanho máximo for atingido, os trabalhos mais antigos concluídos com êxito serão excluídos. Se não houver nenhum trabalho concluído com êxito no log, os trabalhos mais antigos concluídos com avisos serão excluídos. Se não houver nenhum trabalho concluído com êxito nem com avisos no log, os trabalhos mais antigos concluídos com erros serão excluídos.

Procedimento

Conclua uma destas etapas para exibir o log de trabalhos.

- Na barra de título XClarity Administrator, clique em **Trabalhos** para exibir um resumo de trabalhos que estão em execução, concluídos e que têm erros.

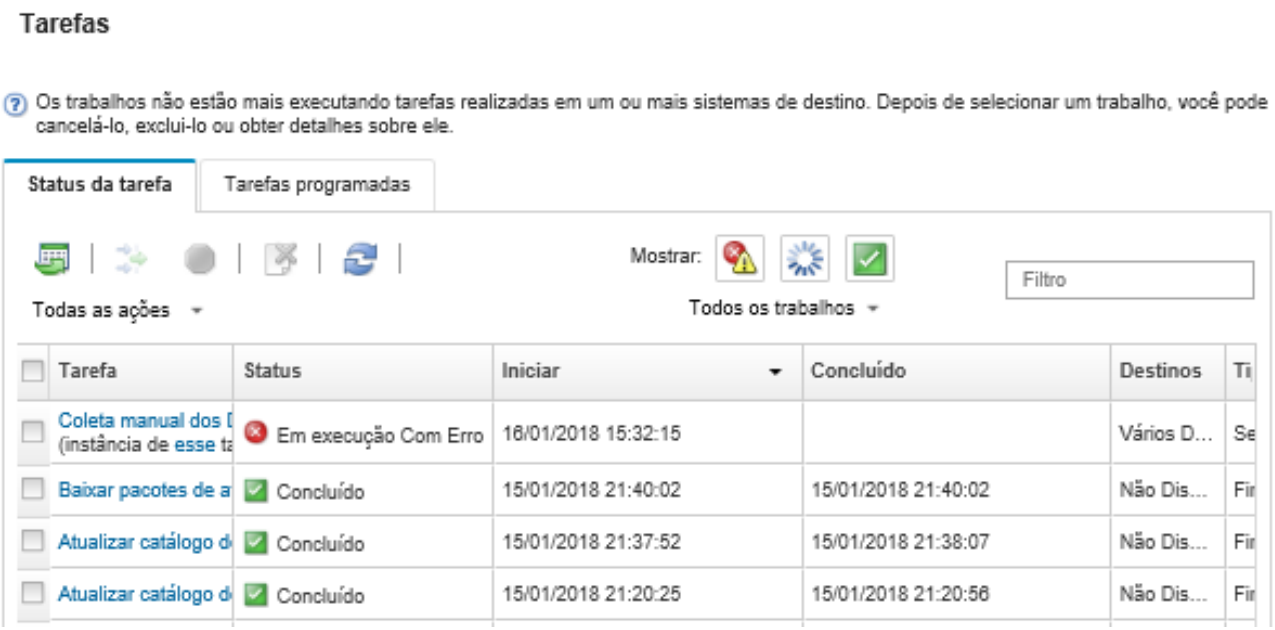


  Nesse menu, você pode clicar nas seguintes guias:
  - **Erros**. Exibe uma lista de todos os trabalhos com os erros associados.
  - **Avisos**. Exibe uma lista de todos os trabalhos com os avisos associados.
  - **Em execução**. Exibe uma lista de todos os trabalhos que estão atualmente em andamento.
  - **Concluído**. Exibe uma lista de todos os trabalhos que foram concluídos.

  Passe o ponteiro do mouse sobre uma entrada de trabalho no menu para obter mais informações sobre o trabalho, incluindo o status, andamento e o usuário que criou o trabalho.
- Na barra de título do XClarity Administrator, clique em **Trabalhos** e clique no link **Exibir todos os trabalhos** para exibir a página Status dos Trabalhos.
- Na barra de menu do XClarity Administrator, clique em **Monitor → Trabalhos** e clique na guia **Status do Trabalho** para exibir a página Status dos trabalhos.

Depois de concluir

A página Trabalhos é exibida com uma lista de todos os trabalhos para o XClarity Administrator.



Nesta página, é possível executar as ações a seguir:

- Crie programações de tarefa clicando na guia **Tarefas programadas** (consulte Programando trabalhos).
- Exiba mais informações sobre um trabalho específico clicando na coluna **Trabalhos**. Uma caixa de diálogo é exibida com uma lista de subtarefas (subtrabalhos) e seus destinos, um resumo dos subtarefas incluindo quaisquer ações necessárias e detalhes do log, incluindo a severidade e o carimbo de data/hora para cada mensagem. É possível ocultar ou mostrar logs para tarefas filho.
- Para trabalhos programados, exibir informações sobre a programação do trabalho clicando "neste" link na descrição do trabalho na coluna **Trabalhos**.
- Alterar o número de trabalhos que são exibidos por página. O valor padrão é 10 trabalhos. É possível exibir 25, 50 ou todos os trabalhos.
- Limitar a lista de trabalhos que são exibidos:
  - Liste apenas os trabalhos de uma origem específica clicando em **Tipos de Trabalho** e escolhendo as opções a seguir.
    - **Todos os Tipos de Trabalho**
    - **Service**
    - **Management**
    - **Configuration**
    - **Firmware**
    - **Health**
    - **Power**
    - **Acesso remoto**
    - **ID do Sistema**
    - **Imagens do SO**
    - **Implantação do SO**
    - **Exportação de Perfil de SO**
    - **Custom**
    - **Inventory**
    - **Unknown**
  - Listar apenas os trabalhos programados que estão associados a um tipo de programação específico clicando em **Tipos de Programação** e escolhendo as opções a seguir.
    - **Todos os Tipos de Programação**

  - **Única**
  - **Recorrente**
  - **Acionado**
- Ocultar ou mostrar trabalhos com erros ou avisos clicando no ícone **Ocultar trabalhos com erro/ avisos** ().
- Ocultar ou mostrar trabalhos em execução clicando no ícone **Ocultar trabalhos em execução** ().
- Ocultar ou mostrar trabalhos concluídos clicando no ícone **Ocultar trabalhos concluídos** ().
- Listar apenas os trabalhos que contêm texto específico inserindo o texto no campo **Filtro**.
- Se a filtragem for aplicada à página, remova o filtro clicando no ícone **Mostrar Todos os Trabalhos** ().
- Classificar os trabalhos por coluna clicando em um título de coluna.

- Exportar a lista de trabalhos como um arquivo CSV clicando no ícone **Exportar como CSV** ().

  Nota: Os registros de data e hora no log exportado usam a hora local que é especificada pelo navegador da Web.
- Cancelar trabalhos em execução ou subtarefas selecionando um ou mais trabalhos ou subtarefas e clicando no ícone **Interromper** ().

  Nota: Cancelar o trabalho pode levar vários minutos.
- Excluir trabalhos ou subtarefas concluídos do log de trabalhos selecionando um ou mais trabalhos ou subtarefas concluídos e clicando no ícone **Excluir** ().
- Exporte informações sobre tarefas específicas selecionando as tarefas e clicando no ícone **Exportar como CSV** ().
- Atualizar o log de trabalhos clicando no ícone **Atualizar** ().

Programando trabalhos

É possível criar programações no Lenovo XClarity Administrator para executar determinadas tarefas em momentos específicos.

Sobre esta tarefa

É possível programar os tipos de trabalho a seguir:
- Tarefas simples, como desligar e reinicializar
- Coletando dados de serviço para dispositivos específicos
- Atualizando os catálogos de atualização de firmware e do driver de dispositivo do SO do site da Lenovo
- Atualizando o catálogo de atualizações do XClarity Administrator no site da Lenovo
- Baixando firmware no site da Lenovo
- Atualizando o firmware e drivers de dispositivo do SO em dispositivos gerenciados
- Fazendo backup de dados e configurações do XClarity Administrator
- Fazendo backup e restaurando dados de configuração do comutador

Você pode programar trabalhos para serem executados:
- Apenas uma vez (imediatamente ou posteriormente)
- De maneira recorrente
- Quando ocorre um evento específico

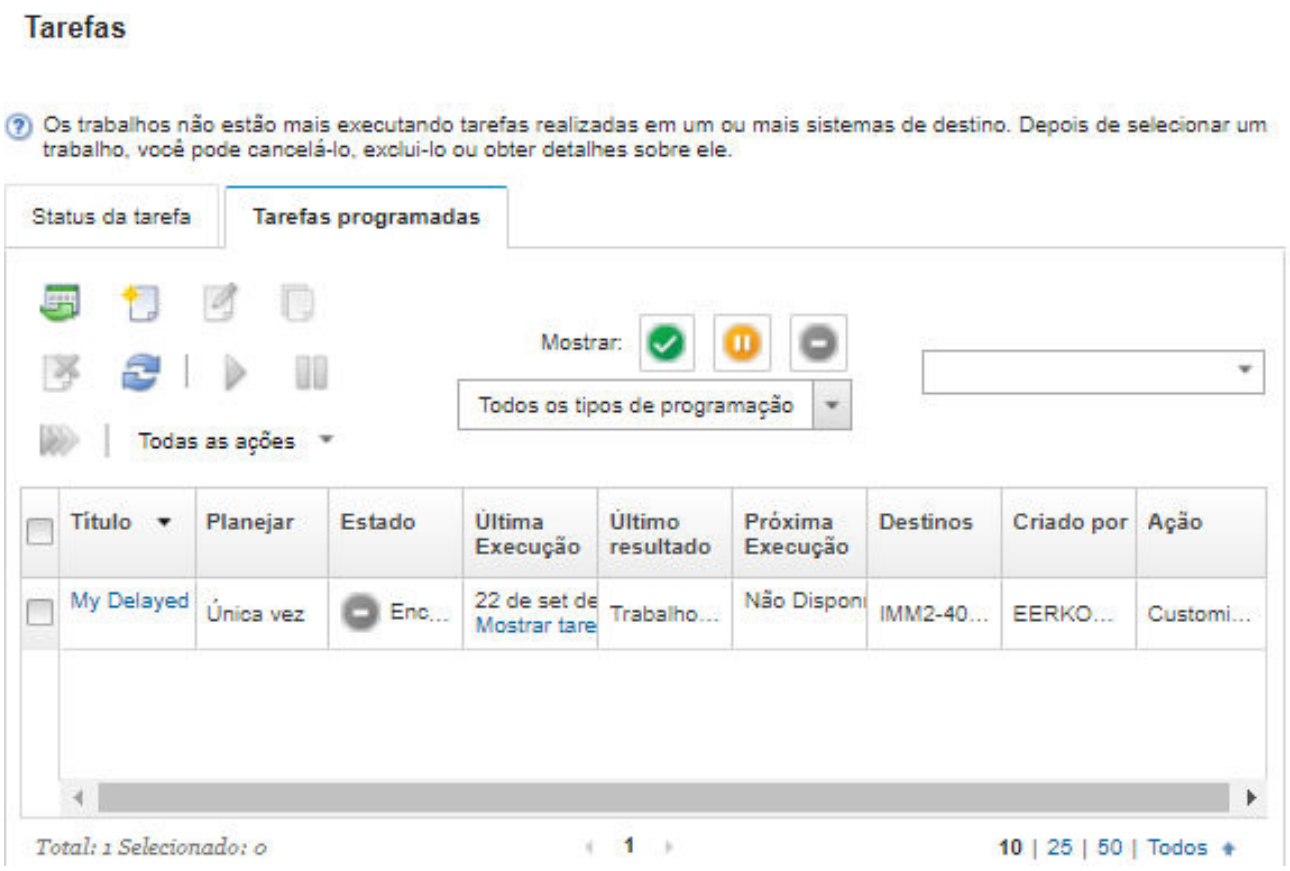
Procedimento

Para criar e programar um trabalho, conclua as etapas a seguir.

- Para tarefas complexas, como atualizar o firmware e coletar dados de serviço, crie o trabalho na página ou caixa de diálogo da tarefa atual.
  1. Clique em **Programação** para criar uma programação para executar essa tarefa. A caixa de diálogo Programar Novo Trabalho é exibida.
  2. Insira um nome para o trabalho.
  3. Especifique quando o trabalho deve ser executado. As opções disponíveis dependem do tipo de trabalho. Alguns trabalhos não podem ser recorrentes nem acionados por um evento
     - **Única**. Esses trabalhos são executados apenas uma vez. Especifique a data e hora em que deseja que o trabalho seja executado.
     - **Recorrente**. Esses trabalhos são executados mais de uma vez. Especifique quando e com que frequência deseja que o trabalho seja executado.
     - **Acionado pelo evento**. Esses trabalhos são executados quando ocorre um evento específico.
       a. Especifique a data e hora em que deseja que o trabalho seja executado e clique em **Avançar**.
       b. Selecione o evento para acionar o trabalho.
  4. Clique em **Criar Trabalho**.
- Para tarefas simples, como ligar e reinicializar, crie a programação do trabalho na página Trabalhos.
  1. Na barra de menu do XClarity Administrator, clique em **Monitor → Trabalhos** e clique na guia **Trabalho Programado** para exibir a página Trabalhos Programados.
  2. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Programar Novos Trabalhos.
  3. Insira um nome para o trabalho.
  4. Especifique quando o trabalho deve ser executado.
     - **Única**. Esses trabalhos são executados apenas uma vez.
       a. Especifique a data e hora em que deseja que o trabalho seja executado e clique em **Avançar**.
       b. Selecione os dispositivos gerenciados em que o trabalho deve ser executado.
     - **Recorrente**. Esses trabalhos são executados mais de uma vez.
       a. Especifique quando e com que frequência deseja que o trabalho seja executado.
       b. Selecione os dispositivos gerenciados em que o trabalho deve ser executado**.**
     - **Acionado pelo evento**. Esses trabalhos são executados quando ocorre um evento específico.
       a. Especifique a data e hora em que deseja que o trabalho seja executado e clique em **Avançar**.
       b. Selecione os dispositivos gerenciados em que o trabalho deve ser executado e clique em **Avançar**.
       c. Selecione o evento para acionar o trabalho.
  5. Clique em **Criar**.

Depois de concluir

A guia Trabalhos Programados é exibida com uma lista de todas as programações de trabalho no XClarity Administrator.



Nesta página, é possível executar as ações a seguir:

- Exibir informações sobre todos os trabalhos concluídos e ativos de uma programação de trabalho específica clicando no link na coluna **Trabalho**.
  - Refinar a lista de programações de trabalho que são exibidas por um tipo de programação específico clicando em **Tipos de Programação** e escolhendo as opções a seguir:
    - **Todos os Tipos de Programação**
    - **Única**
    - **Recorrente**
    - **Acionado**
  - Ocultar ou mostrar somente programações de trabalho que estão em um estado específico clicando em um dos seguintes ícones:
    - Todos os trabalhos programados que estão ativos clicando no ícone **Ativo** ( ).
    - Todos os trabalhos programados que não estão ativos clicando no ícone **Pausado** ( ).
    - Todos os trabalhos programados que já foram executados e não estão programados para serem executados novamente clicando no ícone **Finalizado** ( ).
  - Listar apenas os trabalhos programados que contêm texto específico inserindo o texto no campo **Filtro**.
  - Classificar os trabalhos programados por coluna clicando em um título de coluna.
- Visualizar quando o trabalho foi executado pela última vez examinando a coluna **Última Execução**. Exibir o status do último trabalho executado clicando no link "Status do Trabalho" nessa coluna.
- Visualizar quando o trabalho está programado para ser executado novamente examinando a coluna **Próxima Execução**. Exibir uma lista de todas datas e horas futuras clicando no link "Mais" nessa coluna.

- Executar imediatamente o trabalho que está associado à programação clicando no ícone **Executar** ().
- Habilitar ou desabilitar uma programação de trabalho clicando no ícone **Pausar** () ou **Ativar** (), respectivamente.
- Copiar e modificar uma programação de trabalho clicando no ícone **Copiar** ().
- Editar uma programação de trabalho clicando no ícone **Editar** ().
- Excluir uma ou mais programações de trabalho selecionadas clicando no ícone **Excluir** ().
- Exporte informações sobre programações de tarefa específicas selecionando as programações e clicando no ícone **Exportar como CSV** ().
- Atualizar a lista de programação do trabalho clicando em **Todas as Ações → Atualizar**.

Adicionando uma resolução e comentários a um trabalho

É possível adicionar uma resolução e comentários a um trabalho concluído, independentemente do estado de sucesso ou erro. É possível fazer isso para uma tarefa pai e para subtarefas da tarefa.

Procedimento

Conclua uma das seguintes etapas para adicionar uma resolução e comentários a um trabalho.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitor → Trabalhos** e clique na guia **Status do Trabalho** para exibir a página Status dos trabalhos.

Etapa 2. Clique no link para a tarefa na coluna **Tarefa** para exibir os detalhes da tarefa.

Etapa 3. Clique no ícone **Notas** () para exibir a caixa de diálogo Notas.

Nessa caixa de diálogo, você pode ver um histórico de todas as notas e resoluções que foram adicionadas à tarefa. Você pode limpar o histórico clicando em **Limpar todos os registros**.

Etapa 4. Escolha uma das seguintes resoluções.
- **Sem alterações**
- **Investigação**
- **Resolvido**
- **Interrompido**

Etapa 5. Inclua um lembrete no campo **Nota**.

Etapa 6. Clique em **Aplicar**.

Na página Status da tarefa, a resolução é exibida na coluna **Status** da tarefa.

Exibir relações entre os trabalhos e eventos

Um *fluxograma* é uma exibição gráfica que mostra as relações entre atividades (incluindo trabalhos e eventos) que são iniciadas manualmente por um usuário ou iniciadas automaticamente pelo Lenovo XClarity Administrator. O fluxograma ajuda a identificar problemas ilustrando a sequência de ações que foram iniciadas e eventos que foram gerados, e o que fez com que fossem gerados.

Antes de iniciar

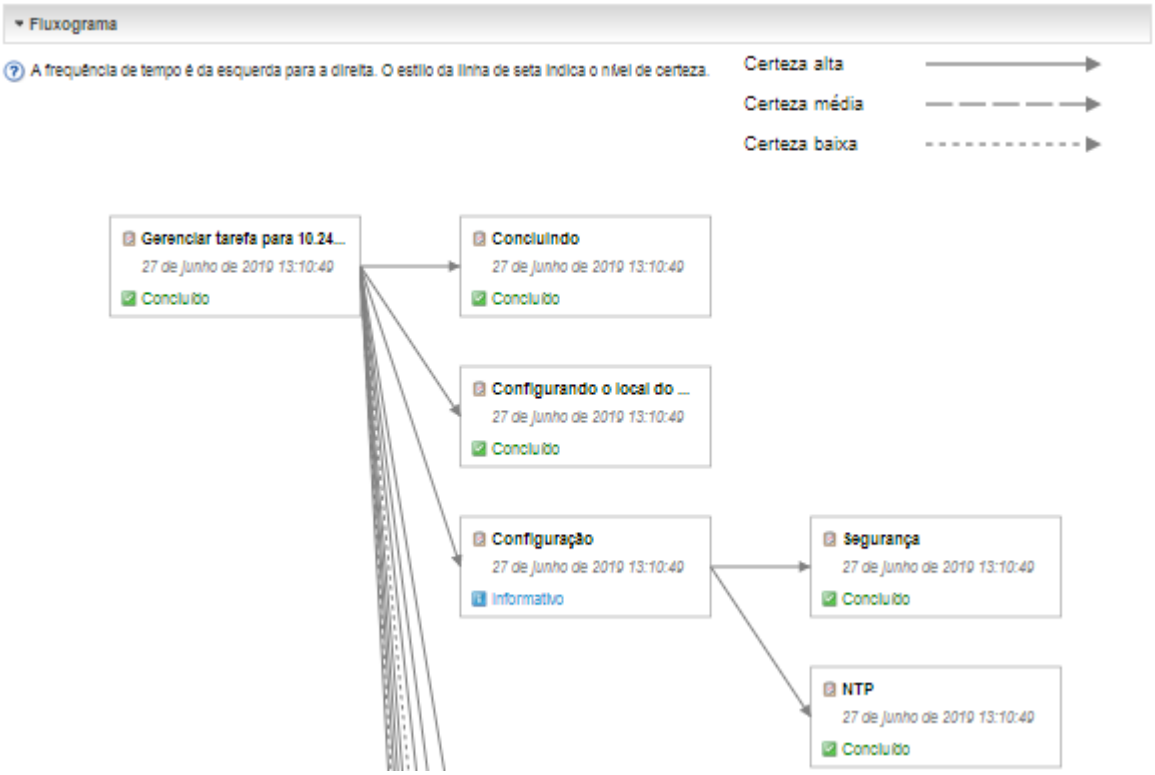
Os fluxos de atividades são desativados por padrão. Você deve ativar os fluxos de atividades antes que os fluxos possam ser gerados para uma atividade. É possível exibir os fluxos somente para atividades que ocorrem quando o Fluxo de atividades está habilitado.

Atenção: Os fluxos de atividades aumentam o uso de memória do XClarity Administrator. É recomendável que não ativar fluxos de atividades se o uso de memória do XClarity Administrator já estiver alto.

Sobre esta tarefa

O exemplo a seguir ilustra um diagrama de fluxo. A sequência de fluxo de eventos da esquerda para a direita. Cada nó no fluxo representa uma única atividade e inclui a descrição da atividade, data e status. Você pode passar o cursor sobre o título do nó para exibir informações adicionais sobre a atividade.

O estilo das linhas entre os nós indica a certeza de relação entre os nós.
- Linhas sólidas representam um nível alto de certeza.
- Linhas tracejadas longas representam um nível médio de certeza.
- Linhas tracejadas curtas representam um nível baixo de certeza.



Procedimento

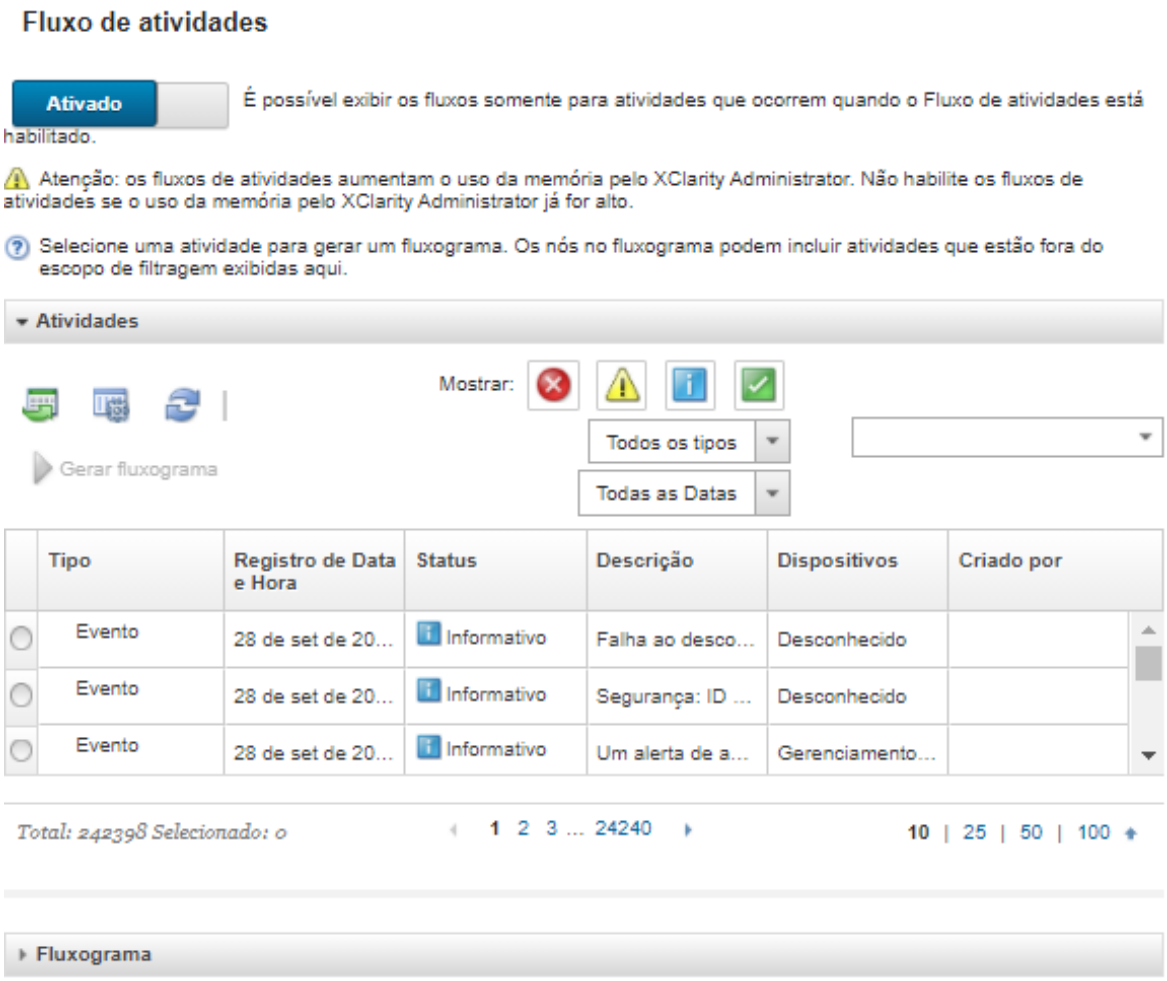
Conclua as etapas a seguir para visualizar o diagrama de fluxo para uma atividade específica.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Fluxos ativos** para visualizar a página de Fluxos ativos.

Etapa 2. Ative os fluxos de atividades selecionando **Ativar fluxo de atividades**.

Etapa 3. Na seção **Atividades**, selecione o trabalho ou o evento.

É possível classificar as colunas da tabela para facilitar a localização das atividades específicas. Além disso, você pode selecionar um tipo de status, tipo de atividade, data, inserir um filtro personalizado ou um texto (como um nome ou endereço IP) no campo **Filtro** e listar somente as atividades que correspondem aos critérios selecionados



Etapa 4. Clique em **Gerar Diagrama de Fluxo** para exibir o diagrama de fluxo na seção **Diagrama de Fluxo**

Depois de concluir

Nesta página, é possível executar as ações a seguir:

- Exibir informações adicionais sobre cada atividade no diagrama de fluxo, posicionando o cursor sobre a atividade.
- Exportar fluxo relacionado das atividades selecionados para um arquivo CSV clicando em **Ações → Exportar para CSV**.

Capítulo 4. Considerações sobre gerenciamento

Há várias alternativas quando se trata de gerenciar dispositivos. Dependendo dos dispositivos que estiverem sendo gerenciados, talvez você precise de várias soluções de gerenciamento em execução ao mesmo tempo.

Um dispositivo pode ser gerenciado somente por uma instância do Lenovo XClarity Administrator. No entanto, você pode usar outro software de gerenciamento (como o VMware vRealize Operations Manager) com Lenovo XClarity Administrator para *monitorar* dispositivos gerenciados pelo XClarity Administrator.

Atenção: É necessário tomar cuidado ao usar diversas ferramentas de gerenciamento para gerenciar dispositivos a fim de evitar conflitos imprevistos. Por exemplo, o envio de alterações de estado de energia usando outra ferramenta pode entrar em conflito com trabalhos de configuração ou de atualização em execução no XClarity Administrator.

Dispositivos ThinkSystem, ThinkServer e System x

Caso pretenda usar outro software de gerenciamento para monitorar seus dispositivos gerenciados, crie um novo usuário local com configurações de SNMP ou IPMI corretas da interface IMM. Conceda privilégios de SNMP ou IPMI, dependendo de suas necessidades.

Dispositivos Flex System

Caso pretenda usar outro software de gerenciamento para monitorar seus dispositivos gerenciados, e se esse software de gerenciamento usar comunicação SNMPv3 ou IPMI, você deverá preparar seu ambiente executando as seguintes etapas para cada CMM gerenciado:

1. Faça logon na interface da Web do controlador de gerenciamento do chassi usando o nome de usuário e a senha `RECOVERY_ID`.
2. Se a política de segurança for definida como **Seguro**, altere o método de autenticação do usuário.
   a. Clique em **Gerenciamento do Módulo de Gerenciamento → Contas do Usuário**.
   b. Clique na guia **Contas**.
   c. Clique em **Configurações de login global**.
   d. Clique na guia **Geral**.
   e. Selecione **Primeiro autenticação externa, depois local** para o método de autenticação do usuário.
   f. Clique em **OK**.
3. Crie um novo usuário local com as configurações SNMP ou IPMI corretas na interface da Web do controlador de gerenciamento.
4. Se a política de segurança for definida como **Seguro**, faça logout e login na interface da Web do controlador de gerenciamento usando o novo nome de usuário e senha. Quando solicitado, altere a senha para o novo usuário.

Agora você poderá usar o novo usuário como um usuário SNMP ou IPMI ativo.

Nota: Se você cancelar o gerenciamento e, em seguida, gerenciar o chassi novamente, essa nova conta do usuário ficará bloqueada e desativada. Nesse caso, repita essas etapas para criar uma nova conta de usuário.

Capítulo 5. Gerenciando grupos de recursos

É possível usar o grupo de recursos em Lenovo XClarity Administrator para criar um conjunto lógico de dispositivos gerenciados que você pode exibir em conjunto e trabalhar.

Saiba mais: XClarity Administrator: Grupos de recursos

Sobre esta tarefa

Há três tipos de grupos de recursos:

- **Static**. Grupo personalizado de dispositivos específicos.
- **Dinâmico**. Grupo de dispositivos com base em regras (por exemplo, todos os servidores de um tipo específico). Esse grupo contém uma lista dinâmica de dispositivos com base em um conjunto de propriedades de inventário.

Ações não podem ser executadas em um grupo de recursos. No entanto, você pode selecionar todos os dispositivos no grupo e executar ações coletivamente em todos os dispositivos selecionados.

Exibindo o status dos dispositivos em um grupo de recursos

É possível exibir o status de todos os dispositivos gerenciados em um grupo de recursos.

Sobre esta tarefa

Os seguintes ícones de status são usados para indicar a integridade geral de todos os dispositivos do grupo de recursos. A integridade geral do grupo indica o dispositivo com a gravidade mais alta no grupo.

- Ícone **Crítico** ( )
- Ícone **Aviso** ( )
- Ícone **Normal** ( )

Procedimento

Conclua as etapas a seguir para exibir o status dos dispositivos em um grupo de recursos.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Painel**. A página Painel é exibida com uma visão geral e o status de todos os dispositivos gerenciados e outros recursos, incluindo os grupos de recursos.

Etapa 2. Na barra de menu do XClarity Administrator, clique em **Hardware → Grupos de Recursos**. A página Todos os Grupos de Recursos é exibida.

A página Todos os Grupos de Recursos lista cada grupo de recursos, incluindo o nome do grupo, a quantidade de dispositivos gerenciados que estão no grupo e o status do dispositivo com a gravidade mais alta no grupo.

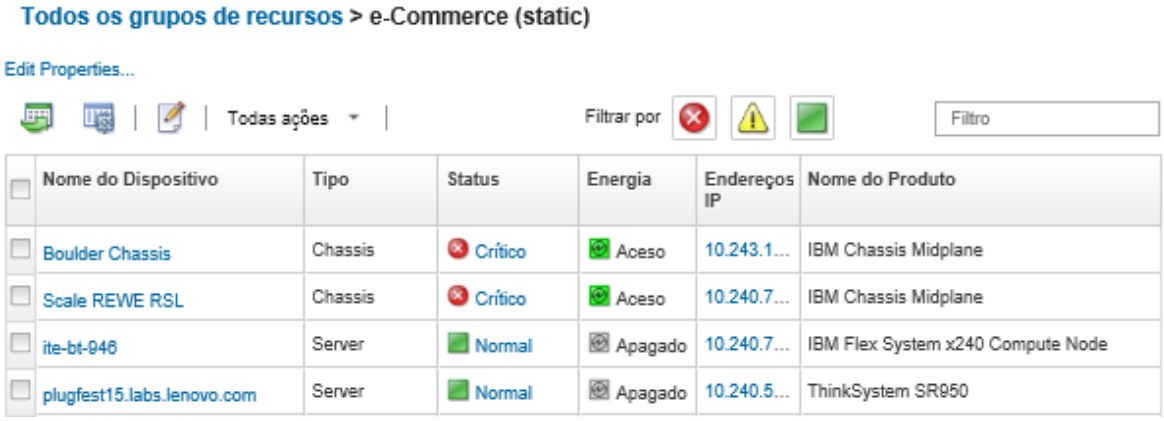
Nesta página, é possível executar as ações a seguir:

- Criar um novo grupo de recursos (consulte Criando um grupo de recursos dinâmico e Criando um grupo de recursos estático)
- Edite a associação do grupo selecionando um grupo e clicando no ícone **Editar** ( ).
- Edite as propriedades do grupo selecionando o grupo e clicando em **Todas as Ações → Editar propriedades**.
- Remova um grupo de recursos selecionando um grupo e clicando no ícone **Excluir** ( ).

  Nota: Remover um grupo remove apenas a definição do grupo. Isso não afeta os dispositivos no grupo.

- Exporte informações detalhadas sobre todos os dispositivos em um ou mais grupos de recursos para um arquivo CSV clicando no ícone **Exportar** ( ).

Etapa 3. Na página Todos os Grupos de Recursos, clique no nome na coluna **Grupos** para exibir a lista de dispositivos nesse grupo.



Nesta página, é possível executar as ações a seguir:

- Adicione ou remova dispositivos em um grupo de recursos estático clicando no ícone **Editar** ( ).
- Exiba informações detalhadas sobre um dispositivo específico no grupo de recursos clicando no nome do dispositivo na coluna **Nome do Dispositivo**.
- Exporte informações detalhadas sobre todos os dispositivos em um ou mais grupos de recursos para um arquivo CSV clicando no ícone **Exportar** ( ).

Exibindo os membros de um grupo de recursos

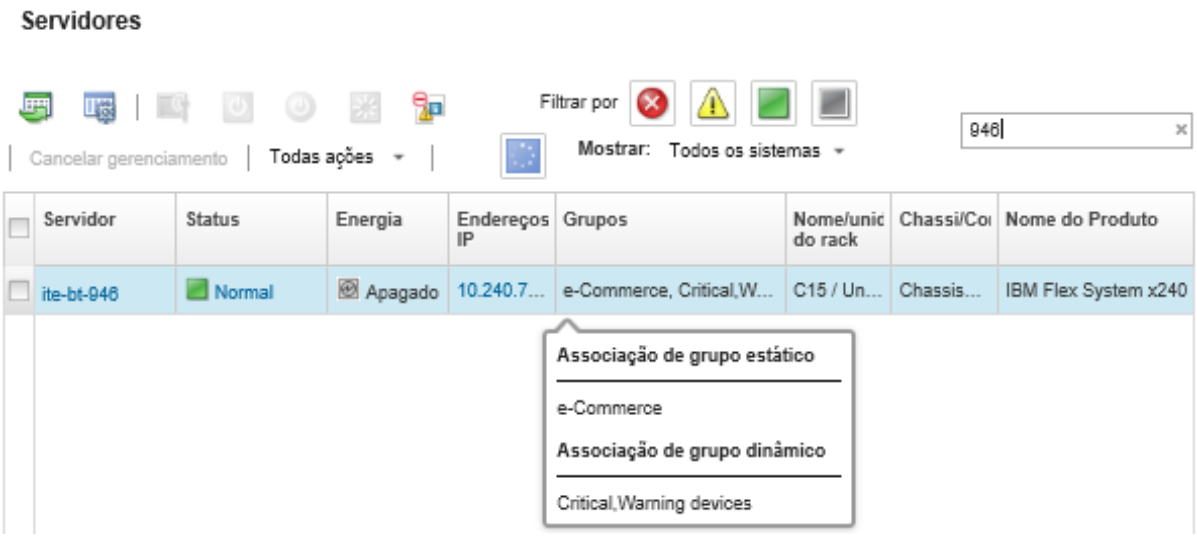
É possível exibir informações detalhadas sobre os grupos de recursos, incluindo membros do grupo.

Procedimento

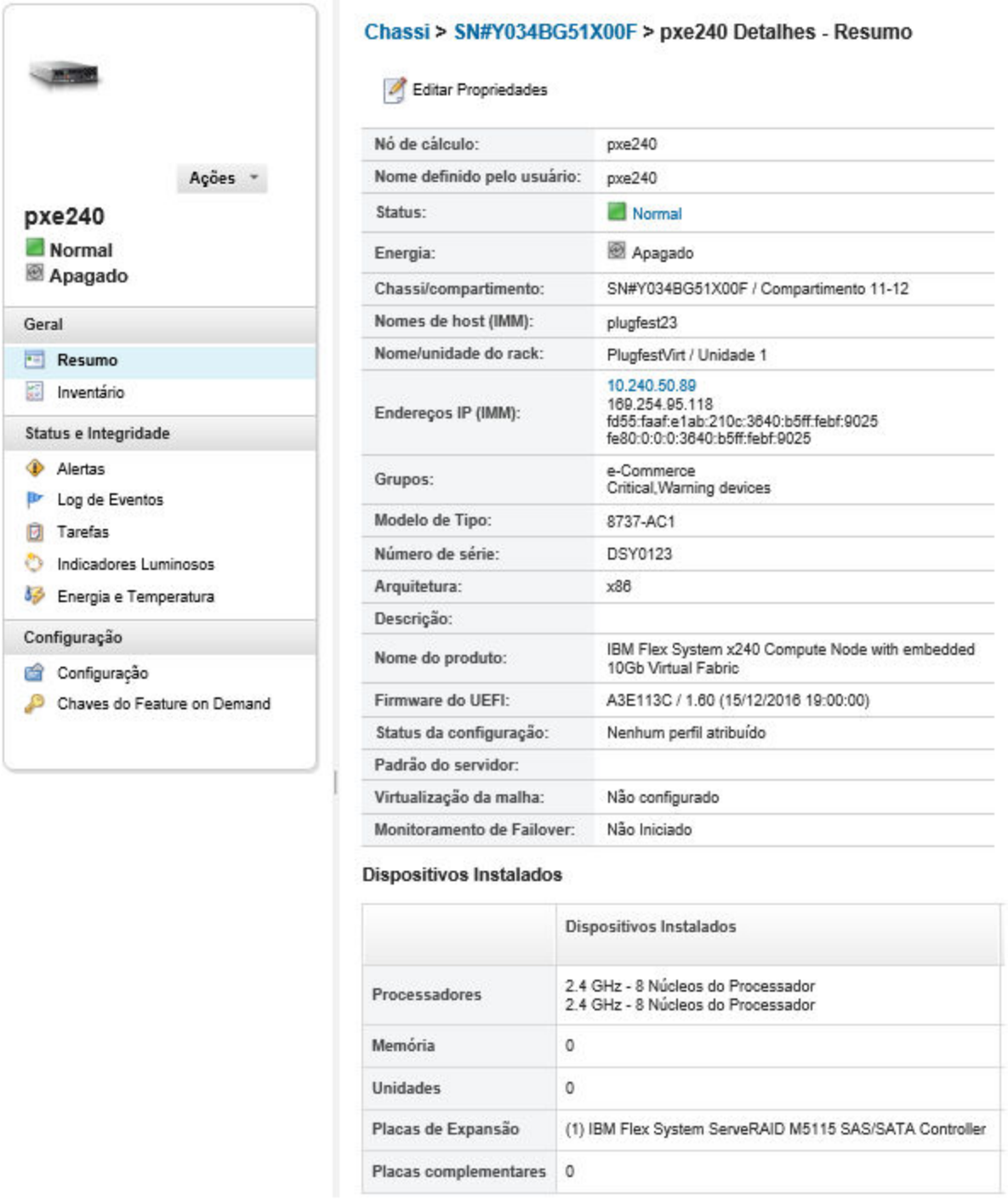
Conclua as etapas a seguir para exibir a associação do grupo.

- Para exibir todos os grupos dos quais um dispositivo é membro.
  1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware** e, em seguida, clique no tipo de dispositivo para exibir a página de todos os dispositivos.

     Passe o mouse sobre as listas de grupos na coluna **Grupos** para listar os grupos dos quais o dispositivo é membro.



2. Clique no link do nome do dispositivo na primeira coluna. A página de resumo desse dispositivo é exibida, incluindo uma lista de grupos de recursos dos quais o dispositivo é membro.

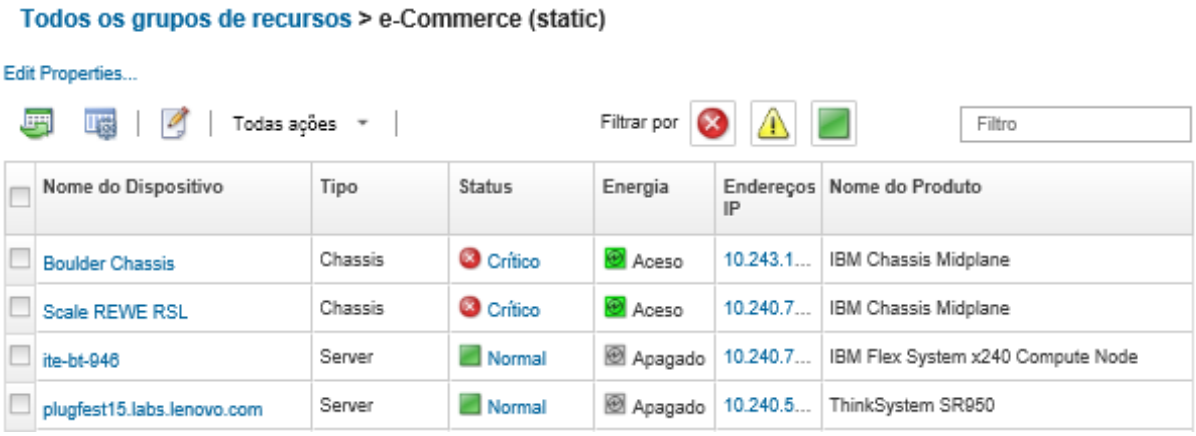


- Para exibir os membros de um grupo.
  1. Na barra de menus XClarity Administrator, clique em **Painel**. A página Painel é exibida com uma visão geral e o status de todos os dispositivos gerenciados e outros recursos, incluindo os racks.
  2. Na barra de menu do XClarity Administrator, clique em **Hardware → Grupos**. A página Grupos de Recursos é exibida.

     Essa página lista o número total de membros e o número de membro de cada tipo de dispositivo do grupo.

3. Na página Todos os Grupos de Recursos, clique no nome na coluna **Grupos** para exibir os detalhes do grupo de recursos.

   Essa página lista cada dispositivo que é membro do grupo de recursos.



Criando um grupo de recursos dinâmico

Você pode criar um grupo de recursos para um conjunto dinâmico de dispositivos gerenciados com base em um conjunto de critérios.

Sobre esta tarefa

É possível criar um grupo de recursos dinâmico usando um ou mais dos seguintes critérios para cada tipo de dispositivo.

Critérios	Chassi	Chassi denso.	Servido-res	Comuta-dor Flex System	comuta-dor RackS-witch	Dispositi-vo de armaze-namento
Nome da placa complementar			✓ (exceto ThinkSer-ver)			
Entre em contato	✓		✓		✓	✓
Descrição	✓	✓	✓		✓	✓

Critérios	Chassi	Chassi denso.	Servido-res	Comuta-dor Flex System	comuta-dor RackS-witch	Dispositi-vo de armaze-namento
Nome de domínio totalmente qualificado	✓		✓			
Nome do Host	✓		✓	✓	✓	
Endereço IPv4*	✓		✓	✓	✓	✓
Endereço IPv6	✓		✓	✓	✓	
Local	✓	✓	✓		✓	✓
Tipo de máquina	✓		✓	✓	✓	✓
Modelo	✓		✓	✓	✓	✓
Estado de funcionamento geral	✓		✓	✓	✓	✓
Núcleos do processador			✓			
Nome do produto	✓		✓	✓	✓	✓
Rack	✓	✓	✓		✓	✓
Sala	✓	✓	✓		✓	✓
Nome definido pelo usuário	✓	✓	✓	✓	✓	✓

Nota: Para endereços IPv4, é possível especificar um único endereço ou um intervalo de endereços, separados por hífen ou usando um asterisco como curinga (por exemplo, `1.1.1.*` ou `1.1.1.1-1.1.1.255` sem espaços).

Procedimento

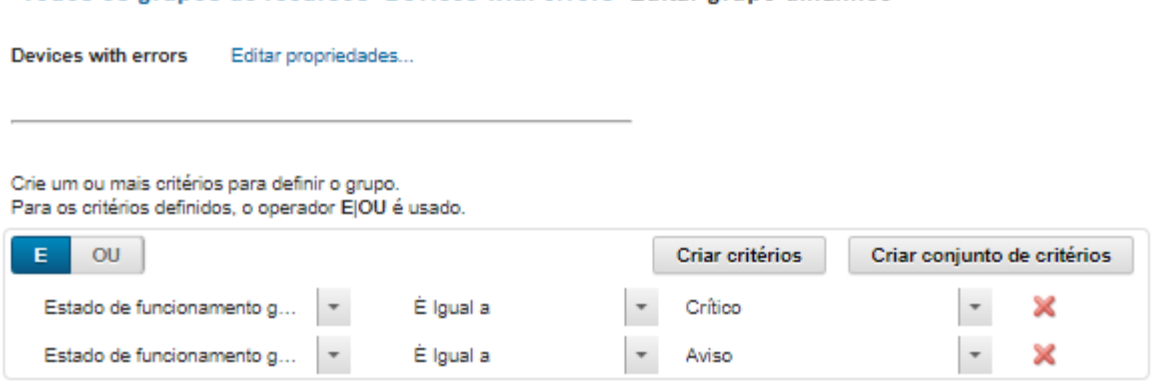
Para criar e preencher um grupo de recursos dinâmico, conclua as etapas a seguir

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Grupos de Recursos**. A página Todos os Grupos de Recursos é exibida.

Etapa 2. Clique no ícone **Criar** ( ) para criar um grupo vazio. A caixa de diálogo Criar Grupo Vazio é exibida.

Etapa 3. Selecione **Grupo Dinâmico** para agrupar dispositivos com base em um conjunto de critérios.

Etapa 4. Clique em **Criar**. A caixa de diálogo Editar Grupo Dinâmico é exibida.



Etapa 5. Adicione critérios para esse grupo dinâmico.

- Selecione o operador a ser usado para o conjunto de grupos. Este pode ser um dos valores a seguir:
  - **E**. Os membros devem satisfazer todos os valores especificados.
  - **OU**. Os membros devem satisfazer um ou mais dos valores especificados.
- Clique em **Criar Critérios** para adicionar uma nova regra de critérios ao conjunto.
- Clique em **Criar Conjunto de Critérios** para adicionar um subconjunto de regras de critérios.

Nota: Novos critérios e conjuntos de critérios são sempre incluídos na parte inferior da lista.

Etapa 6. Clique em **Aplicar** para salvar os critérios de grupo e criar o grupo ou clique em **Visualizar** para ver quais dispositivos são incluídos no grupo usando os critérios atuais sem criar o grupo.

Depois de concluir

- É possível ver a quais grupos de recursos um dispositivo pertence na coluna **Grupos** nas páginas de todos os dispositivos e nas páginas de resumo do dispositivo.
- É possível modificar os critérios do grupo dinâmico selecionando o grupo de recursos e clicando no ícone **Editar** ( ).
- É possível modificar as propriedades do grupo de recursos clicando em **Todas as Ações → Editar propriedades**.

Criando um grupo de recursos estático

Você pode criar um grupo de recursos que contém um conjunto personalizado de dispositivos gerenciados.

Procedimento

Para criar e preencher um grupo de recursos estático, conclua as etapas a seguir.

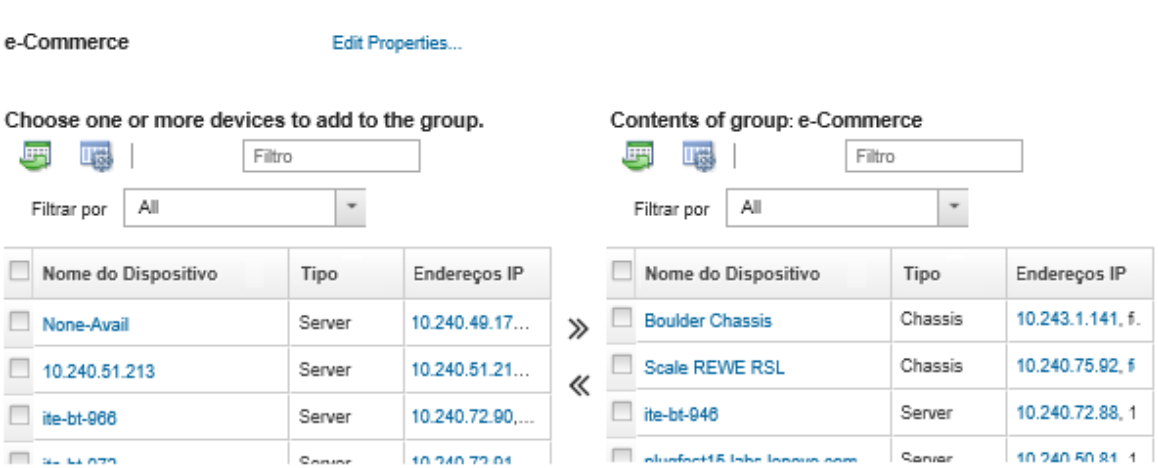
Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Grupos de Recursos**. A página Grupos de Recursos é exibida.

Etapa 2. Clique no ícone **Criar** ( ) para criar um grupo vazio. A caixa de diálogo Criar Grupo Vazio é exibida.

Etapa 3. Especifique o nome do grupo e a descrição opcional.

Etapa 4. Selecione **Grupo Estático** para criar um grupo de dispositivos definidos explicitamente.

Etapa 5. Clique em **Criar**. A página Editar Grupo Estático é exibida.



Etapa 6. Selecione os dispositivos que você deseja incluir no grupo na lista **Todos os dispositivos disponíveis que não estão no grupo** e clique no ícone **Adicionar** (») para mover os dispositivos selecionados para a lista **Conteúdo do grupo**.

Notas:

- É possível classificar as listas para facilitar a localização dos dispositivos específicos clicando nos cabeçalhos da coluna. Além disso, é possível selecionar um tipo de dispositivo na lista suspensa **Filtrar por**, selecionar um chassi na lista suspensa ou inserir texto (como nome ou endereço IP) no campo **Filtro** e para listar somente os dispositivos que correspondem aos critérios selecionados
- Se você optar por mover um chassi para o grupo, os dispositivos no chassi não serão adicionados automaticamente ao grupo. Para adicionar todos os componentes do chassi ao grupo, selecione **Chassi** → <*chassis_name*> no menu suspenso **Mostrar** para listar todos os componentes no chassi especificado, marque a caixa de seleção ao lado do cabeçalho da coluna Nome do dispositivo para selecionar todos os dispositivos e, em seguida, clique no ícone **Adicionar** (») para mover os dispositivos selecionados para a lista **Conteúdo do grupo**.

Depois de concluir

- É possível ver a quais grupos de recursos um dispositivo pertence na coluna **Grupos** nas páginas de todos os dispositivos e nas páginas de resumo do dispositivo.
- É possível adicionar ou remover um dispositivo de um grupo de recursos estático nas páginas de todos os dispositivos e nas páginas de detalhes do dispositivo clicando em **Todas as Ações** → **Grupos** → **Adicionar ao grupo** ou **Todas as Ações** → **Grupos** → **Remover do grupo**.

  Nota: Você pode adicionar e remover dispositivos apenas dos grupos de recursos estáticos. Não é possível removê-los de grupos dinâmicos.
- É possível modificar as propriedades do grupo de recursos clicando em **Todas as Ações** → **Editar propriedades**.

Removendo um grupo de recursos

É possível remover um grupo de recursos do Lenovo XClarity Administrator.

Sobre esta tarefa

Excluir um grupo exclui apenas a definição do grupo. Isso não afeta os dispositivos nesse grupo.

Procedimento

Conclua as seguintes etapas para remover um grupo de recursos.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware** → **Grupos de Recursos**. A página Todos os Grupos de Recursos é exibida.

A página Todos os Grupos de Recursos lista cada grupo de recursos, incluindo o nome do grupo, a quantidade de dispositivos gerenciados que estão no grupo e o status do dispositivo com a gravidade mais alta no grupo.

Etapa 2. Selecione o grupo de recursos a ser removido.

Etapa 3. Clique no ícone **Excluir** ( ).

Etapa 4. Clique em **Excluir**.

Modificando propriedades do grupo de recursos

É possível alterar as propriedades de um grupo de recursos específico.

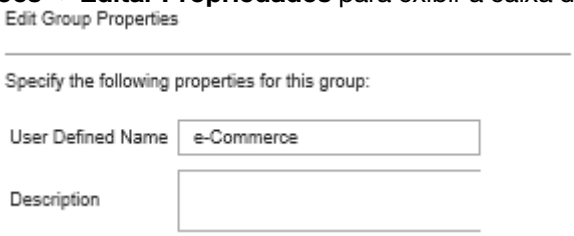
Procedimento

Conclua as etapas a seguir para modificar as propriedades do grupo de recursos

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Grupos de Recursos** para exibir a página Todos os Grupos de Recursos

Etapa 2. Selecione o grupo de recursos a ser atualizado.

Etapa 3. Clique em **Todas as Ações → Editar Propriedades** para exibir a caixa de diálogo Editar Propriedades do Grupo.



Etapa 4. Altere as seguintes informações, conforme necessário.
- Nome do grupo
- Descrição

Etapa 5. Clique em **Salvar**.

Nota: Quando você alterar essas propriedades, poderá haver um pequeno atraso até as alterações aparecerem na interface da Web do XClarity Administrator

Capítulo 6. Gerenciando racks

É possível usar racks do Lenovo XClarity Administrator para agrupar seus dispositivos gerenciados e refletir a configuração física do rack em seu datacenter.

Antes de iniciar

Depois de mover um nó de um chassi para outro, aguarde 5 a 10 minutos antes de tentar editar os racks do XClarity Administrator que contém o chassi.

Quando você move um dispositivo para fora de um rack, o nome do rack e os menores valores da unidade de rack são limpos no inventário do dispositivo. Os valores de espaço e local não são limpos.

Sobre esta tarefa

Este procedimento descreve como criar e preencher um único rack com dispositivos gerenciados e preenchimentos interativamente.

Se você adicionar muitos dispositivos nos racks ou editar vários racks, considere utilizar a planilha para executar a importação em massa ou implementar um script do PowerShell para automatizar a tarefa. Para obter mais informações sobre como usar a importação em massa, consulte Gerenciando chassi e Gerenciando servidores. Para obter informações sobre os scripts do PowerShell, consulte Kit de ferramentas PowerShell (LXCAPSTool) na documentação online do XClarity Administrator.

O XClarity Administrator reconhece as propriedades do rack definidas em um dispositivo gerenciável. Quando você gerencia esse dispositivo, o XClarity Administrator configura as propriedades do sistema para esse dispositivo e atualiza a exibição do rack. Se o rack não existe no XClarity Administrator, um novo rack é criado e o dispositivo é adicionado no rack.

Notas:

- Os servidores System x3500 M5, NeXtScale nx360 M5, ThinkServer SD350 e em torre não têm suporte na exibição de rack.
- Nos sistemas complexos escaláveis System x3850 X5, você deverá adicionar cada nó (servidor) no rack individualmente.
- O hardware da demonstração não é persistente nas exibições do rack quando o XClarity Administrator é reiniciado.

Procedimento

Para criar e preencher racks, conclua as etapas a seguir.

- Crie e preencha um único rack com dispositivos gerenciados.
  1. Na barra de menu do XClarity Administrator, clique em **Hardware → Racks**. A página Todos os racks é exibida.

     A página Todos os racks mostra cada rack como uma imagem de miniatura o nome do rack, quantidade de dispositivos gerenciados que estão no rack e o status do dispositivo com a severidade mais alta.

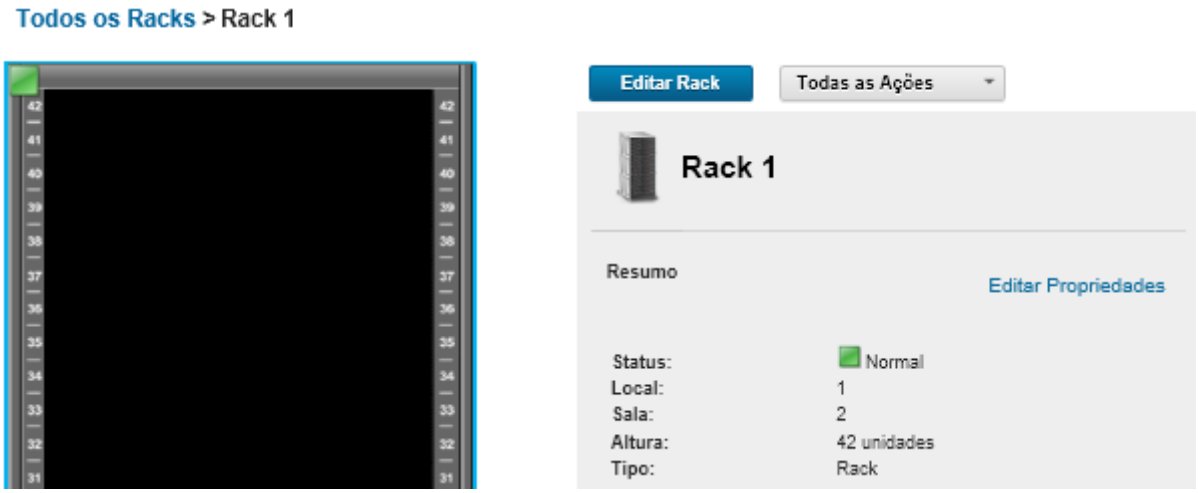
     Notas: É possível filtrar os racks por severidade, clicando nos seguintes ícones na barra de ferramentas. Também é possível inserir um nome do rack no campo **Filtro** para filtrar mais racks a serem exibidos.

- Ícone **Alertas críticos** ( )
- Ícone **Alertas de avisos** ( )
- Ícone **Alertas normais** ( )

2. Clique no ícone **Criar** ( ) para criar um rack vazio. A caixa de diálogo Criar Rack Vazio é exibida.
3. Preencha a caixa de diálogo com o nome, altura, local, e o espaço do rack.

   Notas:

   - Os nomes de racks não precisam ser exclusivos. Você pode criar racks com o mesmo nome, desde que a localização ou sala ou ambos sejam diferentes.
   - O nome do rack pode incluir apenas letras maiúsculas e minúsculas, números e os seguintes caracteres especiais: ponto (.), hífen (-) e sublinhado (_).
   - O local pode conter no máximo 23 caracteres.
4. Clique em **Criar**. Uma imagem em miniatura para o novo rack é adicionado na página Todos os Racks.
5. Clique duas vezes na imagem em miniatura do rack. A página de exibição do rack é exibida rack com uma imagem do rack vazia e suas propriedades.



6. Clique em **Editar Rack** para exibir a página Editar Rack.

7. Adicione todos dispositivos gerenciados e preenchimentos apropriados à exibição gráfica:

   Nota: Somente dispositivos gerenciados que estão no estado Online podem ser incluídos no rack.

   - Clique na guia **Chassi** para exibir uma lista de chassis gerenciados que não foram adicionados em um rack. Arraste e solte um chassi gerenciado para o local apropriado no rack para adicioná-lo ao rack.
   - Clique na guia **Gabinetes do Servidor** para exibir uma lista de servidores de rack e gabinetes do servidor de vários nós gerenciados que não foram incluídos em um rack. Arraste e solte um servidor do rack ou gabinetes do servidor no rack no local desejado para incluir o servidor do rack no rack.
   - Clique na guia **RackSwitch** para exibir uma lista de comutadores RackSwitch gerenciados que não foram adicionados em um rack. Arraste e solte um comutador RackSwitch ao rack no local desejado para adicioná-lo ao rack.
   - Clique na guia **Armazenamento** para exibir uma lista de diversos dispositivos de armazenamento. Arraste e solte o dispositivo de armazenamento apropriado ao rack no local desejado para adicioná-lo ao rack.
   - Clique na guia **Preenchimentos** para exibir uma lista de diversos preenchimentos. Arraste e solte o preenchimento apropriado ao rack no local desejado para adicioná-lo ao rack.

     Um *preenchimento* é qualquer dispositivo que esteja no rack que não é gerenciado por XClarity Administrator. Os preenchimentos a seguir estão disponíveis:
     - Preenchimentos genéricos
     - Comutadores do rack genéricos
     - Controladores de armazenamento e gabinetes
     - Controladores de armazenamento e gabinetes de parceiros (como a IBM, NetApp e EMC)

     - As propriedades de local, sala, rack e menor unidade do rack são atualizadas para o dispositivo ao incluir ou remover dispositivos de um rack.
     - É possível classificar a lista dispositivos em cada guia usando a lista suspensa **Exibir por**. Além disso, é possível digitar texto (como um nome ou endereço IP) no campo **Filtro** para filtrar mais dispositivos que são exibidos.

– É possível remover dispositivos gerenciados e preenchimentos do rack arrastando e soltando os objetos fora do rack.

8. Clique em **Salvar** para salvar o configuração do rack.

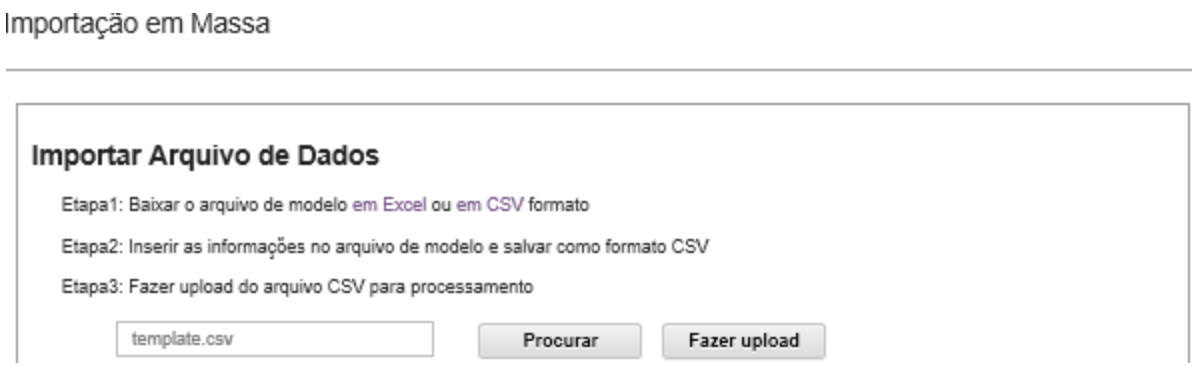
   O processo de configuração pode levar vários minutos para ser concluído. Durante a configuração, as informações do rack e de locais são enviadas por push para o CMM ou Baseboard Management Controller para dispositivos gerenciados.

9. Personalize os preenchimentos adicionado ao rack clicando no preenchimento e, em seguida, em **Editar Propriedades**. Na caixa de diálogo Editar Propriedades, é possível especificar um nome, a menor unidade de rack (LRU) e uma URL a ser usada para iniciar a interface do usuário de gerenciamento para esse dispositivo.

   Dica: após a configuração do rack ser salva, é possível iniciar a interface do usuário de gerenciamento para um preenchimento clicando no preenchimento no rack e no link **Abrir URL**.

- Crie e preencha racks usando um arquivo de importação em massa.

1. Na barra de menu do XClarity Administrator, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos**. A página Descobrir e Gerenciar é exibida.
2. Clique em **Importação em Massa**. O assistente de Importação em Massa é exibido.



3. Clique no link **no Excel** ou **no CSV** na página Importar Arquivo de Dados para baixar o arquivo de importação em massa do modelo no formato Excel ou CSV.

   Importante: O arquivo de modelo pode ser alterado de uma versão para outra. Use sempre o modelo mais recente.

4. Preencha a planilha de dados no arquivo de modelo e salve o arquivo em formato CSV.

   Dica: o modelo em Excel inclui uma planilha **Dados** e uma planilha **Leia-me**. Use a planilha **Dados** para preencher os dados do dispositivo. A planilha **Leia-me** fornece informações sobre como preencher cada campo na planilha **Dados** (incluindo os campos obrigatórios) e dados de exemplo.

   Importante:

   – Os dispositivos são gerenciados na ordem listada no arquivo de importação em massa.

   – O XClarity Administrator usa as informações de atribuição de rack que estão definidas na configuração do dispositivo quando o dispositivo é gerenciado. Se você alterar a atribuição do rack no XClarity Administrator, o XClarity Administrator atualizará a configuração do dispositivo. Se você atualizar a configuração do dispositivo após o gerenciamento do dispositivo, as mudanças serão refletidas no XClarity Administrator.

   – É recomendável, mas não é necessário criar um rack explicitamente na planilha antes de atribuir o rack a um dispositivo. Se um rack não for definido explicitamente e o rack ainda não existir no XClarity Administrator, as informações de atribuição do rack que são especificadas para um dispositivo serão usadas para criar o rack com uma altura padrão de 52U.

Se você deseja usar outra altura de rack, defina explicitamente o rack na planilha antes de atribuí-lo a um dispositivo.

Para definir os racks no arquivo de importação em massa, complete as seguintes colunas necessárias.
- (Colunas A) Especifique o "rack" para o tipo de dispositivo.
- (Colunas V) Especifique o nome do rack.
- (Colunas X) Especifique a altura do rack. As seguintes alturas de rack são suportadas: Racks 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U e 52U.

A figura a seguir mostra um arquivo de importação em massa de exemplo com racks definidos.

A	V	W	X
Type	Rack name	Lowest rack unit	Height
rack	Rack_01		37
rack	Rack_02		52

Nota: É possível usar o mesmo arquivo de importação em massa para gerenciar dispositivos e adicionar esses dispositivos a um rack (consulte Gerenciando sistemas na documentação online do Lenovo XClarity Administrator).

5. No assistente de Importação em Massa, insira o nome do arquivo CSV para fazer upload do arquivo para processamento. Clique em **Procurar** para ajudá-lo a localizar o arquivo.
6. Clique em **Fazer upload** para fazer upload e validar o arquivo.
7. Clique em **Avançar** para exibir a página Resumo da Entrada com uma lista de racks e outros dispositivos a serem gerenciados e revise o resumo de racks e outros dispositivos que você deseja gerenciar.
8. Clique em **Avançar** para exibir a página Credenciais do Dispositivo. Clique em cada guia e, como opção, especifique as configurações globais e as credenciais a serem usadas para todos os dispositivos de um tipo específico. Os dispositivos que usarão as configurações globais e as credenciais são listados no lado direito de cada guia.
9. Clique em **Gerenciar**. A página Monitoramento dos Resultados é exibida com informações sobre o status de gerenciamento de cada dispositivo no arquivo de importação em massa.

   Um trabalho é criado para o processo de gerenciamento. Se você fechar o Assistente de importação em massa, o processo de gerenciamento continuará sendo executado em segundo plano. É possível monitorar o status do processo de gerenciamento no log de trabalhos. Para obter informações sobre o log de trabalhos, consulte "Monitorando trabalhos" na página 176.

Depois de concluir

É possível alterar a preferência de ordem de numeração do rack (consulte Definindo preferências de inventário).

Exibindo status dos dispositivos em um rack

Em cada rack, é possível exibir o status de todos os dispositivos gerenciados no rack.

Procedimento

Conclua uma ou mais atualizações da ação a seguir para exibir o status de todos os dispositivos em um rack.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Painel**. A página Painel é exibida com uma visão geral e o status de todos os dispositivos gerenciados e outros recursos, incluindo os racks.

Etapa 2. Na barra de menu do XClarity Administrator, clique em **Hardware → Racks**. A página Racks é exibida.

A página Racks mostra cada rack como uma imagem de miniatura o nome do rack, quantidade de dispositivos gerenciados que estão no rack e o status do dispositivo com a severidade mais alta.

Notas: É possível classificar a lista por nome do rack, número de dispositivos no rack ou por severidade para facilitar a localização de racks específicos. A classificação é ordenada da esquerda para a direita, de cima para baixo. Além disso, é possível filtrar os racks por severidade clicando nos seguintes ícones na barra de ferramentas ou insira o nome de um rack no campo **Filtro** para filtrar mais os racks exibidos.

- Ícone **Alertas críticos** ( )
- Ícone **Alertas de avisos** ( )
- Ícone **Alertas normais** ( )

Etapa 3. Na página Todos os racks, clique no nome do rack ou o clique duas vezes em uma miniatura do rack para exibir a exibição gráfica e as propriedade do rack.

A *exibição do rack* é uma exibição gráfica do rack frontal que mostra cada dispositivo no rack, incluindo chassi, servidores de rack, comutadores top-of-rack e preenchimentos. Um ícone de status de cada dispositivo indica o status atual desse dispositivo.

Nesta página, é possível executar as ações a seguir:

- Adiciona ou remove os dispositivos no rack clicando em **Editar Rack**.

  Nota: Quando você altera os componente no rack, pode haver um pequeno atraso até as informações aparecerem na interface do XClarity Administrator.
- Modifique as propriedades do dispositivo e do filtro (incluindo nome, local e URL para iniciar a interface da Web de gerenciamento) clicando no dispositivo ou no preenchimento e, em seguida, clicando em **Editar Propriedades** no painel de resumo do dispositivo.
- Exiba a interface da Web do controlador de gerenciamento de um dispositivo ou preenchimento clicando no dispositivo ou no preenchimento e, em seguida, clicando no link **Abrir URL** no painel de resumo do dispositivo.

Etapa 4. Exibe um status resumido ou detalhado para um dispositivo ou componente:

a. Clique em um dispositivo ou um componente no rack para exibir o resumo do status e as propriedades do dispositivo ou componente.

b. Clique duas vezes em um dispositivo para exibir a página de detalhes do dispositivo.

Procedimento

É possível alterar a preferência de ordem de numeração do rack (consulte Definindo preferências de inventário).

Removendo um rack

É possível remover um rack do Lenovo XClarity Administrator.

Procedimento

Conclua as seguintes etapas para remover um rack.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Racks**. A página Todos os racks é exibida.

A página Todos os racks mostra cada rack como uma imagem de miniatura o nome do rack, quantidade de dispositivos gerenciados que estão no rack e o status do dispositivo com a severidade mais alta.

Notas: É possível classificar a lista por nome do rack, número de dispositivos no rack ou por severidade para facilitar a localização de racks específicos. A classificação é ordenada da esquerda para a direita, de cima para baixo. Além disso, é possível filtrar os racks por severidade clicando nos seguintes ícones na barra de ferramentas ou insira o nome de um rack no campo **Filtro** para filtrar mais os racks exibidos.

- Ícone **Alertas críticos** ( )
- Ícone **Alertas de avisos** ( )
- Ícone **Alertas normais** ( )

Etapa 2. Selecione a miniatura para o rack a ser removido.

Etapa 3. Clique no ícone **Remover** ( ).

Etapa 4. Clique em **Remover**.

Resultados

A miniatura do rack é removido da página Todos os racks e todos os dispositivos que estavam no rack, estão agora disponíveis para inclusão em outro rack na página Editar Racks.

Capítulo 7. Gerenciando chassi

O Lenovo XClarity Administrator pode gerenciar diversos tipos de sistema, incluindo o chassi do Flex System.

Saiba mais: XClarity Administrator: descoberta

Antes de iniciar

Nota: Os componentes do chassi (como CMMs, nós de cálculo Flex e comutadores Flex) são descobertos e gerenciados automaticamente ao gerenciar o chassi que os contêm. Não é possível descobrir e gerenciar componentes do chassi separados do chassi.

Antes de gerenciar chassis, assegure-se de que as condições a seguir sejam atendidas:

- Reveja as considerações de gerenciamento antes de gerenciar um dispositivo. Para obter mais informações, consulte Considerações sobre gerenciamento na documentação online do XClarity Administrator.
- Algumas portas devem estar disponíveis para se comunicar com o CMM do chassi que está sendo gerenciado. Assegure-se de que essas portas estejam disponíveis antes de tentar gerenciar um chassi. Para obter mais informações sobre portas, consulte Disponibilidade de porta na documentação online do XClarity Administrator.
- Verifique se o firmware mínimo necessário está instalado em cada chassi que você deseja gerenciar usando o XClarity Administrator. É possível localizar os níveis mínimos de firmware necessários em Página da Web Suporte do XClarity Administrator – Compatibilidade clicando na guia **Compatibilidade** e, em seguida, clicando no link para os tipos de dispositivo apropriados.
- Assegure-se de que a configuração **Número de sessões ativas simultâneas para usuários LDAP** no CMM seja configurada como 0 (zero) para o chassi. Para verificar essa configuração na interface da Web do CMM, clique em **Gerenciamento do Módulo de Gerenciamento → Contas do Usuário**, clique em **Configurações Globais de Login** e depois clique na guia **Geral**.
- Verifique se há pelo menos três sessões do modo de comando TCP configuradas para comunicação fora da banda com o CMM. Para obter informações sobre como configurar o número de sessões, consulte Comando tcpcmdmode na documentação online do CMM.
- Para descobrir um chassi que está em uma sub-rede *diferente* do XClarity Administrator, certifique-se de que uma das seguintes condições seja atendida:
  - Certifique-se de habilitar o encaminhamento SLP multicast em comutadores top-of-rack, bem como nos roteadores do seu ambiente. Consulte a documentação que foi fornecida com seu comutador ou roteador específico para determinar se o encaminhamento SLP de multicast está ativado e para encontrar procedimentos para ativá-lo caso esteja desativado.
  - Se SLP estiver desabilitado no terminal ou na rede, você poderá usar o método de descoberta DNS, adicionando manualmente um registro de serviço (registro do servidor) ao servidor de nomes de domínio (DNS), para o XClarity Administrator, por exemplo.
    ```
    _lxca._tcp.labs.lenovo.com      service = 0 0 443 fvt-xhmc3.labs.lenovo.com.
    ```
    Em seguida, habilite a descoberta de DNS no CMM na interface da Web de gerenciamento, clicando em **Gerenciamento do Módulo de Gerenciamento → Protocolo de Rede**, clicando na guia **DNS** e selecionando **Usar DNS para descobrir o Lenovo XClarity Administrator**.

    Notas:

- O CMM deve estar executando um nível de firmware com data de maio de 2017 para dar suporte à descoberta automática usando DNS.
- Se houver várias instâncias do XClarity Administrator no seu ambiente, o chassi será descoberto apenas pela instância que for a primeira a responder à solicitação de descoberta. O chassi não será descoberto por todas as instâncias.

Avalie a possibilidade de implementar endereços IPv4 *ou* IPv6 para todos os CMMs e comutadores Flex gerenciados pelo XClarity Administrator. Se implementar IPv4 para alguns CMMs e comutadores Flex e IPv6 para outros, alguns eventos não serão recebidos no log de auditoria (ou como interceptações de auditoria).

Atenção: Caso pretenda gerenciar CMMs que estão executando um nível de firmware na versão 1.3.2.1 2PET12K da pilha Flex com 2PET12Q, que vem sendo executado há mais de três semanas e que estejam em uma configuração dupla do CMM, você deve reposicionar virtualmente os CMMs antes de atualizar o firmware, usando o XClarity Administrator.

Importante: Caso pretenda usar outro software de gerenciamento além do Lenovo XClarity Administrator para monitorar o chassi, e se esse software de gerenciamento usar comunicação SNMPv3, você deve primeiro criar um ID do usuário do CMM local que seja configurado com as informações de SNMPv3 apropriadas e depois fazer login no CMM usando esse ID do usuário e alterar a senha. Para obter mais informações, consulte Considerações sobre gerenciamento na documentação online do XClarity Administrator.

Sobre esta tarefa

O XClarity Administrator pode descobrir automaticamente o chassi em seu ambiente sondando sistemas gerenciáveis que estão na mesma sub-rede IP que o XClarity Administrator. Para descobrir os chassis que estão em outras sub-redes, especifique um endereço IP ou intervalo de endereços IP, ou importe informações de uma planilha.

Após os chassis serem gerenciados pelo XClarity Administrator, o XClarity Administrator sonda cada chassi gerenciado periodicamente para coletar informações, como inventário, dados vitais do produto e status. É possível exibir e monitorar cada chassi gerenciado e executar a ação de gerenciamento (como configurar informações do sistema, a configuração de rede e failover). Para chassis que estão no modo protegido, as ações de gerenciamento são desativadas.

Chassis são gerenciados usando a autenticação gerenciada do *XClarity Administrator*.

Por padrão, os dispositivos são gerenciados usando a autenticação gerenciada do XClarity Administrator para fazer login nos dispositivos. Ao gerenciar servidores em rack e chassis da Lenovo, você pode optar por usar autenticação local ou autenticação gerenciada para fazer login nos dispositivos.

- Quando a *autenticação local* é usada para servidores em rack, chassi da Lenovo e comutadores de rack da Lenovo, o XClarity Administrator usa uma credencial armazenada para autenticar o dispositivo. A *credencial armazenada* pode ser uma conta do usuário ativa no dispositivo ou uma conta do usuário em um servidor do Active Directory.

  Você deve criar uma credencial armazenada no XClarity Administrator que corresponda a uma conta do usuário ativa no dispositivo ou uma conta do usuário em um servidor do Active Directory antes de gerenciar o dispositivo usando a autenticação local (consulte Gerenciando credenciais compartilhadas na documentação online do XClarity Administrator).

  Notas:

  - Dispositivos RackSwitch oferecem suporte apenas a credenciais armazenadas para autenticação. Não há suporte para as credenciais do usuário do XClarity Administrator.

- Usar a *autenticação gerenciada* permite gerenciar e monitorar vários dispositivos usando as credenciais no servidor de autenticação do XClarity Administrator em vez de credenciais locais. Quando a autenticação gerenciada é usada para um dispositivo (diferente de servidores ThinkServer, servidores System x M4 e comutadores), o XClarity Administrator configura o dispositivo e seus componentes instalados para usar o servidor de autenticação do XClarity Administrator para gerenciamento centralizado.
  - Quando a autenticação gerenciada estiver habilitada, você poderá gerenciar dispositivos usando credenciais armazenadas ou inseridas manualmente (consulte Gerenciando contas de usuário e na documentação online do XClarity Administrator).

    A credencial armazenada é usada somente até que o XClarity Administrator configure as definições LDAP no dispositivo. Depois disso, qualquer mudança nas credenciais armazenadas não tem impacto no gerenciamento ou no monitoramento desse dispositivo.

    Nota: Quando a autenticação gerenciada é ativada para um dispositivo, não é possível editar credenciais armazenadas para esse dispositivo usando o XClarity Administrator.
  - Se um servidor LDAP local ou externo for usado como servidor de autenticação do XClarity Administrator, as contas de usuário definidas no servidor de autenticação serão usadas para fazer login no XClarity Administrator, em CMMs e no Baseboard Management Controllers no domínio XClarity Administrator. As contas de usuário do CMM local e do controlador de gerenciamento são desativadas.
  - Se um provedor de identidade SAML 2.0 for usado como servidor de autenticação do XClarity Administrator, as contas de SAML não estarão acessíveis para dispositivos gerenciados. Entretanto, ao usar um provedor de identidade SAML e um servidor LDAP juntos, se o provedor de identidade usar contas existentes no servidor LDAP, as contas de usuário LDAP poderão ser usadas para fazer login nos dispositivos gerenciados, enquanto os métodos de autenticação mais avançados fornecidos por SAML 2.0 (como autenticação de vários fatores e logon único) podem ser usados para fazer login no XClarity Administrator.
  - O login único permite que um usuário já conectado ao XClarity Administrator faça login automaticamente no Baseboard Management Control. O login único é ativado por padrão quando um servidor ThinkSystem ou ThinkAgile é trazido para o gerenciamento pelo XClarity Administrator (a menos que o servidor seja gerenciado com senhas do CyberArk). É possível definir a configuração global para ativar ou desabilitar o login único para todos os servidores ThinkSystem e ThinkAgile gerenciados. Ativar o login único para um servidor ThinkSystem e ThinkAgile específico substitui a configuração global para todos os servidores ThinkSystem e ThinkAgile (consulte).

    Nota: O logon único é desativado automaticamente ao usar o sistema de gerenciamento de identidade CyberArk para autenticação.
  - Quando a autenticação gerenciada está ativada para servidores ThinkSystem SR635 e SR655:
    - O firmware do controlador de gerenciamento do baseboard oferece suporte a até cinco funções de usuário LDAP. O XClarity Administrator adiciona essas funções de usuário LDAP aos servidores durante o gerenciamento: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** e **lxc-os-admin**.

      Os usuários devem ser atribuídos a pelo menos uma das funções de usuário LDAP especificadas para se comunicar com os servidores ThinkSystem SR635 e SR655.
    - O firmware do controlador de gerenciamento não oferece suporte aos usuários LDAP com o mesmo nome do usuário local do servidor.
  - Para servidores ThinkServer e System x M4, o servidor de autenticação do XClarity Administrator não é usado. Em vez disso, uma conta IPMI é criada no dispositivo com o prefixo "LXCA_" acompanhado por uma sequência aleatória. (As contas do usuário do IPMI local existente estão desabilitadas.) Quando você cancelar o gerenciamento de um servidor ThinkServer, a conta do usuário do "LXCA_" será desabilitada e o prefixo "LXCA_" será substituído por "DISABLED_". Para determinar se um servidor ThinkServer é gerenciado por outra instância, o XClarity Administrator verifica as contas de

IPMI com o prefixo "LXCA_". Se você escolher forçar o gerenciamento de um servidor ThinkServer gerenciado, todas as contas de IPMI no dispositivo com o prefixo "LXCA_" serão desabilitadas e renomeadas. Considere apagar manualmente as contas de IPMI que não são mais usadas.

Se você usar credenciais inseridas manualmente, o XClarity Administrator criará uma credencial armazenada automaticamente e usará essa credencial armazenada para gerenciar o dispositivo.

Notas: Quando a autenticação gerenciada é ativada para um dispositivo, não é possível editar credenciais armazenadas para esse dispositivo usando o XClarity Administrator.

- Cada vez que você gerencia um dispositivo usando credenciais inseridas manualmente, uma nova credencial armazenada é criada para o dispositivo, mesmo se outra credencial armazenada foi criada para o dispositivo durante um processo de gerenciamento anterior.
- Quando você cancela o gerenciamento de um dispositivo, o XClarity Administrator não exclui credenciais armazenadas que foram criadas automaticamente para esse dispositivo durante o processo de gerenciamento.

Um dispositivo pode ser gerenciado somente por uma instância do XClarity Administrator por vez. Não há suporte para o gerenciamento por várias instâncias do XClarity Administrator. Se um dispositivo for gerenciado por um XClarity Administrator, e você desejar gerenciá-lo com outro XClarity Administrator, primeiro cancele o gerenciamento do dispositivo no XClarity Administrator inicial e gerencie-o com o novo XClarity Administrator. Se um erro ocorrer durante o processo de cancelamento de gerenciamento, você poderá selecionar a opção **Forçar gerenciamento** durante o gerenciamento no novo XClarity Administrator.

Nota: Ao procurar dispositivos gerenciáveis na rede, o XClarity Administrator não sabe se um dispositivo já é gerenciado por outro gerenciador até após tentar gerenciar o dispositivo.

Durante o processo de gerenciamento, o XClarity Administrator executa as seguintes ações:

- Efetua login no chassi usando as credenciais fornecidas.
- Coleta o inventário de todos os componentes em cada chassi, como CMM, nós de cálculo, dispositivos de armazenamento e o Comutadores Flex.

  Nota: Alguns dados do inventário são coletados após o processo de gerenciamento ser concluído. O chassi fica no status pendente até que todos os dados do inventário sejam coletados. Não é possível executar determinadas tarefas em um dispositivo gerenciado (como implantar um padrão de servidor) até que todos os dados do inventário sejam coletados para esse dispositivo e o chassi não esteja mais no estado pendente.
- Define as configurações do servidor NTP para que todos os dispositivos gerenciados usem o servidor NTP do XClarity Administrator.
- Designa a última política de conformidade de firmware editada para o chassi.
- Para dispositivos Lenovo Flex, opcionalmente configura as regras de firewall de dispositivos para que solicitações de entrada sejam aceitas somente no XClarity Administrator.
- Troca certificados de segurança com o CMM, copiando o certificado de segurança do CMM para o armazenamento confiável do XClarity Administrator e enviando o certificado de segurança CA do XClarity Administrator ao CMM. O CMM carrega o certificado no armazenamento confiável do CMM e o distribui para processadores de serviço do nó de cálculo para inclusão em seus armazenamentos confiáveis.
- Configura a autenticação gerenciada. As configurações do cliente LDAP CMM são alteradas para usar o XClarity Administrator como servidor de autenticação, e as configurações globais de login no CMM são alteradas para **Somente Servidor de Autenticação Externo**. Para obter mais informações sobre autenticação gerenciada, consulte Gerenciando o servidor de autenticação.
- Cria a conta de usuário de recuperação (`RECOVERY_ID`). Para obter mais informações sobre a conta `RECOVERY_ID`, consulte Gerenciando o servidor de autenticação.

Atenção: Ao gerenciar um chassi, o XClarity Administrator altera o número máximo de conexões simultâneas do Modo de Comando TCP Seguro para 15 e define o número máximo de conexões simultâneas do Modo de Comando TCP Herdado como 0. Ele substitui configurações que podem já sido definidas no CMM.

Nota: O XClarity Administrator não altera as configurações de segurança ou configurações criptográficas (modo criptográfico e modo usado para comunicações seguras) durante o processo de gerenciamento. É possível alterar as configurações de criptografia depois que o chassi é gerenciado (consulte Definindo configurações de criptografia no servidor de gerenciamento).

Procedimento

Conclua um dos procedimentos a seguir para descobrir e gerenciar o chassi usando XClarity Administrator.

- Descubra e gerencie um grande número de chassis e outros dispositivos usando um arquivo de importação em massa (consulte Gerenciando sistemas na documentação online do Lenovo XClarity Administrator).
- Descubra e gerencie os chassis que estão na mesma sub-rede IP que o XClarity Administrator.
  1. Na barra de menu do XClarity Administrator, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos**. A página Descobrir e Gerenciar Novos Dispositivos é exibida.

É possível classificar as colunas da tabela para facilitar a localização do chassi que deseja gerenciar. Além disso, é possível digitar texto (como um nome de sistema ou endereço IP) no campo **Filtro** para filtrar mais chassis que são exibidos. É possível alterar as colunas que são exibidas e a ordem de classificação padrão clicando no ícone **Personalizar colunas** ().

2. Clique no ícone **Atualizar** () para descobrir todos os dispositivos gerenciáveis no domínio XClarity Administrator. A descoberta pode levar vários minutos.
3. Clique na caixa de seleção **Habilitar encapsulamento em todos os dispositivos gerenciados futuros** para alterar as regras de firewall em todos os dispositivos durante o processo de gerenciamento para que as solicitações de entrada sejam aceitas somente de XClarity Administrator.

   O encapsulamento pode ser ativado ou desativado em dispositivos específicos após serem gerenciados.

   Atenção: Se o encapsulamento estiver ativado e XClarity Administrator ficar indisponível antes que o gerenciamento de um dispositivo seja cancelado, as etapas necessárias deverão ser tomadas para desativar o encapsulamento e estabelecer comunicação com o dispositivo. Para procedimentos de recuperação, consulte o arquivo lenovoMgrAlert.mib e Recuperando o gerenciamento com um CMM após uma falha no servidor de gerenciamento.
4. Selecione um ou mais chassis que você deseja gerenciar.
5. Clique em **Gerenciar Selecionado**.
6. Opte por usar a autenticação gerenciada do XClarity Administrator ou a autenticação local para esse dispositivo. A autenticação gerenciada é selecionada por padrão. Para usar autenticação local, desmarque **Autenticação Gerenciada**.

   Nota: Autenticação gerenciada e local não são suportadas para servidores ThinkServer e System x M4.
7. Escolha o tipo de credenciais a ser usado para o dispositivo e especifique as credenciais apropriadas:
   - **Usar credenciais inseridas manualmente**
     - Especifique o ID do usuário local e a senha com autoridade **lxc-supervisor** para autenticação no CMM.
     - (Opcional) Especifique uma nova senha para a conta do usuário do CMM se a senha estiver expirada atualmente no dispositivo.
   - **Usar credenciais armazenadas**

     Selecione as credenciais armazenadas com autoridade **lxc-supervisor** a serem usadas para esse dispositivo gerenciado. Você pode adicionar credenciais armazenadas clicando em **Gerenciar Credenciais Armazenadas**.

     Nota: Se você optar por usar autenticação local, selecione uma credencial armazenada para gerenciar o dispositivo.

   Dica: é recomendável usar uma conta de supervisor ou administrador para gerenciar o dispositivo. Se uma conta com autoridade de nível mais baixo for usada, o gerenciamento poderá falhar ou poderá ser bem-sucedido, mas outras operações futuras do XClarity Administrator no dispositivo poderão falhar (principalmente se o dispositivo for gerenciado sem autenticação gerenciada).

   Para obter mais informações sobre as credenciais normais e armazenadas, consulte Gerenciando contas de usuário e Gerenciando credenciais compartilhadas.
8. Especifique a senha de recuperação se a autenticação gerenciada estiver selecionada.

Uma conta de recuperação (RECOVERY_ID) é criada no CMM, e todas as contas de usuário locais são desativadas. Se houver um problema com XClarity Administrator, e ele parar de funcionar por alguma razão, *não* será possível fazer login no CMM usando as contas de usuário normais. No entanto, é possível fazer login usando a conta RECOVERY_ID.

Nota:

- A senha de recuperação é necessária se você optar por usar autenticação gerenciada e não é permitida se você optar por usar autenticação local.
- É possível optar por usar uma conta de recuperação local ou credenciais de recuperação armazenadas. Em qualquer um dos casos, o nome do usuário é sempre RECOVERY_ID.
- Verifique se a senha segue as políticas de segurança e senha para o dispositivo. As políticas de segurança e senha podem variar.
- Certifique-se de gravar a senha de recuperação para uso futuro.

Para obter mais informações sobre o ID de recuperação, consulte Gerenciando o servidor de autenticação.

9. Clique em **Alterar** para alterar os grupos de funções que devem ser atribuídos aos dispositivos.

   Notas:

   - É possível selecionar de uma lista de grupos de funções que são atribuídos ao usuário atual.
   - Se você não alterar os grupos de funções, os grupos de função padrão serão usados. Para obter mais informações sobre os grupos de função padrão, consulte Alterando as permissões padrão.

10. Clique em **Gerenciar**.

    Uma caixa de diálogo é exibida e mostra o progresso desse processo de gerenciamento. Para assegurar que o processo seja concluído com êxito, monitore o progresso.

    Quando o processo for concluído, a caixa de diálogo exibirá o número de dispositivos no chassi e o status do chassi.

    Nota: Alguns dados do inventário são coletados após o processo de gerenciamento ser concluído. O chassi fica no status pendente até que todos os dados do inventário sejam coletados. Não é possível executar determinadas tarefas em um dispositivo gerenciado (como implantar um padrão de servidor) até que todos os dados do inventário sejam coletados para esse dispositivo e o chassi não esteja mais no estado pendente.

11. Quando o processo for concluído, clique em **OK**.

    O dispositivo agora é gerenciado por XClarity Administrator, que sonda automaticamente o dispositivo gerenciado regularmente para coletar informações atualizadas, como inventário.

    Se o gerenciamento não tiver sido bem-sucedido por causa de uma das seguintes condições de erro, repita esse procedimento usando a opção **Forçar gerenciamento**.

    - Se o gerenciamento do XClarity Administrator falhar e não puder ser recuperado.

      Nota: Se a instância de substituição do XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, você poderá gerenciar o dispositivo novamente usando a conta e senha de RECOVERY_ID (se aplicável) e a opção **Forçar gerenciamento**.
    - Se o gerenciamento do XClarity Administrator tiver sido desligado antes do cancelamento do gerenciamento dos dispositivos.
    - Se o cancelamento do gerenciamento dos dispositivos não tiver sido bem-sucedido.

    Atenção: Os dispositivos podem ser gerenciados somente por uma instância do XClarity Administrator por vez. Não há suporte para o gerenciamento por várias instâncias do XClarity

Administrator. Se um dispositivo for gerenciado por um XClarity Administrator, e você desejar gerenciá-lo com outro XClarity Administrator, primeiro cancele o gerenciamento do dispositivo no XClarity Administrator original e gerencie-o com o novo XClarity Administrator.

12. Se o chassi for novo, clique em **Continuar para Configuração de Chassi** para validar e alterar configurações de rede de gerenciamento para o chassi inteiro (incluindo nós de cálculo e comutadores Flex) e configurar informações de nó de cálculo, armazenamento local, adaptadores de E/S, destinos de inicialização e configurações de firmware criando e implantando padrões de servidor. Para obter informações adicionais, consulte Alterando as configurações de IP de gerenciamento de um chassi e Configurando servidores com padrões de configuração.

- Descubra e gerencie os chassis que não estiverem na mesma sub-rede IP que o XClarity Administrator especificando manualmente endereços IP.
  1. Na barra de menu do XClarity Administrator, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos**. A página Descobrir e Gerenciar é exibida.
  2. Clique na caixa de seleção **Habilitar encapsulamento em todos os dispositivos gerenciados futuros** para alterar as regras de firewall em todos os dispositivos durante o processo de gerenciamento para que as solicitações de entrada sejam aceitas somente de XClarity Administrator.

     O encapsulamento pode ser ativado ou desativado em dispositivos específicos após serem gerenciados.

     Atenção: Se o encapsulamento estiver ativado e XClarity Administrator ficar indisponível antes que o gerenciamento de um dispositivo seja cancelado, as etapas necessárias deverão ser tomadas para desativar o encapsulamento e estabelecer comunicação com o dispositivo. Para procedimentos de recuperação, consulte o arquivo lenovoMgrAlert.mib e Recuperando o gerenciamento com um CMM após uma falha no servidor de gerenciamento.
  3. Selecione **Entrada Manual**.
  4. Especifique os endereços de rede do chassi que deseja gerenciar:
     - Clique em **Sistema Único** e insira um nome de domínio de endereço IP único ou o nome de domínio totalmente qualificado (FQDN).

       Nota: Para especificar um FQDN, verifique se um nome de domínio válido foi especificado na página Acesso à Rede (consulte Configurando o acesso à rede).
     - Clique em **Vários Sistemas** e insira um intervalo de endereços IP. Para adicionar outro intervalo, clique no ícone **Adicionar** (➕). Para remover um intervalo, clique no ícone **Remover** (✖).
  5. Clique em **OK**.
  6. Opte por usar a autenticação gerenciada do XClarity Administrator ou a autenticação local para esse dispositivo. A autenticação gerenciada é selecionada por padrão. Para usar autenticação local, desmarque **Autenticação Gerenciada**.

     Nota: Autenticação gerenciada e local não são suportadas para servidores ThinkServer e System x M4.
  7. Escolha o tipo de credenciais a ser usado para o dispositivo e especifique as credenciais apropriadas:
     - **Usar credenciais inseridas manualmente**
       - Especifique o ID do usuário local e a senha com autoridade **lxc-supervisor** para autenticação no CMM.
       - (Opcional) Especifique uma nova senha para a conta do usuário do CMM se a senha estiver expirada atualmente no dispositivo.
     - **Usar credenciais armazenadas**

Selecione as credenciais armazenadas com autoridade **lxc-supervisor** a serem usadas para esse dispositivo gerenciado. Você pode adicionar credenciais armazenadas clicando em **Gerenciar Credenciais Armazenadas**.

Nota: Se você optar por usar autenticação local, selecione uma credencial armazenada para gerenciar o dispositivo.

Dica: é recomendável usar uma conta de supervisor ou administrador para gerenciar o dispositivo. Se uma conta com autoridade de nível mais baixo for usada, o gerenciamento poderá falhar ou poderá ser bem-sucedido, mas outras operações futuras do XClarity Administrator no dispositivo poderão falhar (principalmente se o dispositivo for gerenciado sem autenticação gerenciada).

Para obter mais informações sobre as credenciais normais e armazenadas, consulte Gerenciando contas de usuário e Gerenciando credenciais compartilhadas.

8. Especifique a senha de recuperação se a autenticação gerenciada estiver selecionada.

   Uma conta de recuperação (`RECOVERY_ID`) é criada no CMM, e todas as contas de usuário locais são desativadas. Se houver um problema com XClarity Administrator, e ele parar de funcionar por alguma razão, *não* será possível fazer login no CMM usando as contas de usuário normais. No entanto, é possível fazer login usando a conta `RECOVERY_ID`.

   Nota:

   - A senha de recuperação é necessária se você optar por usar autenticação gerenciada e não é permitida se você optar por usar autenticação local.
   - É possível optar por usar uma conta de recuperação local ou credenciais de recuperação armazenadas. Em qualquer um dos casos, o nome do usuário é sempre `RECOVERY_ID`.
   - Verifique se a senha segue as políticas de segurança e senha para o dispositivo. As políticas de segurança e senha podem variar.
   - Certifique-se de gravar a senha de recuperação para uso futuro.

   Para obter mais informações sobre o ID de recuperação, consulte Gerenciando o servidor de autenticação.

9. Clique em **Alterar** para alterar os grupos de funções que devem ser atribuídos aos dispositivos.

   Notas:

   - É possível selecionar de uma lista de grupos de funções que são atribuídos ao usuário atual.
   - Se você não alterar os grupos de funções, os grupos de função padrão serão usados. Para obter mais informações sobre os grupos de função padrão, consulte Alterando as permissões padrão.

10. Clique em **Gerenciar**.

    Uma caixa de diálogo é exibida e mostra o progresso desse processo de gerenciamento. Monitore o progresso para assegurar que o processo seja concluído.

    Quando o processo for concluído, a caixa de diálogo exibirá o número de dispositivos no chassi e o status do chassi.

    Nota: Alguns dados do inventário são coletados após o processo de gerenciamento ser concluído. O chassi fica no status pendente até que todos os dados do inventário sejam coletados. Não é possível executar determinadas tarefas em um dispositivo gerenciado (como implantar um padrão de servidor) até que todos os dados do inventário sejam coletados para esse dispositivo e o chassi não esteja mais no estado pendente.

11. Quando o processo for concluído, clique em **OK**.

    O dispositivo agora é gerenciado por XClarity Administrator, que sonda automaticamente o dispositivo gerenciado regularmente para coletar informações atualizadas, como inventário.

Se o gerenciamento não tiver sido bem-sucedido por causa de uma das seguintes condições de erro, repita esse procedimento usando a opção **Forçar gerenciamento**.

- Se o gerenciamento do XClarity Administrator falhar e não puder ser recuperado.

  Nota: Se a instância de substituição do XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, você poderá gerenciar o dispositivo novamente usando a conta e senha de RECOVERY_ID (se aplicável) e a opção **Forçar gerenciamento**.
- Se o gerenciamento do XClarity Administrator tiver sido desligado antes do cancelamento do gerenciamento dos dispositivos.
- Se o cancelamento do gerenciamento dos dispositivos não tiver sido bem-sucedido.

Atenção: Os dispositivos podem ser gerenciados somente por uma instância do XClarity Administrator por vez. Não há suporte para o gerenciamento por várias instâncias do XClarity Administrator. Se um dispositivo for gerenciado por um XClarity Administrator, e você desejar gerenciá-lo com outro XClarity Administrator, primeiro cancele o gerenciamento do dispositivo no XClarity Administrator original e gerencie-o com o novo XClarity Administrator.

12. Se o chassi for novo, clique em **Continuar para Configuração de Chassi** para validar e alterar configurações de rede de gerenciamento para o chassi inteiro (incluindo nós de cálculo e comutadores Flex) e configurar informações de nó de cálculo, armazenamento local, adaptadores de E/S, destinos de inicialização e configurações de firmware criando e implantando padrões de servidor. Para obter informações adicionais, consulte Alterando as configurações de IP de gerenciamento de um chassi e Configurando servidores com padrões de configuração.

Depois de concluir

- Descubra e gerencie dispositivos adicionais.
- Implante imagens do sistema operacional nos servidores que ainda não tenham um sistema operacional instalado. Para obter mais informações, consulte Instalando sistemas operacionais em servidores bare-metal.
- Atualize o firmware em dispositivos que não estão em conformidade com as políticas atuais (Atualizando firmware em dispositivos gerenciados).
- Adicione os dispositivos recém-gerenciados ao rack adequado para refletir o ambiente físico (consulte Gerenciando racks).
- Monitore o status e os detalhes de hardware (consulte Visualizando o status de um servidor gerenciado).
- Monitore eventos e alertas (consulte Trabalhando com eventos e Trabalhando com alertas).

Visualizando o status de um chassi gerenciado

É possível exibir um resumo e o status detalhado do chassi gerenciado e os componentes instalados no Lenovo XClarity Administrator.

Saiba mais:

- XClarity Administrator: inventário
- XClarity Administrator: monitoramento

Sobre esta tarefa

Os seguintes ícones de status são usados para indicar a integridade geral do dispositivo. Se os certificados não corresponderem, "(Não confiável)" será anexado ao status de cada dispositivo aplicável, por exemplo, Aviso (Não confiável). Se houver um problema de conectividade ou uma conexão com o dispositivo não for

confiável, "(Conectividade)" será anexado ao status de cada dispositivo aplicável, por exemplo, Aviso (Conectividade).

- () Crítico
- () Aviso
- () Pendente
- () Informativo
- () Normal
- () Offline
- () Desconhecido

Procedimento

Conclua as seguintes etapas para exibir o status de um chassi gerenciado.

- Exibir informações detalhadas sobre o chassi clicando no link **Detalhes** ou clicando em **Ações → Exibições → Detalhes**.
- Iniciar a interface da Web do CMM do chassi clicando no link **Endereço IP** (consulte Iniciando a interface da Web do CMM para um chassis).
- Modificar informações (como contato, local e descrição de suporte) clicando em **Ações → Inventário → Editar Propriedades**.
- Modificar as configurações de IP de gerenciamento do chassi inteiro, incluindo nós de cálculo e comutadores Flex, clicando em **Ações → Inventário → Editar endereços IP de gerenciamento**.
- Exportar informações detalhadas sobre um ou mais chassis para um único arquivo CSV selecionando o chassi e clicando em **Ações → Inventário → Exportar Inventário**.

  Nota: Você pode exportar os dados do inventário para no máximo 60 dispositivos ao mesmo tempo.

  Dica: Ao importar um arquivo CSV no Microsoft Excel, o Excel trata os valores de texto que contêm apenas números como valores numéricos (por exemplo, de UUIDs). Formate cada célula como texto para corrigir esse erro.
- Resolver problemas que podem ocorrer entre o certificado de segurança do Lenovo XClarity Administrator e o certificado de segurança do CMM no chassi selecionando um chassi e clicando em **Ações → Segurança → Resolver Certificados Não Confiáveis**.

Visualizando os detalhes de um chassi gerenciado

É possível exibir informações detalhadas sobre o chassi gerenciado do Lenovo XClarity Administrator, incluindo os níveis de firmware, os endereços IP e o identificador exclusivo universalmente (UUID).

Saiba mais:

- XClarity Administrator: inventário
- XClarity Administrator: monitoramento

Sobre esta tarefa

A temperatura do ar no nível do sistema é medida por um sensor na frente do servidor. Essa temperatura representa a temperatura de entrada do ar para o servidor. Observe que a temperatura do ar registrada pelo XClarity Administrator e pelo CMM pode ser diferente se a temperatura for capturada em momentos diferentes.

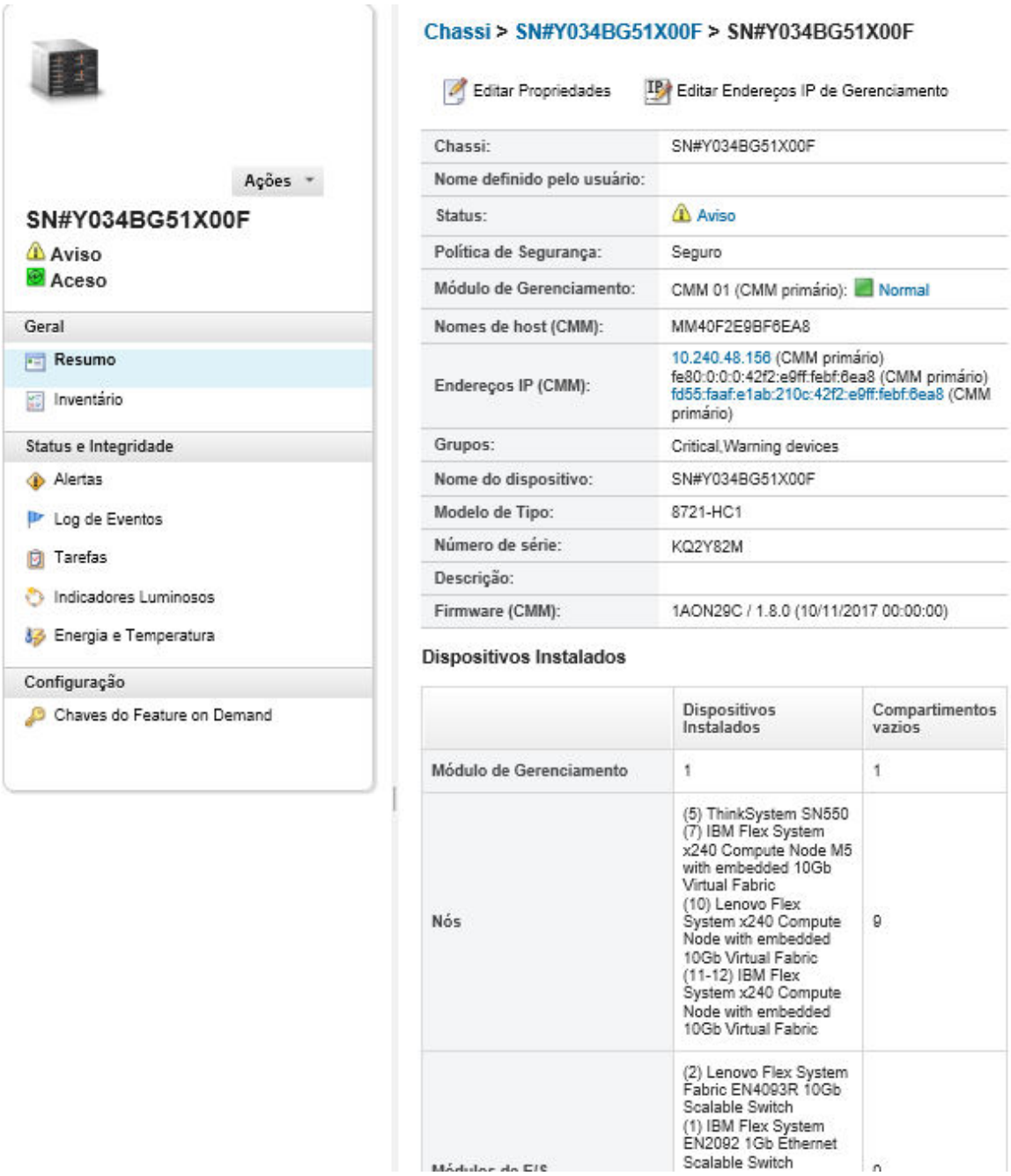
Procedimento

Conclua as seguintes etapas para exibir os detalhes de um chassi gerenciado.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Chassi**. A página Chassi é exibida uma página com uma exibição tabular de todos os chassis gerenciados.

É possível classificar as colunas da tabela para facilitar a localização do chassi que deseja gerenciar. Além disso, é possível digitar texto (como um nome de chassi ou endereço IP) no campo **Filtro** para filtrar mais chassis que são exibidos.

Etapa 2. Clique no nome do chassi na coluna **Chassi**. A página de resumo de status desse chassi é exibida, mostrando as propriedades e componentes do chassi instalados no chassi.



Etapa 3. Conclua uma ou mais das seguintes ações:

- Clique em **Resumo** para exibir um resumo do chassi, incluindo informações do sistema e componentes instalados (consulte Visualizando o status de um chassi gerenciado).
- Clique em **Detalhes de Inventário** para exibir detalhes sobre os componentes do chassi, incluindo:
  - Níveis de firmware para todos os componentes do chassi.
  - Detalhes do CMM, como nome do host, endereço IPv4, endereço IPv6 e endereços MAC.
  - Detalhes de ativo do chassi e CMM instalado no chassi, incluindo nome, identificador universalmente exclusivo (UUID) e local.

- Clique em **Alertas** para exibir a lista de alertas atuais para esse chassi (consulte Trabalhando com alertas).
- Clique em **Log de Eventos** para exibir a lista de eventos para esse chassi (consulte Monitorando eventos no log de eventos).
- Clique em **Trabalhos** para exibir uma lista de trabalhos associados ao chassi (consulte Monitorando trabalhos).
- Clique em **Light Path** para exibir o status atual dos LEDs do chassi, incluindo local, falha e informações. Isso equivale a examinar o painel frontal do chassi.
- Clique em **Energia e Temperatura** para exibir detalhes sobre energia e fluxo de ar.

  Dica: use o botão Atualizar em seu navegador da Web para coletar os dados mais recentes de energia e temperatura. A coleta de dados pode levar vários minutos.
- Clique em **Chaves do Feature on Demand** para acessar informações necessárias para solicitar uma chave do Feature on Demand e outras informações sem agente (consulte Exibindo chaves do Features on Demand).

Depois de concluir

Além de exibir o resumo e informações detalhadas sobre um chassi, você pode executar as seguintes ações:

- Exibir um chassi em exibição gráfica de rack ou de chassi clicando em **Ações → Exibições → Mostrar na Exibição do Rack** ou **Ações → Exibições → Mostrar na Exibição do Chassi**.
- Iniciar a interface da Web do CMM clicando no link **Endereço IP** (consulte Iniciando a interface da Web do CMM para um chassis).
- Modificar informações (como contato, local e descrição de suporte) clicando em **Editar Propriedades** (consulte Alterando as propriedades do sistema para um chassi).
- Modificar as configurações de IP de gerenciamento do chassi inteiro, incluindo nós de cálculo e comutadores Flex, clicando em **Todas as Ações → Inventário → Editar endereços IP de gerenciamento** (consulte Alterando as configurações de IP de gerenciamento de um chassi).
- Exportar informações detalhadas sobre o chassi para um arquivo CSV clicando em **Ações → Inventário → Exportar Inventário**.

  Notas:

  – Para obter mais informações sobre os dados do inventário no arquivo CSV, consulte o GET /chassis/*<UUID_list>* na documentação online do XClarity Administrator.

  – Ao importar um arquivo CSV no Microsoft Excel, o Excel trata os valores de texto que contêm apenas números como valores numéricos (por exemplo, de UUIDs). Formate cada célula como texto para corrigir esse erro.
- Cancelar gerenciamento de um chassi (consulte Cancelando o gerenciamento de um chassi).
- Habilitar ou desabilitar as mudanças de regra de firewall em um chassi que limita as solicitações de entrada somente de XClarity Administrator selecionando o chassi e clicando em **Ações → Segurança → Ativar encapsulamento** ou **Ações → Segurança → Desabilitar Encapsulamento**.

  A configuração de encapsulamento global é desativada por padrão. Quando desativado, o modo de encapsulamento do dispositivo é definido como "normal" e as regras de firewall não são alteradas como parte do processo de gerenciamento.

  A configuração de encapsulamento global é desativada por padrão. Quando desativado, o modo de encapsulamento do dispositivo é definido como "normal" e as regras de firewall não são alteradas como parte do processo de gerenciamento.

Quando a configuração de encapsulamento global é ativada e o dispositivo suporta o encapsulamento, o XClarity Administrator se comunica com o dispositivo durante o processo de gerenciamento para alterar o modo de encapsulamento do dispositivo para "encapsulationLite" e modificar as regras de firewall no dispositivo para delimitar as solicitações de entrada àquelas do XClarity Administrator.

Atenção: Se o encapsulamento estiver ativado e XClarity Administrator ficar indisponível antes que o gerenciamento de um dispositivo seja cancelado, as etapas necessárias deverão ser tomadas para desativar o encapsulamento e estabelecer comunicação com o dispositivo. Para procedimentos de recuperação, consulte o arquivo lenovoMgrAlert.mib e Recuperando o gerenciamento com um CMM após uma falha no servidor de gerenciamento.

- Resolver problemas que podem ocorrer entre o certificado de segurança do XClarity Administrator e o certificado de segurança do CMM no chassi selecionando um chassi e clicando em **Ações → Segurança → Resolver Certificados Não Confiáveis** (consulte Resolvendo um certificado de servidor não confiável).

Fazendo backup e restaurando dados de configuração do CMM

O Lenovo XClarity Administrator não inclui funções de backup internas para dados de configuração do CMM. Em vez disso, use as funções de backup disponíveis para o CMM gerenciado.

Use a interface da Web de gerenciamento ou a interface da linha de comandos (CLI) para fazer backup e restaurar o CMM.

- Backup dos dados de configuração do CMM
  - Na interface da Web de gerenciamento, clique em **Gerenciamento do Módulo de Gerenciamento → Configuração → Configuração de Backup**. Para obter mais informações, consulte Salvando uma configuração do CMM por meio da interface da Web na documentação online do Flex Systems.
  - Na CLI, use o comando `write`. Para obter informações adicionais, veja Comando write do CMM na documentação online do Flex Systems
- Restaurar dados de configuração do CMM
  - Na interface da Web de gerenciamento, clique em **Gerenciamento do Módulo de Gerenciamento → Configuração → Restaurar Configuração do Arquivo**. Para obter mais informações, consulte Restaurando uma configuração do CMM por meio da interface da Web na documentação online do Flex Systems.
  - Na CLI, use o comando `read`. Para obter mais informações, consulte Comando read do CMM na documentação online do Flex Systems.

Nota: Dica: é possível localizar informações adicionais sobre como fazer backup e restaurar os componentes de chassi no Guia de melhores práticas de Backup e Restauração do PureFlex e do Flex System .

Iniciando a interface da Web do CMM para um chassis

Você pode iniciar a interface da Web do CMM para um chassi específico no Lenovo XClarity Administrator.

Procedimento

Conclua as etapas a seguir para iniciar uma interface da Web do CMM.

Nota: Iniciar essa interface da Web do CMM do XClarity Administrator usando o navegador da Web Safari não é permitido.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Chassi** para exibir a página Chassi.

É possível classificar as colunas da tabela para facilitar a localização do chassi que deseja gerenciar. Além disso, é possível digitar texto (como um nome de chassi ou endereço IP) no campo **Filtro** para filtrar mais chassis que são exibidos.

Etapa 2. Clique no link do chassi na coluna **Chassi**. A página de resumo de status desse chassi é exibida.

Etapa 3. Clique em **Todas as Ações → Iniciar → Interface da Web de Gerenciamento**. A interface da Web do CMM é iniciada.

Dica: também é possível clicar no endereço IP para iniciar o CMM.

Etapa 4. Efetue login na interface da Web do CMM usando as credenciais de usuário do XClarity Administrator.

Alterando as propriedades do sistema para um chassi

É possível alterar as propriedades do sistema para um chassi específico.

Procedimento

Conclua as etapas a seguir para alterar as propriedades do sistema.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Chassi** para exibir a página Chassi.

Etapa 2. Selecione o chassi a ser atualizado.

Etapa 3. Clique em **Todas as Ações → Inventário → Editar Propriedades** para exibir a caixa de diálogo Editar.

Etapa 4. Altere as seguintes informações, conforme necessário.
- Nome do servidor
- Contato de suporte
- Descrição

Nota: As propriedades de local, sala, rack e menor unidade do rack são atualizadas pelo XClarity Administrator ao incluir ou remover dispositivos de um rack na interface da Web (consulte Gerenciando racks).

Etapa 5. Clique em **Salvar**.

Nota: Quando você altera essas propriedades, pode haver um pequeno atraso até as alterações aparecerem na interface da Web do XClarity Administrator.

Alterando as configurações de IP de gerenciamento de um chassi

É possível alterar as configurações de IP de gerenciamento para o chassi inteiro, incluindo nós de cálculo, dispositivos de armazenamento e Comutadores Flex.

Procedimento

Conclua as seguintes etapas para modificar as configurações de IP de gerenciamento.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Chassi** para exibir a página Chassi.

Etapa 2. Selecione o chassi.

Etapa 3. Clique em **Todas as Ações → Inventário → Editar endereços IP de gerenciamento** para exibir a página Configurações de IP do chassi e dos componentes.

Etapa 4. Altere as seguintes configurações globais, conforme necessário.

- Escolha entre ativar ou desativar endereços IPv4.

  Se você ativar endereços IPv4, especifique as seguintes configurações. As configurações globais IPv4 são aplicadas a um componente quando seu endereço IPv4 é atualizado.
  - (Opcional) Escolha obter endereços IP usando endereços IP atribuídos estaticamente.
  - Especifique a máscara de sub-rede e o endereço do gateway.
- Especifique as seguintes configurações para endereços IPv6. As configurações globais IPv6 são aplicadas a um componente quando seu endereço IPv6 é atualizado.
  - (Opcional) Escolha obter endereços IP usando endereços IP atribuídos estaticamente.

    Se endereços IP estáticos forem usados, você também poderá optar por usar configuração automática de endereço IP sem estado e configuração de endereço IP com estado.
  - Especifique o comprimento de prefixo e o endereço do gateway.
- Escolha entre ativar ou desativar servidores DNS.

  Se ativar servidores DNS:
  - Escolha a preferência de pesquisa do servidor DNS.
  - Insira os endereços IP a serem usados para a ordem de pesquisa de DNS.
  - Insira o nome do domínio.

Etapa 5. Altere as seguintes configurações de IP do CMM.

- Insira o nome do host e o endereço IP do CMM.
- Clique em **Gerar automaticamente endereços IP** para criar endereços IP para nós de cálculo, dispositivos de armazenamento e Comutadores Flex usando o endereço IP do CMM como ponto de partida.

Etapa 6. Insira o nome do host e endereços IP para cada nó de cálculo no chassi

Etapa 7. Insira o nome do host e endereços IP para cada dispositivo de armazenamento no chassi.

Etapa 8. Insira os endereços IP para cada Comutador Flex no chassi.

Etapa 9. Clique em **Salvar**. Será exibida uma caixa de diálogo com um resumo de configurações de rede.

Etapa 10. Clique em **Aplicar**.

Todos os componentes existentes no chassi são atualizados para as configurações globais especificadas. Quando a atualização terminar, a caixa de diálogo exibirá as configurações que foram alteradas.

Nota: Quando você altera essas informações, pode haver um pequeno atraso até as informações aparecerem na interface do Lenovo XClarity Administrator.

Etapa 11. Clique em **Fechar**.

Configurando o failover do CMM

Ao instalar um segundo CMM em um chassi, o segundo CMM é configurado automaticamente como um CMM de espera por padrão. Se o CMM primário falhar, o endereço IP do CMM de espera mudará para o endereço IP que foi usado para o CMM primário, e o CMM de espera assumirá o gerenciamento do chassi. Entretanto, é possível executar uma configuração de failover mais avançado na interface da Web do controlador de gerenciamento do chassi.

Sobre esta tarefa

Por exemplo, é possível optar por:

- Desativar a interface de rede para o CMM de espera para evitar failover.
- Ativar a interface de rede para o CMM de espera e permitir que os endereços IP sejam trocados entre os dois CMMs durante o failover.
- Ativar a interface de rede para o CMM de espera e evitar que os endereços IP sejam trocados entre os dois CMMs durante o failover.

Para obter informações adicionais sobre recursos de failover avançado do CMM, consulte Comando advfailover na documentação online do CMM.

Procedimento

Para ativar a troca de endereço IP para os CMMs primário e de espera, conclua as seguintes etapas.

Etapa 1. Na interface da Web do controlador de gerenciamento do chassi, clique em **Gerenciamento do Módulo de Gerenciamento → Rede → Ethernet** para exibir a página Configuração Ethernet.

Etapa 2. Selecione entre **IPv4** e **IPv6** para seu sistema.

Etapa 3. Em **Configurar endereço IP**, selecione a opção para usar um endereço IP estático. Repita para o outro protocolo.

Etapa 4. Clique em **Gerenciamento do Módulo de Gerenciamento → Propriedades → Failover Avançado** e ative a opção de failover avançado.

Etapa 5. Selecione **Trocar endereço IP do Módulo de Gerenciamento**.

Etapa 6. Realize cenários de teste para verificar se o failover funciona corretamente e se o Lenovo XClarity Administrator pode se conectar aos CMMs primários e de backup.

Reiniciando um CMM

É possível reiniciar um Chassis Management Module (CMM) no Lenovo XClarity Administrator.

Procedimento

Conclua o procedimento a seguir para reiniciar um chassi.

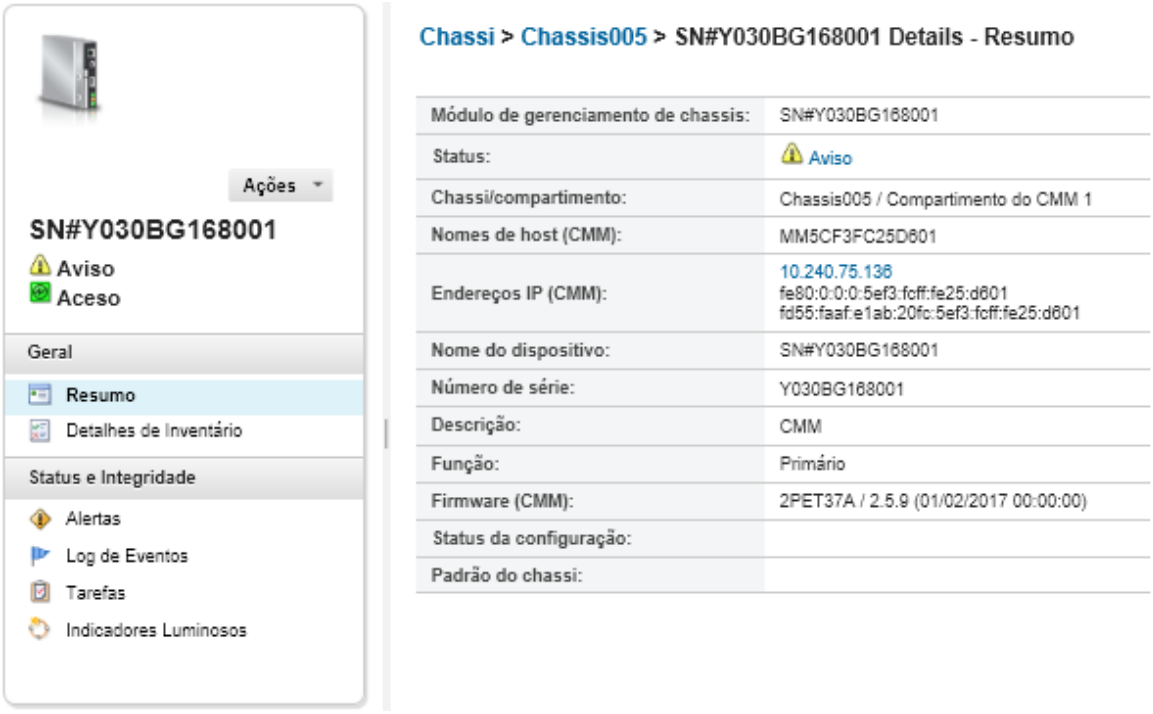
Nota: Quando o CMM é reiniciado, todas as conexões de rede existentes com o CMM são temporariamente perdidas.

Etapa 1. No menu XClarity Administrator, clique em **Hardware → Chassi**. A página Chassi é exibida uma página com uma exibição tabular de todos os chassis gerenciados.

Etapa 2. Clique no nome do chassi na coluna **Chassi** para exibir a exibição gráfica do chassi.

Etapa 3. Clique no gráfico do CMM para exibir a página Resumo do CMM.

Dica: também é possível clicar em **Exibição de tabela** e no nome do CMM na coluna **Nome** para exibir a página Resumo do CMM.



Etapa 4. Clique em **Ações → Ações de Energia → Reiniciar**.

Etapa 5. Clique em **Reiniciar Imediatamente**.

Esta operação pode levar alguns minutos para ser concluída, e talvez você precise atualizar a página para ver os resultados.

Reposicionando virtualmente um CMM

É possível simular a remoção e recolocação de um Chassis Management Module (CMM) em um chassi

Sobre esta tarefa

Durante o reposicionamento virtual, todas as conexões de rede existentes com o CMM são perdidas, e o estado de energia do CMM é alterado.

Atenção: Antes de executar um reposicionamento virtual, salve todos os dados do usuário no CMM.

Procedimento

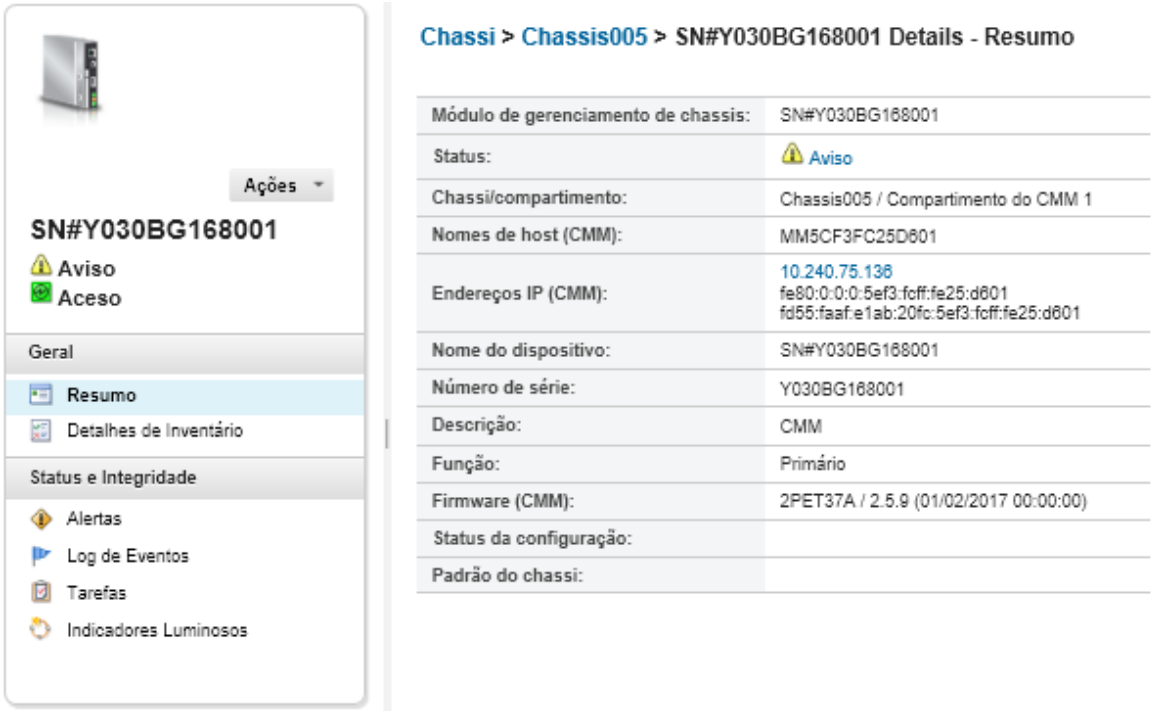
Execute as seguintes etapas para reposicionar virtualmente um CMM.

Etapa 1. No menu Lenovo XClarity Administrator, clique em **Hardware → Chassi**. A página Chassi é exibida uma página com uma exibição tabular de todos os chassis gerenciados.

Etapa 2. Clique no nome do chassi na coluna **Chassi** para exibir a exibição gráfica do chassi.

Etapa 3. Clique no gráfico do CMM para exibir a página Resumo do CMM.

Dica: também é possível clicar em **Exibição de tabela** e no nome do CMM na coluna **Nome** para exibir a página Resumo do CMM.



Etapa 4. Clique em **Ações → Serviço → Reposicionamento Virtual**.

Etapa 5. Clique em **Reposicionamento Virtual**.

Resolvendo credenciais armazenadas expiradas ou inválidas para um chassi

Quando uma credencial armazenada expira ou fica inoperante em um dispositivo, o status desse dispositivo é mostrado como "Offline".

Procedimento

Para resolver credenciais armazenadas expiradas ou inválidas para um chassi.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Chassi**. A página Chassi é exibida uma página com uma exibição tabular de todos os chassis gerenciados.

Etapa 2. Clique no cabeçalho da coluna **Energia** para agrupar todos os chassis offline na parte superior da tabela.

É possível classificar as colunas da tabela para facilitar a localização do chassi que deseja gerenciar. Além disso, é possível digitar texto (como um nome de chassi ou endereço IP) no campo **Filtro** para filtrar mais chassis que são exibidos.

Etapa 3. Selecione o chassi a ser resolvido.

Etapa 4. Clique em **Todas as Ações → Segurança → Editar Credenciais Armazenadas**.

Etapa 5. Altere a senha para a credencial armazenada ou selecione outra credencial armazenada a ser usada para o dispositivo gerenciado.

Nota: Se você gerenciou mais de um dispositivo usando as mesmas credenciais armazenadas e alterar a senha para as credenciais armazenadas, essa alteração de senha afetará todos os dispositivos que atualmente são usando as credenciais armazenadas.

Recuperando o gerenciamento com um CMM após uma falha no servidor de gerenciamento

Se um chassi estiver sendo gerenciado pelo Lenovo XClarity Administrator, e o XClarity Administrator falhar, você poderá restaurar as funções de gerenciamento e as contas de usuário locais para um CMM até o nó de gerenciamento ser restaurado ou substituído.

Procedimento

Conclua um dos seguintes procedimentos para restaurar o gerenciamento em um CMM.

- Se a instância de substituição do XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, gerencie o dispositivo novamente usando a conta e senha de RECOVERY_ID e a opção **Forçar gerenciamento** (consulte Gerenciando chassi).
- Redefina o CMM para os padrões de fábrica pressionando o botão de orifício no CMM usando um clipe por pelo menos 10 segundos. Para obter mais informações sobre como reconfigurar o CMM, incluindo avisos importantes, consulte Redefinição do CMM na documentação online do Flex Systems.
- Redefina a configuração do CMM usando as seguintes etapas:
  1. Por meio de uma sessão SSH, abra uma interface da linha de comandos de gerenciamento para o chassi e efetue login com a conta `RECOVERY_ID`.

     Nota: A senha para a conta `RECOVERY_ID` foi configurada quando você selecionou o chassi para gerenciamento na página Domínio de Gerenciamento. Para obter mais informações sobre o gerenciamento centralizado da conta, consulte Gerenciando chassi.

     Se esta for a primeira vez que você usou a conta `RECOVERY_ID` para fazer login no CMM, será necessário alterar a senha.
  2. Se for solicitado, digite a nova senha para a conta `RECOVERY_ID`.
  3. Restaure a configuração do CMM realizando uma das seguintes etapas:
     - Se estiver executando a versão de junho de 2015 ou mais recente do firmware do CMM, execute o seguinte comando:
       ```
       read -f unmanage -T mm[p]
       ```

Para obter mais informações, consulte o Comando read na documentação online do CMM.

- Se estiver executando a versão anterior a junho de 2015 do firmware do CMM, execute os seguintes comandos na ordem mostrada:

  a. `env -T mm[p]`

  b. `sslcfg -client disabled -tc1 remove`

  c. `accseccfg -am local`

  d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`

  e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`

  f. `cimsub -clear all`

  g. `fsmcm -off`

     O comando `fsmcm` desativa o gerenciamento da conta do usuário XClarity Administrator e permite usar contas do usuário do CMM locais para autenticar-se no CMM e em qualquer processador de gerenciamento que esteja instalado no chassi.

     Depois que o comando `fsmcm -off` é executado, a conta `RECOVERY_ID` é removida do registro de usuário do CMM. Ao executar o comando `fsmcm -off`, a sessão de CLI do CMM é encerrada. Agora é possível se autenticar no CMM e em outros componentes de chassi usando as credenciais locais do CMM, e usar credenciais locais do CMM para acessar a interface da Web do CMM ou a CLI do chassi até que o gerenciamento de usuários do XClarity Administrator seja restaurado.

     Para obter mais informações, consulte o Comando fsmcm na documentação online do CMM.

Após XClarity Administrator ser restaurado ou substituído, é possível gerenciar o chassi novamente (consulte Gerenciando chassi). Todas as informações sobre o chassi (como configurações de rede) são retidas.

Cancelando o gerenciamento de um chassi

É possível remover um chassi do gerenciamento do Lenovo XClarity Administrator. Esse processo é chamado de *cancelamento de gerenciamento*. Após o gerenciamento do chassi ser cancelado, é possível fazer login no CMM do chassi usando as contas do usuário do CMM locais.

Antes de iniciar

É possível habilitar o XClarity Administrator para cancelar automaticamente o gerenciamento de dispositivos que estão offline por um período específico. Isso é desativado por padrão. Para habilitar o cancelamento de gerenciamento automático de dispositivos offline, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos** no menu do XClarity Administrator e, em seguida, clique em **Editar** próximo a **Cancelamento de gerenciamento de dispositivos está desabilitado**. Em seguida, selecione **Habilitar cancelamento de gerenciamento de dispositivos offline** e defina o intervalo de tempo. Por padrão, o gerenciamento dos dispositivos são cancelados após estarem offline por 24 horas.

Antes de cancelar o gerenciamento de um chassi, verifique se não há nenhum trabalho ativo em execução nos dispositivos instalados no chassi.

Quando Call Home é ativado no XClarity Administrator, Call Home é desativado em todos os chassis e servidores gerenciados para evitar a criação de registros de problema duplicados. Se você pretende deixar de usar o XClarity Administrator para gerenciar dispositivos, poderá reativar Call Home em todos os dispositivos gerenciados no XClarity Administrator em vez de reativar Call Home para cada dispositivo individual posteriormente (consulte Reativando call home em todos os dispositivos gerenciados na documentação online do XClarity Administrator).

Sobre esta tarefa

Quando você cancela o gerenciamento de um chassi, o XClarity Administrator executa as seguintes ações:

- Limpa a configuração usada para gerenciamento de usuários centralizado.
- Remove o certificado de segurança do CMM do armazenamento confiável do XClarity Administrator.
- Se o Encapsulamento estiver ativado no dispositivo, configura as regras de firewall de dispositivos para as configurações anteriores ao gerenciamento do dispositivo.
- Remove o acesso ao servidor NTP do CMM.
- Remove as assinaturas de CIM para o CMM da configuração do XClarity Administrator para que XClarity Administrator não receba mais eventos do chassi.

Quando o gerenciamento de um chassi é cancelado, o XClarity Administrator retém determinadas informações sobre o chassi. Essa informação é reaplicada ao gerenciar o mesmo chassi novamente.

Quando você cancela o gerenciamento de um chassi, os eventos que foram enviados dos componentes de chassi são rejeitados. É possível manter esses eventos encaminhando-os para um repositório externo, como um syslog (consulte Encaminhamento de eventos).

Dica: todos os dispositivos de demonstração que são incluídos opcionalmente durante a configuração inicial são nós em um chassi. Para cancelar o gerenciamento dos dispositivos da demonstração, cancele o gerenciamento do chassi usando a opção **Forçar cancelamento de gerenciamento mesmo se o dispositivo não estiver acessível**.

Procedimento

Para cancelar o gerenciamento de um chassi, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Chassi** para exibir a página Chassi.

Etapa 2. Selecione um ou mais chassis na lista de chassis gerenciados.

Etapa 3. Clique em **Cancelar gerenciamento de Chassi**. A caixa de diálogo Cancelar gerenciamento é exibida.

Etapa 4. **Opcional:** selecione **Forçar cancelamento de gerenciamento mesmo se o dispositivo não estiver acessível**.

Importante: Ao cancelar o gerenciamento do hardware da demonstração, selecione essa opção.

Etapa 5. Clique em **Cancelar Gerenciamento**.A caixa de diálogo Cancelar gerenciamento mostra o progresso de cada etapa no processo de cancelamento de gerenciamento.

Etapa 6. Quando esse processo for concluído, clique em **OK**.

Depois de concluir

Após o processo de cancelamento de gerenciamento ser concluído, é possível fazer login no CMM usando as contas do usuário do CMM locais. Se você não se lembra dos nomes de usuário ou das senhas de alguma conta de usuário do CMM local, redefina o CMM para os padrões de fábrica para fazer login no CMM. Para obter informações sobre como reconfigurar o CMM para padrões de fábrica, consulte Redefinição do CMM na documentação online do Flex Systems na documentação do CMM.

Recuperando um chassi cujo gerenciamento não foi cancelado corretamente

Se o gerenciamento de um chassi não tiver sido cancelado corretamente, será necessário recuperar o chassi antes de gerenciá-lo novamente.

Procedimento

Conclua um dos seguintes procedimentos para restaurar o gerenciamento em um CMM.

- Se a instância de substituição do XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, gerencie o dispositivo novamente usando a conta e senha de RECOVERY_ID e a opção **Forçar gerenciamento** (consulte Gerenciando chassi).
- Redefina o CMM para os padrões de fábrica pressionando o botão de orifício no CMM usando um clipe por pelo menos 10 segundos. Para obter mais informações sobre como reconfigurar o CMM, incluindo avisos importantes, consulte Redefinição do CMM na documentação online do Flex Systems.
- Redefina a configuração do CMM usando as seguintes etapas:
  1. Por meio de uma sessão SSH, abra uma interface da linha de comandos de gerenciamento para o chassi e efetue login com a conta `RECOVERY_ID`.

     Nota: A senha para a conta `RECOVERY_ID` foi configurada quando você selecionou o chassi para gerenciamento na página Domínio de Gerenciamento. Para obter mais informações sobre o gerenciamento centralizado da conta, consulte Gerenciando chassi.

     Se esta for a primeira vez que você usou a conta `RECOVERY_ID` para fazer login no CMM, será necessário alterar a senha.
  2. Se for solicitado, digite a nova senha para a conta `RECOVERY_ID`.
  3. Restaure a configuração do CMM realizando uma das seguintes etapas:
     - Se estiver executando a versão de junho de 2015 ou mais recente do firmware do CMM, execute o seguinte comando:
       ```
       read -f unmanage -T mm[p]
       ```
       Para obter mais informações, consulte o Comando read na documentação online do CMM.
     - Se estiver executando a versão anterior a junho de 2015 do firmware do CMM, execute os seguintes comandos na ordem mostrada:
       a. `env -T mm[p]`
       b. `sslcfg -client disabled -tc1 remove`
       c. `accseccfg -am local`
       d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`
       e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`
       f. `cimsub -clear all`
       g. `fsmcm -off`

          O comando `fsmcm` desativa o gerenciamento da conta do usuário XClarity Administrator e permite usar contas do usuário do CMM locais para autenticar-se no CMM e em qualquer processador de gerenciamento que esteja instalado no chassi.

          Depois que o comando `fsmcm -off` é executado, a conta `RECOVERY_ID` é removida do registro de usuário do CMM. Ao executar o comando `fsmcm -off`, a sessão de CLI do CMM é encerrada. Agora é possível se autenticar no CMM e em outros componentes de chassi usando as credenciais locais do CMM, e usar credenciais locais do CMM para acessar a interface da Web do CMM ou a CLI do chassi até que o gerenciamento de usuários do XClarity Administrator seja restaurado.

Para obter mais informações, consulte o Comando fsmcm na documentação online do CMM.

Após XClarity Administrator ser restaurado ou substituído, é possível gerenciar o chassi novamente (consulte Gerenciando chassi). Todas as informações sobre o chassi (como configurações de rede) são retidas.

Capítulo 8. Gerenciando servidores

O Lenovo XClarity Administrator pode gerenciar diversos tipos de sistema, incluindo servidores ThinkAgile, ThinkSystem, Converged, Flex System, NeXtScale, System x® e ThinkServer®.

Saiba mais: XClarity Administrator: descoberta

Antes de iniciar

Nota: Os nós de cálculo Flex são descobertos e gerenciados automaticamente ao gerenciar o chassi que os contêm. Não é possível descobrir e gerenciar nós de cálculo Flex independentes do chassi.

Antes de gerenciar servidores, assegure-se de que as condições a seguir sejam atendidas:

- Reveja as considerações de gerenciamento antes de gerenciar um dispositivo. Para obter mais informações, consulte Considerações sobre gerenciamento na documentação online do XClarity Administrator.
- Algumas portas podem estar disponíveis para comunicação com os dispositivos. Assegure-se de todas as portas necessárias estejam disponíveis antes de tentar gerenciar servidores. Para obter informações sobre portas, consulte Disponibilidade de porta na documentação online do XClarity Administrator.
- Verifique se o firmware mínimo necessário está instalado em cada servidor que você deseja gerenciar usando o XClarity Administrator. É possível localizar os níveis mínimos de firmware necessários em Página da Web Suporte do XClarity Administrator – Compatibilidade clicando na guia **Compatibilidade** e, em seguida, clicando no link para os tipos de dispositivo apropriados.
- Verifique se CIM sobre HTTPS está ativado no dispositivo.
  1. Faça login na interface da Web de gerenciamento do servidor usando a conta do usuário de `RECOVERY_ID`
  2. Clique em **Gerenciamento do IMM → Segurança**.
  3. Clique na guia **CIM sobre HTTPS** e certifique-se de que **Habilitar CIM sobre HTTPS** esteja selecionado.
- Para servidores ThinkSystem SR635 e SR655:
  - Certifique-se de que um sistema operacional esteja instalado e que o servidor tenha sido inicializado para o SO, mídia inicializável montada ou efishell pelo menos uma vez para que o XClarity Administrator possa coletar o inventário desses servidores.
  - Verifique se a IPMI sobre LAN está ativada. O IPMI sobre LAN é desabilitado por padrão nesses servidores e deve ser habilitado manualmente para que os servidores possam ser gerenciados. Para ativar o IPMI sobre LAN usando o TSM, clique em **Configurações → Configuração de IPMI**. Talvez seja necessário reiniciar o servidor para ativar a mudança.
- Se o certificado do servidor do dispositivo for assinado por uma autoridade de certificado externa, garanta que o certificado de autoridade de certificado e todos os certificados intermediários sejam importados para o armazenamento confiável do XClarity Administrator (consulte Implantando certificados de servidor personalizado em dispositivos gerenciados).
- Para descobrir um servidor que está em uma sub-rede *diferente* do XClarity Administrator, certifique-se de que uma das seguintes condições seja atendida:
  - Certifique-se de habilitar o encaminhamento SLP multicast em comutadores top-of-rack, bem como nos roteadores do seu ambiente. Consulte a documentação que foi fornecida com seu comutador ou roteador específico para determinar se o encaminhamento SLP de multicast está ativado e para encontrar procedimentos para ativá-lo caso esteja desativado.

  - Se SLP estiver desabilitado no terminal ou na rede, você poderá usar o método de descoberta DNS, adicionando manualmente um registro de serviço (registro do servidor) ao servidor de nomes de domínio (DNS), para o XClarity Administrator, por exemplo
    `_lxca._tcp.labs.lenovo.com  service = 0 0 443 fvt-xhmc3.labs.lenovo.com.`

    Em seguida, habilite a descoberta de DNS no console de gerenciamento Baseboard na interface da Web de gerenciamento, clicando em **Gerenciamento IMM → Protocolo de Rede**, clicando na guia **DNS** e selecionando **Usar DNS para descobrir o Lenovo XClarity Administrator**.

    Notas:

    - O controlador de gerenciamento deve estar executando um nível de firmware com data de maio de 2017 ou posterior para dar suporte à descoberta automática usando DNS.
    - Se houver várias instâncias do XClarity Administrator no seu ambiente, o servidor será descoberto apenas pela instância que for a primeira a responder à solicitação de descoberta. O servidor não será descoberto por todas as instâncias.
- Para descobrir e gerenciar servidores ThinkServer, assegure que os seguintes requisitos sejam atendidos. Para obter mais informações, consulte Não é possível descobrir um dispositivo e Não é possível gerenciar um dispositivo na documentação online do XClarity Administrator.
  - O nome do host do servidor deve ser configurado usando um nome de host ou endereço IP válido caso você queira que o XClarity Administrator descubra os servidores automaticamente.
  - A configuração de rede deve permitir o tráfego SLP entre XClarity Administrator e o servidor.
  - Unicast SLP é necessário.
  - Se desejar que o XClarity Administrator descubra os servidores ThinkServer automaticamente, multicast SLP será necessário. Além disso, SLP deve ser ativado no ThinkServer System Manager (TSM).
  - Se os servidores ThinkServer estiverem em uma rede diferente do XClarity Administrator, verifique se a rede está configurada para permitir UDP de entrada pela porta 162 para que o XClarity Administrator possa receber eventos para esses dispositivos.
- Para ThinkAgile, ThinkSystem, Converged, Flex System. NeXtScale e System x, se você remover, substituir ou configurar qualquer adaptador no servidor, reinicie o servidor pelo menos uma vez para atualizar as informações do novo adaptador nos relatórios do Baseboard Management Controller e do XClarity Administrator (Ligando e desligando um servidor).
- Ao executar ações de gerenciamento em um servidor, verifique se o servidor está desligado ou ligado na configuração do BIOS/UEFI ou em um sistema operacional em execução. Você pode inicializar a configuração do BIOS/UEFI na página Servidores do XClarity Administrator. Para fazer isso, clique em **Todas as Ações → Ações de Energia → Reiniciar para Configuração BIOS/UEFI**. Se o servidor estiver ligado sem um sistema operacional, o controlador de gerenciamento redefinirá continuamente o servidor para tentar localizar um sistema operacional.
- Verifique se as configurações `UEFI_Ethernet_*` e `UEFI_Slot_*` estão ativadas nas Configurações UEFI do servidor. Para verificar as configurações, reinicie o servidor e, quando o prompt `<F1> Setup` for exibido, pressione `F1` para iniciar o Setup Utility. Vá até **System Settings → Devices and I/O Ports → Enable / Disable Adapter Option ROM Support** e localize a seção **Enable / Disable UEFI Option ROM(s)** para verificar se as configurações estão ativadas.

  Nota: Se suportado, você também poderá usar o recurso Console Remoto na interface de gerenciamento de placa-mãe para examinar e alterar as configurações remotamente.
- Os servidores System x3950 X6 devem ser gerenciados como dois gabinetes 4U, cada com seu próprio Baseboard Management Controller.

Sobre esta tarefa

O XClarity Administrator pode descobrir automaticamente o rack e os servidores em torre em seu ambiente, sondando dispositivos gerenciáveis que estão na mesma sub-rede IP que o XClarity Administrator. Para descobrir o rack e os servidores em torre que estão em outras sub-redes, especifique um endereço IP ou intervalo de endereços IP, ou importe informações de uma planilha.

Importante: Para os servidores System x3850 e x3950 X6, você deve gerenciar cada servidor no ambiente de rack escalável.

Após os servidores serem gerenciados pelo XClarity Administrator, o Lenovo XClarity Administrator sonda cada servidor gerenciado periodicamente para coletar informações, como inventário, dados vitais do produto e status. É possível exibir e monitorar cada servidor gerenciado e executar ações de gerenciamento (como definir configurações do sistema, implantar imagens do sistema operacional e ligar e desligar o equipamento).

Por padrão, os dispositivos são gerenciados usando a autenticação gerenciada do XClarity Administrator para fazer login nos dispositivos. Ao gerenciar servidores em rack e chassis da Lenovo, você pode optar por usar autenticação local ou autenticação gerenciada para fazer login nos dispositivos.

- Quando a *autenticação local* é usada para servidores em rack, chassi da Lenovo e comutadores de rack da Lenovo, o XClarity Administrator usa uma credencial armazenada para autenticar o dispositivo. A *credencial armazenada* pode ser uma conta do usuário ativa no dispositivo ou uma conta do usuário em um servidor do Active Directory.

  Você deve criar uma credencial armazenada no XClarity Administrator que corresponda a uma conta do usuário ativa no dispositivo ou uma conta do usuário em um servidor do Active Directory antes de gerenciar o dispositivo usando a autenticação local (consulte Gerenciando credenciais compartilhadas na documentação online do XClarity Administrator).

  Notas:

  – Dispositivos RackSwitch oferecem suporte apenas a credenciais armazenadas para autenticação. Não há suporte para as credenciais do usuário do XClarity Administrator.
- Usar a *autenticação gerenciada* permite gerenciar e monitorar vários dispositivos usando as credenciais no servidor de autenticação do XClarity Administrator em vez de credenciais locais. Quando a autenticação gerenciada é usada para um dispositivo (diferente de servidores ThinkServer, servidores System x M4 e comutadores), o XClarity Administrator configura o dispositivo e seus componentes instalados para usar o servidor de autenticação do XClarity Administrator para gerenciamento centralizado.

  – Quando a autenticação gerenciada estiver habilitada, você poderá gerenciar dispositivos usando credenciais armazenadas ou inseridas manualmente (consulte Gerenciando contas de usuário e na documentação online do XClarity Administrator).

    A credencial armazenada é usada somente até que o XClarity Administrator configure as definições LDAP no dispositivo. Depois disso, qualquer mudança nas credenciais armazenadas não tem impacto no gerenciamento ou no monitoramento desse dispositivo.

    Nota: Quando a autenticação gerenciada é ativada para um dispositivo, não é possível editar credenciais armazenadas para esse dispositivo usando o XClarity Administrator.

  – Se um servidor LDAP local ou externo for usado como servidor de autenticação do XClarity Administrator, as contas de usuário definidas no servidor de autenticação serão usadas para fazer login no XClarity Administrator, em CMMs e no Baseboard Management Controllers no domínio XClarity Administrator. As contas de usuário do CMM local e do controlador de gerenciamento são desativadas.

  – Se um provedor de identidade SAML 2.0 for usado como servidor de autenticação do XClarity Administrator, as contas de SAML não estarão acessíveis para dispositivos gerenciados. Entretanto, ao usar um provedor de identidade SAML e um servidor LDAP juntos, se o provedor de identidade usar

contas existentes no servidor LDAP, as contas de usuário LDAP poderão ser usadas para fazer login nos dispositivos gerenciados, enquanto os métodos de autenticação mais avançados fornecidos por SAML 2.0 (como autenticação de vários fatores e logon único) podem ser usados para fazer login no XClarity Administrator.

- O login único permite que um usuário já conectado ao XClarity Administrator faça login automaticamente no Baseboard Management Control. O login único é ativado por padrão quando um servidor ThinkSystem ou ThinkAgile é trazido para o gerenciamento pelo XClarity Administrator (a menos que o servidor seja gerenciado com senhas do CyberArk). É possível definir a configuração global para ativar ou desabilitar o login único para todos os servidores ThinkSystem e ThinkAgile gerenciados. Ativar o login único para um servidor ThinkSystem e ThinkAgile específico substitui a configuração global para todos os servidores ThinkSystem e ThinkAgile (consulte).

  Nota: O logon único é desativado automaticamente ao usar o sistema de gerenciamento de identidade CyberArk para autenticação.

- Quando a autenticação gerenciada está ativada para servidores ThinkSystem SR635 e SR655:
  - O firmware do controlador de gerenciamento do baseboard oferece suporte a até cinco funções de usuário LDAP. O XClarity Administrator adiciona essas funções de usuário LDAP aos servidores durante o gerenciamento: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** e **lxc-os-admin**.

    Os usuários devem ser atribuídos a pelo menos uma das funções de usuário LDAP especificadas para se comunicar com os servidores ThinkSystem SR635 e SR655.
  - O firmware do controlador de gerenciamento não oferece suporte aos usuários LDAP com o mesmo nome do usuário local do servidor.
- Para servidores ThinkServer e System x M4, o servidor de autenticação do XClarity Administrator não é usado. Em vez disso, uma conta IPMI é criada no dispositivo com o prefixo "LXCA_" acompanhado por uma sequência aleatória. (As contas do usuário do IPMI local existente estão desabilitadas.) Quando você cancelar o gerenciamento de um servidor ThinkServer, a conta do usuário do "LXCA_" será desabilitada e o prefixo "LXCA_" será substituído por "DISABLED_". Para determinar se um servidor ThinkServer é gerenciado por outra instância, o XClarity Administrator verifica as contas de IPMI com o prefixo "LXCA_". Se você escolher forçar o gerenciamento de um servidor ThinkServer gerenciado, todas as contas de IPMI no dispositivo com o prefixo "LXCA_" serão desabilitadas e renomeadas. Considere apagar manualmente as contas de IPMI que não são mais usadas.

  Se você usar credenciais inseridas manualmente, o XClarity Administrator criará uma credencial armazenada automaticamente e usará essa credencial armazenada para gerenciar o dispositivo.

  Notas: Quando a autenticação gerenciada é ativada para um dispositivo, não é possível editar credenciais armazenadas para esse dispositivo usando o XClarity Administrator.
  - Cada vez que você gerencia um dispositivo usando credenciais inseridas manualmente, uma nova credencial armazenada é criada para o dispositivo, mesmo se outra credencial armazenada foi criada para o dispositivo durante um processo de gerenciamento anterior.
  - Quando você cancela o gerenciamento de um dispositivo, o XClarity Administrator não exclui credenciais armazenadas que foram criadas automaticamente para esse dispositivo durante o processo de gerenciamento.

Um dispositivo pode ser gerenciado somente por uma instância do XClarity Administrator por vez. Não há suporte para o gerenciamento por várias instâncias do XClarity Administrator. Se um dispositivo for gerenciado por um XClarity Administrator, e você desejar gerenciá-lo com outro XClarity Administrator, primeiro cancele o gerenciamento do dispositivo no XClarity Administrator inicial e gerencie-o com o novo XClarity Administrator. Se um erro ocorrer durante o processo de cancelamento de gerenciamento, você poderá selecionar a opção **Forçar gerenciamento** durante o gerenciamento no novo XClarity Administrator.

Nota: Ao procurar dispositivos gerenciáveis na rede, o XClarity Administrator não sabe se um dispositivo já é gerenciado por outro gerenciador até após tentar gerenciar o dispositivo.

Nota: Ao buscar dispositivos gerenciáveis na rede, o XClarity Administrator não sabe se um dispositivo ThinkServer já é gerenciado. Portanto, os dispositivos ThinkServer gerenciados podem aparecer na lista de dispositivos gerenciáveis.

Durante o processo de gerenciamento, o XClarity Administrator executa as seguintes ações:

- Faz login no servidor usando as credenciais fornecidas.
- Coleta o inventário para cada servidor.

  Nota: Alguns dados do inventário são coletados após o processo de gerenciamento ser concluído. Não é possível executar determinadas tarefas em um servidor gerenciado (como implantar um padrão de servidor) até que todos os dados do inventário sejam coletados para esse servidor e o servidor não esteja mais no estado pendente.
- Define as configurações do servidor NTP para que todos os dispositivos gerenciados usem a mesma configuração de servidor NTP definida no XClarity Administrator.
- (Somente servidores System x e NeXtScale) Atribui a última política de conformidade de firmware editada ao servidor.
- (Somente servidores Lenovo System x e NeXtScale) Configura opcionalmente as regras de firewall de dispositivos para que solicitações de entrada sejam aceitas somente no XClarity Administrator.
- (Somente servidores System x e NeXtScale) Troca certificados de segurança com o controlador de gerenciamento, copiando o certificado do servidor CIM e o certificado de cliente LDAP do controlador de gerenciamento para o armazenamento confiável do XClarity Administrator e enviando o certificado segurança CA e os certificados LDAP confiáveis do XClarity Administrator para o controlador de gerenciamento. O controlador de gerenciamento carrega os certificados em seu próprio armazenamento confiável para que ele possa confiar em conexões com os servidores LDAP e CIM no XClarity Administrator.

  Nota: Se o certificado do servidor CIM ou o certificado de cliente LDAP não existir, ele será criado durante o processo de gerenciamento.
- Configura a autenticação gerenciada, se aplicável. Para obter mais informações sobre autenticação gerenciada, consulte Gerenciando o servidor de autenticação.
- Cria a conta do usuário de recuperação (`RECOVERY_ID`), quando aplicável. Para obter mais informações sobre a conta de `RECOVERY_ID`, consulte Gerenciando o servidor de autenticação.

Nota: O XClarity Administrator não altera as configurações de segurança ou configurações criptográficas (modo criptográfico e modo usado para comunicações seguras) durante o processo de gerenciamento. É possível alterar as configurações de criptografia depois que o servidor é gerenciado (consulte Definindo configurações de criptografia no servidor de gerenciamento).

Importante: Se você altera o endereço IP de um servidor quando o servidor é gerenciado pelo XClarity Administrator, o XClarity Administrator reconhece o novo endereço IP e continua gerenciando o servidor. No entanto, o XClarity Administrator não reconhece a alteração de endereço IP para alguns servidores. Se o XClarity Administrator mostrar que o servidor está offline após a alteração do endereço IP, gerencie o servidor novamente usando a opção **Forçar gerenciamento**.

Procedimento

Para gerenciar seus servidores de rack e em torre usando o XClarity Administrator, conclua um dos procedimentos a seguir.

- Descubra e gerencie um grande número de servidores em torre e em rack, além de outros dispositivos usando um arquivo de importação em massa (consulte Gerenciando sistemas na documentação online do XClarity Administrator).
- Descubra e gerencie os servidores de rack e em torre que estão na mesma sub-rede IP que o XClarity Administrator.
  1. Na barra de menu do XClarity Administrator, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos**. A página Descobrir e Gerenciar Novos Dispositivos é exibida.

     É possível classificar as colunas da tabela para facilitar a localização dos servidores que deseja gerenciar. Além disso, é possível digitar texto (como um nome ou endereço IP) no campo **Filtro** para filtrar mais servidores que são exibidos. É possível alterar as colunas que são exibidas e a ordem de classificação padrão, clicando no ícone **Personalizar colunas** ( ).

  2. Clique no ícone **Atualizar** ( ) para descobrir todos os dispositivos gerenciáveis no domínio XClarity Administrator. A descoberta pode levar vários minutos.
  3. Clique na caixa de seleção **Habilitar encapsulamento em todos os dispositivos gerenciados futuros** para alterar as regras de firewall em todos os dispositivos durante o processo de gerenciamento para que as solicitações de entrada sejam aceitas somente de XClarity Administrator.

     O encapsulamento pode ser ativado ou desativado em dispositivos específicos após serem gerenciados.

Nota: Quando a interface de rede de gerenciamento é configurada para usar o Protocolo de Configuração de Host Dinâmico (DHCP) e o encapsulamento é ativado, pode demorar para gerenciar um servidor em rack.

Atenção: Se o encapsulamento estiver ativado e XClarity Administrator ficar indisponível antes que o gerenciamento de um dispositivo seja cancelado, as etapas necessárias deverão ser tomadas para desativar o encapsulamento e estabelecer comunicação com o dispositivo. Para procedimentos de recuperação, consulte o arquivo lenovoMgrAlert.mib e Recuperando o gerenciamento com um CMM após uma falha no servidor de gerenciamento.

4. Selecione um ou mais servidores que você deseja gerenciar.
5. Clique em **Gerenciar Selecionado**. A caixa de diálogo Gerenciar é exibida.
6. Opte por usar a autenticação gerenciada do XClarity Administrator ou a autenticação local para esse dispositivo. A autenticação gerenciada é selecionada por padrão. Para usar autenticação local, desmarque **Autenticação Gerenciada**.
7. Escolha o tipo de credenciais a ser usado para autenticar o dispositivo e especifique as credenciais apropriadas:
   - **Usar credenciais inseridas manualmente**
     - Especifique o ID do usuário e a senha para autenticação no servidor.
     - (Opcional) Defina uma nova senha para o nome do usuário especificado se a senha estiver expirada atualmente no dispositivo.

     Nota: Para usar credenciais inseridas manualmente, você deve selecionar a autenticação gerenciada do XClarity Administrator.
   - **Usar credenciais armazenadas**

     Selecione as credenciais armazenadas a serem usadas para esse dispositivo gerenciado. Você pode criar uma nova credencial armazenada clicando em **Criar Novo**.
   - **Use um sistema externo de gerenciamento de identidade**.

     Selecione o sistema de gerenciamento de identidade que deseja usar para este dispositivo gerenciado. Em seguida, preencha os campos restantes, incluindo o endereço IP ou o nome do host do servidor gerenciado, nome do usuário e, opcionalmente, o ID do aplicativo, o cofre e a pasta.

     Se você especificar o ID do aplicativo, também deverá especificar o cofre e a pasta, se aplicável.

     Se você não especificar o ID do aplicativo, o XClarity Administrator usará os caminhos definidos quando você configurar o CyberArk para identificar as contas integradas ao CyberArk.

     Nota: Apenas os servidores ThinkSystem ou ThinkAgile são suportados. O sistema de gerenciamento de identidade deve ser configurado no XClarity Administrator, e o Lenovo XClarity Controller para os servidores ThinkSystem ou ThinkAgile devem ser integrados ao CyberArk.

   É recomendável usar uma conta de supervisor ou administrador para gerenciar o dispositivo. Se uma conta com autoridade de nível mais baixo for usada, o gerenciamento poderá falhar ou poderá ser bem-sucedido, mas outras operações do XClarity Administrator no dispositivo poderão falhar (principalmente se o dispositivo for gerenciado sem autenticação gerenciada).

   Para obter mais informações sobre as credenciais normais e armazenadas, consulte Gerenciando contas de usuário e Gerenciando credenciais compartilhadas.
8. Especifique a senha de recuperação se a autenticação gerenciada estiver selecionada.

   Quando uma senha é especificada, a conta de recuperação (`RECOVERY_ID`) é criada no servidor, e todas as contas de usuário locais são desativadas. Se houver um problema com XClarity Administrator e

ele parar de funcionar por alguma razão, *não* será possível fazer login no controlador de gerenciamento usando contas de usuário normais. No entanto, é possível fazer login usando a conta de recuperação.

Notas:

- A senha de recuperação é opcional se você optar por usar autenticação gerenciada e não é permitida se você optar por usar autenticação local.
- É possível optar por usar uma conta de recuperação local ou credenciais de recuperação armazenadas. Em qualquer um dos casos, o nome do usuário é sempre `RECOVERY_ID`.
- Verifique se a senha segue as políticas de segurança e senha para o dispositivo. As políticas de segurança e senha podem variar.
- Certifique-se de gravar a senha de recuperação para uso futuro.
- Não há suporte para a conta de recuperação para servidores ThinkServer e System x M4.

Para obter mais informações sobre o ID de recuperação, consulte Gerenciando o servidor de autenticação.

9. Clique em **Alterar** para alterar os grupos de funções que devem ser atribuídos aos dispositivos.

   Notas:

   - É possível selecionar de uma lista de grupos de funções que são atribuídos ao usuário atual.
   - Se você não alterar os grupos de funções, os grupos de função padrão serão usados. Para obter mais informações sobre os grupos de função padrão, consulte Alterando as permissões padrão.

10. Clique em **Gerenciar**.

    Uma caixa de diálogo é exibida e mostra o progresso desse processo de gerenciamento. Para assegurar que o processo seja concluído com êxito, monitore o progresso.

11. Quando o processo for concluído, clique em **OK**.

    O dispositivo agora é gerenciado por XClarity Administrator, que sonda automaticamente o dispositivo gerenciado regularmente para coletar informações atualizadas, como inventário.

    Se o gerenciamento não tiver sido bem-sucedido por causa de uma das seguintes condições de erro, repita esse procedimento usando a opção **Forçar gerenciamento**.

    - Se o gerenciamento do XClarity Administrator falhar e não puder ser recuperado.

      Nota: Se a instância de substituição do XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, você poderá gerenciar o dispositivo novamente usando a conta e senha de RECOVERY_ID (se aplicável) e a opção **Forçar gerenciamento**.
    - Se o gerenciamento do XClarity Administrator tiver sido desligado antes do cancelamento do gerenciamento dos dispositivos.
    - Se o cancelamento do gerenciamento dos dispositivos não tiver sido bem-sucedido.

    Atenção: Os dispositivos podem ser gerenciados somente por uma instância do XClarity Administrator por vez. Não há suporte para o gerenciamento por várias instâncias do XClarity Administrator. Se um dispositivo for gerenciado por um XClarity Administrator, e você desejar gerenciá-lo com outro XClarity Administrator, primeiro cancele o gerenciamento do dispositivo no XClarity Administrator original e gerencie-o com o novo XClarity Administrator.

- Descubra e gerencie os servidores de rack e em torre que não estiverem na mesma sub-rede IP que o XClarity Administrator especificando manualmente endereços IP.

  1. Na barra de menu do XClarity Administrator, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos**. A página Descobrir e Gerenciar é exibida.

2. Clique na caixa de seleção **Habilitar encapsulamento em todos os dispositivos gerenciados futuros** para alterar as regras de firewall em todos os dispositivos durante o processo de gerenciamento para que as solicitações de entrada sejam aceitas somente de XClarity Administrator.

   O encapsulamento pode ser ativado ou desativado em dispositivos específicos após serem gerenciados.

   Nota: Quando a interface de rede de gerenciamento é configurada para usar o Protocolo de Configuração de Host Dinâmico (DHCP) e o encapsulamento é ativado, pode demorar para gerenciar um servidor em rack.

   Atenção: Se o encapsulamento estiver ativado e XClarity Administrator ficar indisponível antes que o gerenciamento de um dispositivo seja cancelado, as etapas necessárias deverão ser tomadas para desativar o encapsulamento e estabelecer comunicação com o dispositivo. Para procedimentos de recuperação, consulte o arquivo lenovoMgrAlert.mib e Recuperando o gerenciamento com um CMM após uma falha no servidor de gerenciamento.
3. Selecione **Entrada Manual**.
4. Especifique os endereços de rede dos servidores que deseja gerenciar:
   - Clique em **Sistema Único** e insira um nome de domínio de endereço IP único ou o nome de domínio totalmente qualificado (FQDN).

     Nota: Para especificar um FQDN, verifique se um nome de domínio válido foi especificado na página Acesso à Rede (consulte Configurando o acesso à rede).
   - Clique em **Vários Sistemas** e insira um intervalo de endereços IP. Para adicionar outro intervalo, clique no ícone **Adicionar** (). Para remover um intervalo, clique no ícone **Remover** ().
5. Clique em **OK**. A caixa de diálogo Gerenciar é exibida
6. Opte por usar a autenticação gerenciada do XClarity Administrator ou a autenticação local para esse dispositivo. A autenticação gerenciada é selecionada por padrão. Para usar autenticação local, desmarque **Autenticação Gerenciada**.
7. Escolha o tipo de credenciais a ser usado para autenticar o dispositivo e especifique as credenciais apropriadas:
   - **Usar credenciais inseridas manualmente**
     - Especifique o ID do usuário e a senha para autenticação no servidor.
     - (Opcional) Defina uma nova senha para o nome do usuário especificado se a senha estiver expirada atualmente no dispositivo.

     Nota: Para usar credenciais inseridas manualmente, você deve selecionar a autenticação gerenciada do XClarity Administrator.
   - **Usar credenciais armazenadas**

     Selecione as credenciais armazenadas a serem usadas para esse dispositivo gerenciado. Você pode criar uma nova credencial armazenada clicando em **Criar Novo**.
   - **Use um sistema externo de gerenciamento de identidade**.

     Selecione o sistema de gerenciamento de identidade que deseja usar para este dispositivo gerenciado. Em seguida, preencha os campos restantes, incluindo o endereço IP ou o nome do host do servidor gerenciado, nome do usuário e, opcionalmente, o ID do aplicativo, o cofre e a pasta.

     Se você especificar o ID do aplicativo, também deverá especificar o cofre e a pasta, se aplicável.

     Se você não especificar o ID do aplicativo, o XClarity Administrator usará os caminhos definidos quando você configurar o CyberArk para identificar as contas integradas ao CyberArk.

Nota: Apenas os servidores ThinkSystem ou ThinkAgile são suportados. O sistema de gerenciamento de identidade deve ser configurado no XClarity Administrator, e o Lenovo XClarity Controller para os servidores ThinkSystem ou ThinkAgile devem ser integrados ao CyberArk.

É recomendável usar uma conta de supervisor ou administrador para gerenciar o dispositivo. Se uma conta com autoridade de nível mais baixo for usada, o gerenciamento poderá falhar ou poderá ser bem-sucedido, mas outras operações do XClarity Administrator no dispositivo poderão falhar (principalmente se o dispositivo for gerenciado sem autenticação gerenciada).

Para obter mais informações sobre as credenciais normais e armazenadas, consulte Gerenciando contas de usuário e Gerenciando credenciais compartilhadas.

8. Especifique a senha de recuperação se a autenticação gerenciada estiver selecionada.

   Quando uma senha é especificada, a conta de recuperação (`RECOVERY_ID`) é criada no servidor, e todas as contas de usuário locais são desativadas. Se houver um problema com XClarity Administrator e ele parar de funcionar por alguma razão, *não* será possível fazer login no controlador de gerenciamento usando contas de usuário normais. No entanto, é possível fazer login usando a conta de recuperação.

   Notas:

   - A senha de recuperação é opcional se você optar por usar autenticação gerenciada e não é permitida se você optar por usar autenticação local.
   - É possível optar por usar uma conta de recuperação local ou credenciais de recuperação armazenadas. Em qualquer um dos casos, o nome do usuário é sempre `RECOVERY_ID`.
   - Verifique se a senha segue as políticas de segurança e senha para o dispositivo. As políticas de segurança e senha podem variar.
   - Certifique-se de gravar a senha de recuperação para uso futuro.
   - Não há suporte para a conta de recuperação para servidores ThinkServer e System x M4.

   Para obter mais informações sobre o ID de recuperação, consulte Gerenciando o servidor de autenticação.

9. Clique em **Alterar** para alterar os grupos de funções que devem ser atribuídos aos dispositivos.

   Notas:

   - É possível selecionar de uma lista de grupos de funções que são atribuídos ao usuário atual.
   - Se você não alterar os grupos de funções, os grupos de função padrão serão usados. Para obter mais informações sobre os grupos de função padrão, consulte Alterando as permissões padrão.

10. Clique em **Gerenciar**.

    Uma caixa de diálogo é exibida e mostra o progresso desse processo de gerenciamento. Para assegurar que o processo seja concluído com êxito, monitore o progresso.

11. Quando o processo for concluído, clique em **OK**.

    O dispositivo agora é gerenciado por XClarity Administrator, que sonda automaticamente o dispositivo gerenciado regularmente para coletar informações atualizadas, como inventário.

    Se o gerenciamento não tiver sido bem-sucedido por causa de uma das seguintes condições de erro, repita esse procedimento usando a opção **Forçar gerenciamento**.

    - Se o gerenciamento do XClarity Administrator falhar e não puder ser recuperado.

      Nota: Se a instância de substituição do XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, você poderá gerenciar o dispositivo novamente usando a conta e senha de RECOVERY_ID (se aplicável) e a opção **Forçar gerenciamento**.

- Se o gerenciamento do XClarity Administrator tiver sido desligado antes do cancelamento do gerenciamento dos dispositivos.
- Se o cancelamento do gerenciamento dos dispositivos não tiver sido bem-sucedido.

Atenção: Os dispositivos podem ser gerenciados somente por uma instância do XClarity Administrator por vez. Não há suporte para o gerenciamento por várias instâncias do XClarity Administrator. Se um dispositivo for gerenciado por um XClarity Administrator, e você desejar gerenciá-lo com outro XClarity Administrator, primeiro cancele o gerenciamento do dispositivo no XClarity Administrator original e gerencie-o com o novo XClarity Administrator.

Depois de concluir

- Descubra e gerencie dispositivos adicionais.
- Configure as informações do sistema, o armazenamento local, os adaptadores de E/S, os tópicos de inicialização e as configurações de firmware criando e implantando padrões de servidor (consulte Configurando servidores com padrões de configuração).
- Implante imagens do sistema operacional nos servidores que ainda não tenham um sistema operacional instalado (consulte Instalando sistemas operacionais em servidores bare-metal).
- Atualizar o firmware em dispositivos que não estão em conformidade com as políticas atuais (consulte Atualizando firmware em dispositivos gerenciados).
- Adicione os dispositivos ao rack adequado para refletir o ambiente físico (consulte Gerenciando racks).
- Monitore o status e os detalhes de hardware (consulte Visualizando o status de um servidor gerenciado).
- Monitore eventos e alertas (consulte Trabalhando com eventos e Trabalhando com alertas).
- Apague o log SEL de um servidor clicando em **Hardware → Servidores** na barra de menus do XClarity Administrator, selecionando o servidor e clicando em **Todas as Ações → Segurança → Limpar log SEL**. Esta ação é suportada apenas para servidores ThinkSystem e ThinkAgile.
- Resolva credenciais armazenadas que se tornaram expiradas ou inválidas (consulte Gerenciando credenciais compartilhadas).
- Ative ou desative o login único para todos os servidores ThinkSystem e ThinkAgile gerenciados clicando em **Administração → Segurança** na barra de menu do XClarity Administrator, clicando em **Sessões Ativas** e, em seguida, ativando ou desabilitando o **Logon Único**.
- Desative ou ative o login único para servidores gerenciados ThinkSystem e ThinkAgile.
  - Para todos os servidores ThinkSystem e ThinkAgile gerenciados (globalmente), clique em **Administração → Segurança** na barra de menus XClarity Administrator, clique em **Sessões Ativas** e, em seguida, ative ou desative o **Logon Único**.
  - Para um servidor ThinkSystem e ThinkAgile específico, clique em **Hardware → Servidor** na barra de menus do XClarity Administrator e, em seguida, clique em **Todas as Ações → Segurança → Ativar Logon Único** ou **Todas as Ações → Segurança → Desativar Logon Único**.

Nota: O login único permite que um usuário já conectado ao XClarity Administrator faça login automaticamente no Baseboard Management Control. O login único é ativado por padrão quando um servidor ThinkSystem ou ThinkAgile é trazido para o gerenciamento pelo XClarity Administrator (a menos que o servidor seja gerenciado com senhas do CyberArk). É possível definir a configuração global para ativar ou desabilitar o login único para todos os servidores ThinkSystem e ThinkAgile gerenciados. Ativar o login único para um servidor ThinkSystem e ThinkAgile específico substitui a configuração global para todos os servidores ThinkSystem e ThinkAgile.

Visualizando o status de um servidor gerenciado

É possível exibir um resumo e o status detalhado dos servidores gerenciados e os componentes instalados no Lenovo XClarity Administrator.

Saiba mais:

- XClarity Administrator: inventário
- XClarity Administrator: monitoramento

Sobre esta tarefa

Os seguintes ícones de status são usados para indicar a integridade geral do dispositivo. Se os certificados não corresponderem, "(Não confiável)" será anexado ao status de cada dispositivo aplicável, por exemplo, Aviso (Não confiável). Se houver um problema de conectividade ou uma conexão com o dispositivo não for confiável, "(Conectividade)" será anexado ao status de cada dispositivo aplicável, por exemplo, Aviso (Conectividade).

- ( ) Crítico
- ( ) Aviso
- ( ) Pendente
- ( ) Informativo
- ( ) Normal
- ( ) Offline
- ( ) Desconhecido

Um dispositivo pode estar em um dos seguintes estados de energia:

- Aceso
- Apagado
- Desligando o
- Em espera
- Hibernar
- Desconhecido

Procedimento

Para exibir o status de um servidor gerenciado, conclua uma ou mais das seguintes ações.

- Na barra de menu do XClarity Administrator, clique em **Painel**. A página Painel é exibida com uma visão geral e o status de todos os dispositivos gerenciados e outros recursos.

- Na barra de menu do XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados (servidores de rack e em torre, e nós de cálculo).

  É possível classificar as colunas da tabela para facilitar a localização dos servidores específicos. Além disso, é possível selecionar um tipo de sistema na lista suspensa **Todos os Sistemas**, inserir texto (como nome ou endereço IP) no campo **Filtro** e clicar no ícone de status para listar somente os servidores que correspondem aos critérios selecionados.

  Nesta página, é possível executar as ações a seguir:

  – Exibir informações detalhadas sobre o servidor e seus componentes (consulte Visualizando os detalhes de um servidor gerenciado).

  – Exibir um servidor em exibição gráfica de rack ou de chassi clicando em **Todas as Ações → Exibições → Mostrar na Exibição do Rack** ou **Todas as Ações → Exibições → Mostrar na Exibição do Chassi**.

- Iniciar a interface da Web do controlador de gerenciamento do servidor clicando no link **Endereço IP** (consulte Iniciando a interface do controlador de gerenciamento para um servidor).
- Gerenciar remotamente o servidor (consulte Usando o controle remoto para gerenciar servidores Converged, Flex System, NeXtScale e System x).
- Ligar e desligar o servidor (consulte Ligando e desligando um servidor).
- Modificar as informações do sistema selecionando um servidor e clicando em **Todas as Ações → Inventário → Editar Propriedades**.
- Atualizar o inventário selecionando um servidor e clicando em **Todas as Ações → Inventário → Atualizar Inventário**.
- Exportar informações detalhadas sobre um ou mais servidores para um único arquivo CSV selecionando os servidores e clicando em **Todas as Ações → Inventário → Exportar Inventário**.

  Nota: Você pode exportar os dados do inventário para no máximo 60 dispositivos ao mesmo tempo.

  Dica: Ao importar um arquivo CSV no Microsoft Excel, o Excel trata os valores de texto que contêm apenas números como valores numéricos (por exemplo, de UUIDs). Formate cada célula como texto para corrigir esse erro.
- Cancelar gerenciamento de um servidor (consulte Cancelando o gerenciamento de um servidor de rack ou em torre).
- Redefinir os adaptadores de armazenamento local para as configurações padrão de fabricação clicando em **Todas as Ações → Serviço → Redefinir Armazenamento Local para Padrões**.
- Alterar o estado do LED de Local em um servidor para aceso, apagado ou piscando selecionando o servidor e clicando em **Todas as Ações → Serviço → Alternar Estado do LED de Local**, selecionando o estado e clicando em **Aplicar**.
  - A alternância do LED de Local para servidores ThinkSystem SR635 e SR655 não é compatível.
  - O LED de Local nos servidores ThinkServer pode estar aceso ou apagado. Não há suporte para piscar.
- Reposicionar virtualmente o servidor (consulte Reposicionando virtualmente um servidor em um chassi do Flex System).
- Excluir eventos que não são de seu interesse de todas as páginas nas quais os eventos são exibidos clicando no ícone **Excluir eventos** () (consulte Excluindo eventos).
- Reiniciar o servidor usando uma interrupção não mascarável (NMI) clicando em **Todas as Ações → Serviço → Acionar NMI**.
- Habilitar ou desabilitar as alterações de regra de firewall em um servidor que limita as solicitações de entrada somente do XClarity Administrator selecionando o servidor e clicando em **Todas as Ações → Segurança → Habilitar Encapsulamento** ou **Todas as Ações → Segurança → Desabilitar Encapsulamento**.A configuração de encapsulamento global é desativada por padrão. Quando desativado, o modo de encapsulamento do dispositivo é definido como "normal" e as regras de firewall não são alteradas como parte do processo de gerenciamento.

  Quando a configuração de encapsulamento global é ativada e o dispositivo suporta o encapsulamento, o XClarity Administrator se comunica com o dispositivo durante o processo de gerenciamento para alterar o modo de encapsulamento do dispositivo para "encapsulationLite" e modificar as regras de firewall no dispositivo para delimitar as solicitações de entrada àquelas do XClarity Administrator.

  Atenção: Se o encapsulamento estiver ativado e XClarity Administrator ficar indisponível antes que o gerenciamento de um dispositivo seja cancelado, as etapas necessárias deverão ser tomadas para desativar o encapsulamento e estabelecer comunicação com o dispositivo. Para procedimentos de recuperação, consulte o arquivo lenovoMgrAlert.mib e Recuperando o gerenciamento com um CMM após uma falha no servidor de gerenciamento.

- (Somente servidores Converged, Flex System, NeXtScale, System x e ThinkSystem) Resolver problemas que podem ocorrer entre o certificado de segurança do XClarity Administrator e o certificado de segurança do Baseboard Management Controller no servidor selecionando um servidor e clicando em **Todas as Ações → Segurança → Resolver Certificados Não Confiáveis** (consulte Resolvendo um certificado de servidor não confiável).
- Resolver as credenciais armazenadas expiradas ou inválidas para um dispositivo no grupo de (consulte Resolvendo credenciais armazenadas expiradas ou inválidas para um servidor).
- Adicionar ou remover um servidor de um grupo de recursos estático clicando em **Todas as Ações → Grupos → Adicionar ao grupo** ou **Todas as Ações → Grupos → Remover do grupo**.

Visualizando os detalhes de um servidor gerenciado

É possível exibir informações detalhadas sobre os servidores gerenciados do Lenovo XClarity Administrator, incluindo os níveis de firmware, o nome do servidor e o identificador universal exclusivo (UUID).

Saiba mais:

-  XClarity Administrator: inventário
-  XClarity Administrator: monitoramento

Sobre esta tarefa

Uso da CPU é uma medida da residência agregada do estado C. É medido como porcentagem da residência C0 usada e máxima, por segundo.

O uso de memória é uma medida dos volumes de leitura/gravação agregados de todos os canais de memória. Isso é calculado como porcentagem da largura de banda de memória usada e máxima disponível, por segundo.

A temperatura do ar no nível do sistema é medida por um sensor na frente do servidor. Essa temperatura representa a temperatura de entrada do ar para o servidor. Observe que a temperatura do ar registrada pelo XClarity Administrator e pelo CMM pode ser diferente se a temperatura for capturada em momentos diferentes.

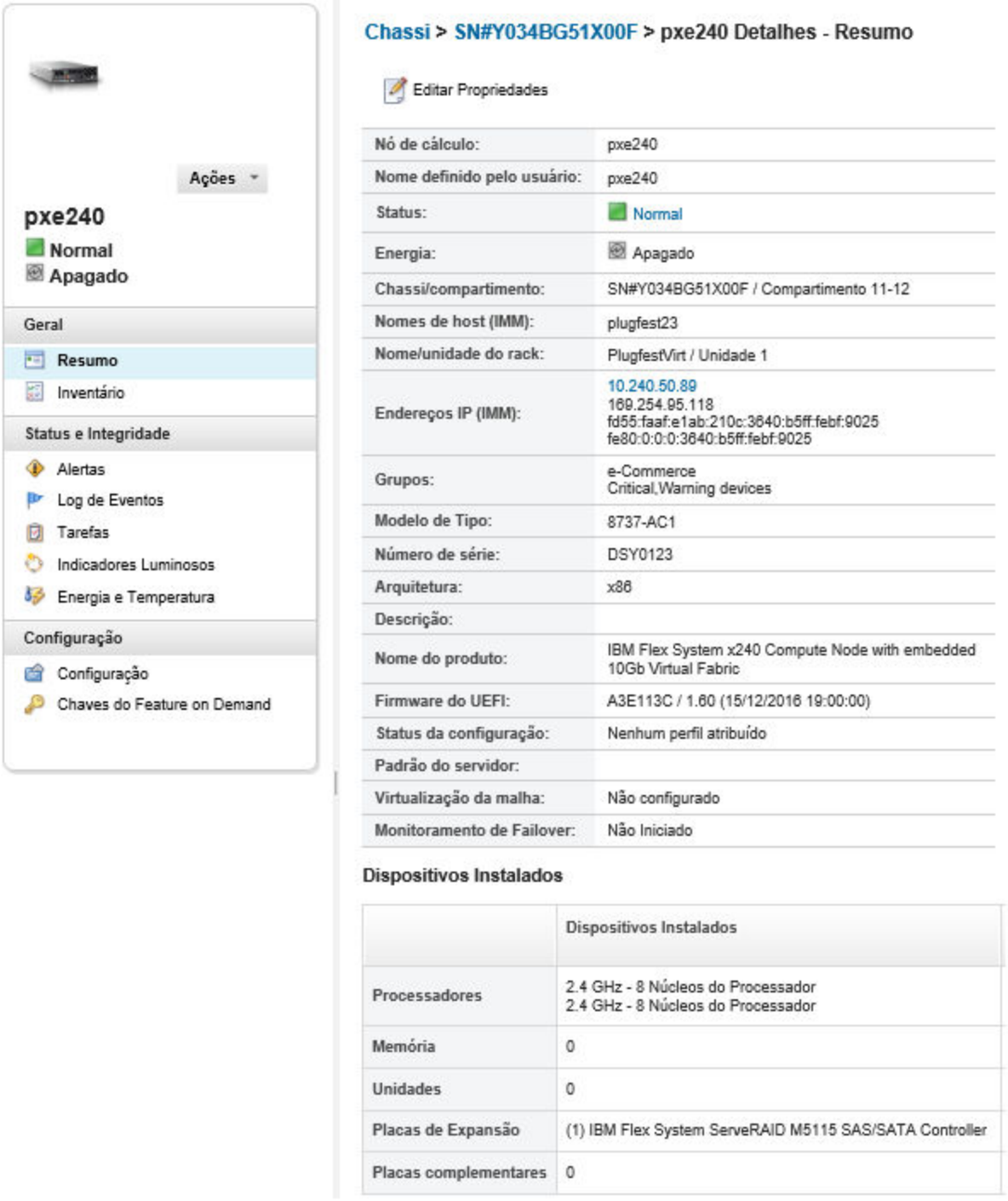
Procedimento

Conclua as seguintes etapas para exibir os detalhes de um servidor gerenciado.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados (servidores de rack e nós de cálculo).

É possível classificar as colunas da tabela para facilitar a localização dos servidores específicos. Além disso, é possível selecionar um tipo de sistema na lista suspensa **Todos os Sistemas** e inserir texto (como nome de sistema ou endereço IP) no campo **Filtro** para filtrar mais os servidores que são exibidos.

Etapa 2. Clique no link do servidor na coluna **Servidor**. A página de resumo de status desse servidor é exibida, mostrando as propriedades e a lista de componentes do servidor instalados nele.



Nota: Para servidores System x e NeXtScale, o endereço LAN por USB é listado nessa página. Entretanto, não é possível alterar esse endereço no XClarity Administrator. Em vez de isso, você deve usar a interface do Baseboard Management Controller para o servidor. Para obter mais informações, consulte "Acessando o IMM2 usando a interface LAN por USB" na documentação do produto para o servidor. É possível localizar a documentação do produto para o servidor no Documentação online do BladeCenter.

Etapa 3. Conclua uma ou mais das seguintes ações:

- Clique em **Resumo** para exibir um resumo do servidor, incluindo informações do sistema e componentes instalados (consulte Visualizando o status de um servidor gerenciado).

- Clique em **Detalhes de Inventário** para exibir detalhes sobre os componentes do servidor, incluindo:
  - Níveis de firmware para o servidor e o controlador de gerenciamento.
  - Detalhes de rede do módulo de gerenciamento, como nome do host, endereço IPv4, endereço IPv6 e endereços MAC.
  - Detalhes de ativo, incluindo nome de servidor, identificador universal exclusivo (UUID) e local.
  - Detalhes de componentes, incluindo CPUs, memória, unidades e placas de expansão.

  Notas:

  - Todos os endereços IP para o servidor estão listados. O endereço IP da porta do controlador de gerenciamento é listado primeiro. Se o endereço IP do controlador de gerenciamento estiver disponível, ele será usado para conectar-se ao servidor.
  - Se os dados não estiverem disponíveis para um determinado adaptador, alguns campos do adaptador (como nome do produto) poderão ficar vazios.
  - Se um novo adaptador for instalado no servidor, o servidor deverá ser reinicializado para que o adaptador apareça no inventário.
  - Para algumas placas suplementares, as informações FoD (Feature on Demand) serão exibidas sob o nome do dispositivo.
  - Você pode passar o mouse sobre os links na coluna Tipo para obter mais informações sobre componentes específicos, como a memória Intel Optain DCPMM.
- Clique em **Alertas** para exibir a lista de alertas atuais para esse servidor (consulte Trabalhando com alertas).

  Nota: É possível configurar preferências de limite para gerar um alerta e um evento quando um determinado valor, como a vida útil de um SSD em um servidor ThinkSystem ou ThinkServer excede um nível crítico ou de aviso (consulte Configurando preferências de limite para gerar alertas e eventos).
- Clique em **Log de Eventos** para exibir a lista de eventos para esse servidor (consulte Monitorando eventos no log de eventos).
- Clique em **Trabalhos** para exibir uma lista de trabalhos associados ao servidor (consulte Monitorando trabalhos).
- Clique em **Light Path** para exibir o status atual dos LEDs do servidor, incluindo local, falha e informações. Isso equivale a examinar o painel frontal do servidor.
- Clique em **Energia e Temperatura** para exibir detalhes sobre uso de energia e temperatura do ar.

  Dica: use o botão Atualizar em seu navegador da Web para coletar os dados mais recentes de energia e temperatura. A coleta de dados pode levar vários minutos.
- Clique em **Configuração** para exibir as informações de configuração atuais do servidor (incluindo armazenamento local, adaptadores de E/S, configurações de inicialização de SAN e configurações de firmware) e sua conformidade com o padrão de configuração atribuído (consulte Configurando servidores com padrões de configuração).
- Clique em **Chaves do Feature on Demand** para exibir uma lista de Chaves do Feature on Demand instaladas atualmente o servidor gerenciado (consulte Exibindo chaves do Features on Demand).

Depois de concluir

Além de exibir o resumo e informações detalhadas sobre um servidor, você pode executar as seguintes ações:

- Exiba o rack ou o chassi associado ao servidor, clicando no nome do rack ou do chassi na página Resumo.
- Exiba um servidor selecionado em exibição gráfica de rack ou de chassi clicando em **Todas as Ações → Exibições → Mostrar na Exibição do Rack** ou **Todas as Ações → Exibições → Mostrar na Exibição do Chassi**.
- Iniciar a interface da Web do controlador de gerenciamento de um servidor selecionado clicando no link **Endereço IP** (consulte Iniciando a interface do controlador de gerenciamento para um servidor).
- Acesse remotamente um servidor (consulte Usando o controle remoto para gerenciar servidores Converged, Flex System, NeXtScale e System x).
- Ligue e desligue um servidor selecionado (consulte Ligando e desligando um servidor).
- Modifique as informações do sistema de um servidor selecionado clicando em **Editar Propriedades**.
- Atualize o inventário de um servidor selecionado clicando em **Ações → Inventário → Atualizar Inventário**.
- Exporte informações detalhadas sobre os servidores para um arquivo CSV clicando em **Ações → Inventário → Exportar inventário**.

  Notas:

  – Para obter mais informações sobre os dados do inventário no arquivo CSV, consulte a GET /nodes/*<UUID_list>* na documentação online do XClarity Administrator.

  – Ao importar um arquivo CSV no Microsoft Excel, o Excel trata os valores de texto que contêm apenas números como valores numéricos (por exemplo, de UUIDs). Formate cada célula como texto para corrigir esse erro.
- Excluir eventos que não são de seu interesse de todas as páginas as quais os eventos são exibidos clicando no ícone **Ações → Redefinição de Serviços → Excluir eventos** (consulte Excluindo eventos).
- Reinicie um servidor selecionado usando uma interrupção não mascarável (NMI) clicando em **Ações → Serviço → Acionar NMI**.
- Altere o estado do LED de Local em um servidor selecionado para aceso, apagado ou piscando clicando em **Ações → Serviço → Alternar Estado do LED de Local**, selecionando o estado e clicando em **Aplicar**.

  Notas:
  – A alternância do LED de Local para servidores ThinkSystem SR635 e SR655 não é compatível.
  – O LED de Local nos servidores ThinkServer pode estar aceso ou apagado. Não há suporte para piscar.
- Desative ou ative o logon único para um servidor ThinkSystem e ThinkAgile clicando em **Todas as Ações → Segurança → Ativar Logon Único** ou **Todas as Ações → Segurança → Desativar Logon Único**.

  O login único permite que um usuário já conectado ao XClarity Administrator faça login automaticamente no Baseboard Management Control. O login único é ativado por padrão quando um servidor ThinkSystem ou ThinkAgile é trazido para o gerenciamento pelo XClarity Administrator (a menos que o servidor seja gerenciado com senhas do CyberArk). É possível definir a configuração global para ativar ou desabilitar o login único para todos os servidores ThinkSystem e ThinkAgile gerenciados. Ativar o login único para um servidor ThinkSystem e ThinkAgile específico substitui a configuração global para todos os servidores ThinkSystem e ThinkAgile.

  Nota: O logon único é desativado automaticamente ao usar o sistema de gerenciamento de identidade CyberArk para autenticação.
- Ative ou desative as alterações de regra de firewall em um servidor selecionado que limita as solicitações de entrada somente do XClarity Administrator clicando em **Ações → Segurança → Ativar encapsulamento** ou **Ações → Segurança → Desabilitar Encapsulamento**. A configuração de encapsulamento global é desativada por padrão. Quando desativado, o modo de encapsulamento do

dispositivo é definido como "normal" e as regras de firewall não são alteradas como parte do processo de gerenciamento.

Quando a configuração de encapsulamento global é ativada e o dispositivo suporta o encapsulamento, o XClarity Administrator se comunica com o dispositivo durante o processo de gerenciamento para alterar o modo de encapsulamento do dispositivo para "encapsulationLite" e modificar as regras de firewall no dispositivo para delimitar as solicitações de entrada àquelas do XClarity Administrator.

Atenção: Se o encapsulamento estiver ativado e XClarity Administrator ficar indisponível antes que o gerenciamento de um dispositivo seja cancelado, as etapas necessárias deverão ser tomadas para desativar o encapsulamento e estabelecer comunicação com o dispositivo. Para procedimentos de recuperação, consulte o arquivo lenovoMgrAlert.mib e Recuperando o gerenciamento com um CMM após uma falha no servidor de gerenciamento.

- (Somente servidores não ThinkServer) Resolva problemas que podem ocorrer entre o certificado de segurança do Lenovo XClarity Administrator e o certificado de segurança do controlador de gerenciamento no servidor selecionado clicando em **Ações → Segurança → Resolver Certificados Não Confiáveis** (consulte Resolvendo um certificado de servidor não confiável).

Fazendo backup e restaurando dados de configuração do servidor

O Lenovo XClarity Administrator não inclui funções de backup internas para dados de configuração do servidor. Em vez disso, use as funções de backup disponíveis para o servidor gerenciado.

- **Servidores convergidos, Flex System, System x, ThinkSystem e NeXtScale**
  - Fazer backup dos dados de configuração do servidor

    Use a interface da Web de gerenciamento ou a CLI para fazer backup do firmware.

    - Na interface da Web do IMM, clique em **Gerenciamento do IMM → Configuração do IMM**.
    - Na CLI, use o comando `backup`.

    Para obter mais informações sobre backup de servidores usando o IMM, consulte Documentação online do Integrated Management Module II.

    Use as ferramentas fornecidas pelo sistema operacional para fazer backup dos aplicativos em execução no servidor. Para obter informações adicionais, consulte a documentação fornecida com o sistema operacional.

    Para dispositivos de cálculo Flex System, faça backup das configurações para as opções instaladas nos nós de cálculo. É possível fazer backup de todas as configurações de nó de cálculo, incluindo configurações de opção, usando o Advanced Setup Utility (ASU). Para obter informações sobre o ASU, consulte Site do Advanced Settings Utility (ASU).
  - Restaurar dados de configuração do servidor

    Use a interface da Web de gerenciamento ou a CLI para restaurar o firmware. Para obter mais informações sobre restauração de servidores por meio do BMC, consulte Documentação online do Integrated Management Module II.

    Use a documentação fornecida com o sistema operacional e os aplicativos que estão em execução no servidor para restaurar o software instalado no servidor.

    - Na interface da Web do IMM, clique em **Gerenciamento do IMM → Configuração do IMM**.
    - Na CLI, use o comando `restore`.

Nota: Dica: é possível localizar informações adicionais sobre como fazer backup e restaurar os componentes de chassi no Guia de melhores práticas de Backup e Restauração do PureFlex e do Flex System .

- **Servidores ThinkServer**Os procedimentos de restauração variam para cada tipo de servidor ThinkServer. Consulte a documentação do produto que é fornecida com o servidor para informações sobre como restaurar o dispositivo.

Habilitando o protetor do sistema

O protetor do sistema monitora os desvios no inventário de hardware dos servidores ThinkSystem com XCC2.

Sobre esta tarefa

O inventário monitorado inclui processadores, memória, adaptadores PCI, unidades, placa-mãe e placas riser. Alterações nos níveis de firmware e configurações não são detectadas.

Quando o protetor do sistema está habilitado, uma captura de tela do inventário de hardware é tomada como referência confiável para cada dispositivo selecionado. Quando um dispositivo é reinicializado, o Baseboard Management Controller no dispositivo coleta a configuração atual do sistema e o compara com a captura de tela. Quando um desvio é detectado para um ou mais componentes, o protetor do sistema gera um evento. Se um desvio for detectado para um processador ou memória, o protetor do sistema vai gerar um evento e, opcionalmente, impedirá que o servidor seja inicializado no SO.

Procedimento

Para habilitar o protetor do sistema em mais um servidores com XCC2, conclua as etapas a seguir.

Etapa 1. No menu XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados.

Etapa 2. Selecione um ou mais servidores com XCC2s.

Etapa 3. Clique em **Todas as Ações → Segurança → Habilitar o protetor do sistema** para exibir a caixa de diálogo Habilitar o protetor do sistema.

Etapa 4. Escolha a ação a ser tomada quando o protetor do sistema é habilitado, uma alteração de inventário é detectada e o servidor se torna não conforme.

- **Habilitar, manter o comportamento padrão do sistema**. O comportamento atual é utilizado. . O comportamento padrão é gerar um evento.
- **Habilitar, impedir a inicialização do SO quando não conforme**. Um evento é gerado. Se você tentar inicializar no SO, será avisado se o protetor do sistema detectar alterações de configuração em processadores ou memória. Nesse caso, você será solicitado a fazer login no Baseboard Management Controller se as alterações forem inesperadas; caso contrário, você poderá continuar o processo de inicialização ou encerramento. Se você não responder em 5 minutos, o servidor será desligado por padrão.
- **Habilitar, gerar evento quando não conforme**. Um evento é gerado, mas nenhuma outra ação é realizada.

Etapa 5. Clique em **Aplicar**.

Um trabalho é criado para criar capturas de tela de inventário para o servidor selecionado. É possível monitorar o andamento do trabalho no log de trabalhos. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Trabalhos**. Para obter mais informações sobre o log de trabalhos, consulte Monitorando trabalhos.

Depois de concluir

Para desabilitar o protetor do sistema em servidores selecionados, clique em **Todas as Ações → Segurança → Desabilitar o protetor do sistema** e, em seguida, clique em **Aplicar**.

Apagando dados da unidade com segurança

O Lenovo XClarity Administrator pode apagar com segurança dados em todas as unidades nos servidores ThinkSystem e ThinkAgile que estejam executando a versão 22B e posteriores. Essa operação regrava permanentemente cada unidade preenchendo a unidade inteira com um zero binário, um binário ou dados aleatórios, tornando difícil descobrir o que foi salvo na unidade.

Atenção:

- Essa operação apaga de forma *permanente* e *irreversível* todos os dados nas unidades.
- Não há como cancelar essa operação após o envio do trabalho.

Antes de iniciar

Você deve ter autoridade **lxc-supervisor** para apagar dados de unidades.

Verifique se a senha de administrador UEFI não está definida nos servidores gerenciados a serem apagados. Se a senha de administrador UEFI estiver definida em qualquer servidor, as unidades nesses servidores não serão apagadas.

É possível apagar com segurança dados da unidade de até três servidores por vez por padrão. É possível configurar o número de servidores permitidos ao mesmo tempo clicando em **Administração → Preferências de inventário** e definindo o **Número máximo de servidores que podem ser apagados em um lote** como o valor desejado. É possível escolher um número entre `3 - 100` servidores.

Apenas um trabalho de apagamento seguro é permitido ao mesmo tempo. Você deve aguardar a conclusão do trabalho atual antes de iniciar outro trabalho de apagamento seguro.

Pode levar algumas horas para apagar unidades muito grandes.

Não é possível apagar com segurança volumes SDD SATA conectados aos controladores RAID da Marvell. Em vez disso, considere as seguintes recomendações.

- Para SSDs SATA de 7 mm, conecte-se aos controladores Broadcom RAID para executar o apagamento seguro.
- Para SSDs SATA M.2, conecte-se a controladores Marvell não RAID (como o Kit de ativação de dois compartimentos ThinkSystem M.2 SATA/NVMe) para realizar o apagamento seguro.

Sobre esta tarefa

É possível apagar dados nas unidades a seguir.

- NVMe
- SAS
- SAS HBA
- SAS RAID
- SATA
- Dispositivos de armazenamento conectados externos
  - Lenovo Storage D1212 (MT 4587)
  - Lenovo Storage D1224 (MT 4587)
  - Lenovo Storage D3284 (MT 6413)

A operação de apagamento seguro cria uma entrada no log de auditoria. É possível encaminhar esses eventos usando a função de encaminhamento de evento (consulte Encaminhando eventos para o syslog, gerenciador SNMP remoto, e-mail e outros serviços de evento).

Para solucionar problemas de apagamento seguro, consulte Não é possível apagar com segurança os dados em unidades paralisadas e Não é possível apagar com segurança volumes SDD SATA quando conectados ao Marvel RAID na documentação online do XClarity Administrator.

Procedimento

Para apagar com segurança todas as unidades em servidores gerenciados específicos, conclua as etapas a seguir.

Etapa 1. No menu XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados.

Etapa 2. Selecione o servidor.

Etapa 3. Clique em **Todas as Ações → Serviço → Apagamento seguro da unidade (HDD/SDD)**.

Etapa 4. INsira sua senha de supervisor para confirmar se deseja apagar todas as unidades nos servidores selecionados.

Etapa 5. Clique em **Apagar**.

Se você optar por executar uma apagamento de unidades em massa em mais de três servidores, será solicitado que você insira o ID do usuário e a senha. Insira as mesmas credenciais do usuário que você usou para fazer login no XClarity Administrator.

Um trabalho é criado para executar esta operação. Você pode monitorar o andamento da página Trabalhos clicando em **Monitoramento → Trabalhos** na barra de menus do XClarity Administrator. Se o trabalho não foi concluído com êxito, clique no link do trabalho para exibir detalhes sobre o trabalho (consulte Monitorando trabalhos).

Usando o controle remoto

Na interface da Web do Lenovo XClarity Administrator, é possível abrir uma sessão de controle remoto de um servidor gerenciado como se estivesse em um console local. É possível usar a sessão de controle remoto para executar operações, como ligar ou desligar o servidor, e montar logicamente uma unidade local ou remota.

Para iniciar uma sessão de controle remoto para qualquer dispositivo, você deve ter os privilégios **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-fw-admin**, **lxc-os-admin**, **lxc-hw-admin**, **lxc-service-admin** ou **lxc-hw-manager**.

Usando o controle remoto para gerenciar servidores ThinkSystem ou ThinkAgile

A partir da interface da Web do Lenovo XClarity Administrator, é possível abrir uma sessão de controle remoto de um servidor ThinkSystem gerenciado ou ThinkAgile como se estivesse em um console local. É possível usar a sessão de controle remoto para executar operações de energia e montar logicamente uma unidade local ou de rede.

Antes de iniciar

O encapsulamento deve ser desativado no servidor.

Para abrir uma sessão de controle remoto para um servidor, ele deve ter um estado Online ou Normal. Se o servidor tiver qualquer outro estado de acesso, a sessão de controle remoto não pode conectar-se ao servidor. Para obter mais informações sobre como exibir o status do servidor, consulte Visualizando os detalhes de um servidor gerenciado.

Leia as considerações a seguir para servidores ThinkSystem SR635 e SR655.
- É necessário ter o firmware do Baseboard Management Controller v2.94 ou posterior.
- Apenas o modo de vários usuários é suportado; o modo de usuário único não tem suporte.
- O Internet Explorer11 não é suportado.
- Não é possível ligar nem desligar um servidor a partir de uma sessão de controle remoto.

Sobre esta tarefa

Você pode iniciar uma sessão de controle remoto para um único servidor ThinkSystem ou ThinkAgile do XClarity Administrator.

Para obter mais informações sobre como usar os recursos do console remoto e mídia, consulte a documentação do servidor ThinkSystem ou ThinkAgile.

Nota: Para servidores ThinkSystem e ThinkAgile, não é necessário um Java Runtime Environment (JRE) com suporte a Java WebStart.

Procedimento

Para abrir uma sessão do controle remoto para um servidor específico, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados (servidores de rack e nós de cálculo).

É possível classificar as colunas da tabela para facilitar a localização dos servidores específicos. Além disso, é possível selecionar um tipo de sistema na lista suspensa **Todos os Sistemas** e inserir texto (como nome ou endereço IP) no campo **Filtro** para filtrar mais os servidores que são exibidos.

Etapa 2. Selecione o servidor os quais deseja abrir uma sessão de controle remoto.

Etapa 3. Clique no ícone **Controle Remoto** ().

Etapa 4. Aceite todos os avisos de segurança do navegador da Web.

Depois de concluir

Se a sessão de controle remoto não abrir com sucesso, consulte Problemas de controle remoto na documentação online do XClarity Administrator.

Usando o controle remoto para gerenciar servidores ThinkServer e NeXtScale sd350 M5

A partir da interface da Web do Lenovo XClarity Administrator, é possível abrir uma sessão de controle remoto dos servidores ThinkServer e NeXtScale sd350 M5 gerenciados como se estivesse em um console local. É possível usar a sessão de controle remoto para executar operações de energia e redefinição, montar logicamente uma unidade de rede ou local no servidor, fazer capturas de tela e gravar vídeos.

Antes de iniciar

- O controle remoto para esses servidores requer um Java Runtime Environment (JRE) com suporte a Java WebStart instalado no lado do cliente. Um JDK de código aberto é altamente recomendado. Se você estiver usando o JRE ou o JDK de um fornecedor, ele deve estar corretamente licenciado para uso comercial. Os seguintes JREs são suportados:
  - Oracle JRE 7 (consulte Site de download do Oracle Java)

    Atenção:
    - O Java 7 requer, no mínimo, suporte a TLSv1.2 (consulte Definindo configurações de criptografia no servidor de gerenciamento).
    - O suporte para Java 7 será descontinuado em uma data futura.
  - Oracle JRE 8, que requer uma licença paga (consulte Site de download do Oracle Java)
  - Adoptium OpenJDK 8 com o plug-in IcedTea-Web v1.8 (consulte Site do Adoptium OpenJDK)
  - Amazon Corretto 8 (consulte Site de download do Amazon Corretto 8)

  O Java WebStart não está incluído nos pacotes de instalação do OpenJDK nem do Coretto e precisa ser instalado separadamente. O IcedTea-Web ou o OpenWebStart podem ser usados na licença GNU GPLV2 (consulte Site de download do IcedTea-OpenJDK e Site do OpenWebStart).
- O controle remoto requer que uma chave Features on Demand para o ThinkServer System Manager Premium Upgrade esteja instalada nos servidores ThinkServer. Para obter mais informações sobre chaves FoD instaladas nos seus servidores, consulte Exibindo chaves do Features on Demand .

Sobre esta tarefa

Você pode iniciar uma sessão de controle remoto para um único servidor ThinkServer do XClarity Administrator.

Para abrir uma sessão de controle remoto para um servidor, ele deve ter um estado Online ou Normal. Se o servidor tiver qualquer outro estado de acesso, a sessão de controle remoto não pode conectar-se ao servidor. Para obter mais informações sobre como exibir o status do servidor, consulte Visualizando os detalhes de um servidor gerenciado.

Para obter mais informações sobre como usar os recursos do console remoto e mídia do ThinkServer, consulte a documentação do servidor ThinkServer.

Procedimento

Para abrir uma sessão do controle remoto para um servidor específico, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados (servidores de rack e nós de cálculo).

É possível classificar as colunas da tabela para facilitar a localização dos servidores específicos. Além disso, é possível selecionar um tipo de sistema na lista suspensa **Todos os Sistemas** e inserir texto (como nome ou endereço IP) no campo **Filtro** para filtrar mais os servidores que são exibidos.

Etapa 2. Selecione o servidor os quais deseja abrir uma sessão de controle remoto.

Etapa 3. Clique no ícone **Controle Remoto** ().

Etapa 4. Aceite todos os avisos de segurança do navegador da Web.

Depois de concluir

Se a sessão de controle remoto não abrir com sucesso, consulte Problemas de controle remoto na documentação online do XClarity Administrator.

Usando o controle remoto para gerenciar servidores Converged, Flex System, NeXtScale e System x

A partir da interface da Web do Lenovo XClarity Administrator, é possível abrir uma sessão de controle remoto para gerenciar servidores Converged, Flex System, NeXtScale e System x como se estivessem em um console local.

Antes de iniciar

Saiba mais:  XClarity Administrator: controle remoto

- O controle remoto para esses servidores requer um Java Runtime Environment (JRE) com suporte a Java WebStart instalado no lado do cliente. Um JDK de código aberto é altamente recomendado. Se você estiver usando o JRE ou o JDK de um fornecedor, ele deve estar corretamente licenciado para uso comercial. Os seguintes JREs são suportados:
  - Oracle JRE 7 (consulte Site de download do Oracle Java)

    Atenção:
    - O Java 7 requer, no mínimo, suporte a TLSv1.2 (consulte Definindo configurações de criptografia no servidor de gerenciamento).
    - O suporte para Java 7 será descontinuado em uma data futura.
  - Oracle JRE 8, que requer uma licença paga (consulte Site de download do Oracle Java)
  - Adoptium OpenJDK 8 com o plug-in IcedTea-Web v1.8 (consulte Site do Adoptium OpenJDK)
  - Amazon Corretto 8 (consulte Site de download do Amazon Corretto 8)

  O Java WebStart não está incluído nos pacotes de instalação do OpenJDK nem do Coretto e precisa ser instalado separadamente. O IcedTea-Web ou o OpenWebStart podem ser usados na licença GNU GPLV2 (consulte Site de download do IcedTea-OpenJDK e Site do OpenWebStart).
- É possível iniciar uma sessão de controle remoto em servidores executando os seguintes sistemas operacionais (de 32 bits ou 64 bits):
  - Microsoft Windows 7
  - Microsoft Windows 8
  - Microsoft Windows 10
- O controle remoto requer que uma chave Features on Demand para presença remota seja instalada nos servidores Converged, NeXtScale e System x. Se a chave FoD não for detectada em um servidor, a sessão de controle remoto exibe a mensagem `Chave de ativação ausente` para esse servidor ao exibir a lista de servidores disponíveis. Você pode determinar se a presença remota está ativada, desativada ou não está instalada em um servidor na página Servidores (consulte Visualizando o status de um servidor gerenciado). Para obter mais informações sobre chaves FoD instaladas nos seus servidores, consulte Exibindo chaves do Features on Demand.
- A conta do usuário usada para iniciar a sessão de controle remoto deve ser um ID de usuário válido que foi definido no servidor de autenticação XClarity Administrator. A conta do usuário também deve ter autoridade de usuário suficiente para acessar e gerenciar um servidor.
- Revise as considerações sobre segurança, desempenho e teclado antes de abrir uma sessão de controle remoto. Para obter mais informações sobre essas considerações, consulte Considerações sobre controle remoto.
- A caixa de diálogo Controle Remoto usa as configurações de idioma definidas para o sistema operacional no sistema local.Se o sistema local é executado no Windows, consulte Site do Java para obter informações sobre como alterar a configuração de idioma. Para alterar o idioma de exibição, instale uma cópia localizada do Windows ou um pacote de idioma em Site do Windows.

Sobre esta tarefa

É possível iniciar várias sessões de controle remoto do Lenovo XClarity Administrator. Cada sessão pode gerenciar diversos servidores.

Para abrir uma sessão de controle remoto para um servidor, ele deve ter um estado Online ou Normal. Se o servidor tiver qualquer outro estado de acesso, a sessão de controle remoto não pode conectar-se ao servidor. Para obter mais informações sobre como exibir o status do servidor, consulte Visualizando os detalhes de um servidor gerenciado.

É possível abrir uma sessão de controle remoto não destinada clicando em **Fornecimento → Controle Remoto** na barra de menus do Lenovo XClarity Administrator. Em seguida, aceite todos os avisos de segurança do navegador da Web.

Nota: Para nós de cálculo Flex System x280, x480 e x880, é possível iniciar uma sessão de controle remoto só para o nó primário. Se você tentar iniciar uma sessão de controle remoto para um nó não primário em um sistema de vários nós, a caixa de diálogo do controle remoto é iniciada, mas nenhum vídeo é exibido.

Procedimento

Conclua as seguintes etapas para abrir uma sessão de controle remoto para um servidor Converged, Flex System, NeXtScale e System x específico.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados (servidores de rack e nós de cálculo).

É possível classificar as colunas da tabela para facilitar a localização dos servidores específicos. Além disso, é possível selecionar um tipo de sistema na lista suspensa **Todos os Sistemas** e inserir texto (como nome ou endereço IP) no campo **Filtro** para filtrar mais os servidores que são exibidos.

Etapa 2. Selecione o servidor os quais deseja abrir uma sessão de controle remoto.

Etapa 3. Clique no ícone **Controle Remoto** ().

Etapa 4. Aceite todos os avisos de segurança do navegador da Web.

Etapa 5. Opcionalmente, escolha salvar o ícone Controle Remoto para desktop. É possível usar esse ícone para iniciar uma sessão de controle remoto sem fazer login na interface da Web do XClarity Administrator.

Etapa 6. Quando solicitado, selecione um dos seguintes modos de conexão:

- **Modo de usuário único**. Estabelece uma sessão de controle remoto exclusiva com o servidor. Todas as outras sessões de controle remoto para esse servidor são bloqueadas até que você se desconecte do servidor. Essa opção só estará disponível se não houver outras sessões de controle remoto estabelecidas com o servidor.
- **Modo multiusuário**. Permite que diversas sessões de controle remoto sejam estabelecidas com o mesmo servidor. O XClarity Administrator suporta até seis sessões de controle remoto simultâneas com o mesmo servidor.

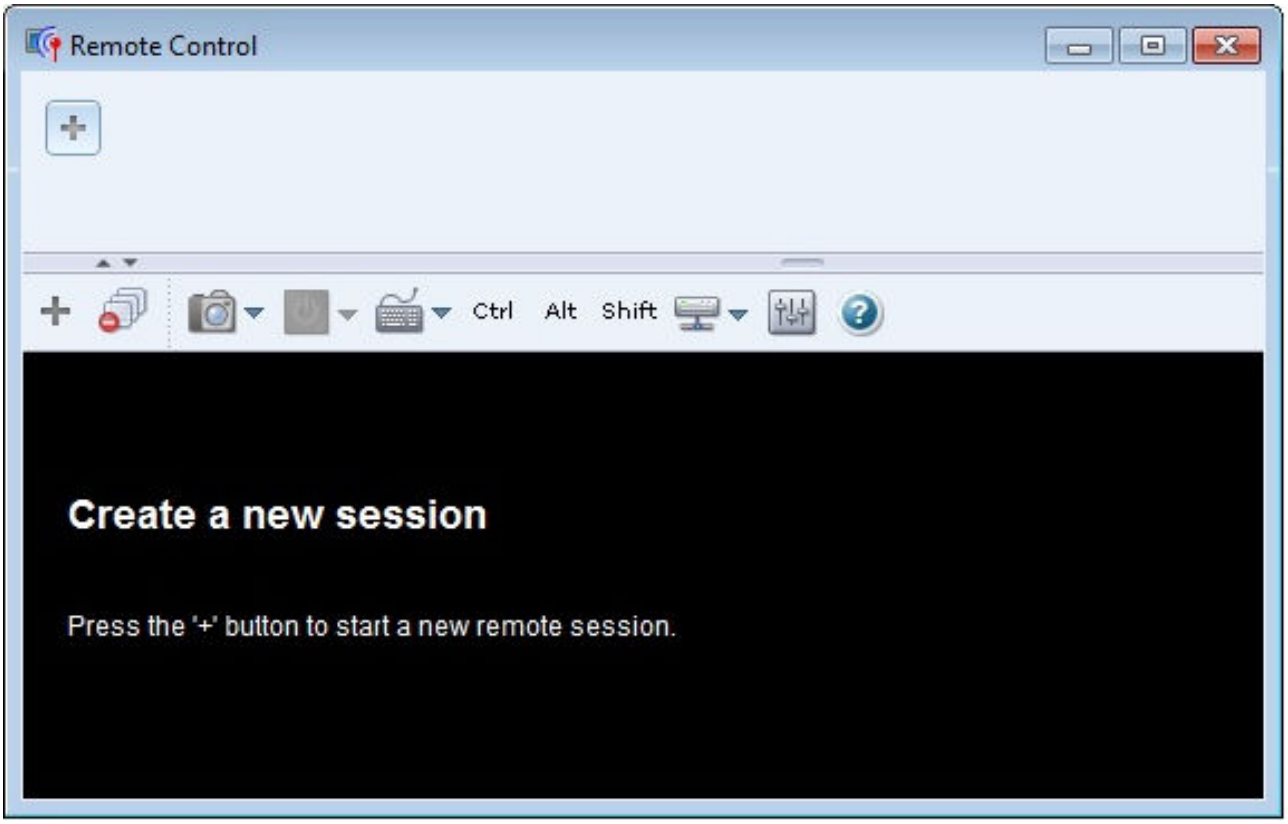
Etapa 7. Quando solicitado, escolha se deseja salvar um atalho para a sessão de controle remoto no sistema local.

Se optar por salvar o atalho, é possível então usá-lo para abrir a sessão de controle remoto para o servidor especificado sem precisar ativá-lo a partir da interface da Web do XClarity Administrator. Entretanto, seu sistema local deve ter acesso ao XClarity Administrator para validar a conta de usuário com o servidor de autenticação XClarity Administrator.

O atalho contém um link que abre uma sessão de controle remoto a qual pode ser usada para adicionar servidores manualmente.

Resultados

A janela Controle Remoto é exibida.



A área de miniatura exibe miniaturas de todas as seções de servidores que são atualmente gerenciadas por meio da sessão de controle remoto.

É possível exibir diversas sessões de servidor e mover entre as sessões clicando em uma miniatura, que exibe o console do servidor na área de sessão de vídeo. Se você estiver acessando mais servidores do que a quantidade permitida na área de miniatura, clique no ícone **Rolar para a direita** ( ) e **Rolar para a esquerda** ( ) para rolar as miniaturas adicionais do servidor. Clique no ícone **Todas as sessões** ( ) para ver uma lista de todas as sessões do servidor abertas.

Da área de miniatura, clique no ícone **Adicionar servidor** ( ) para adicionar um novo servidor à lista de servidores que você está gerenciando. Para obter mais informações sobre como adicionar uma sessão, consulte Adicionando um console do servidor para a sessão de controle remoto. É possível controlar se a área de miniatura é exibida e a frequência com que as miniaturas são atualizadas na página Miniatura. Para obter mais informações sobre configurações de miniatura, consulte Configurando preferências de controle remoto.

Depois de concluir

Se a sessão de controle remoto não abrir com sucesso, consulte Problemas de controle remoto na documentação online do XClarity Administrator.

Na caixa de diálogo Controle Remoto, é possível executar as seguintes ações:

- Adicione uma sessão de outros servidores para a sessão de controle remoto atual (consulte Adicionando um console do servidor para a sessão de controle remoto).
- Oculte ou mostre a área de miniatura clicando no ícone **Alternar Miniaturas** ().
- Exiba a sessão de controle remoto como uma janela ou uma tela cheia clicando no ícone **Tela** () e em **Entrar em tela cheia** ou **Sair da tela cheia**.
- Use as teclas CTRL, Alt, e Shift em uma sessão de controle remoto (consulte Usando as teclas Ctrl, Alt e Shift).
- Defina as sequências de teclas personalizadas, conhecidas como teclas de função (consulte Configurando teclas de função).
- Faça uma captura de tela da sessão do servidor selecionado atualmente e salve-a em vários formatos clicando no ícone **Tela** () e, em seguida, em **Captura de tela**.
- Monte a mídia remota (como um CD, DVD, dispositivo USB, imagem de disco ou uma imagem de CD [ISO]) no servidor selecionado ou mova um dispositivo montado para outro servidor (consulte Montando ou movendo mídia remota).
- Faça upload de imagens para um servidor a partir da mídia remota (consulte Upload de uma imagem no servidor).
- Liga ou desliga o servidor a partir de um console remoto (consulte Ligando ou desligando um servidor a partir de uma sessão de controle remoto).
- Altere as preferências de controle remoto (consulte Configurando preferências de controle remoto).

Considerações sobre controle remoto

Esteja atento a segurança, desempenho e as considerações sobre o teclado relacionadas ao acesso aos servidores gerenciados usando uma sessão de controle remoto.

Considerações sobre segurança

A conta do usuário usada para iniciar a sessão de controle remoto deve ser um ID de usuário válido que foi definido no servidor de autenticação Lenovo XClarity Administrator. A conta do usuário também deve ter autoridade de usuário suficiente para acessar e gerenciar um servidor.

Por padrão, diversas sessões de controle remoto podem ser estabelecidas para um servidor. Entretanto, quando você inicia uma sessão de controle remoto, tem a opção de iniciá-la no modo de usuário único, que estabelece uma sessão exclusiva com o servidor. Todas as outras sessões de controle remoto para esse servidor são bloqueadas até que você se desconecte do servidor.

Nota: Essa opção só estará disponível se não houver outras sessões de controle remoto estabelecidas atualmente com o servidor.

Para usar o FIPS (Federal Information Processing Standard) 140, você deverá habilitá-lo manualmente concluindo as seguintes etapas no sistema local:

1. Localize o nome do provedor de criptografia certificada FIPS 140 instalada no seu sistema local.

   Dica: para obter mais informações sobre conformidade FIPS 140, consulte o Site FIPS 140 Compliant Mode for SunJSSE.
2. Edite o arquivo `$(java.home)/lib/security/java.security`.
3. Altere a linha que inclui o `com.sun.net.ssl.internal.ssl.Provider` criando o nome do provedor do seu provedor criptográfico certificado FIPS 140. Por exemplo, altere:
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider`
   para:
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11-NSS`

Considerações de desempenho

Se uma sessão de controle remoto se tornar lenta ou não responder, feche todas as sessões de vídeo e mídia remota que você tenha estabelecido com o servidor selecionado para reduzir o número de conexões de servidor abertas. Além disso, você pode aumentar o desempenho alterando as preferências a seguir. Para obter mais informações, consulte Configurando preferências de controle remoto.

- **KVM**
  - Diminua a porcentagem da largura de banda de vídeo usada pelo aplicativo. A qualidade da imagem da sessão de controle remoto será reduzida.
  - Diminua a porcentagem de quadros atualizados pelo aplicativo. A taxa de atualização da sessão de controle remoto será reduzida.
- **Miniaturas**
  - Aumente a taxa do intervalo de atualização de miniatura. O aplicativo atualizará as miniaturas em uma taxa mais lenta.
  - Desative a exibição de miniaturas completamente.

O tamanho da janela da sessão de controle remoto e o número de sessões ativas podem afetar os recursos da estação de trabalho, como memória e largura de banda da rede, que podem influenciar o desempenho. A sessão de controle remoto usa um limite de 32 sessões abertas. Se mais de 32 sessões estiverem abertas, o desempenho pode ser reduzido severamente e a sessão de controle remoto pode ficar sem resposta. Você poderá consultar a degradação de desempenho com menos de 32 sessões abertas se os recursos, incluindo a largura de banda da rede e a memória local não forem suficientes.

Considerações de teclado

A sessão de controle remoto suporta os seguintes tipos de teclado:
- Belga com 105 teclas
- Português do Brasil
- Chinês
- Francês com 105 teclas
- Alemão com 105 teclas
- Italiano com 105 teclas
- Japonês com 109 teclas
- Koreano
- Português
- Russo
- Espanhol com 105 teclas
- Suíço com 105 teclas
- Britânico com 105 teclas
- Americano com 104 teclas

Para obter informações sobre as preferências do teclado, consulte Configurando preferências de controle remoto.

Adicionando um console do servidor para a sessão de controle remoto

É possível incluir um ou mais consoles de servidores para a sessão atual do controle remoto.

Procedimento

Para adicionar um ou mais consoles de servidores para a sessão atual do controle remoto, conclua as seguintes etapas.

Etapa 1. Na janela Controle Remoto, clique no ícone **Nova sessão** ().

Uma caixa de diálogo é exibida com uma lista de chassis e servidores de rack disponíveis gerenciados por Lenovo XClarity Administrator e que sua conta do usuário tem permissão para gerenciar.

Dica: se nenhum servidor for mostrado na lista, consulte Problemas de controle remoto na documentação online do XClarity Administrator para que os procedimentos potencialmente resolvam o problema.

Etapa 2. Selecione um ou mais servidores aos quais você deseja conectar-se.

É possível filtrar os servidores exibidos selecionando um tipo de sistema na lista suspensa **Tipo** e inserindo o texto (como o nome do sistema ou nome do gabinete) no campo **Filtro**.

É possível selecionar **Selecionar tudo** para selecionar todos os servidores na lista.

Etapa 3. **Opcional:** selecione **Modo de usuário único** para abrir uma sessão exclusiva para cada servidor selecionado.

Se você selecionar essa opção, as outras sessões de controle remoto com os servidores selecionados são bloqueadas até que você se desconecte do servidor selecionado. Essa opção só estará disponível se não houver outras sessões de controle remoto estabelecidas com os servidores selecionados.

Se não selecionar essa opção, o modo multiusuário será usado por padrão.

Etapa 4. Clique em **Conectar**.

Ligando ou desligando um servidor a partir de uma sessão de controle remoto

É possível ligar ou desligar um servidor a partir de uma sessão de controle remoto.

Procedimento

Conclua as etapas a seguir para ligar e desligar um servidor.

Etapa 1. Na janela Controle Remoto, clique na miniatura do servidor que deseja ligar/desligar.

Etapa 2. Clique no ícone **Ligar/Desligar** () e, em seguida, clique em uma das ações de energia a seguir:
- **Ligar**
- **Desligar normalmente**
- **Desligar imediatamente**
- **Reiniciar normalmente**
- **Reiniciar Imediatamente**
- **Acionar NMI**
- **Reiniciar para Configuração do Sistema** (somente servidores Lenovo Converged, Flex System, NeXtScale e System x)

Dica: o ícone **Ligar/Desligar** é verde quando o servidor selecionada está ligado no momento.

Configurando teclas de função

É possível definir suas próprias sequências de teclas, chamadas de *teclas de função, para a sessão atual de controle remoto.*

Antes de iniciar

Para exibir a lista atual de definições da tecla de função, clique no ícone **Teclado** ().

As definições de tecla de função são armazenadas no sistema a partir do qual você iniciou a sessão de controle remoto. Portanto, se você iniciar a sessão de controle remoto a partir de outro sistema, terá que definir as teclas de função novamente.

É possível escolher exportar as configurações do usuário (as quais incluem teclas de função) na guia **Configurações do Usuário** na caixa de diálogo Preferências. Para obter mais informações, consulte Importando e exportando configurações de usuário.

Nota: Se você usar um teclado internacional e configurar as teclas de função que requerem a chave Gráficos Alternativos (AltGr), certifique-se de que o sistema operacional na estação de trabalho que você usa para chamar o aplicativo de controle remoto seja do mesmo tipo de sistema operacional do servidor que você está acessando remotamente. Por exemplo, se o servidor estiver executando Linux, certifique-se de chamar a sessão de controle remoto a partir de uma estação de trabalho que execute o Linux.

Procedimento

Conclua o procedimento a seguir para adicionar uma nova tecla de função.

Etapa 1. Na janela Controle Remoto, clique no ícone **Teclado** () e, em seguida, em **Adicionar tecla de função**. A guia **Programador de Teclas de função** na caixa de diálogo Preferência é exibida.

Etapa 2. Clique em **Novo**.

Etapa 3. Digite a sequência-chave que deseja configurar.

Etapa 4. Clique em **OK**. A nova tecla de função é adicionada na lista de tecla de função.

Usando as teclas Ctrl, Alt e Shift

Alguns sistemas operacionais interceptam determinadas teclas em vez de transmiti-las ao servidor remoto. É possível usa os botões de tecla de aderência para enviar pressionamentos de tecla diretamente para o servidor que você está gerenciando.

Procedimento

Para enviar uma combinação de tecla Ctrl ou Alt, clique em **Ctrl** ou **Alt** na barra de ferramentas, coloque o cursor na área de sessão de vídeo e pressione uma tecla no teclado.

Por exemplo, para enviar uma combinação de teclas Ctrl+Alt+Del, conclua as etapas a seguir:

1. Clique em **CTRL** na barra de ferramentas.
2. Clique em **Alt** na barra de ferramentas.
3. Clique com o botão esquerdo do mouse em qualquer lugar dentro da área da sessão de vídeo.
4. Pressione a tecla Delete do teclado.

Nota: Se o modo de captura de mouse estiver ativado, pressione a tecla Alt esquerda para mover o cursor para fora da área da sessão de vídeo. Mesmo que o modo de captura do mouse esteja desabilitado por padrão, é possível habilitá-lo na página Barra de ferramentas (consulte Configurando preferências de controle remoto).

Quando você clicar na tecla **Ctrl**, **Alt** ou **Shift** na barra de ferramentas para torná-la ativo, ela permanecerá ativa até que você pressione uma tecla do teclado ou clique no botão novamente.

Montando ou movendo mídia remota

É possível usar o recurso de mídia remota para montar mídia remota (como um CD, DVD, dispositivo USB, imagem de disco ou uma imagem de CD [ISO]) que está no sistema local para o servidor selecionado. Também é possível fazer upload de uma imagem para o armazenamento local que está disponível no Baseboard Management Controller (BMC).

Antes de iniciar

Somente um usuário por vez pode montar e fazer upload de dados para o armazenamento local no controlador de gerenciamento. Os outros usuários são impedidos de acessar o armazenamento local no controlador de gerenciamento enquanto ele está sendo montados ou os dados estão sendo transferidos por upload para o armazenamento local.

Em um servidor que executa o sistema operacional Linux, a montagem de mais de uma imagem ISO não é suportada.

Procedimento

Conclua as seguintes etapas para montar ou mover mídia remota.

Etapa 1. Na janela Controle Remoto, clique no ícone **Mídia Remota** ().

Etapa 2. Clique em uma das ações a seguir:

- **Monte a mídia remota**

  Essa ação torna os recursos de mídia local disponíveis para o servidor atualmente selecionado. Um recurso de mídia pode ser montado em apenas um servidor por vez em uma única sessão de controle remoto.

  Quando você clica em **Montar mídia remota**, as opções a seguir estão disponíveis:

  - **Selecione uma imagem que deve ser montada**. Esta imagem está disponível para o servidor atualmente selecionado até você desmontar o dispositivo ou fechar a sessão do controle remoto. Diversas imagens podem ser montadas em um único servidor e cada imagem pode ser montada em diversos servidores.
  - **Selecione uma unidade, como um CD, DVD ou dispositivo USB, que deve ser montada**. O dispositivo está disponível para o servidor atualmente selecionado até você desmontar a unidade ou fechar a sessão do controle remoto. Diversos dispositivos podem ser montados em um único servidor, mas cada dispositivo pode ser montado em apenas um servidor por vez.

    Nota: Se você selecionar uma unidade, certifique-se de desmontá-la antes de remover a mídia da unidade.
  - **Fazer upload da imagem para o IMM**. Use essa opção para armazenar uma imagem no armazenamento local no controlador de gerenciamento para o servidor selecionado. Esta imagem permanece no controlador de gerenciamento, mesmo que você finalize a sessão de controle remoto ou que o servidor seja reiniciado.

    É possível armazenar aproximadamente 50 MB de dados no controlador de gerenciamento.

    É possível fazer upload de diversas imagens para o controlador de gerenciamento desde que o espaço total que é usado para todas as imagens seja menor que 50 MB.

    Cada imagem que é transferida por upload para o controlador de gerenciamento é montada automaticamente no servidor. Depois de ter transferido por upload uma imagem para o controlador de gerenciamento, você também poderá mover essa imagem transferida por upload para o controlador de gerenciamento para um servidor diferente. Ao mover a imagem, a imagem transferida por upload anteriormente é removida do servidor atual e transferida por upload para um servidor selecionado.

- **Mover mídia remota**

  Essa ação move um recurso de mídia montada anteriormente entre servidores.

  Conclua as seguintes etapas para tornar um recurso disponível para o servidor:

1. Selecione um ou mais recursos.
2. Clique em **Adicionar** para mover os recursos para a lista **Recursos Selecionados**.
3. Clique em **Montar** para montar os recursos para uso pelo servidor. A sessão de controle remoto define um dispositivo para o recurso e mapeia esse dispositivo para um ponto de montagem do servidor atualmente selecionado. Você tem a opção de proteger contra gravação a mídia montada.

Upload de uma imagem no servidor

É possível fazer upload de uma imagem para o armazenamento local que está disponível no Baseboard Management Controller (BMC) para o servidor selecionado.

Sobre esta tarefa

Esta imagem permanece no controlador de gerenciamento, mesmo que você finalize a sessão de controle remoto ou que o servidor seja reiniciado.

É possível armazenar aproximadamente 50 MB de dados no controlador de gerenciamento.

É possível fazer upload de diversas imagens para o controlador de gerenciamento desde que o espaço total que é usado para todas as imagens seja menor que 50 MB.

Cada imagem que é transferida por upload para o controlador de gerenciamento é montada automaticamente no servidor. Depois de ter transferido por upload uma imagem para o controlador de gerenciamento, você também poderá mover essa imagem transferida por upload para o controlador de gerenciamento para um servidor diferente. Ao mover a imagem, a imagem transferida por upload anteriormente é removida do servidor atual e transferida por upload para um servidor selecionado.

Procedimento

Conclua as seguintes etapas para fazer upload de uma imagem no servidor.

Etapa 1. Na janela Controle Remoto, clique no ícone **Mídia Remota** ().

Etapa 2. Clique em **Montar mídia remota**.

Etapa 3. Clique em **Fazer upload da imagem para o IMM**.

Importando e exportando configurações de usuário

É possível escolher entre importar ou exportar as configurações do usuário para a sessão de controle remoto atual.

Sobre esta tarefa

Quando você exporta as configurações do usuário, todas as configurações do usuário para a sessão atual de controle remoto são armazenadas em um arquivo de propriedades em seu sistema local. É possível copiar esse arquivo de propriedades para outro sistema e importar essas configurações no aplicativo de controle remoto para usar as configurações.

Procedimento

Conclua as seguintes etapas para importar ou exportar as configurações do usuário para a sessão de controle remoto atual.

Etapa 1. Na janela Controle Remoto, clique no ícone **Preferência** ().

Etapa 2. Clique na guia **Configurações do Usuário**.

Etapa 3. Clique em **Importar** para importar configurações de um arquivo exportado ou clique em **Exportar** para salvar as configurações atuais do usuário em um arquivo de propriedades no sistema local.

Configurando preferências de controle remoto

É possível alterar as configurações de preferências para a sessão atual de controle remoto.

Procedimento

Conclua as seguintes etapas para modificar as preferências do controle remoto.

Etapa 1. Para modificar as preferências do controle remoto, clique no ícone **Preferências** (). Todas as alterações têm efeito imediatamente.

- **KVM**
  - **Porcentagem de Largura de Banda de Vídeo**. O aumento da largura de banda melhora a qualidade na aparência da sessão de controle remoto, mas pode afetar o desempenho da sessão de controle remoto.
  - **Porcentagem de Quadros Atualizados**. O aumento da porcentagem de atualização de quadro aumenta a frequência com que a sessão de controle remoto é atualizada, mas pode afetar o desempenho da sessão de controle remoto.
  - **Tipo de teclado**. Selecione o tipo de teclado que você está usando para a sessão de controle remoto. O tipo de teclado que você seleciona deve corresponder configurações do teclado no sistema local e corresponde as configurações do teclado no host remoto.

    Nota: Se você selecionar um teclado internacional e precisar inserir combinações de teclas que requerem a chave Gráficos Alternativos (AltGr), certifique-se de que o sistema operacional na estação de trabalho que você usa para chamar a sessão de controle remoto seja do mesmo tipo de sistema operacional do servidor que você deseja acessar remotamente. Por exemplo, se o servidor estiver executando Linux, certifique-se de chamar o aplicativo de controle remoto a partir de uma estação de trabalho que execute o Linux.
  - **Dimensionar imagem na janela**. Selecione essa opção para dimensionar a imagem de vídeo recebida do servidor para o tamanho da área da sessão de vídeo.
- **Segurança**
  - **Preferir conexões no modelo de usuário único**. Especifique se as conexões no modo de usuário único é a opção padrão ao conectar-se a um servidor. Quando uma conexão é feita no modo de usuário único, apenas um usuário pode ser conectado a um servidor por vez. Se essa caixa não estiver selecionada, a função padrão será conectar-se ao servidor no modo multiusuário.
  - **Requerer (assegurar) conexões de tunelamento**. Selecione essa opção para acessar um servidor por meio do nó de gerenciamento. É possível usar essa opção para acessar um servidor de um cliente que não está na mesma rede que o servidor.

    Nota: O aplicativo de controle remoto sempre tentará se conectar diretamente ao servidor do sistema local onde o controle remoto foi iniciado. Se você selecionar essa opção, o aplicativo de controle remoto acessará o servidor por meio do Lenovo XClarity Administrator se a estação de trabalho do cliente não puder acessar o servidor diretamente.
- **Barra de ferramentas**

  Nota: Clique em **Restaurar Padrões** para restaurar todas as configurações nesta página para as definições padrões
  - **Fixar a barra de ferramentas na janela**. Por padrão, a barra de ferramentas fica oculta acima da janela da sessão de controle remoto e exibe apenas quando você move o ponteiro

do mouse sobre ela. Se você selecionar esta opção, a barra de ferramentas é fixada à janela e é sempre exibida entre o painel miniatura e a janela da sessão do controle remoto.

- **Mostrar botões do teclado**. Especifique onde mostrar os ícones de botões do teclado (CapsLock, NumLock e ScrollLock) na barra de ferramentas.
- **Mostrar controle de energia**. Especifique se as opções de controle de energia devem ser exibidos na barra de ferramentas.
- **Mostrar botões de tecla fixa**. Especifique se os ícones de botão de tecla fixa (Ctrl, Alt e Delete) devem ser exibidos na barra de ferramentas.
- **Ocultar ponteiro do mouse local**. Especifique se você deseja exibir o ponteiro do mouse local quando posicionar o cursor na sessão do servidor exibida atualmente na área de sessão de vídeo.
- **Ativar modo de captura de mouse**. Por padrão, o modo de captura de mouse fica desativado. Isso significa que você pode mover livremente o cursor para dentro e para fora da área da sessão de vídeo. Se você ativar o modo de captura de mouse, deverá pressionar a tecla Alt esquerda para poder mover o cursor para fora da área da sessão de vídeo. Se o modo de captura de mouse estiver ativado, será possível especificar o uso ou não das teclas Ctrl+Alt para sair do modo de captura de mouse. O padrão é usar a tecla Alt esquerda.
- **Especificar opacidade do plano de fundo da barra de ferramentas**. A redução da porcentagem de opacidade permite exibir mais da área de sessão de vídeo através do plano de fundo da barra de ferramentas.

  Nota: Essa opção está disponível apenas quando a barra de ferramentas não está fixada na janela.

- **Miniaturas**
  - **Mostrar miniaturas**. Selecione essa opção para mostrar a área de miniatura na sessão de controle remoto.
  - **Especificar intervalo de atualização de miniatura**. A diminuição do intervalo para atualizar miniaturas aumenta a frequência com que as miniaturas do servidor são atualizadas.
- **Geral**
  - **Modo de depuração**. Especifica se o modo de depuração deve ser configurado para o aplicativo de controle remoto. As configurações determinam a granularidade de eventos que são registrados nos arquivos de log. Por padrão, apenas eventos graves são registrados. Para obter mais informações sobre locais de arquivos de log, consulte Visualizando logs e rastreamentos de controle remoto.
  - **Herdar configurações de aparência do sistema**. Essa configuração altera a aparência para corresponder aos esquemas de cores configurados para o servidor local (executando o Windows). Você deve reiniciar o aplicativo de controle remoto para que essas configurações tenham efeito.
  - **Criar ícone do desktop**. Essa configuração cria um ícone de desktop em seu sistema local para que você possa iniciar o aplicativo de controle remoto diretamente do seu sistema. Você deve ainda ter acesso ao software de gerenciamento do seu sistema.
  - **Sincronizar com servidor de gerenciamento**. Essa definição assegura que os dados do servidor que são exibidos no aplicativo de controle remoto correspondam aos dados do servidor que são exibidos pelo software de gerenciamento.

Visualizando logs e rastreamentos de controle remoto

Quando você inicia uma sessão de controle remoto, os arquivos de log são criados. Estes tipos de eventos que estão logados nesses arquivos baseados no modo de depuração, definido na guia **Geral** na caixa de diálogo Preferências. É possível usar esses arquivos de log para resolver problemas.

Procedimento

Os arquivos de log de controle remoto estão armazenados nos seguintes locais.

Sistema Operacional	Diretório de log
Windows 7 e 8	`%USERPROFILE%\lenovo\remoteaccess` Por exemplo: `C:\Users\win_user\lenovo\remoteaccess`

Para obter mais informações sobre como coletar arquivos de diagnóstico e enviar arquivos para o Suporte da Lenovo, consulte Trabalhando com serviço e suporte na documentação online do Lenovo XClarity Administrator.

Gerenciando o acesso a sistemas operacionais em servidores gerenciados

Você pode gerenciar o acesso a sistemas operacionais nos servidores gerenciados.

Antes de iniciar

Você deve ter autoridade **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** ou **lxc-hw-admin** para gerenciar e implantar drivers de dispositivo e executar ações de energia em servidores gerenciados nas páginas Atualizações de drivers Windows.

Sobre esta tarefa

Para que o Lenovo XClarity Administrator possa atualizar drivers de dispositivo do SO em um sistema gerenciado, você deve fornecer informações para acessar o sistema operacional do host, incluindo o endereço IP do SO e a credencial armazenada do administrador para acessar o sistema operacional do host. Para obter mais informações sobre como atualizar os drivers de dispositivo do SO, consulte Atualizando drivers de dispositivo Windows em servidores gerenciados.

O XClarity Administrator usa as credenciais armazenadas para efetuar a autenticação com o sistema operacional do host. Para obter mais informações sobre como criar credenciais armazenadas no XClarity Administrator, consulte Gerenciando credenciais compartilhadas.

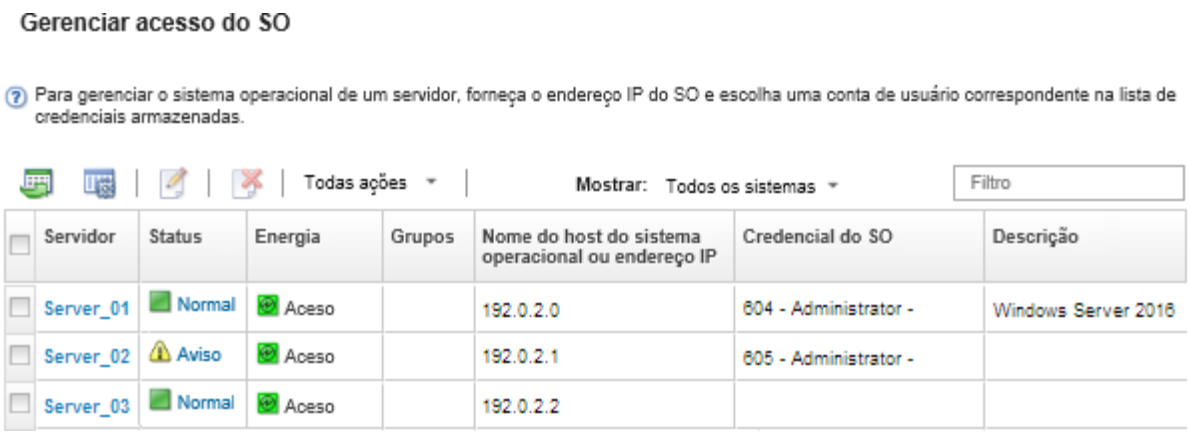
Dica: o XClarity Administrator não valida automaticamente as informações especificadas nesta página.

Procedimento

Execute as seguintes etapas para modificar as propriedades do sistema operacional.

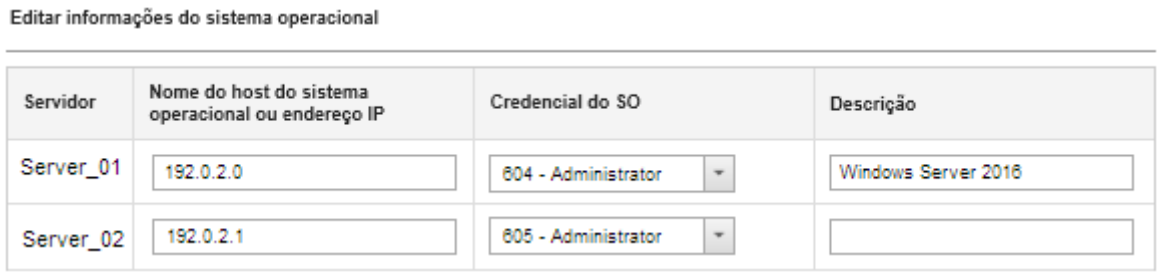
Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Gerenciar acesso do SO** para exibir a página Gerenciar acesso do SO.

É possível classificar as colunas da tabela para facilitar a localização dos servidores específicos. Além disso, é possível selecionar um tipo de sistema na lista suspensa **Todos os Sistemas** e inserir texto (como nome de sistema ou endereço IP) no campo **Filtro** para filtrar mais os servidores que são exibidos.



Etapa 2. Selecione os servidores a serem atualizados.

Etapa 3. Clique no ícone **Editar informações do SO** ( ) para exibir a caixa de diálogo Editar informações do SO.



Etapa 4. Para cada servidor de destino, especifique as seguintes informações:
- Endereço IP ou nome de host do sistema operacional do host
- (Opcional) Credencial armazenada para acessar o sistema operacional do host
- (Opcional) Descrição do sistema operacional do host

Etapa 5. Clique em **Salvar**.

Depois de concluir

É possível executar as ações a seguir para gerenciar o acesso do sistema operacional.

- Limpar as informações do sistema operacional (endereço IP, credenciais e descrição) selecionando o servidor e clicando no ícone **Remover informações do SO** ( ).
- Testar a autenticação em servidores Windows clicando em **Fornecimento → Atualizações de drivers do Windows: Aplicar** selecionando o servidor de destino e, em seguida, clicando em **Verificar autenticação**.
- Exiba informações de implantação do sistema operacional em um servidor específico passando o mouse sobre o nome do servidor.

  Nota: As informações de implantação estão disponíveis apenas para sistemas operacionais que foram implantados com êxito pela instância do XClarity Administrator. As informações de implantação não estão disponíveis para implantações com falha e para implantações executadas por outros meios, incluindo outra instância do XClarity Administrator.

Exibindo chaves do Features on Demand

É possível exibir uma lista de chaves do Features on Demand atualmente instaladas nos servidores gerenciados.

Sobre esta tarefa

Não é possível comprar, instalar ou gerenciar chave do Features on Demand na interface da Web do Lenovo XClarity Administrator. Para obter informações sobre a aquisição e a instalação de chaves do Features on Demand, consulte Features on Demand na documentação online do XClarity Administrator.

Procedimento

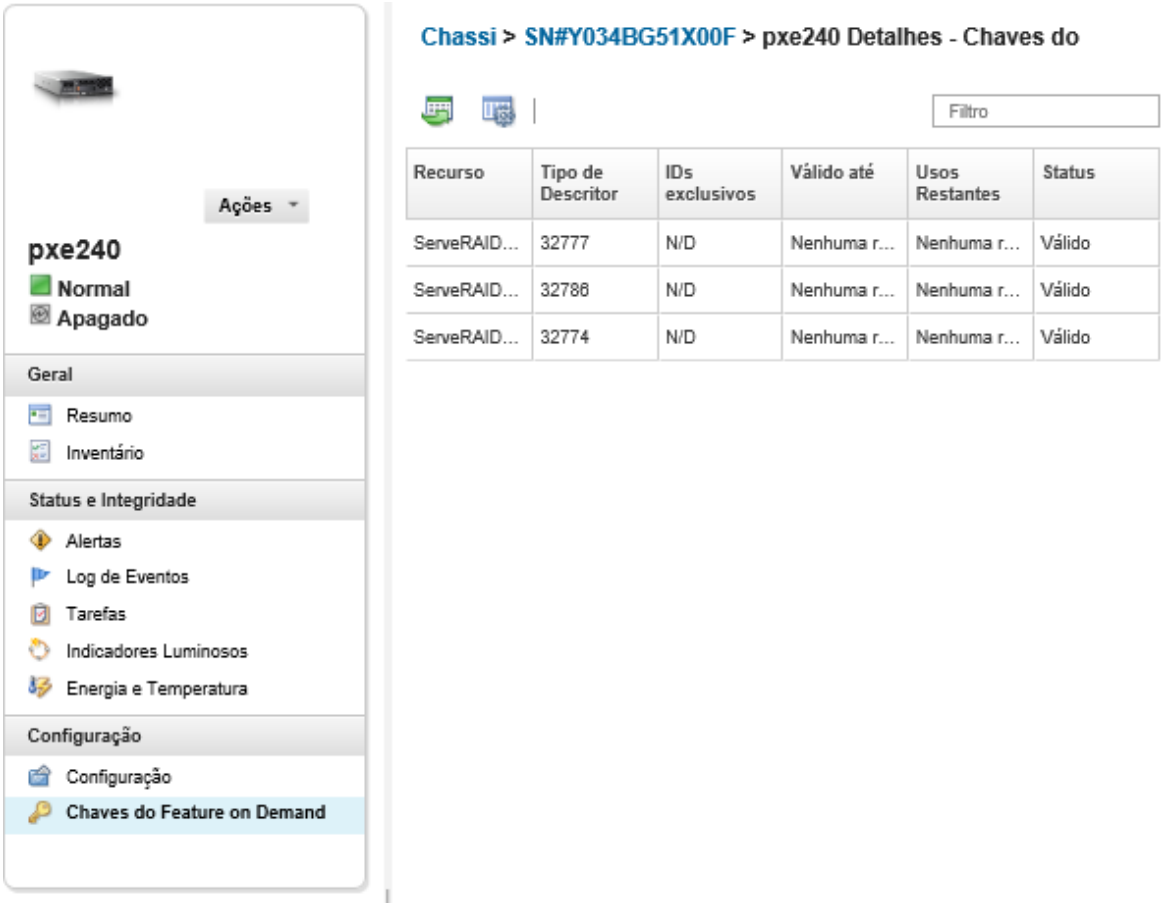
Conclua as etapas a seguir para exibir uma lista de chaves FoD instaladas em um servidor gerenciado específico.

Etapa 1. No menu XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados (servidores de rack e em torre e nós de cálculo).

Etapa 2. Clique no nome do servidor na coluna **Servidor**. A página de resumo de status desse servidor é exibida, mostrando as propriedades e a lista de componentes do servidor instalados nele.

Etapa 3. Clique em **Detalhes de Inventário** em Geral, na navegação esquerda, e expanda cada seção do componente de hardware para exibir os IDs exclusivos do FoD para esses componentes.

Etapa 4. Clique em **Chaves do Features on Demand** em Configuração, na navegação esquerda, para exibir informações sobre todas as chaves FoD instaladas no servidor.



Gerenciando energia e temperatura

Você pode monitorar e gerenciar o consumo de energia e a temperatura de servidores Converged, NeXtScale, System x e ThinkServer, e melhorar a eficiência no consumo de energia usando o Lenovo XClarity Energy Manager.

Saiba mais:  Lenovo XClarity Energy Manager

Sobre esta tarefa

XClarity Administrator é uma interface de usuário autônoma que você pode usar para monitorar e gerenciar o consumo de energia e a temperatura dos servidores compatíveis, incluindo:

- Monitoramento do consumo de energia, estimativa da demanda de energia e realocação da energia a servidores conforme necessário.
- Monitoramento da temperatura e capacidade de resfriamento dos servidores.
- Envio de notificações quando determinados eventos ocorrem ou quando os limites são excedidos.
- Limite da quantidade de energia que um dispositivo consome usando políticas.
- Otimização da eficiência do consumo de energia monitorando temperaturas de entrada em tempo real, identificando os servidores pouco utilizados com base em dados de energia OOB, avaliando medidores de energia para outros modelos de servidor e avaliando como os servidores acomodam novas cargas de trabalho com base na disponibilidade de recursos.
- Redução do consumo de energia para um nível mínimo para prolongar o tempo de serviço durante um evento de energia de emergência (como uma falha de energia de datacenter).

Para obter mais informações sobre como baixar, instalar e usar XClarity Administrator, consulte Site do Lenovo XClarity Energy Manager.

Ligando e desligando um servidor

É possível ligar e desligar um servidor no Lenovo XClarity Administrator.

Antes de iniciar

- Para o Red Hat® Enterprise Linux (RHEL) v7 e posterior, reiniciar o sistema operacional de um modo gráfico suspende o servidor por padrão. Antes de executar as ações **Reiniciar normalmente** ou **Reiniciar imediatamente** no XClarity Administrator, você deverá configurar manualmente o sistema operacional para alterar o comportamento do botão liga/desliga para desligar. Para obter instruções, consulte Guia de administração e migração de dados Red Hat: Mudar o comportamento ao pressionar o botão de ligar no modo de destino gráfico .
- Para SUSE Linux Enterprise Server (SLES), desligar o sistema operacional requer que você insira a senha raiz na sessão do SLES. Antes de executar as ações **Desligar Normalmente** ou **Desligar Imediatamente** no XClarity Administrator, você precisa desligar manualmente o servidor usando a interface de SLES local e selecionar a opção **Lembrar autenticação** ao inserir a senha ou conferir a política de segurança para ver se a autenticação obrigatória pode ser desabilitada.
- Quando ativada, a opção de inicialização Wake-on-LAN pode interferir nas operações do XClarity Administrator que desligam que o servidor, incluindo atualizações de firmware se houver um cliente Wake-on-LAN na rede que emite comandos "Wake on Magic Packet".
- A ação de energia **Reiniciar para Configuração do Sistema** reinicia o servidor e abre o utilitário de inicialização de BIOS/UEFI em uma sessão de controle remoto em vez de uma inicialização do sistema operacional normal.

- As ações de energia **Desligar Normalmente** e **Desligar Imediatamente** dependem das configurações do sistema operacional que está instalado no dispositivo e funcionam apenas quando o sistema operacional está configurado para dar suporte a elas.
- É possível reiniciar o dispositivo com interrupção não mascarável (NMI) clicando em **Todas as Ações → Serviço → Acionar NMI**.

Procedimento

Conclua o procedimento a seguir para ligar ou desligar um servidor.

Etapa 1. No menu XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados (servidores de rack e nós de cálculo).

Etapa 2. Selecione o servidor.

Etapa 3. Clique em **Todas as Ações → Ações de Energia** e, em seguida, clique em uma destas ações de energia:
- **Ligar** liga o dispositivo.
- **Desligar Normalmente** desliga o sistema operacional e o dispositivo.
- **Desligar Imediatamente** desliga o dispositivo.
- **Reiniciar Normalmente** desliga o sistema operacional e reinicia o dispositivo.
- **Reiniciar imediatamente** reinicia o dispositivo
- **Reiniciar para Configuração do Sistema** reinicia o dispositivo para Configuração de BIOS/UEFI (F1). Isso é permitido para servidores não ThinkServer que são aceitos sem limitações.
- **Reiniciar controlador de gerenciamento** reinicia o BMC.
- **Reiniciar imediatamente e tentar a Inicialização da Rede PXE** reinicia o servidor imediatamente e reinicializa o servidor à rede Preboot Execution Environment (PXE). Isso é suportado para servidores Lenovo Flex System, System x e ThinkSystem.

  Nota: As configurações UEFI relacionadas à inicialização de PXE devem ser definidas no servidor.

Reposicionando virtualmente um servidor em um chassi do Flex System

É possível simular a remoção e a reinserção de um servidor em um chassi do Flex System reiniciando o servidor usando uma interrupção não mascarável (NMI).

Sobre esta tarefa

Durante o reposicionamento virtual, todas as conexões de rede existentes com o servidor são perdidas, e o estado de energia do servidor é alterado. Antes de executar um reposicionamento virtual, salve todos os dados do usuário.

Atenção:

- Não execute um reposicionamento virtual a menos que seja instruído pelo Suporte da Lenovo.
- Executar um reposicionamento virtual pode resultar na perda de dados. Antes de reposicionar o servidor, execute as operações necessárias para proteger os dados do usuário.
- Em vez de executar um reposicionamento virtual, considere a possibilidade de desligar o servidor. Para obter informações sobre ações de energia, consulte Ligando e desligando um servidor).

Procedimento

Conclua as seguintes etapas para reposicionar virtualmente um servidor em um chassi do Flex System.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados.

É possível classificar as colunas da tabela para facilitar a localização do servidor que você deseja reposicionar. Além disso, é possível selecionar um tipo de dispositivo na lista suspensa **Todos os Dispositivos** e inserir texto (como nome ou endereço IP) no campo **Filtro** para filtrar mais os servidores que são exibidos.

Etapa 2. Selecione o servidor na tabela.

Etapa 3. Clique em **Todas as Ações → Serviço → Reposicionamento Virtual**.

Etapa 4. Clique em **Reposicionamento Virtual**.

Iniciando a interface do controlador de gerenciamento para um servidor

Você pode iniciar a interface da Web do controlador de gerenciamento para um servidor específico do Lenovo XClarity Administrator.

Antes de iniciar

Para acessar os servidores ThinkSystem SR635 SR655 por meio do XClarity Administrator, um usuário deverá ter a autoridade **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** ou **lxc-os-admin** (consulte Gerenciando o servidor de autenticação).

Ao usar um único login, é possível iniciar a interface de gerenciamento de um servidor gerenciado de XClarity Administrator sem ter o login. O login único é compatível com servidores ThinkSystem e ThinkAgile (exceto SR635 e SR655). Servidores ThinkSystem SR645 e SR665 requerem firmware XCC 21A ou posterior.

Para fazer login diretamente no controlador de gerenciamento usando contas de usuário LDAP locais ou externas sem fazer login no XClarity Administrator, use o URL `https://{XCC_IP_adderss}/#/login`.

Procedimento

Conclua as seguintes etapas para iniciar a interface do controlador de gerenciamento para um servidor.

Nota: Iniciar qualquer interface do controlador de gerenciamento do Lenovo XClarity Administrator usando o navegador da Web Safari não é permitido.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Servidores** para exibir a página Servidores.

É possível classificar as colunas da tabela para facilitar a localização dos servidores específicos. Além disso, é possível selecionar um tipo de sistema na lista suspensa **Todos os Sistemas** e inserir texto (como nome ou endereço IP) no campo **Filtro** para filtrar mais os servidores que são exibidos.

Etapa 2. Clique no link do servidor na coluna **Servidor**. A página de resumo de status desse servidor é exibida.

Etapa 3. Clique em **Todas as Ações → Iniciar → Interface da Web de Gerenciamento**. A interface da Web do controlador de gerenciamento do servidor é iniciada.

Dica: também é possível clicar no endereço IP na coluna **Endereços IP** para iniciar a interface do controlador de gerenciamento.

Etapa 4. Faça login na interface do controlador de gerenciamento usando as credenciais de usuário do XClarity Administrator.

Depois de concluir

Para obter mais informações sobre como usar a interface do controlador de gerenciamento para um servidor, consulte Documentação online do Integrated Management Module II e Documentação online do XClarity Controller.

Alterando as propriedades do sistema para um servidor

É possível alterar as propriedades do sistema para um servidor específico.

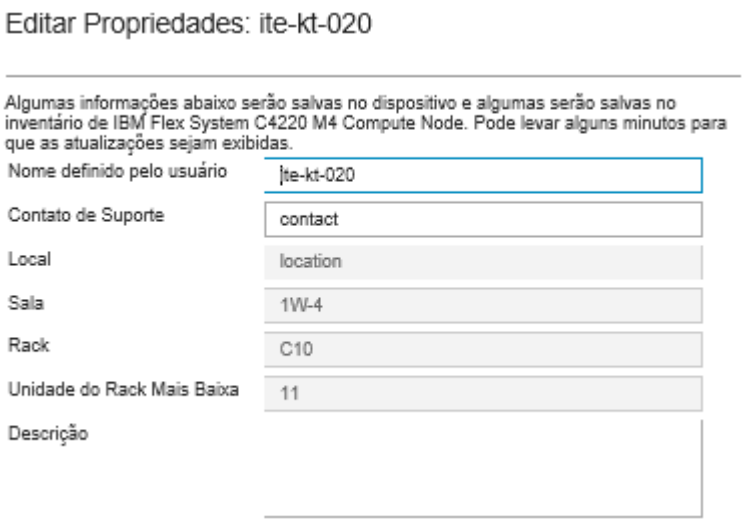
Procedimento

Conclua as etapas a seguir para alterar as propriedades do sistema.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Servidores** para exibir a página Servidores.

Etapa 2. Selecione o servidor a ser atualizado.

Etapa 3. Clique em **Todas as Ações → Inventário → Editar Propriedades** para exibir a caixa de diálogo Editar.



Etapa 4. Altere as seguintes informações, conforme necessário.
- Nome do servidor definido pelo usuário
- Contato de suporte
- Descrição

Nota: As propriedades de local, sala, rack e menor unidade do rack são atualizadas pelo XClarity Administrator ao incluir ou remover dispositivos de um rack na interface da Web (consulte Gerenciando racks).

Etapa 5. Clique em **Salvar**.

Nota: Quando você altera essas propriedades, pode haver um pequeno atraso até as alterações aparecerem na interface da Web do XClarity Administrator.

Resolvendo credenciais armazenadas expiradas ou inválidas para um servidor

Quando uma credencial armazenada expira ou fica inoperante em um dispositivo, o status desse dispositivo é mostrado como "Offline".

Procedimento

Para resolver credenciais armazenadas expiradas ou inválidas para um servidor.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados (servidores de rack e nós de cálculo).

Etapa 2. Clique no cabeçalho da coluna **Energia** para agrupar todo o servidor offline na parte superior da tabela.

Além disso, é possível selecionar um tipo de sistema na lista suspensa Todos os Sistemas e inserir texto (como nome de sistema ou endereço IP) no campo **Filtro** para filtrar mais os servidores que são exibidos.

Etapa 3. Selecione o servidor a ser resolvido.

Etapa 4. Clique em **Todas as Ações → Segurança → Editar Credenciais Armazenadas**.

Etapa 5. Altere a senha para a credencial armazenada ou selecione outra credencial armazenada a ser usada para o dispositivo gerenciado.

Nota: Se você gerenciou mais de um dispositivo usando as mesmas credenciais armazenadas e alterar a senha para as credenciais armazenadas, essa alteração de senha afetará todos os dispositivos que atualmente são usando as credenciais armazenadas.

Recuperando um servidor com falha após implantar um padrão de servidor

Se o servidor falhar após você implantar um padrão de servidor, é possível recuperar o servidor cancelando a atribuição do perfil no servidor com falha e depois reatribuindo esse perfil a um servidor de espera.

Procedimento

Conclua as etapas a seguir para recuperar o servidor com falha que usa a autenticação gerenciada do Lenovo XClarity Administrator.

Etapa 1. Identifique o servidor com falha.

Etapa 2. Cancele a atribuição do perfil de servidor no servidor com falha (consulte Desativando um perfil de servidor).

Atenção: O servidor com falha deve ser desligado para desativar os endereços virtuais atribuídos *antes* de reatribuir o perfil. Quando você cancelar a atribuição do perfil de servidor, selecione **Desligar servidor** na caixa de diálogo Cancelar Atribuição de Perfil de Servidor para desligar o servidor com falha (consulte Ligando e desligando um servidor).

Etapa 3. Atribua o perfil de servidor a um servidor de espera (consulte Ativando um perfil de servidor).

Etapa 4. Ative o perfil ligando o servidor de espera se estiver desligado atualmente ou reiniciando o servidor de espera se estiver ligado atualmente (consulte Ligando e desligando um servidor).

Etapa 5. Migre as configurações de VLAN nos comutadores conectados ao servidor de espera.

Etapa 6. Certifique-se de que o servidor com falha esteja desligado.

Etapa 7. Substitua ou repare o servidor com falha. Se você reparar o servidor, execute as etapas a seguir para assegurar que o servidor recém-reparado seja redefinido para as configurações padrão:

a. Redefina o BMC para os padrões de fábrica usando a interface da Web de gerenciamento do servidor. Para obter informações sobre como redefinir o BMC, consulte Recuperando o gerenciamento do servidor ThinkSystem, Converged, NeXtScale ou System x M5 ou M6 após uma falha no servidor de gerenciamento redefinindo o controlador de gerenciamento.

b. Apague as informações de Unified Extensible Firmware Interface (UEFI), incluindo os endereços virtuais de adaptador de E/S usando os menus UEFI. Para obter informações, consulte a documentação do UEFI.

Recuperando configurações de inicialização após a implantação do padrão de servidor

Se um ou mais servidores não iniciarem após você ter implantado um novo padrão de servidor neles, o problema poderá ser que as configurações de inicialização foram substituídas pelas configurações de inicialização do padrão de servidor. Para sistemas operacionais instalados no modo UEFI, restaurar as configurações padrão pode requerer etapas de configuração adicionais para restaurar a configuração de inicialização.

Procedimento

Conclua o procedimento de recuperação manual a seguir para cada servidor afetado para restaurar as configurações de inicialização originais.

- Para um servidor com Red Hat Enterprise Linux instalado:
  1. Se você estiver acessando o servidor remotamente, estabeleça uma sessão de controle remoto com o servidor (consulte Usando o controle remoto para gerenciar servidores Converged, Flex System, NeXtScale e System x).
  2. Reinicie o servidor clicando em **Ferramentas → Energia → Ligar**. Quando a tela inicial do UEFI do servidor for exibida na sessão do Controle Remoto, pressione F1 para exibir o Setup Utility.
  3. Selecione **Boot Manager**.
  4. Selecione **Add Boot Option**.
  5. Selecione **UEFI Full Path Option**.
  6. Na lista exibida, selecione a entrada que inclui `SAS`.
  7. Selecione **EFI**.
  8. Selecione **redhat**.
  9. Selecione **grub.efi**.
  10. Selecione o campo **Input the Description**.
  11. Digite `Red Hat Enterprise Linux`.
  12. Selecione **Commit Changes**.
  13. Torne o `Red Hat Enterprise Linux` a primeira opção na Ordem de Inicialização e remova todas as outras opções na Ordem de Inicialização.
  14. Pressione Escape e, em seguida, selecione **Save changes then exit this menu**.
  15. Pressione Escape e, em seguida, selecione **Exit the Configuration Utility and Reboot**. O nó de cálculo é reiniciado.
- Para um servidor com o Microsoft Windows Server 2008 instalado:

1. Ligue o servidor e, quando solicitado, pressione F1 para entrar na configuração.
2. Selecione **Boot Manager**.
3. Selecione **Boot from File**.
4. Selecione a partição do sistema GUID Partition Tables (GPT) onde você instalou o Microsoft Windows Server 2008.
5. Selecione **EFI**.
6. Selecione **Microsoft**.
7. Selecione **Boot**.
8. Selecione **bootmgfw.EFI**.

Nota: Para obter mais informações, consulte Dica RETAIN 5079636.

Recuperando o gerenciamento do servidor em torre ou do rack após uma falha no servidor de gerenciamento

Se um servidor de rack ou em torre estiver sendo gerenciado pelo Lenovo XClarity Administrator e se o XClarity Administrator falhar, será possível restaurar as funções de gerenciamento até que XClarity Administrator seja restaurado ou substituído.

Sobre esta tarefa

Para recuperar o gerenciamento para um servidor Flex System, consulte Recuperando o gerenciamento com um CMM após uma falha no servidor de gerenciamento.

Recuperando o gerenciamento do servidor em torre ou de rack após uma falha no servidor de gerenciamento por gerenciamento forçado

É possível recuperar o gerenciamento do servidor gerenciando o servidor novamente com a opção Forçar gerenciamento

Procedimento

Se a instância de substituição do Lenovo XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, você poderá gerenciar o dispositivo novamente usando a conta e senha de `RECOVERY_ID` e a opção **Forçar gerenciamento** (consulte Gerenciando servidores).

Recuperando um servidor System x ou NeXtScale M4 cujo gerenciamento não foi cancelado corretamente usando o controlador de gerenciamento

É possível recuperar o gerenciamento de um servidor System x ou NeXtScale M4 usando o Baseboard Management Controller (BMC).

Procedimento

Conclua as etapas a seguir para recuperar o gerenciamento do servidor de um servidor que usa a autenticação gerenciada do Lenovo XClarity Administrator.

Etapa 1. Faça login na interface da Web do controlador de gerenciamento usando a conta de usuário e senha criadas antes que o servidor seja gerenciado pelo XClarity Administrator

Etapa 2. Apague as configurações de trap SNMP.

a. Clique em **Gerenciamento do IMM → Rede**.

b. Clique na guia **SNMP**.

c. Clique na guia **Comunidades**.

d. Localize a entrada da comunidade para o XClarity Administrator anterior, por exemplo.
   - **Endereço IP do LXCA:** 10.240.198.84
   - **Host do LXCA:** LXCA_maqCBlt86d
   - **Comunidade 2:**
   - **Nome da comunidade:** LXCA_maqCBlt86d
   - **Tipo de acesso:** Trap
   - **Permitir que hosts específicos recebam traps nessa comunidade:** 10.240.198.84

e. Remova o valor nos campos da entrada da comunidade.

f. Dê um clique em **Aplicar**.

Etapa 3. Apague as contas de usuário.

a. Clique em **Gerenciamento do IMM → Usuários**.

b. Clique na guia **Contas de Usuário**.

c. Exclua todas as contas de usuário do XClarity Administrator, incluindo contas de usuário com os prefixos a seguir:
   - DISABLE_*
   - LXCA_*
   - OBSOLETE_*
   - SNMPCFGUSER

Depois de concluir

Após o XClarity Administrator ser restaurado ou substituído, é possível gerenciar o servidor System x ou NeXtScale novamente (consulte Gerenciando servidores). Todas as informações sobre o servidor (como configurações de rede, políticas do servidor e políticas de conformidade de firmware) são retidas.

Recuperando o gerenciamento do servidor ThinkSystem, Converged, NeXtScale ou System x M5 ou M6 após uma falha no servidor de gerenciamento redefinindo o controlador de gerenciamento

É possível recuperar o gerenciamento de um servidor ThinkSystem, Converged, NeXtScale ou System x M5 ou M6 redefinindo o Baseboard Management Controller no servidor para os padrões de fábrica.

Procedimento

Conclua as etapas a seguir para recuperar o gerenciamento de um servidor que usa a autenticação gerenciada do Lenovo XClarity Administrator.

Etapa 1. Se o Encapsulamento estiver ativado no dispositivo, conecte o controlador de gerenciamento de destino de um sistema que esteja configurado para usar o endereço IP do dispositivo virtual do XClarity Administrator com falha.

Etapa 2. Redefina o controlador de gerenciamento para os padrões de fábrica.

a. Faça login na interface da Web do controlador de gerenciamento do servidor usando a conta de usuário e senha de recuperação criadas antes que o servidor seja gerenciado pelo XClarity Administrator.

b. Clique na **Guia Gerenciamento do IMM**.

c. Clique em **Redefinição do IMM para padrões de fábrica**.

d. Clique em **OK** para confirmar a ação de redefinição.

Importante: Depois que a configuração do BMC for concluída, o BMC será reiniciado. Se este for um servidor local, a conexão TCP/IP será interrompida e você deverá reconfigurar a interface de rede para restaurar a conectividade.

Etapa 3. Faça logon na interface da Web do controlador de gerenciamento do servidor novamente.

- O BMC é configurado inicialmente para tentar obter um endereço IP de um servidor DHCP. Se não conseguir, ele usará o endereço IPv4 estático `192.168.70.125`.
- O IMMBMC é configurado inicialmente com um nome de usuário `USERID` e senha de `PASSWORD` (com um zero). Essa conta de usuário padrão tem acesso de Supervisor. Altere esse nome de usuário e senha durante a configuração inicial para segurança aprimorada.

Etapa 4. Reconfigure a interface de rede para restaurar a conectividade. Para obter mais informações, consulte o Documentação online do Integrated Management Module II.

Depois de concluir

Após XClarity Administrator ser restaurado ou substituído, é possível gerenciar o servidor novamente (consulte Gerenciando servidores). Todas as informações sobre o servidor (como configurações de rede, políticas do servidor e políticas de conformidade de firmware) são retidas.

Se o servidor foi configurado usando Padrões de Configuração, é possível desativar e reativar o perfil de servidor que foi designado ao servidor para aplicar a configuração (consulte Trabalhando com perfis de servidor).

Recuperando o gerenciamento do servidor ThinkSystem, Converged, NeXtScale ou System x M5 ou M6 após uma falha no servidor de gerenciamento usando cimcli

É possível recuperar o gerenciamento de um servidor ThinkSystem, Converged, NeXtScale ou System x M5 ou M6 usando o utilitário `cimcli` para apagar as assinaturas de CIM.

Antes de iniciar

O OpenPegasus com o utilitário cimcli deve ser instalado em um sistema que tenha acesso à rede no servidor de destino. Para obter informações sobre como baixar, configurar e compilar o OpenPegasus, consulte Site OpenPegasus Release RPMs for Linux.

Nota: Para o Red Hat Enterprise Linux (RHEL) Server 7 e superior, a origem do OpenPegasus e os RPMs binários são incluídos como parte da distribuição do Red Hat. O pacote `top-pegasus-test.x86_64` inclui o utilitário cimcli.

Sobre esta tarefa

Após o servidor ser recuperado, é possível gerenciar o servidor novamente. Todas as informações sobre o servidor (como configurações de rede, políticas do servidor e políticas de conformidade de firmware) são retidas.

Procedimento

Conclua as etapas a seguir de um servidor que usa a autenticação gerenciada do Lenovo XClarity Administrator e com o OpenPegasus instalado para recuperar o gerenciamento do servidor.

Etapa 1. Se o Encapsulamento estiver ativado no dispositivo:

a. Conecte o servidor de destino de um sistema que esteja configurado para usar o endereço IP do dispositivo virtual do XClarity Administrator com falha.

b. Desative o Encapsulamento abrindo uma sessão SSH para dispositivo e executando o seguinte comando:
```
encaps lite off
```

Etapa 2. Execute os seguintes comandos para determinar as instâncias do CIM para CIM_ListenerDestinationCIMXML, CIM_Indicationfilter e CIM_IndicationSubscription.
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

em que <*IP_address*>, <*user_ID*> e <*password*> são o endereço IP, o ID do usuário e a senha do controlador de gerenciamento. Exemplo:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Etapa 3. Execute o seguinte comando para excluir cada instância do CIM para CIM_ListenerDestinationCIMXML, CIM_Indicationfilter e CIM_IndicationSubscription, uma de cada vez.
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

em que <*IP_address*>, <*user_ID*> e <*password*> são o endereço IP, o ID do usuário e a senha do controlador de gerenciamento, e <*cim_instance*> são as informações retornadas para cada instância do CIM na etapa anterior, entre aspas simples. Exemplo:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
```

```
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

Depois de concluir

Após o Lenovo XClarity Administrator ser restaurado ou substituído, é possível gerenciar o servidor System x ou NeXtScale novamente (consulte Gerenciando servidores). Todas as informações sobre o servidor (como configurações de rede, políticas do servidor e políticas de conformidade de firmware) são retidas.

Recuperando o gerenciamento do servidor ThinkServer após uma falha no servidor de gerenciamento usando a interface do controlador de gerenciamento

É possível recuperar o gerenciamento de um servidor ThinkServer na interface do controlador de gerenciamento.

Procedimento

Conclua as etapas a seguir para recuperar o gerenciamento do servidor.

Etapa 1. Faça login na interface da Web do controlador de gerenciamento do servidor como administrador (consulte Iniciando a interface do controlador de gerenciamento para um servidor).

Etapa 2. Remova as contas IPMI criadas pelo Lenovo XClarity Administrator selecionando Usuários no menu principal e depois removendo todas as contas de usuário com o prefixo "LXCA_".

Como alternativa, é possível renomear o nome de usuário da conta e remover o prefixo "LXCA_".

Etapa 3. Remova os destinos de trap SNMP selecionando **Gerenciamento PEF** no menu principal, clique na guia **Destino de LAN** e remova a entrada que aponta para o endereço IP da instância do XClarity Administrator.

Etapa 4. Verifique se você tem configurações de NTP válidas selecionando **Configurações de NTP** no menu principal e configurando data e hora manualmente ou fornecendo um endereço válido do servidor NTP.

Cancelando o gerenciamento de um servidor de rack ou em torre

É possível remover um servidor de rack ou em torre do gerenciamento pelo Lenovo XClarity Administrator. Esse processo é chamado de *cancelamento de gerenciamento*.

Antes de iniciar

É possível habilitar o XClarity Administrator para cancelar automaticamente o gerenciamento de dispositivos que estão offline por um período específico. Isso é desativado por padrão. Para habilitar o cancelamento de gerenciamento automático de dispositivos offline, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos** no menu do XClarity Administrator e, em seguida, clique em **Editar** próximo a **Cancelamento de gerenciamento de dispositivos está desabilitado**. Em seguida, selecione **Habilitar cancelamento de gerenciamento de dispositivos offline** e defina o intervalo de tempo. Por padrão, o gerenciamento dos dispositivos são cancelados após estarem offline por 24 horas.

Antes de cancelar o gerenciamento de um servidor de rack ou em torre, verifique se não há trabalhos ativos em execução no servidor.

Caso deseje remover o padrão de servidor e os endereços virtuais no servidor de rack ou em torre, desative o perfil de servidor antes de cancelar o gerenciamento do servidor (consulte Desativando um perfil de servidor).

Quando Call Home é ativado no XClarity Administrator, Call Home é desativado em todos os chassis e servidores gerenciados para evitar a criação de registros de problema duplicados. Se você pretende deixar de usar o XClarity Administrator para gerenciar dispositivos, poderá reativar Call Home em todos os dispositivos gerenciados no XClarity Administrator em vez de reativar Call Home para cada dispositivo individual posteriormente (consulte Reativando call home em todos os dispositivos gerenciados na documentação online do XClarity Administrator).

Sobre esta tarefa

Quando você cancela o gerenciamento de um servidor de rack ou em torre, o Lenovo XClarity Administrator executa as seguintes ações:

- Limpa a configuração usada para gerenciamento de usuários centralizado.
- Remove o certificado de segurança do Baseboard Management Controller do armazenamento confiável do XClarity Administrator.
- Se o Encapsulamento estiver ativado no dispositivo, configura as regras de firewall de dispositivos para as configurações anteriores ao gerenciamento do dispositivo.
- Remove as assinaturas de CIM da configuração do XClarity Administrator para que o XClarity Administrator não receba mais eventos do servidor de rack ou em torre.
- Desativa Call Home no servidor de rack ou em torre se Call Home estiver ativado atualmente no XClarity Administrator.
- Descarta eventos que foram enviados do servidor de rack ou em torre. É possível manter esses eventos encaminhando-os para um repositório externo, como um syslog (consulte Encaminhamento de eventos).

Quando o gerenciamento de um servidor de rack ou em torre é cancelado, o XClarity Administrator retém determinadas informações sobre o servidor. Essas informações são reaplicadas ao gerenciar o mesmo servidor de rack ou em torre novamente.

Importante: Se você tiver cancelado o gerenciamento de um servidor ThinkServer e gerenciar o servidor usando outra instância do XClarity Administrator, as informações sobre o servidor serão perdidas.

Dica: todos os dispositivos de demonstração que são incluídos opcionalmente durante a configuração inicial são nós em um chassi. Para cancelar o gerenciamento dos dispositivos da demonstração, cancele o gerenciamento do chassi usando a opção **Forçar cancelamento de gerenciamento mesmo se o dispositivo não estiver acessível**.

Procedimento

Para cancelar o gerenciamento de um servidor de rack ou em torre, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Servidores** para exibir a página Servidores.

Etapa 2. Selecione um ou mais servidores de rack ou em torre cujo gerenciamento será cancelado.

Etapa 3. Clique em **Cancelar Gerenciamento**. A caixa de diálogo Cancelar gerenciamento é exibida.

Etapa 4. **Opcional:** selecione **Forçar cancelamento de gerenciamento mesmo se o dispositivo não estiver acessível**.

Importante: Ao cancelar o gerenciamento do hardware da demonstração, selecione essa opção.

Etapa 5. Clique em **Cancelar Gerenciamento**.A caixa de diálogo Cancelar gerenciamento mostra o progresso de cada etapa no processo de cancelamento de gerenciamento.

Etapa 6. Quando esse processo for concluído, clique em **OK**.

Recuperando um servidor de rack ou em torre cujo gerenciamento não foi cancelado corretamente

Se o gerenciamento de um servidor Converged, NeXtScale, System x ou ThinkServer não foi cancelado corretamente, é necessário recuperar o servidor para poder gerenciá-lo novamente.

Recuperando um servidor de rack ou em torre cujo gerenciamento não foi cancelado corretamente por gerenciamento forçado

É possível recuperar o gerenciamento do servidor gerenciando o servidor novamente com a opção Forçar gerenciamento

Procedimento

Se a instância de substituição do Lenovo XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, você poderá gerenciar o dispositivo novamente usando a conta e senha de `RECOVERY_ID` e a opção **Forçar gerenciamento** (consulte Gerenciando servidores).

Recuperando um servidor System x ou NeXtScale M4 cujo gerenciamento não foi cancelado corretamente usando o controlador de gerenciamento

É possível recuperar o gerenciamento de um servidor System x ou NeXtScale M4 usando o controlador de gerenciamento.

Procedimento

Conclua as etapas a seguir para recuperar o gerenciamento do servidor.

Etapa 1. Faça login na interface da Web do controlador de gerenciamento usando a conta de usuário e senha criadas antes que o servidor seja gerenciado pelo XClarity Administrator

Etapa 2. Apague as configurações de trap SNMP.

a. Clique em **Gerenciamento do IMM → Rede**.

b. Clique na guia **SNMP**.

c. Clique na guia **Comunidades**.

d. Localize a entrada da comunidade para o XClarity Administrator anterior, por exemplo.
- **Endereço IP do LXCA:** 10.240.198.84
- **Host do LXCA:** LXCA_maqCBIt86d
- **Comunidade 2:**
- **Nome da comunidade:** LXCA_maqCBIt86d
- **Tipo de acesso:** Trap
- **Permitir que hosts específicos recebam traps nessa comunidade:** 10.240.198.84

e. Remova o valor nos campos da entrada da comunidade.

f. Dê um clique em **Aplicar**.

Etapa 3. Apague as contas de usuário.

a. Clique em **Gerenciamento do IMM → Usuários**.

b. Clique na guia **Contas de Usuário**.

c. Exclua todas as contas de usuário do XClarity Administrator, incluindo contas de usuário com os prefixos a seguir:
   - DISABLE_*
   - LXCA_*
   - OBSOLETE_*
   - SNMPCFGUSER

Etapa 4. Gerencie o servidor usando o Lenovo XClarity Administrator.

a. Na barra de menu do XClarity Administrator, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos**. A página Descobrir e Gerenciar é exibida.

b. Selecione **Entrada Manual**.

c. Clique em **Sistema Único**, insira o endereço IP do servidor que você deseja gerenciar e clique em **OK**.

d. Especifique o ID do usuário e a senha para autenticação no servidor.

e. Clique em **Gerenciar**.

   Uma caixa de diálogo é exibida e mostra o progresso desse processo de gerenciamento. Monitore o progresso para assegurar que o processo seja concluído.

f. Quando o processo for concluído, clique em **OK**.

Recuperando um servidor ThinkSystem, Converged, NeXtScale ou System x M5 ou M6 cujo gerenciamento não foi cancelado corretamente redefinindo o controlador de gerenciamento aos padrões de fábrica

É possível recuperar o gerenciamento do servidor ThinkSystem, Converged, NeXtScale ou System x M5 ou M6 redefinindo o Baseboard Management Controller (BMC) no servidor para os padrões de fábrica.

Procedimento

Conclua as etapas a seguir para recuperar o gerenciamento do servidor.

Etapa 1. Se o Encapsulamento estiver ativado no dispositivo, conecte o controlador de gerenciamento de destino de um sistema que esteja configurado para usar o endereço IP do dispositivo virtual do XClarity Administrator com falha.

Etapa 2. Redefina o controlador de gerenciamento para os padrões de fábrica.

a. Faça login na interface da Web do controlador de gerenciamento do servidor usando a conta de usuário e senha de recuperação criadas antes que o servidor seja gerenciado pelo XClarity Administrator.

b. Clique na **Guia Gerenciamento do IMM**.

c. Clique em **Redefinição do IMM para padrões de fábrica**.

d. Clique em **OK** para confirmar a ação de redefinição.

Importante: Depois que a configuração do BMC for concluída, o BMC será reiniciado. Se este for um servidor local, a conexão TCP/IP será interrompida e você deverá reconfigurar a interface de rede para restaurar a conectividade.

Etapa 3. Faça logon na interface da Web do controlador de gerenciamento do servidor novamente.

- O BMC é configurado inicialmente para tentar obter um endereço IP de um servidor DHCP. Se não conseguir, ele usará o endereço IPv4 estático `192.168.70.125`.
- O IMMBMC é configurado inicialmente com um nome de usuário `USERID` e senha de `PASSWORD` (com um zero). Essa conta de usuário padrão tem acesso de Supervisor. Altere esse nome de usuário e senha durante a configuração inicial para segurança aprimorada.

Etapa 4. Reconfigure a interface de rede para restaurar a conectividade. Para obter mais informações, consulte o Documentação online do Integrated Management Module II.

Etapa 5. Gerencie o servidor usando o Lenovo XClarity Administrator.

a. Na barra de menu do XClarity Administrator, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos**. A página Descobrir e Gerenciar é exibida.

b. Selecione **Entrada Manual**.

c. Clique em **Sistema Único**, insira o endereço IP do servidor que você deseja gerenciar e clique em **OK**.

d. Especifique o ID do usuário e a senha para autenticação no servidor.

e. Clique em **Gerenciar**.

Uma caixa de diálogo é exibida e mostra o progresso desse processo de gerenciamento. Monitore o progresso para assegurar que o processo seja concluído.

f. Quando o processo for concluído, clique em **OK**.

Etapa 6. Se o servidor foi configurado usando Padrões de Configuração, reative o perfil de servidor que foi designado ao servidor.

a. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Perfis de Servidor**. A página Padrões de Configuração: Perfis de Servidor é exibida.

b. Selecione o perfil de servidor e clique no ícone **Desativar perfil de servidor** ( ).

c. Clique em **Desligar o ITE** para desligar o servidor. Quando o servidor é ligado novamente, as atribuições de endereço virtual são revertidas para os padrões gravados.

d. Clique em **Desativar**. O estado do perfil muda para "Inativo" na coluna Status de Perfil. Observação: os servidores retêm as informações de identificação (por exemplo, nome do host, endereço IP, endereço MAC virtual) quando um perfil está desativado.

e. Selecione o perfil de servidor novamente e clique no ícone **Ativar perfil de servidor** ( ).

f. Clique em **Ativar** para ativar os perfis no servidor. O estado do perfil muda para "Ativo" na coluna Status de Perfil.

Etapa 7. Se uma política de conformidade foi atribuída ao servidor, atribua novamente a política de conformidade.

a. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Aplicar/Ativar**. A página Atualizações de Firmware: Aplicar/Ativar é exibida com uma lista de dispositivos gerenciados.

b. Selecione a política apropriada para o servidor no menu suspenso na coluna **Política Atribuída**.

Recuperando um servidor ThinkSystem, Converged, NeXtScale ou System x M5 ou M6 cujo gerenciamento não foi cancelado corretamente usando o cimcli

É possível recuperar o gerenciamento de um servidor ThinkSystem, Converged, NeXtScale ou System x usando o `cimcli` para apagar as assinaturas de CIM.

Antes de iniciar

O OpenPegasus com o utilitário cimcli deve ser instalado em um sistema que tenha acesso à rede no servidor de destino. Para obter informações sobre como baixar, configurar e compilar o OpenPegasus, consulte Site OpenPegasus Release RPMs for Linux.

Nota: Para o Red Hat Enterprise Linux (RHEL) Server 7 e superior, a origem do OpenPegasus e os RPMs binários são incluídos como parte da distribuição do Red Hat. O pacote `top-pegasus-test.x86_64` inclui o utilitário cimcli.

Sobre esta tarefa

Após o servidor ser recuperado, é possível gerenciar o servidor novamente. Todas as informações sobre o servidor (como configurações de rede, políticas do servidor e políticas de conformidade de firmware) são retidas.

Procedimento

Conclua as etapas a seguir de um servidor que usa a autenticação gerenciada do Lenovo XClarity Administrator e com o OpenPegasus instalado para recuperar o gerenciamento do servidor.

Etapa 1. Se o Encapsulamento estiver ativado no dispositivo:

a. Conecte o servidor de destino de um sistema que esteja configurado para usar o endereço IP do dispositivo virtual do XClarity Administrator com falha.

b. Desative o Encapsulamento abrindo uma sessão SSH para dispositivo e executando o seguinte comando:
```
encaps lite off
```

Etapa 2. Execute os seguintes comandos para determinar as instâncias do CIM para CIM_ListenerDestinationCIMXML, CIM_Indicationfilter e CIM_IndicationSubscription.
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

em que <*IP_address*>, <*user_ID*> e <*password*> são o endereço IP, o ID do usuário e a senha do controlador de gerenciamento. Exemplo:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Etapa 3. Execute o seguinte comando para excluir cada instância do CIM para CIM_ListenerDestinationCIMXML, CIM_Indicationfilter e CIM_IndicationSubscription, uma de cada vez.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

em que <*IP_address*>, <*user_ID*> e <*password*> são o endereço IP, o ID do usuário e a senha do controlador de gerenciamento, e <*cim_instance*> são as informações retornadas para cada instância do CIM na etapa anterior, entre aspas simples. Exemplo:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

Etapa 4. Gerencie o servidor usando o Lenovo XClarity Administrator.

a. Na barra de menu do XClarity Administrator, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos**. A página Descobrir e Gerenciar é exibida.

b. Selecione **Entrada Manual**.

c. Clique em **Sistema Único**, insira o endereço IP do servidor que você deseja gerenciar e clique em **OK**.

d. Especifique o ID do usuário e a senha para autenticação no servidor.

e. Clique em **Gerenciar**.

   Uma caixa de diálogo é exibida e mostra o progresso desse processo de gerenciamento. Monitore o progresso para assegurar que o processo seja concluído.

f. Quando o processo for concluído, clique em **OK**.

Recuperando o gerenciamento de um servidor ThinkServer cujo gerenciamento não foi cancelado corretamente usando a interface do controlador de gerenciamento

É possível recuperar o gerenciamento de um servidor ThinkServer usando a interface da Web do controlador de gerenciamento.

Procedimento

Conclua as etapas a seguir para recuperar o gerenciamento do servidor.

Etapa 1. Faça login na interface da Web do controlador de gerenciamento do servidor como administrador (consulte Iniciando a interface do controlador de gerenciamento para um servidor).

Etapa 2. Remova as contas IPMI criadas pelo Lenovo XClarity Administrator selecionando Usuários no menu principal e depois removendo todas as contas de usuário com o prefixo "LXCA_".

   Como alternativa, é possível renomear o nome de usuário da conta e remover o prefixo "LXCA_".

Etapa 3. Remova os destinos de trap SNMP selecionando **Gerenciamento PEF** no menu principal, clique na guia **Destino de LAN** e remova a entrada que aponta para o endereço IP da instância do XClarity Administrator.

Etapa 4. Verifique se você tem configurações de NTP válidas selecionando **Configurações de NTP** no menu principal e configurando data e hora manualmente ou fornecendo um endereço válido do servidor NTP.

Capítulo 9. Gerenciando dispositivos de armazenamento

O Lenovo XClarity Administrator pode gerenciar diversos tipos de dispositivos de armazenamento, incluindo os sistemas de armazenamento Lenovo Storage, Flex System e bibliotecas de fitas.

Saiba mais:  XClarity Administrator: descoberta

Antes de iniciar

Atenção: Revise Considerações sobre gerenciamento de armazenamento antes de gerenciar um dispositivo de armazenamento.

Nota: Os dispositivos de armazenamento Flex System são descobertos e gerenciados automaticamente ao gerenciar o chassi que os contêm. Não é possível descobrir e gerenciar dispositivos de armazenamento Flex System independentes do chassi.

Algumas portas podem estar disponíveis para comunicação com os dispositivos. Assegure-se de todas as portas necessárias estejam disponíveis antes de tentar gerenciar dispositivos de armazenamento. Para obter informações sobre portas, consulte Disponibilidade de porta na documentação online do XClarity Administrator.

Verifique se o firmware mínimo necessário está instalado em cada dispositivo de armazenamento que você deseja gerenciar usando o XClarity Administrator. É possível localizar os níveis mínimos de firmware necessários em Página da Web Suporte do XClarity Administrator – Compatibilidade clicando na guia **Compatibilidade** e, em seguida, clicando no link para os tipos de dispositivo apropriados.

Importante: Certifique-se de que os seguintes requisitos sejam atendidos antes de descobrir e gerenciar dispositivos de armazenamento do rack (que não sejam ThinkSystem série DE). Para obter mais informações, consulte Não é possível descobrir um dispositivo e Não é possível gerenciar um dispositivo na documentação online do XClarity Administrator.

- A configuração de rede deve permitir o tráfego SLP entre XClarity Administrator e o dispositivo de armazenamento em rack.
- Unicast SLP é necessário.
- O SLP multicast é necessário se você deseja que o XClarity Administrator descubra automaticamente os dispositivos Lenovo Storage. Além, SLP deve ser ativado no dispositivo de armazenamento em rack.

Sobre esta tarefa

O XClarity Administrator pode descobrir automaticamente os dispositivos de armazenamento em seu ambiente sondando dispositivos gerenciáveis que estão na mesma sub-rede IP que o XClarity Administrator. Para descobrir os dispositivos de armazenamento que estão em outras sub-redes, especifique um endereço IP ou intervalo de endereços IP, ou importe informações de uma planilha.

Após os dispositivos de armazenamento serem gerenciados pelo XClarity Administrator, o XClarity Administrator sonda cada dispositivo de armazenamento gerenciado periodicamente para coletar informações, como inventário, dados vitais do produto e status. É possível exibir e monitorar cada dispositivo de armazenamento gerenciado e executar ações de gerenciamento (como definir configurações do sistema, atualizar o firmware e ligar e desligar o equipamento).

Um dispositivo pode ser gerenciado somente por uma instância do XClarity Administrator por vez. Não há suporte para o gerenciamento por várias instâncias do XClarity Administrator. Se um dispositivo for

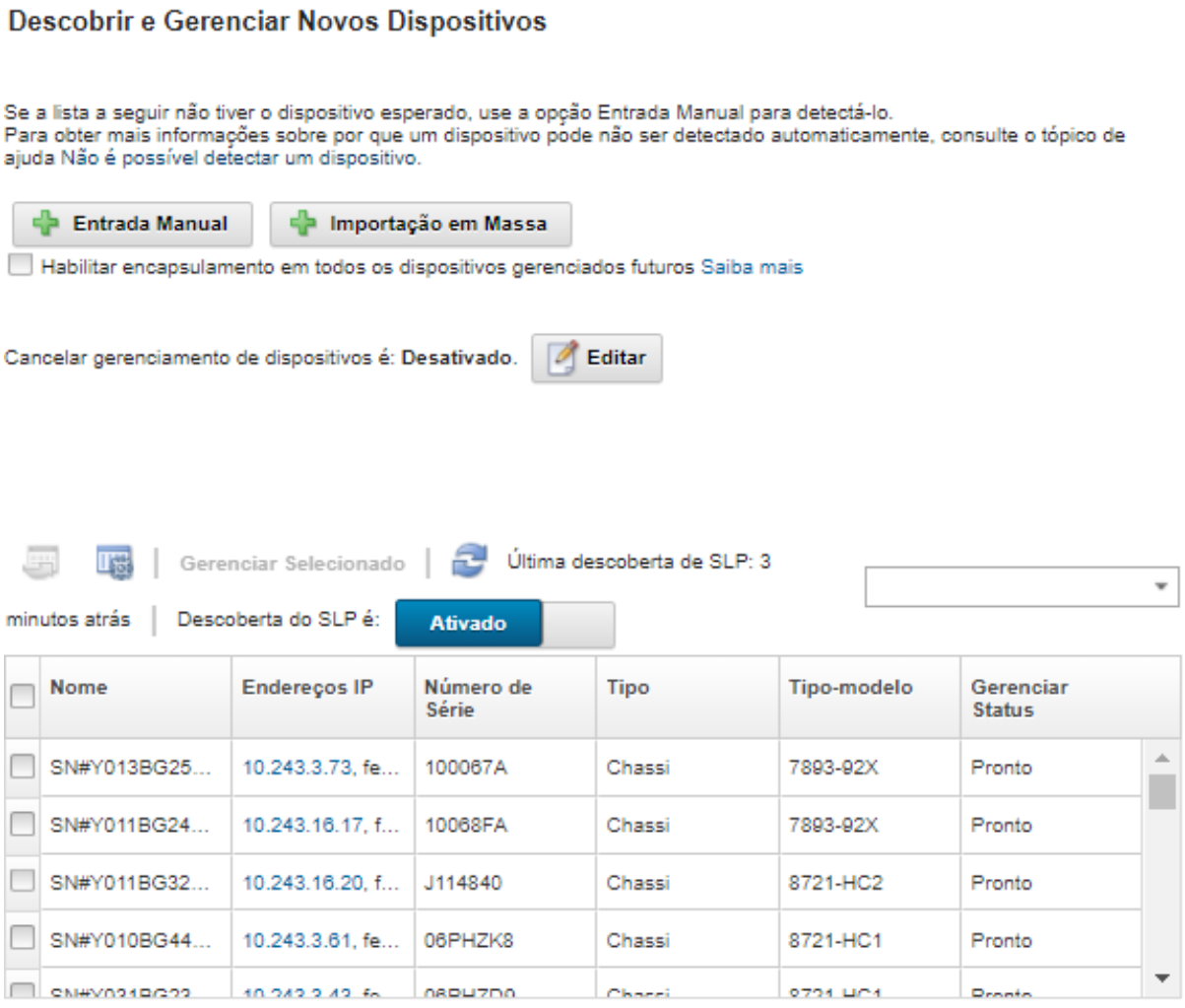
gerenciado por um XClarity Administrator, e você desejar gerenciá-lo com outro XClarity Administrator, primeiro cancele o gerenciamento do dispositivo no XClarity Administrator inicial e gerencie-o com o novo XClarity Administrator. Se um erro ocorrer durante o processo de cancelamento de gerenciamento, você poderá selecionar a opção **Forçar gerenciamento** durante o gerenciamento no novo XClarity Administrator.

Nota: Ao procurar dispositivos gerenciáveis na rede, o XClarity Administrator não sabe se um dispositivo já é gerenciado por outro gerenciador até após tentar gerenciar o dispositivo.

Procedimento

Execute um dos procedimentos a seguir para gerenciar dispositivos de armazenamento usando o XClarity Administrator.

- Descubra e gerencie um grande número de servidores de armazenamento, além de outros tipos de dispositivos usando um arquivo de importação em massa (consulte Gerenciando sistemas na documentação online do XClarity Administrator).
- Descubra e gerencie os dispositivos de armazenamento que estão na mesma sub-rede IP que o XClarity Administrator.
  1. Na barra de menu do XClarity Administrator, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos**. A página Descobrir e Gerenciar Novos Dispositivos é exibida.



É possível classificar as colunas da tabela para facilitar a localização dos dispositivos de armazenamento que deseja gerenciar. Além disso, é possível digitar texto (como um nome ou endereço IP) no campo **Filtro** para filtrar mais sistemas de armazenamento que são exibidos. É possível alterar as colunas que são exibidas e a ordem de classificação padrão clicando no ícone **Personalizar colunas** ( ).

2. Clique no ícone **Atualizar** ( ) para descobrir todos os dispositivos gerenciáveis no domínio XClarity Administrator. A descoberta pode levar vários minutos.
3. Selecione um ou mais dispositivos de armazenamento que você deseja gerenciar.
4. Clique em **Gerenciar Selecionado**. A caixa de diálogo Gerenciar é exibida.
5. Especifique o ID do usuário e a senha para autenticação no dispositivo de armazenamento.

   Dica: é recomendável usar uma conta de supervisor ou administrador para gerenciar o dispositivo. Se uma conta com autoridade de nível mais baixo for usada, o gerenciamento poderá falhar ou poderá ser bem-sucedido, mas outras operações futuras do XClarity Administrator no dispositivo poderão falhar (principalmente se o dispositivo for gerenciado sem autenticação gerenciada).
6. Clique em **Alterar** para alterar os grupos de funções que devem ser atribuídos aos dispositivos.

   Notas:

   – É possível selecionar de uma lista de grupos de funções que são atribuídos ao usuário atual.

   – Se você não alterar os grupos de funções, os grupos de função padrão serão usados. Para obter mais informações sobre os grupos de função padrão, consulte Alterando as permissões padrão.
7. Clique em **Gerenciar**.

   Uma caixa de diálogo é exibida e mostra o progresso desse processo de gerenciamento. Para assegurar que o processo seja concluído com êxito, monitore o progresso.
8. Quando o processo for concluído, clique em **OK**.

   O dispositivo agora é gerenciado por XClarity Administrator, que sonda automaticamente o dispositivo gerenciado regularmente para coletar informações atualizadas, como inventário.

   Se o gerenciamento não tiver sido bem-sucedido por causa de uma das seguintes condições de erro, repita esse procedimento usando a opção **Forçar gerenciamento**.

   – Se o gerenciamento do XClarity Administrator falhar e não puder ser recuperado.

     Nota: Se a instância de substituição do XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, você poderá gerenciar o dispositivo novamente usando a conta e senha de RECOVERY_ID (se aplicável) e a opção **Forçar gerenciamento**.

   – Se o gerenciamento do XClarity Administrator tiver sido desligado antes do cancelamento do gerenciamento dos dispositivos.

   – Se o cancelamento do gerenciamento dos dispositivos não tiver sido bem-sucedido.

   Atenção: Os dispositivos podem ser gerenciados somente por uma instância do XClarity Administrator por vez. Não há suporte para o gerenciamento por várias instâncias do XClarity Administrator. Se um dispositivo for gerenciado por um XClarity Administrator, e você desejar gerenciá-lo com outro XClarity Administrator, primeiro cancele o gerenciamento do dispositivo no XClarity Administrator original e gerencie-o com o novo XClarity Administrator.

- Descubra e gerencie os dispositivos de armazenamento que não estiverem na mesma sub-rede IP que o XClarity Administrator especificando manualmente endereços IP.
  1. Na barra de menu do XClarity Administrator, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos**. A página Descobrir e Gerenciar é exibida.
  2. Selecione **Entrada Manual**.

3. Especifique os endereços de rede dos dispositivos de armazenamento que deseja gerenciar:
   - Clique em **Sistema Único** e insira um nome de domínio de endereço IP único ou o nome de domínio totalmente qualificado (FQDN).

     Nota: Para especificar um FQDN, verifique se um nome de domínio válido foi especificado na página Acesso à Rede (consulte Configurando o acesso à rede).
   - Clique em **Vários Sistemas** e insira um intervalo de endereços IP. Para adicionar outro intervalo, clique no ícone **Adicionar** (). Para remover um intervalo, clique no ícone **Remover** ().
4. Clique em **OK**.
5. Especifique o ID do usuário e a senha para autenticação no dispositivo de armazenamento.

   Dica: é recomendável usar uma conta de supervisor ou administrador para gerenciar o dispositivo. Se uma conta com autoridade de nível mais baixo for usada, o gerenciamento poderá falhar ou poderá ser bem-sucedido, mas outras operações futuras do XClarity Administrator no dispositivo poderão falhar (principalmente se o dispositivo for gerenciado sem autenticação gerenciada).
6. Clique em **Alterar** para alterar os grupos de funções que devem ser atribuídos aos dispositivos.

   Notas:
   - É possível selecionar de uma lista de grupos de funções que são atribuídos ao usuário atual.
   - Se você não alterar os grupos de funções, os grupos de função padrão serão usados. Para obter mais informações sobre os grupos de função padrão, consulte Alterando as permissões padrão.
7. Clique em **Gerenciar**.

   Uma caixa de diálogo é exibida e mostra o progresso desse processo de gerenciamento. Para assegurar que o processo seja concluído com êxito, monitore o progresso.
8. Quando o processo for concluído, clique em **OK**.

   O dispositivo agora é gerenciado por XClarity Administrator, que sonda automaticamente o dispositivo gerenciado regularmente para coletar informações atualizadas, como inventário.

   Se o gerenciamento não tiver sido bem-sucedido por causa de uma das seguintes condições de erro, repita esse procedimento usando a opção **Forçar gerenciamento**.
   - Se o gerenciamento do XClarity Administrator falhar e não puder ser recuperado.

     Nota: Se a instância de substituição do XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, você poderá gerenciar o dispositivo novamente usando a conta e senha de RECOVERY_ID (se aplicável) e a opção **Forçar gerenciamento**.
   - Se o gerenciamento do XClarity Administrator tiver sido desligado antes do cancelamento do gerenciamento dos dispositivos.
   - Se o cancelamento do gerenciamento dos dispositivos não tiver sido bem-sucedido.

   Atenção: Os dispositivos podem ser gerenciados somente por uma instância do XClarity Administrator por vez. Não há suporte para o gerenciamento por várias instâncias do XClarity Administrator. Se um dispositivo for gerenciado por um XClarity Administrator, e você desejar gerenciá-lo com outro XClarity Administrator, primeiro cancele o gerenciamento do dispositivo no XClarity Administrator original e gerencie-o com o novo XClarity Administrator.

Depois de concluir

- Descubra e gerencie dispositivos adicionais.
- Atualizar o firmware em dispositivos que não estão em conformidade com as políticas atuais (consulte Atualizando firmware em dispositivos gerenciados).

- Adicione os novos dispositivos ao rack adequado para refletir o ambiente físico (consulte Gerenciando racks).
- Monitore o status e os detalhes de hardware (consulte Exibindo o status dos dispositivos de armazenamento).
- Monitore eventos e alertas (consulte Trabalhando com eventos e Trabalhando com alertas).

Considerações sobre gerenciamento de armazenamento

Antes de gerenciar um dispositivo de armazenamento, revise as seguintes considerações importantes.

Para obter informações sobre requisitos de porta, consulte Disponibilidade de porta na documentação online do Lenovo XClarity Administrator.

Importante: Certifique-se de que os seguintes requisitos sejam atendidos antes de descobrir e gerenciar dispositivos de armazenamento do rack (que não sejam ThinkSystem série DE). Para obter mais informações, consulte Não é possível descobrir um dispositivo e Não é possível gerenciar um dispositivo na documentação online do XClarity Administrator.

- A configuração de rede deve permitir o tráfego SLP entre XClarity Administrator e o dispositivo de armazenamento em rack.
- Unicast SLP é necessário.
- O SLP multicast é necessário se você deseja que o XClarity Administrator descubra automaticamente os dispositivos Lenovo Storage. Além, SLP deve ser ativado no dispositivo de armazenamento em rack.

Para dispositivos Lenovo Storage, a temperatura do ar no nível do sistema é medida pelo sensor de temperatura mais próximo do painel intermediário do sistema e reflete a temperatura ambiente após o fluxo de ar passar pelas unidades. Observe que a temperatura do ar registrada pelo XClarity Administrator e pelo controlador de gerenciamento pode ser diferente se a temperatura for capturada em pontos diferentes.

Para dispositivos de armazenamento Lenovo Série DE, os dois controladores de gerenciamento devem estar acessíveis na rede durante o gerenciamento inicial.

Para alguns dispositivos de armazenamento, traps SNMP estão somente em inglês.

Exibindo o status dos dispositivos de armazenamento

É possível exibir um resumo e o status detalhado dos dispositivos de armazenamento gerenciados no Lenovo XClarity Administrator.

Saiba mais:

- XClarity Administrator: inventário
- XClarity Administrator: monitoramento

Sobre esta tarefa

Os seguintes ícones de status são usados para indicar a integridade geral do dispositivo. Se os certificados não corresponderem, "(Não confiável)" será anexado ao status de cada dispositivo aplicável, por exemplo, Aviso (Não confiável). Se houver um problema de conectividade ou uma conexão com o dispositivo não for confiável, "(Conectividade)" será anexado ao status de cada dispositivo aplicável, por exemplo, Aviso (Conectividade).

- ( ) Crítico

- ( ) Aviso
- ( ) Pendente
- ( ) Informativo
- ( ) Normal
- ( ) Offline
- ( ) Desconhecido

Procedimento

Para exibir o status de um dispositivo de armazenamento gerenciado, conclua uma ou mais das seguintes ações.

- Na barra de menu do Lenovo XClarity Administrator, clique em **Painel**. A página Painel é exibida com uma visão geral e o status de todos os dispositivos de armazenamento gerenciados e outros recursos.

- Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Armazenamento**. A página Armazenamento é exibida com uma exibição tabular de todos os dispositivos de armazenamento que estão instalados no chassi gerenciado.

  É possível classificar as colunas da tabela para facilitar a localização dos dispositivos de armazenamento que deseja gerenciar. Além disso, inserir texto (como um nome do sistema ou endereço IP) no campo **Filtro** e clicar nos ícones de status para listar somente os sistemas de armazenamento que correspondem aos critérios selecionados.

Nesta página, é possível executar as ações a seguir:

- Exibir informações detalhadas sobre o dispositivo de armazenamento e seus componentes (consulte Visualizando os detalhes de um dispositivo de armazenamento).
- Exibir um dispositivo de armazenamento em exibição gráfica de rack ou de chassi clicando em **Todas as Ações → Exibições → Mostrar na Exibição do Rack** ou **Todas as Ações → Exibições → Mostrar na Exibição do Chassi**.
- Iniciar a interface da Web do controlador de gerenciamento do dispositivo de armazenamento clicando no link **Endereço IP** (consulte Iniciando a interface do controlador de gerenciamento para um dispositivo de armazenamento).
- Ligar e desligar o controlador de armazenamento no dispositivo de armazenamento (consulte Ligando e desligando um dispositivo de armazenamento).
- Modificar as informações do sistema selecionando um dispositivo de armazenamento e clicando em **Todas as Ações → Inventário → Editar Propriedades**.
- Atualizar o inventário selecionando um dispositivo de armazenamento e clicando em **Todas as Ações → Inventário → Atualizar Inventário**.
- Exportar informações detalhadas sobre um ou mais dispositivos de armazenamento para um único arquivo CSV selecionando os dispositivos de armazenamento e clicando em **Todas as Ações → Inventário → Exportar Inventário**.

  Nota: Você pode exportar os dados do inventário para no máximo 60 dispositivos ao mesmo tempo.

  Dica: Ao importar um arquivo CSV no Microsoft Excel, o Excel trata os valores de texto que contêm apenas números como valores numéricos (por exemplo, de UUIDs). Formate cada célula como texto para corrigir esse erro.
- Gerenciamento cancelado do dispositivo de armazenamento (consulte Cancelando o gerenciamento de um dispositivo de armazenamento).
- (Somente dispositivos de armazenamento Flex System) Reposicionar virtualmente o controlador de armazenamento no dispositivo de armazenamento (consulte Reposicionando virtualmente controladores de armazenamento em um dispositivo de armazenamento Flex System).
- Excluir eventos que não são de seu interesse de todas as páginas as quais os eventos são exibidos clicando no ícone **Excluir eventos** ( ). (consulte Excluindo eventos).
- Resolver problemas que podem ocorrer entre o certificado de segurança do Lenovo XClarity Administrator e o certificado de segurança do CMM no chassi onde o dispositivo de armazenamento está instalado selecionando um dispositivo de armazenamento e clicando em **Todas as Ações → Segurança → Resolver Certificados Não Confiáveis** (consulte Resolvendo um certificado de servidor não confiável).

– Adicionar ou remover um dispositivo de armazenamento de um grupo de recursos estático clicando em **Todas as Ações → Grupos → Adicionar ao grupo** ou **Todas as Ações → Grupos → Remover do grupo**.

Visualizando os detalhes de um dispositivo de armazenamento

É possível exibir informações detalhadas sobre dispositivos de armazenamento gerenciados no Lenovo XClarity Administrator, incluindo endereço IP, nome do produto, número de série e detalhes sobre cada caixa.

Sobre esta tarefa

Saiba mais:

- XClarity Administrator: inventário
- XClarity Administrator: monitoramento

Para dispositivos Lenovo Storage, a temperatura do ar no nível do sistema é medida pelo sensor de temperatura mais próximo do painel intermediário do sistema e reflete a temperatura ambiente após o fluxo de ar passar pelas unidades. Observe que a temperatura do ar registrada pelo XClarity Administrator e pelo controlador de gerenciamento pode ser diferente se a temperatura for capturada em pontos diferentes.

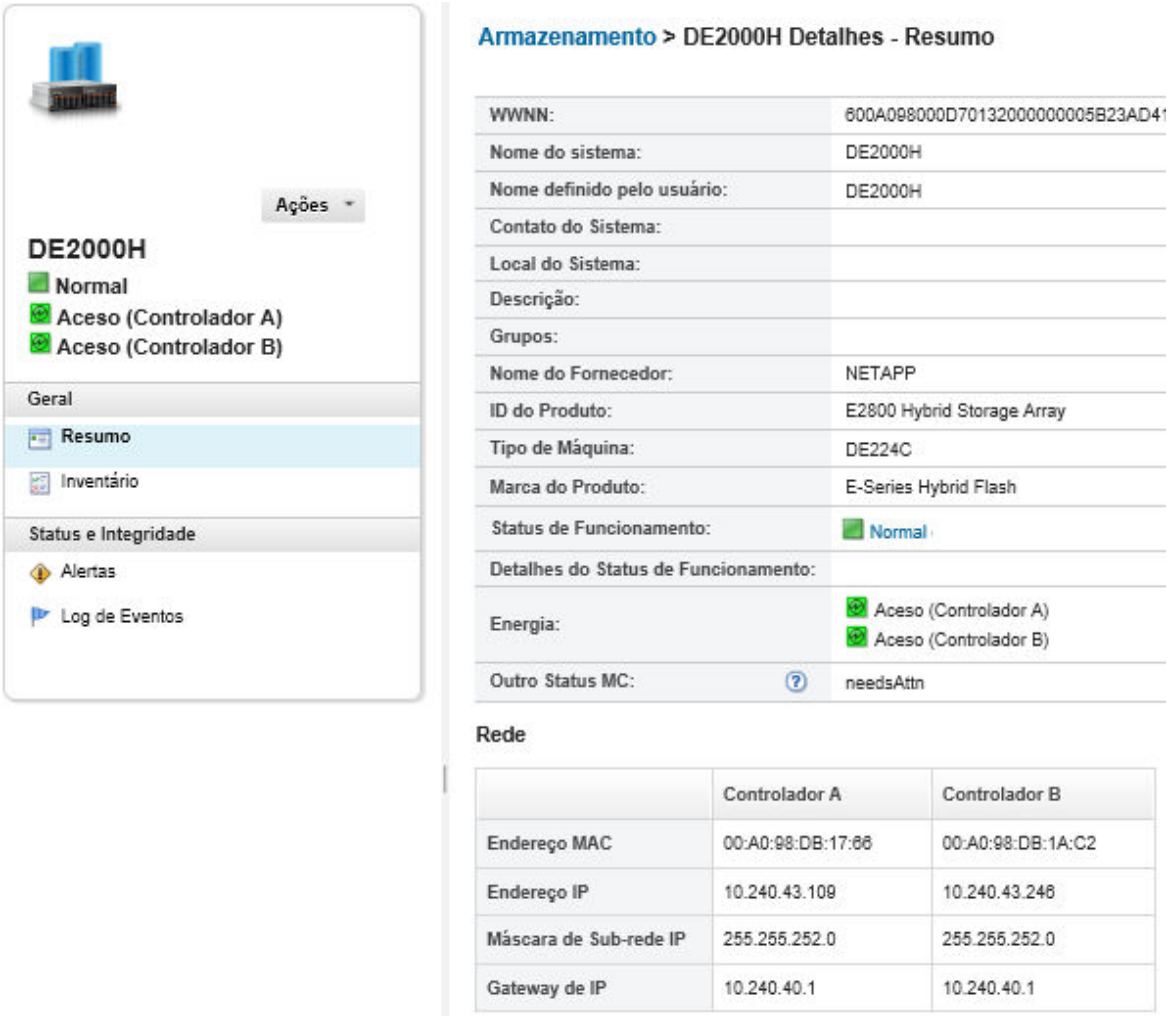
Procedimento

Para exibir os detalhes de um dispositivo de armazenamento gerenciado específico, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Armazenamento**. A página Armazenamento é exibida com uma exibição tabular de todos os dispositivos de armazenamento que estão instalados no chassi gerenciado.

É possível classificar as colunas da tabela para facilitar a localização dos dispositivos de armazenamento específicos. Além disso, é possível digitar texto (como um nome de sistema ou endereço IP) no campo **Filtro** para filtrar mais dispositivos de armazenamento que são exibidos.

Etapa 2. Clique no nome do dispositivo de armazenamento na coluna **Armazenamento**. A página Resumo é exibida, mostrando as propriedades e a lista de componentes instalados no dispositivo de armazenamento.



Etapa 3. Execute uma ou mais das etapas a seguir para visualizar os detalhes de armazenamento. Os dados exibidos podem ser diferentes com base no tipo de dispositivo de armazenamento.

- Clique em **Resumo** para exibir um resumo do servidor e dos componentes instalados, incluindo informações do sistema e dispositivos instalados (consulte Exibindo o status dos dispositivos de armazenamento).
- Clique em **Detalhes de Inventário** para exibir detalhes sobre os componentes do dispositivo de armazenamento, incluindo:
  - Níveis de firmware do dispositivo de armazenamento.
  - Detalhes da rede do controlador de gerenciamento, como nome do host, endereço IPv4, endereço IPv6 e endereços MAC.
  - Detalhes de recursos do dispositivo de armazenamento.
  - Detalhes sobre cada caixa no dispositivo de armazenamento.

  Dica: se um nó de expansão, como o Nó de Expansão de Armazenamento Flex System ou PCIe Expansion Node Flex System, for instalado no chassi e conectado a um dispositivo de armazenamento, os detalhes de inventário do nó de expansão também serão exibidos.
- Clique em **Alertas** para exibir os alertas na lista de alertas que são relacionados ao dispositivo de armazenamento (consulte Trabalhando com alertas).
- Clique em **Log de Eventos** para exibir os eventos no log de eventos que são relacionados ao dispositivo de armazenamento dispositivo de armazenamento (consulte Trabalhando com eventos).

- Clique em **Trabalhos** para exibir uma lista de trabalhos associados ao dispositivo de armazenamento (consulte Monitorando trabalhos).
- Clique em **Light Path** para exibir o estado atual de cada LED no dispositivo de armazenamento.
- Clique em **Energia e Temperatura** para exibir as características de energia e temperatura do dispositivo de armazenamento.

  Dica: use o botão Atualizar em seu navegador da Web para coletar os dados mais recentes de energia e temperatura. A coleta de dados pode levar vários minutos.

Depois de concluir

Além de exibir o resumo e informações detalhadas sobre um dispositivo de armazenamento, você pode executar as seguintes ações:

- Exibir um dispositivo de armazenamento em exibição gráfica de rack ou de chassi clicando em **Ações → Exibições → Mostrar na Exibição do Rack** ou **Ações → Exibições → Mostrar na Exibição do Chassi**.
- Exportar informações detalhadas sobre o dispositivo de armazenamento para um arquivo CSV clicando em **Ações → Inventário → Exportar Inventário**.

  Notas:

  – Para obter mais informações sobre os dados do inventário no arquivo CSV, consulte a GET /storage/*<UUID_list>* na documentação online do Lenovo XClarity Administrator.

  – Ao importar um arquivo CSV no Microsoft Excel, o Excel trata os valores de texto que contêm apenas números como valores numéricos (por exemplo, de UUIDs). Formate cada célula como texto para corrigir esse erro.
- Iniciar a interface da Web do controlador de gerenciamento do dispositivo de armazenamento clicando no link **Endereço IP** (consulte Iniciando a interface do controlador de gerenciamento para um dispositivo de armazenamento).
- Ligar e desligar um controlador de armazenamento no dispositivo de armazenamento (consulte Ligando e desligando um dispositivo de armazenamento).
- Reposicionar virtualmente o controlador de armazenamento no dispositivo de armazenamento (consulte Reposicionando virtualmente um servidor em um chassi do Flex System).
- Modificar as informações do sistema selecionando um dispositivo de armazenamento e clicando em **Editar Propriedades**.
- Atualizar o inventário selecionando um dispositivo de armazenamento e clicando em **Ações → Inventário → Atualizar Inventário**.
- Excluir eventos que não são de seu interesse de todas as páginas as quais os eventos são exibidos clicando no ícone **Ações → Redefinição de Serviços → Excluir eventos** (consulte Excluindo eventos).
- Resolver problemas que podem ocorrer entre o certificado de segurança do XClarity Administrator e o certificado de segurança do CMM no chassi onde o dispositivo de armazenamento está instalado, selecionando um dispositivo de armazenamento e clicando em **Ações → Serviço → Resolver Certificados Não Confiáveis** (consulte Resolvendo um certificado de servidor não confiável).

Fazendo backup e restaurando dados de configuração de armazenamento

O Lenovo XClarity Administrator não inclui funções de backup internas para dados de configuração de armazenamento. Em vez disso, use as funções de backup disponíveis para o servidor de armazenamento gerenciado.

Consulte a documentação do produto que é fornecida com o dispositivo de armazenamento para informações sobre como recuperar o dispositivo.
- Para dispositivos Lenovo Storage, consulte Documentação do produto Lenovo Storage S2200/S3200.
- Para dispositivos Lenovo Storage ThinkSystem, consulte Documentação do produto ThinkSystem Storage.

Ligando e desligando um dispositivo de armazenamento

É possível ligar e desligar um dispositivo de armazenamento no Lenovo XClarity Administrator.

Sobre esta tarefa

Para dispositivos de armazenamento Flex System, quando um controlador de armazenamento é desligado, os dados são armazenados primeiro na unidade interna e o dispositivo de armazenamento entra em um estado em espera. No estado de espera, os volumes que são fornecidos pelo dispositivo de armazenamento não podem mais ser acessados.

Para ativar um dispositivo de armazenamento ThinkSystem Série DM, certifique-se de que o controlador de armazenamento usado para gerenciamento esteja online e que seu endereço IP seja capaz de se comunicar diretamente para o processador do controlador de armazenamento desativado na rede externa.

Procedimento

Conclua as etapas a seguir para ligar e desligar um dispositivo de armazenamento gerenciado.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Armazenamento**. A página Armazenamento é exibida com uma exibição tabular de todos os dispositivos de armazenamento que estão instalados no chassi gerenciado.

É possível classificar as colunas da tabela para facilitar a localização do dispositivo de armazenamento específico. Além disso, digite texto (como um nome de sistema ou endereço IP) no campo **Filtro** para filtrar mais dispositivos de armazenamento que são exibidos.

Etapa 2. Selecione o dispositivo de armazenamento a ser ligado ou desligado.

Etapa 3. Clique em **Todas as Ações** e, em seguida, clique em uma destas ações de energia:
- **Ligar Controlador A**
- **Ligar Controlador B**
- **Desligar Controlador A**
- **Desligar Controlador B**
- **Reiniciar Controlador A**
- **Reiniciar Controlador B**

Reposicionando virtualmente controladores de armazenamento em um dispositivo de armazenamento Flex System

É possível executar um reposicionamento virtual, que simula a remoção e a reinserção de um controlador de armazenamento (caixa) no compartimento do dispositivo de armazenamento

Sobre esta tarefa

Durante o reposicionamento virtual, todas as conexões de rede existentes com o dispositivo de armazenamento são perdidas, e o estado de energia do dispositivo de armazenamento é alterado. Antes de executar um reposicionamento virtual, salve todos os dados do usuário.

Procedimento

Conclua as seguintes etapas para reposicionar virtualmente um controlador de armazenamento.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Armazenamento**. A página Armazenamento é exibida com uma exibição tabular de todos os dispositivos de armazenamento.

É possível classificar as colunas da tabela para facilitar a localização dos dispositivos de armazenamento específicos. Além disso, é possível digitar texto (como um nome de sistema ou endereço IP) no campo **Filtro** para filtrar mais dispositivos de armazenamento que são exibidos.

Etapa 2. Selecione o dispositivo de armazenamento Flex System.

Etapa 3. Clique em **Todas as Ações → Serviço** e, em seguida, em **Reposicionamento Virtual do Controlador A** ou **Reposicionamento Virtual do Controlador B**.

Etapa 4. Clique em **Reposicionamento Virtual**.

Iniciando a interface do controlador de gerenciamento para um dispositivo de armazenamento

É possível iniciar a interface da Web do controlador de gerenciamento do chassi em que o dispositivo de armazenamento está instalado no Lenovo XClarity Administrator.

Procedimento

Para iniciar a interface da Web do controlador de gerenciamento, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Armazenamento**. A página Armazenamento é exibida com uma exibição tabular de todos os dispositivos de armazenamento gerenciados.

É possível classificar as colunas da tabela para facilitar a localização dos dispositivos de armazenamento específicos. Além disso, digite texto (como um nome de dispositivo ou endereço IP) no campo **Filtro** para filtrar mais os dispositivos de armazenamento que são exibidos.

Etapa 2. Selecione o dispositivo de armazenamento.

Etapa 3. Clique em **Ações → Iniciar → Interface da Web de Gerenciamento**. A interface da Web do controlador de gerenciamento é iniciada.

Etapa 4. Faça login na interface do controlador de gerenciamento.

Nota: Para dispositivos de armazenamento Flex System, use as credenciais do usuário do XClarity Administrator.

Alterando as propriedades do sistema para um dispositivo de armazenamento

É possível alterar as propriedades do sistema para um dispositivo de armazenamento específico.

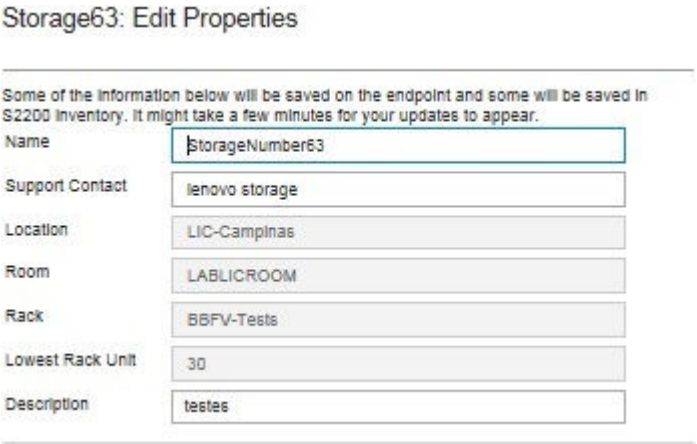
Procedimento

Para alterar as propriedades do sistema, conclua as etapas a seguir.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Armazenamento** para exibir a página Armazenamento.

Etapa 2. Selecione o dispositivo de armazenamento a ser atualizado.

Etapa 3. Clique em **Todas as Ações → Inventário → Editar Propriedades** para exibir a caixa de diálogo Editar.



Etapa 4. Altere as seguintes informações, conforme necessário.

- Nome
- Contato de suporte
- Descrição

Nota: O XClarity Administrator atualiza as propriedades de local, sala, rack e menor unidade do rack ao adicionar ou remover dispositivos de um rack na interface da Web (consulte Gerenciando racks).

Etapa 5. Clique em **Salvar**.

Nota: Quando você altera essas propriedades, pode haver um pequeno atraso até as alterações aparecerem na interface da Web do XClarity Administrator.

Recuperando o gerenciamento de um dispositivo de armazenamento em rack após uma falha no servidor de gerenciamento

Se o gerenciamento de um dispositivo de armazenamento em rack não tiver sido cancelado corretamente, será necessário recuperar o dispositivo de armazenamento antes de gerenciá-lo novamente. É possível recuperar o gerenciamento apagando partes específicas da configuração do dispositivo de armazenamento que foi configurado anteriormente pelo Lenovo XClarity Administrator.

Procedimento

Conclua uma das etapas a seguir para recuperar um dispositivo de armazenamento em rack.

- Se a instância de substituição do XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, você poderá gerenciar o dispositivo novamente usando a opção **Forçar gerenciamento** (consulte Gerenciando dispositivos de armazenamento).
- Remova todas as contas de usuário com o prefixo "LXCA_" e, opcionalmente, remova as contas de usuário com o prefixo "SYSMGR_" e o tipo "SNMPv3" do dispositivo de armazenamento.

Depois de concluir

Após XClarity Administrator ser restaurado ou substituído, é possível gerenciar o dispositivo de armazenamento novamente (consulte Gerenciando dispositivos de armazenamento). Todas as informações sobre o dispositivo de armazenamento (como propriedades do sistema) são retidas.

Recuperando o gerenciamento de um dispositivo de armazenamento Lenovo ThinkSystem Série DE após uma falha no servidor de gerenciamento

Se o gerenciamento de um dispositivo de armazenamento Lenovo ThinkSystem Série D não tiver sido cancelado corretamente, será necessário recuperar o dispositivo de armazenamento antes de gerenciá-lo novamente. É possível recuperar o gerenciamento apagando partes específicas da configuração do dispositivo de armazenamento que foi configurado anteriormente pelo Lenovo XClarity Administrator.

Procedimento

Conclua uma das etapas a seguir para recuperar um dispositivo de armazenamento Lenovo ThinkSystem Série DE.

- Se a instância de substituição do XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, você poderá gerenciar o dispositivo novamente usando a opção **Forçar gerenciamento** (consulte Gerenciando dispositivos de armazenamento).

- Remova o registro do par de chaves "LXCA_REMOTE_MANAGMENT_VERIFICATION" da API de par de chaves do dispositivo de armazenamento.

Depois de concluir

Após XClarity Administrator ser restaurado ou substituído, é possível gerenciar o dispositivo de armazenamento novamente (consulte Gerenciando dispositivos de armazenamento). Todas as informações sobre o dispositivo de armazenamento (como propriedades do sistema) são retidas.

Cancelando o gerenciamento de um dispositivo de armazenamento

É possível remover um dispositivo de armazenamento do gerenciamento do Lenovo XClarity Administrator. Esse processo é chamado de *cancelamento de gerenciamento*.

Antes de iniciar

Antes de cancelar o gerenciamento de um dispositivo de armazenamento, verifique se não há trabalhos ativos em execução no comutador.

Sobre esta tarefa

Quando o gerenciamento de um dispositivo de armazenamento é cancelado, o XClarity Administrator retém determinadas informações sobre o dispositivo de armazenamento. Essa informação é reaplicada ao gerenciar o mesmo dispositivo de armazenamento novamente.

Dica: todos os dispositivos de demonstração que são incluídos opcionalmente durante a configuração inicial são nós em um chassi. Para cancelar o gerenciamento dos dispositivos da demonstração, cancele o gerenciamento do chassi usando a opção **Forçar cancelamento de gerenciamento mesmo se o dispositivo não estiver acessível**.

Procedimento

Para cancelar o gerenciamento de um dispositivo de armazenamento, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Armazenamento** para exibir a página Armazenamento.

Etapa 2. Selecione um ou mais dispositivos de armazenamento na lista de comutadores gerenciados.

Etapa 3. Clique em **Cancelar Gerenciamento**. A caixa de diálogo Cancelar gerenciamento é exibida.

Etapa 4. **Opcional:** selecione **Forçar cancelamento de gerenciamento mesmo se o dispositivo não estiver acessível**.

Importante: Ao cancelar o gerenciamento do hardware da demonstração, selecione essa opção.

Etapa 5. Clique em **Cancelar Gerenciamento**.A caixa de diálogo Cancelar gerenciamento mostra o progresso de cada etapa no processo de cancelamento de gerenciamento.

Etapa 6. Quando esse processo for concluído, clique em **OK**.

Recuperando um dispositivo de armazenamento em rack cujo gerenciamento não foi cancelado corretamente

Se o Lenovo XClarity Administrator estiver gerenciando um dispositivo de armazenamento em rack, e se XClarity Administrator falhar, será possível recuperar as funções de gerenciamento até o servidor de gerenciamento ser restaurado ou substituído. É possível recuperar o gerenciamento do sistema apagando

partes específicas da configuração do dispositivo de armazenamento que foi configurado anteriormente pelo XClarity Administrator.

Procedimento

Conclua uma das etapas a seguir para recuperar um dispositivo de armazenamento em rack.

- Se a instância de substituição do XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, você poderá gerenciar o dispositivo novamente usando a opção **Forçar gerenciamento** (consulte Gerenciando dispositivos de armazenamento).
- Remova todas as contas de usuário com o prefixo "LXCA_" e, opcionalmente, remova as contas de usuário com o prefixo "SYSMGR_" e o tipo "SNMPv3" do dispositivo de armazenamento.

Depois de concluir

Após XClarity Administrator ser restaurado ou substituído, é possível gerenciar o dispositivo de armazenamento novamente (consulte Gerenciando dispositivos de armazenamento). Todas as informações sobre o dispositivo de armazenamento (como propriedades do sistema) são retidas.

Capítulo 10. Gerenciando comutadores

O Lenovo XClarity Administrator pode gerenciar comutadores de rede.

Saiba mais:

- XClarity Administrator: descoberta
- XClarity Administrator: Gerenciando comutadores

Antes de iniciar

Atenção: Reveja as considerações de gerenciamento de comutadores antes de gerenciar um comutador. Para obter informações, consulte Considerações sobre gerenciamento de comutadores.

Nota: Os comutadores Flex são descobertos e gerenciados automaticamente ao gerenciar o chassi que os contêm. Não é possível descobrir e gerenciar comutadores Flex independentes de um chassi.

Algumas portas podem estar disponíveis para comunicação com os comutadores. Assegure-se de todas as portas necessárias estejam disponíveis antes de tentar gerenciar um comutador. Para obter informações sobre portas, consulte Disponibilidade de porta na documentação online do XClarity Administrator.

Verifique se o firmware mínimo necessário está instalado em cada comutador que você deseja gerenciar usando o XClarity Administrator. É possível localizar os níveis mínimos de firmware necessários em Página da Web Suporte do XClarity Administrator – Compatibilidade clicando na guia **Compatibilidade** e, em seguida, clicando no link para os tipos de dispositivo apropriados.

Certifique-se de criar credenciais armazenadas no XClarity Administrator antes de gerenciar comutadores de rack. O XClarity Administrator usa armazenadas apenas as credenciais para autenticar nos comutadores de rack. As credenciais armazenadas devem corresponder a uma conta do usuário ativa no dispositivo. É possível criar credenciais armazenadas nas caixas de diálogo de gerenciamento ou na página Credenciais armazenadas. Para obter mais informações, consulte Gerenciando credenciais compartilhadas.

O gerenciamento usando interfaces de loopback é aceito para todos os dispositivos RackSwitch. Certifique-se de que o XClarity Administrator tenha conectividade com a interface de loopback, adicionando uma rota estática ou publicando o endereço por meio de um protocolo de roteamento. Observe que o roteamento não pode ser executado entre a porta de gerenciamento e *qualquer* porta de dados (incluindo loopback).

Para comutadores Lenovo ThinkSystem série DB:

- FOS 8.2.3 ou posterior é necessário
- Configure o usuário SNMPv3 no índice 1 no comutador *antes* de gerenciar o comutador executando nele o seguinte comando: `snmpconfig --add snmpv3 -index 1 -user snmpadmin1 -groupname rw`
- Verifique se REST está ativado no comutador. Para habilitar REST, execute o seguinte comando: `mgmtapp --enable rest`
- Verifique se o número de sessões REST permitidas é 10. Para configurar a contagem de sessão REST, execute o seguinte comando: `mgmtapp --config -maxrestsession 10`
- Os comutadores Lenovo ThinkSystem série DB não são descobertos usando protocolos de descoberta de serviço. Para gerenciar esses comutadores, use a opção **Entrada Manual**, limpe os **Usar protocolos de detecção de serviços para identificar o tipo de dispositivo** e, em seguida, selecione "Comutador Lenovo ThinkSystem Série DB" na lista **Tipo de Dispositivo**. Para obter mais detalhes, consulte o

procedimento abaixo sobre como descobrir e gerenciar comutadores que não estão na mesma sub-rede IP que o XClarity Administrator.

Para comutadores NVIDIA:

- Cumulus 4.3 ou posterior é necessário
- Os comutadores NVIDIA não são descobertos usando protocolos de descoberta de serviço. Para gerenciar esses comutadores, use a opção **Entrada Manual**, limpe os protocolos de detecção de serviços do usuário para identificar o tipo de dispositivo e, em seguida, selecione "Comutador NVIDIA" na lista **Tipo de Dispositivo**. Para obter mais detalhes, consulte o procedimento abaixo sobre como descobrir e gerenciar comutadores que não estão na mesma sub-rede IP que o XClarity Administrator.

Sobre esta tarefa

O XClarity Administrator pode descobrir automaticamente os comutadores RackSwitch em seu ambiente sondando dispositivos gerenciáveis que estão na mesma sub-rede IP que o XClarity Administrator. Para descobrir os comutadores que estão em outras sub-redes, especifique um endereço IP ou intervalo de endereços IP, ou importe informações de uma planilha.

Nota: Credenciais manuais não são compatíveis com comutadores de rack no XClarity Administrator.

Após os comutadores serem gerenciados pelo XClarity Administrator, o XClarity Administrator sonda cada comutador gerenciado periodicamente para coletar informações, como inventário, dados vitais do produto e status. É possível exibir e monitorar cada comutador gerenciado e executar tarefas de gerenciamento como iniciar o console de gerenciamento, e ligar e desligar.

Se o XClarity Administrator perder a comunicação com o comutador (por exemplo, devido a uma falha de rede ou perda de energia ou se o comutador estiver offline) ao coletar o inventário durante o processo de gerenciamento, o gerenciamento será concluído com êxito. Entretanto, algumas informações de inventário podem estar incompletas. Aguarde o comutador entrar online e o XClarity Administrator pesquisar o comutador quanto ao inventário ou coletar manualmente o inventário no comutador na página Comutadores selecionando o comutador e clicando em **Todas as Ações → Inventário → Atualizar inventário**.

Nota: Os comutadores podem ser empilhados. Um *comutador empilhado* é um grupo de comutadores que funcionam como um único comutador de rede. A pilha inclui um *comutador mestre* e um ou mais *comutadores membros*. Para comutadores Flex, é possível exibir e monitorar cada comutador na pilha e coletar dados diagnóstico. Entretanto, não é possível executar tarefas de gerenciamento (como atualizações de firmware e configuração do servidor) em nenhum comutador empilhado. Essas tarefas de gerenciamento do XClarity Administrator estão desativadas para todos os comutadores empilhados, incluindo o comutador mestre. É possível atualizar o firmware no comutador empilhado diretamente da CLI do comutador mestre. Para comutadores RackSwitch, é possível exibir e monitorar apenas as informações do comutador mestre. Os comutadores membros não são descobertos pelo XClarity Administrator.

As tarefas de gerenciamento também são desativadas para Comutadores Flex que estão no modo protegido.

Um dispositivo pode ser gerenciado somente por uma instância do XClarity Administrator por vez. Não há suporte para o gerenciamento por várias instâncias do XClarity Administrator. Se um dispositivo for gerenciado por um XClarity Administrator, e você desejar gerenciá-lo com outro XClarity Administrator, primeiro cancele o gerenciamento do dispositivo no XClarity Administrator inicial e gerencie-o com o novo XClarity Administrator. Se um erro ocorrer durante o processo de cancelamento de gerenciamento, você poderá selecionar a opção **Forçar gerenciamento** durante o gerenciamento no novo XClarity Administrator.

Nota: Ao procurar dispositivos gerenciáveis na rede, o XClarity Administrator não sabe se um dispositivo já é gerenciado por outro gerenciador até após tentar gerenciar o dispositivo.

Quando o comutador for gerenciado diretamente usando SSH ou indiretamente com um CMM, o comutador será identificado como gerenciado por XClarity Administrator, a configuração necessária será executada para interação e o inventário coletado.

Procedimento

Conclua um dos seguintes procedimentos para gerenciar seus comutadores RackSwitch usando o XClarity Administrator.

- Descubra e gerencie um grande número de comutadores e outros dispositivos usando um arquivo de importação em massa (consulte Gerenciando sistemas na documentação online do Lenovo XClarity Administrator).
- Descubra e gerencie os comutadores RackSwitch que estão na mesma sub-rede IP que o XClarity Administrator.
  1. Na barra de menu do XClarity Administrator, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos**. A página Descobrir e Gerenciar Novos Dispositivos é exibida.

É possível classificar as colunas da tabela para facilitar a localização dos comutadores que deseja gerenciar. Além disso, é possível digitar texto (como um nome ou endereço IP) no campo **Filtro** para filtrar mais comutadores que são exibidos. É possível alterar as colunas que são exibidas e a ordem de classificação padrão clicando no ícone **Personalizar colunas** ( ).

2. Clique no ícone **Atualizar** () para descobrir todos os dispositivos gerenciáveis no domínio XClarity Administrator. A descoberta pode levar vários minutos.
3. Selecione um ou mais comutadores que você deseja gerenciar.
4. Clique em **Gerenciar Selecionado**.
5. Especifique o as credenciais armazenadas para autenticação nos comutadores.

   Dica:

   – Clique em **Gerenciar credenciais armazenadas** para criar e gerenciar credenciais armazenadas em XClarity Administrator (consulte Gerenciando credenciais compartilhadas).
   – É recomendável usar uma conta de supervisor ou administrador para gerenciar o dispositivo. Se uma conta com autoridade de nível mais baixo for usada, o gerenciamento poderá falhar ou poderá ser bem-sucedido, mas outras operações futuras do XClarity Administrator no dispositivo poderão falhar (principalmente se o dispositivo for gerenciado sem autenticação gerenciada).
6. (Somente comutadores que executam ENOS) Se definido, especifique a senha "enable" usada para entrar no Modo Privilegiado/Exec do comutador.

   Quando você gerencia um comutador RackSwitch que executa ENOS, é necessário acesso ao Modo Privilegiado/Exec no comutador. Isso é usado pelo XClarity Administrator ao emitir o comando "enable" ao comutador. Por padrão, não há senha definida para esse comando no comutador. No entanto, se o administrador do comutador tiver configurado uma senha para este comando para ter mais segurança, ela deverá ser especificada para que o XClarity Administrator gerencie o comutador com êxito.
7. Opcional: (Somente comutadores que executam ENOS) opte por habilitar HTTPS no comutador clicando em **Avançado** e, em seguida, selecionando **Habilitar HTTPS**. Isso é ativado por padrão.

   Notas:

   – Para comutadores que executam CNOS, o HTTPS deve ser ativado no comutador do antes do gerenciamento (consulte Considerações sobre gerenciamento de comutadores).
   – Se você optar por não ativar HTTPS, a configuração atual do comutador será usada.
   – Quando o gerenciamento do comutador for cancelado, o XClarity Administrator restaurará o HTTPS para a configuração original.
8. Opcional: escolha se a configuração de NTP no comutador será substituída pela configuração de NTP e fuso horário para o Lenovo XClarity Administrator clicando em **Avançado** e, em seguida, selecionando **Configurar clientes de NTP para usar as configurações de NTP do servidor de gerenciamento**. Isso é ativado por padrão.

   Notas:

   – Se você escolher *não* substituir a configuração de NTP e do fuso horário, a data de entrada de log e eventos pode ficar fora de sincronia entre o comutador gerenciado e o servidor de gerenciamento.
   – Quando o gerenciamento do comutador for cancelado, o XClarity Administrator restaurará a configuração de NTP e do fuso horário para as configurações originais.
9. Clique em **Alterar** para alterar os grupos de funções que devem ser atribuídos aos dispositivos.

   Notas:

   – É possível selecionar de uma lista de grupos de funções que são atribuídos ao usuário atual.
   – Se você não alterar os grupos de funções, os grupos de função padrão serão usados. Para obter mais informações sobre os grupos de função padrão, consulte Alterando as permissões padrão.
10. Clique em **Gerenciar**.

Uma caixa de diálogo é exibida e mostra o progresso desse processo de gerenciamento. Para assegurar que o processo seja concluído com êxito, monitore o progresso do trabalho.

11. Quando o processo for concluído, clique em **OK**.

    O dispositivo agora é gerenciado por XClarity Administrator, que sonda automaticamente o dispositivo gerenciado regularmente para coletar informações atualizadas, como inventário.

    Se o gerenciamento não tiver sido bem-sucedido por causa de uma das seguintes condições de erro, repita esse procedimento usando a opção **Forçar gerenciamento**.

    – Se o gerenciamento do XClarity Administrator falhar e não puder ser recuperado.

      Nota: Se a instância de substituição do XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, você poderá gerenciar o dispositivo novamente usando a conta e senha de RECOVERY_ID (se aplicável) e a opção **Forçar gerenciamento**.

    – Se o gerenciamento do XClarity Administrator tiver sido desligado antes do cancelamento do gerenciamento dos dispositivos.

    – Se o cancelamento do gerenciamento dos dispositivos não tiver sido bem-sucedido.

    Atenção: Os dispositivos podem ser gerenciados somente por uma instância do XClarity Administrator por vez. Não há suporte para o gerenciamento por várias instâncias do XClarity Administrator. Se um dispositivo for gerenciado por um XClarity Administrator, e você desejar gerenciá-lo com outro XClarity Administrator, primeiro cancele o gerenciamento do dispositivo no XClarity Administrator original e gerencie-o com o novo XClarity Administrator.

- Descubra e gerencie os comutadores RackSwitch que não estiverem na mesma sub-rede IP que o XClarity Administrator especificando manualmente endereços IP:

  1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos**. A página Descobrir e Gerenciar é exibida.
  2. Selecione **Entrada Manual**.
  3. Especifique os endereços de rede dos comutadores que deseja gerenciar:

     – Clique em **Sistema Único** e insira um nome de domínio de endereço IP único ou o nome de domínio totalmente qualificado (FQDN).

       Nota: Para especificar um FQDN, verifique se um nome de domínio válido foi especificado na página Acesso à Rede (consulte Configurando o acesso à rede).

     – Clique em **Vários Sistemas** e insira um intervalo de endereços IP. Para adicionar outro intervalo, clique no ícone **Adicionar** (). Para remover um intervalo, clique no ícone **Remover** ().

  4. Se o tipo de dispositivo não for descoberto usando protocolos de detecção de serviço, desmarque Protocolos de detecção do serviço do usuário para identificar o tipo de dispositivo e, em seguida, selecione o tipo de dispositivo a ser gerenciado na lista suspensa.

     Protocolos de detecção de serviço, como SLP e SSDP, permitem que o XClarity Administrator descubra automaticamente o tipo do dispositivo que está prestes a ser gerenciado e, em seguida, use o mecanismo apropriado para gerenciar o dispositivo. Alguns tipos de dispositivos não suportam protocolos de detecção de serviços e, em alguns ambientes, os protocolos de detecção de serviços são propositalmente desligados. Em ambos os casos, você deve escolher o tipo de dispositivo apropriado para completar o processo de gerenciamento. Os seguintes tipos de dispositivo devem ser explicitamente identificados.
     – Comutador Lenovo ThinkSystem Série DB
     – Comutador NVIDIA Mellanox

  5. Clique em **OK**.
  6. Especifique o as credenciais armazenadas para autenticação nos comutadores.

Dica:

- Clique em **Gerenciar credenciais armazenadas** para criar e gerenciar credenciais armazenadas em XClarity Administrator (consulte Gerenciando credenciais compartilhadas).
- É recomendável usar uma conta de supervisor ou administrador para gerenciar o dispositivo. Se uma conta com autoridade de nível mais baixo for usada, o gerenciamento poderá falhar ou poderá ser bem-sucedido, mas outras operações futuras do XClarity Administrator no dispositivo poderão falhar (principalmente se o dispositivo for gerenciado sem autenticação gerenciada).

7. (Somente comutadores que executam ENOS) Se definido, especifique a senha "enable" usada para entrar no Modo Privilegiado/Exec do comutador.

   Quando você gerencia um comutador RackSwitch que executa ENOS, é necessário acesso ao Modo Privilegiado/Exec no comutador. Isso é usado pelo XClarity Administrator ao emitir o comando "enable" ao comutador. Por padrão, não há senha definida para esse comando no comutador. No entanto, se o administrador do comutador tiver configurado uma senha para este comando para ter mais segurança, ela deverá ser especificada para que o XClarity Administrator gerencie o comutador com êxito.

8. Opcional: (Somente comutadores que executam ENOS) opte por habilitar HTTPS no comutador clicando em **Avançado** e, em seguida, selecionando **Habilitar HTTPS**. Isso é ativado por padrão.

   Notas:

   - Para comutadores que executam CNOS, o HTTPS deve ser ativado no comutador do antes do gerenciamento (consulte Considerações sobre gerenciamento de comutadores).
   - Se você optar por não ativar HTTPS, a configuração atual do comutador será usada.
   - Quando o gerenciamento do comutador for cancelado, o XClarity Administrator restaurará o HTTPS para a configuração original.

9. Opcional: escolha se a configuração de NTP no comutador será substituída pela configuração de NTP e fuso horário para o Lenovo XClarity Administrator clicando em **Avançado** e, em seguida, selecionando **Configurar clientes de NTP para usar as configurações de NTP do servidor de gerenciamento**. Isso é ativado por padrão.

   Notas:

   - Se você escolher *não* substituir a configuração de NTP e do fuso horário, a data de entrada de log e eventos pode ficar fora de sincronia entre o comutador gerenciado e o servidor de gerenciamento.
   - Quando o gerenciamento do comutador for cancelado, o XClarity Administrator restaurará a configuração de NTP e do fuso horário para as configurações originais.

10. Clique em **Alterar** para alterar os grupos de funções que devem ser atribuídos aos dispositivos.

    Notas:

    - É possível selecionar de uma lista de grupos de funções que são atribuídos ao usuário atual.
    - Se você não alterar os grupos de funções, os grupos de função padrão serão usados. Para obter mais informações sobre os grupos de função padrão, consulte Alterando as permissões padrão.

11. Clique em **Gerenciar**.

    Uma caixa de diálogo é exibida e mostra o progresso desse processo de gerenciamento. Para assegurar que o processo seja concluído com êxito, monitore o progresso do trabalho.

12. Quando o processo for concluído, clique em **OK**.

    O dispositivo agora é gerenciado por XClarity Administrator, que sonda automaticamente o dispositivo gerenciado regularmente para coletar informações atualizadas, como inventário.

Se o gerenciamento não tiver sido bem-sucedido por causa de uma das seguintes condições de erro, repita esse procedimento usando a opção **Forçar gerenciamento**.

– Se o gerenciamento do XClarity Administrator falhar e não puder ser recuperado.

  Nota: Se a instância de substituição do XClarity Administrator usar o mesmo endereço IP do XClarity Administrator com falha, você poderá gerenciar o dispositivo novamente usando a conta e senha de RECOVERY_ID (se aplicável) e a opção **Forçar gerenciamento**.

– Se o gerenciamento do XClarity Administrator tiver sido desligado antes do cancelamento do gerenciamento dos dispositivos.

– Se o cancelamento do gerenciamento dos dispositivos não tiver sido bem-sucedido.

Atenção: Os dispositivos podem ser gerenciados somente por uma instância do XClarity Administrator por vez. Não há suporte para o gerenciamento por várias instâncias do XClarity Administrator. Se um dispositivo for gerenciado por um XClarity Administrator, e você desejar gerenciá-lo com outro XClarity Administrator, primeiro cancele o gerenciamento do dispositivo no XClarity Administrator original e gerencie-o com o novo XClarity Administrator.

Depois de concluir

- Descubra e gerencie dispositivos adicionais.
- Adicione os dispositivos recém-gerenciados ao rack adequado para refletir o ambiente físico (consulte Gerenciando racks).
- Monitore o status e os detalhes de hardware (consulte Exibindo o status de comutadores).
- Monitorar eventos (consulte Trabalhando com eventos).

Considerações sobre gerenciamento de comutadores

Antes de gerenciar um comutador, revise as seguintes considerações importantes.

Para obter informações sobre requisitos de porta, consulte Disponibilidade de porta na documentação online do Lenovo XClarity Administrator.

Dispositivos RackSwitch podem ser gerenciados por uma porta de gerenciamento ou uma das portas de dados. Dispositivos Rackswitch executando CNOS podem ser gerenciados somente em interfaces pertencentes a um VRF de "gerenciamento" ou "padrão".

Nota: O gerenciamento de dispositivos RackSwitch usando link IPv6 local por meio da porta de dados ou porta de gerenciamento não tem suporte.

Eventos do XClarity e configuração de trap SNMP

Quando um dispositivo RackSwitch que executa ENOS (qualquer versão) é gerenciado, a origem do trap SNMP é definida como a interface com o endereço IP que é usado para gerenciamento.

Quando um dispositivo RackSwitch que execute o CNOS v10.8.1 ou posterior é gerenciado, o VRF de origem do trap SNMP é verificado e alterado para corresponder à porta que é usada para gerenciamento.

Para dispositivos RackSwitch que executam CNOS anteriores à versão v10.8.1, o XClarity Administrator requer que a origem do trap SNMP seja o VRF que está conectado à porta usada para gerenciamento. O valor padrão "todos" permite o gerenciamento ou o uso de portas de dados. Se a configuração do comutador não usar o valor padrão, é necessário alterá-la para corresponder à porta que é usada para gerenciamento.

- Se a porta de gerenciamento for usada para gerenciamento, defina o VRF de origem do trap SNMP como "todos" ou "gerenciamento".
- Se uma das portas de dados for usada para gerenciamento, defina o VRF de origem do trap SNMP como "todos" ou "padrão".

Comutadores RackSwitch que executam CNOS

HTTPS deve ser ativado para gerenciamento e SLP deve ser ativado para descoberta.

Nota: O HTTPS fica ativado por padrão no CNOS. Se você alterou a configuração padrão de restApi (usando o comando `feature restApi http`), é possível alterá-lo para HTTPS usando o comando `feature restApi`. Para verificar o status atual, use o comando `display restApi server`. A saída reflete o status atual. Se o número da porta é seguido por "(HTTP)", isso significa que o HTTPS está *desativado*. Caso contrário, a porta deve ser 443.

Quando o gerenciamento de um dispositivo RackSwitch for cancelado, o XClarity Administrator poderá não restaurar a opção "preferir" para o valor que estava antes do gerenciamento do dispositivo, dependendo da versão de firmware do CNOS.

Comutadores RackSwitch que executam ENOS

- Se os comutadores RackSwitch estiverem em uma rede diferente do XClarity Administrator, a rede deverá ser configurada para permitir UDP de entrada pelas portas 161 e 162 para que o XClarity Administrator possa receber eventos e gerenciar esses dispositivos.
- SSH deve ser ativado para gerenciamento e SLP deve ser ativado para descoberta. HTTPS é opcional, no entanto, deve ser ativado para iniciar a interface da Web do comutador
- Dependendo da versão de firmware do comutador RackSwitch, pode ser necessário ativar o encaminhamento multicast SLP e SSH em cada comutador RackSwitch manualmente usando os seguintes comandos para que o comutador possa ser descoberto e gerenciado pelo XClarity Administrator. Para obter mais informações, consulte Comutadores de rack na documentação online do System x.
  - `ip slp enable`
  - `ssh enable`
- Quando um comutador RackSwitch é gerenciado, o XClarity Administrator modifica as seguintes definições de configuração. Modificar essas configurações em um comutador gerenciado pode interromper a conectividade e evitar a execução correta de ações de gerenciamento. Quando o gerenciamento de um comutador RackSwitch é cancelado, as definições de configuração são restauradas para os valores originais (antes do gerenciamento).
  - snmp-server access 32
  - snmp-server group 16
  - snmp-server notify 16
  - snmp-server target-parameters 16
  - snmp-server target-address 16
  - snmp-server trap-source <*IP interface*>
  - snmp-server user 16
  - snmp-server version <*v3only or v1v2v3*>
  - ntp enable
  - ntp primary-server <*hostname or IP address*> MGT
  - ntp secondary-server <*hostname or IP address*> MGT
  - ntp interval 1500
  - ntp offset 500
  - access https enable

É possível usar o XClarity Administrator para modificar as seguintes definições de configuração alterando as informações de contato de suporte, o nome ou as propriedades de local do comutador. O local é alterado quando o comutador é adicionado a um rack.
  - hostname "<*device_name*>"
  - snmp-server location "Location:<*location*>,Room:<*room*>,Rack:<*rack*>,LRU:<*lru*>"
  - snmp-server contact "<*contact_name*>"

Exibindo o status de comutadores

É possível exibir o status de todos os comutadores gerenciados por Lenovo XClarity Administrator.

Saiba mais:

- XClarity Administrator: inventário
- XClarity Administrator: monitoramento

Sobre esta tarefa

Os seguintes ícones de status são usados para indicar a integridade geral do dispositivo. Se os certificados não corresponderem, "(Não confiável)" será anexado ao status de cada dispositivo aplicável, por exemplo, Aviso (Não confiável). Se houver um problema de conectividade ou uma conexão com o dispositivo não for confiável, "(Conectividade)" será anexado ao status de cada dispositivo aplicável, por exemplo, Aviso (Conectividade).

- ( ) Crítico
  - Um ou mais sensores de temperatura estão no intervalo de falha.
  - Módulos de ventilador ou ventiladores não estão funcionando corretamente, como segue:
    - RackSwitch G8124-E: um ou mais ventiladores estão funcionando com rotação menor ou igual a 100 RPM.
    - RackSwitch G8052: menos de três módulos de ventilador estão em bom estado. Se os ventiladores desse módulo estiverem funcionando com uma rotação maior que 500 RPM, o módulo de ventilador será considerado em boas condições.
    - RackSwitch G8264, G8264CS, G8332, G8272: menos de quatro módulos de ventilador estão em bom estado. Se os ventiladores desse módulo estiverem funcionando com uma rotação maior que 500 RPM, o módulo de ventilador será considerado em boas condições.
    - RackSwitch G8296: menos de três módulos de ventilador estão em bom estado. Se os ventiladores desse módulo estiverem funcionando com uma rotação maior que 480 RPM, o módulo de ventilador será considerado em boas condições.
    - RackSwitch G7028, G7052: menos de três módulos de ventilador estão em bom estado. Se os ventiladores desse módulo estiverem funcionando com uma rotação maior que 500 RPM, o módulo de ventilador será considerado em boas condições.
  - Uma fonte de alimentação está desligada.
- ( ) Aviso
  - Um ou mais sensores de temperatura estão no intervalo de aviso.
  - Existe um dump de pânico em flash.
- ( ) Pendente
- ( ) Informativo
- ( ) Normal
  - Todos os sensores de temperatura estão no intervalo normal.
  - Todos os módulos de ventilador ou ventiladores estão funcionando corretamente.
  - Ambas as fontes de alimentação estão ligadas.
  - Nenhum dump de pânico em flash.
- ( ) Offline

- ( ) Desconhecido

Um dispositivo pode estar em um dos seguintes estados de energia:
- Aceso
- Apagado
- Desligando o
- Em espera
- Hibernar
- Desconhecido

Procedimento

Para exibir o status de um comutador gerenciado, conclua uma ou mais das seguintes ações.

- Na barra de menu do XClarity Administrator, clique em **Painel**. A página Painel é exibida com uma visão geral e o status de todos os comutadores gerenciados e outros recursos.

- Na barra de menu do XClarity Administrator, clique em **Hardware → Comutadores**. A página Comutadores é exibida com uma exibição tabular de todos os comutadores gerenciados.

  É possível classificar as colunas da tabela para facilitar a localização dos comutadores que deseja gerenciar. Além disso, inserir texto (como um nome ou endereço IP) no campo **Filtro** e clicar nos ícones de status para listar somente os comutadores que correspondem aos critérios selecionados.

Nesta página, é possível executar as ações a seguir:

- Exibir informações detalhadas sobre o comutador (consulte Exibindo os detalhes de um comutador).
- Exibir um comutador Flex em exibição gráfica de rack ou de chassi clicando em **Todas as Ações → Exibições → Mostrar na Exibição do Rack** ou **Todas as Ações → Exibições → Mostrar na Exibição do Chassi**.
- Exibir um comutador RackSwitch em exibição gráfica de rack ou de chassi clicando em **Todas as Ações → Exibições → Mostrar na Exibição do Rack**.
- Iniciar a interface da Web do controlador de gerenciamento do comutador clicando no link **Endereço IP** (consulte Iniciando a interface do controlador de gerenciamento para um comutador).
- Inicie o console SSH de comutador (consulte Iniciando uma sessão remota de SSH de um comutador).
- Ligue e desligue o comutador (consulte Ligando e desligando um comutador).
- (Somente comutadores RackSwitch) Modifique as informações do sistema selecionando um comutador e clicando em **Todas as Ações → Inventário → Editar Propriedades**.
- Atualizar o inventário selecionando um servidor e clicando em **Todas as Ações → Inventário → Atualizar Inventário**.
- Exportar informações detalhadas sobre um ou mais servidores para um único arquivo CSV selecionando os comutadores e clicando **Todas as Ações → Inventário → Exportar Inventário** (consulte Excluindo eventos).

  Nota: Você pode exportar os dados do inventário para no máximo 60 dispositivos ao mesmo tempo.

  Dica: Ao importar um arquivo CSV no Microsoft Excel, o Excel trata os valores de texto que contêm apenas números como valores numéricos (por exemplo, de UUIDs). Formate cada célula como texto para corrigir esse erro.
- Excluir eventos que não são de seu interesse de todas as páginas as quais os eventos são exibidos clicando no ícone **Excluir eventos** ( ) (consulte Excluindo eventos).
- (Somente comutadores Flex) Resolva problemas que podem ocorrer entre o certificado de segurança do XClarity Administrator e o certificado de segurança do CMM no chassi onde o comutador está instalado selecionando um comutador e clicando em **Todas as Ações → Segurança → Resolver Certificados Não Confiáveis** (consulte Resolvendo um certificado de servidor não confiável).
- Adicionar ou remover um comutador de um grupo de recursos estático, clicando em **Todas as Ações → Grupos → Adicionar ao grupo** ou **Todas as Ações → Grupos → Remover do grupo**.

Exibindo os detalhes de um comutador

É possível exibir informações detalhadas sobre um comutador gerenciado no Lenovo XClarity Administrator, incluindo os níveis de firmware e endereços IP.

Saiba mais:

- XClarity Administrator: inventário
- XClarity Administrator: monitoramento

Procedimento

Para exibir os detalhes de um comutador específico que é gerenciado por XClarity Administrator, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Comutadores**. A página Comutadores é exibida com uma exibição tabular de todos os comutadores que estão instalados no chassi gerenciado.

É possível classificar as colunas da tabela para facilitar a localização dos comutadores que deseja gerenciar. Além disso, digite texto (como um nome ou endereço IP) no campo **Filtro** para filtrar mais comutadores que são exibidos.

Etapa 2. Clique no comutador na coluna **Comutadores**. A página Resumo é exibida, mostrando as propriedades e a lista de componentes instalados no comutador.

Etapa 3. Conclua uma ou mais das seguintes etapas para exibir informações detalhadas do inventário:

Nota: Alguns detalhes podem não estar disponíveis para todos os comutadores.

- Clique em **Resumo** para exibir um resumo do comutador, incluindo informações do sistema e firmware (consulte Exibindo o status dos dispositivos de armazenamento).
- Clique em **Detalhes de Inventário** para exibir detalhes sobre os componentes do comutador, incluindo:
  - Níveis de firmware do comutador
  - Detalhes da rede do controlador de gerenciamento, como nome do host, endereço IPv4, endereço IPv6 e endereços MAC
  - Detalhes de recursos do comutador
- Clique em **Conectividade de E/S** para exibir detalhes de conectividade do comutador selecionado e dos adaptadores de rede associados instalados no comutador.
- Clique em **Alertas** para exibir os alertas na lista de alertas que são relacionados ao comutador (consulte Trabalhando com alertas).
- Clique em **Log de Eventos** para exibir os eventos no log de eventos que são relacionados ao comutador (consulte Trabalhando com eventos).
- Clique em **Arquivos de Configuração** para fazer backup e restaurar a configuração do comutador (consulte Fazendo backup e restaurando dados de configuração do comutador).
- Clique em **Histórico de Implantação** para exibir informações sobre os modelos de configuração do comutador que foram implantados no comutador (consulte Exibindo o histórico de implantação da configuração do comutador).
- Clique em **Trabalhos** para exibir os arquivos de dados de configuração do comutador (consulte Monitorando trabalhos).
- Clique em **Portas** para exibir o status e a configuração de todas as portas em um comutador gerenciado e habilitar ou desabilitar portas do comutador.

Nota: Para comutadores Flex, clique no ícone **Atualizar** () para coletar os dados de porta atuais. A coleta de dados pode levar vários minutos.

- Clique em **Light Path** para exibir o estado atual de cada LED no comutador.
- Clique em **Energia e Temperatura** para exibir informações sobre temperatura, fontes de alimentação e ventiladores.

  Dica: para coletar os dados mais recentes de energia e temperatura, use o botão Atualizar em seu navegador da Web. A coleta de dados pode levar vários minutos.

Depois de concluir

Além de exibir o resumo e informações detalhadas sobre um comutador, você pode executar as seguintes ações:

- Exibir um comutador Flex em exibição gráfica de rack ou de chassi clicando em **Ações → Exibições → Mostrar na Exibição do Rack** ou **Ações → Exibições → Mostrar na Exibição do Chassi**.
- Exibir um comutador RackSwitch em exibição gráfica de rack ou de chassi clicando em **Ações → Exibições → Mostrar na Exibição do Rack**.
- Iniciar a interface da Web do controlador de gerenciamento do comutador clicando no link **Endereço IP** (consulte Iniciando a interface do controlador de gerenciamento para um comutador).
- Inicie o console SSH de comutador (consulte Iniciando uma sessão remota de SSH de um comutador).
- Ligue e desligue o comutador (consulte Ligando e desligando um comutador).
- (Somente comutadores RackSwitch) Modifique as informações do sistema selecionando um comutador e clicando em **Editar Propriedades**.
- Exportar informações detalhadas sobre o comutador para um arquivo CSV clicando em **Ações → Inventário → Exportar Inventário**.

  Notas:

  – Para obter mais informações sobre os dados do inventário no arquivo CSV, consulte a GET /switches/*<UUID_list>* na documentação online do XClarity Administrator.

  – Ao importar um arquivo CSV no Microsoft Excel, o Excel trata os valores de texto que contêm apenas números como valores numéricos (por exemplo, de UUIDs). Formate cada célula como texto para corrigir esse erro.
- Excluir eventos que não são de seu interesse de todas as páginas as quais os eventos são exibidos clicando no ícone **Ações → Redefinição de Serviços → Eventos Excluídos** (consulte Excluindo eventos).
- Resolva problemas que podem ocorrer entre o certificado de segurança do XClarity Administrator e o certificado de segurança do RackSwitch ou do CMM no chassi onde o comutador Flex System está instalado selecionando um comutador e clicando em **Ações → Segurança → Resolver Certificados Não Confiáveis** (consulte Resolvendo um certificado de servidor não confiável).

Ligando e desligando um comutador

É possível ligar e desligar e reiniciar um comutador Flex System ou RackSwitch no Lenovo XClarity Administrator.

Procedimento

Conclua as etapas a seguir para ligar ou desligar um comutador gerenciado.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Comutadores**. A página Comutadores é exibida com uma exibição tabular de todos os comutadores que estão instalados no chassi gerenciado.

É possível classificar as colunas da tabela para facilitar a localização dos comutadores que deseja gerenciar. Além disso, digite texto (como um nome ou endereço IP) no campo **Filtro** para filtrar mais comutadores que são exibidos.

Etapa 2. Selecione o comutador a ser ligado ou desligado ou reiniciado.

Etapa 3. Clique em **Todas as Ações** e, em seguida, clique em uma destas ações de energia:
- **Ligar** (somente comutadores Flex System)
- **Desligar** (somente comutadores Flex System)
- **Reiniciar**. O comutador será reiniciado depois que todas as operações atualmente em execução forem concluídas. Operações que são iniciadas enquanto o comutador está sendo reiniciado são rejeitadas.

Habilitando e desabilitando portas do comutador

Você pode habilitar ou desabilitar portas específicas em um comutador RackSwitch ou Flex System

Procedimento

Para habilitar ou desabilitar portas do comutador, conclua as etapas a seguir.

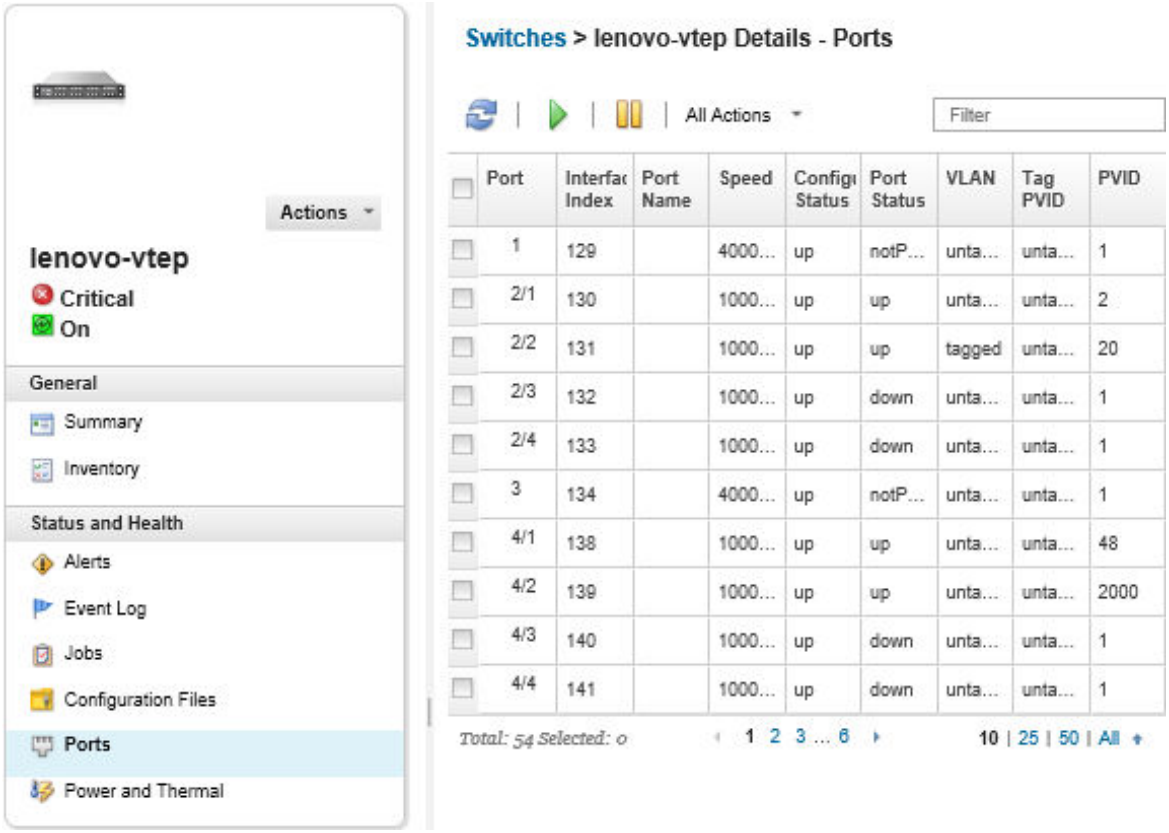
Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Comutadores**. A página Comutadores é exibida com uma exibição tabular de todos os comutadores que estão instalados no chassi gerenciado.

É possível classificar as colunas da tabela para facilitar a localização dos comutadores que deseja gerenciar. Além disso, digite texto (como um nome ou endereço IP) no campo **Filtro** para filtrar mais comutadores que são exibidos.

Etapa 2. Clique no comutador na coluna **Comutadores**. A página Resumo é exibida, mostrando as propriedades e a lista de componentes instalados no comutador.

Etapa 3. Clique em **Portas** na navegação esquerda para exibir o status e a configuração de todas as portas no comutador:

Nota: Para comutadores Flex, clique no ícone **Atualizar** ( ) para coletar os dados de porta atuais. A coleta de dados pode levar vários minutos



Etapa 4. Selecione a porta e, em seguida, clique no ícone **Habilitar** ( ) ou no ícone **Desabilitar** ( ).

Fazendo backup e restaurando dados de configuração do comutador

Você pode usar o Lenovo XClarity Administrator para fazer backup e restaurar dados de configuração para comutadores RackSwitch e Flex System. Também é possível exportar arquivos de configuração do comutador para seu sistema local e importar arquivos de configuração do comutador para o XClarity Administrator.

Fazendo backup dos dados de configuração do comutador

Você pode fazer backup dos dados de configuração para um comutador RackSwitch ou Flex System. Ao fazer backup de um comutador, os dados de configuração são importados para o Lenovo XClarity Administrator do comutador de destino como um arquivo de configuração do comutador.

Procedimento

Para fazer backup dos dados de configuração para um comutador gerenciado, conclua as etapas a seguir.

- Para um único comutador:
  1. Na barra de menu do XClarity Administrator, clique em **Hardware → Comutadores**. A página Comutadores é exibida com uma exibição tabular de todos os comutadores que estão instalados no chassi gerenciado.

     É possível classificar as colunas da tabela para facilitar a localização dos comutadores que deseja gerenciar. Além disso, digite texto (como um nome ou endereço IP) no campo **Filtro** para filtrar mais comutadores que são exibidos.

  2. Clique no comutador na coluna **Comutadores**. A página Resumo é exibida, mostrando as propriedades e a lista de componentes instalados no comutador.
  3. Clique em **Configuração** para exibir os arquivos de configuração do comutador.
  4. Clique no ícone **Fazer backup dos dados de configuração** ( ) para fazer backup da configuração do comutador.
  5. (Opcional) Especifique um nome para o arquivo de configuração do comutador.

     Para dispositivos CNOS, o nome do arquivo pode conter caracteres alfanuméricos e os seguintes caracteres especiais: sublinhado (_), hífen (-) e o ponto (.). Para comutadores ENOS, o nome do arquivo pode conter caracteres alfanuméricos e os caracteres especiais.

     Se o nome do arquivo não for especificado, o nome padrão seguinte será usado: "<*switch_name*>_<*IP_address*>_<*timestamp*>.cfg."

6. (Opcional) Adicione um comentário que descreva o backup.
7. Clique em **Backup** para fazer backup com os dados de configuração do comutador imediatamente ou clique em **Programação** para programar o backup para ser executado posteriormente.

   Se você escolher programar um backup, é possível selecionar **Substituir** para fazer backup dos dados de configuração do comutador para o mesmo arquivo em cada trabalho executado, substituindo seu conteúdo. Se você optar por não substituir o arquivo, os nomes dos arquivos de backups subsequentes serão anexados com um número exclusivo (por exemplo, MyBackup_33.cfg).

   Nota: Durante o planejamento de um backup, não é possível escolher nomes de arquivos dinâmicos ou comentários para cada tarefa programada.

- Para vários comutadores:
  1. Na barra de menu do XClarity Administrator, clique em **Hardware → Comutadores**. A página Comutadores é exibida com uma exibição tabular de todos os comutadores que estão instalados no chassi gerenciado.
  2. Selecione um ou mais comutadores.
  3. Clique em **Todas as Ações → Configuração → Fazer backup do arquivo de configuração**.
  4. (Opcional) Especifique um nome para o arquivo de configuração do comutador.

     Para dispositivos CNOS, o nome do arquivo pode conter caracteres alfanuméricos e os seguintes caracteres especiais: sublinhado (_), hífen (-) e o ponto (.). Para comutadores ENOS, o nome do arquivo pode conter caracteres alfanuméricos e os caracteres especiais.

     Se o nome do arquivo não for especificado, o nome padrão seguinte será usado: "<*switch_name*>_<*IP_address*>_<*timestamp*>.cfg."
  5. (Opcional) Adicione um comentário que descreva o backup.
  6. Clique em **Backup** para fazer backup com os dados de configuração do comutador imediatamente ou clique em **Programação** para programar o backup para ser executado posteriormente.

     Se você escolher programar um backup, é possível selecionar **Substituir** para fazer backup dos dados de configuração do comutador para o mesmo arquivo em cada trabalho executado, substituindo seu conteúdo. Se você optar por não substituir o arquivo, os nomes dos arquivos de backups subsequentes serão anexados com um número exclusivo (por exemplo, MyBackup_33.cfg).

     Nota: Durante o planejamento de um backup, não é possível escolher nomes de arquivos dinâmicos ou comentários para cada tarefa programada.

Depois de concluir

Quando o processo de backup for concluído, o arquivo de configuração do comutador será adicionado à guia **Arquivos de Configuração** na página de detalhes do comutador.

Nesta página, é possível executar as ações a seguir em um arquivo de configuração do comutador selecionado:

- Restaurar a configuração do comutador selecionando o arquivo de configuração do comutador e clicando no ícone **Restaurar dados de configuração** ().
- Excluir arquivos de configuração do comutador do XClarity Administrator clicando no ícone **Excluir** ().
- Exportar arquivos de configuração do comutador para seu sistema local selecionando os arquivos e clicando no ícone **Exportar arquivo de configuração** ().
- Importar arquivos de configuração do comutador para o XClarity Administrator clicando no ícone **Importar arquivo de configuração** ().

Restaurando dados de configuração do comutador

É possível restaurar os dados de configuração com backup ou importados para o Lenovo XClarity Administrator para um comutador Flex System ou RackSwitch. O arquivo de configuração do comutador é baixado do XClarity Administrator no comutador de destino, e a configuração tem efeito automaticamente.

Arquivos de configuração são associados a um comutador específico. É possível restaurar um arquivo de configuração apenas no comutador ao qual ele está associado. Não é possível usar um arquivo de configuração que foi passou por backup para um comutador restaurar a configuração em outro comutador.

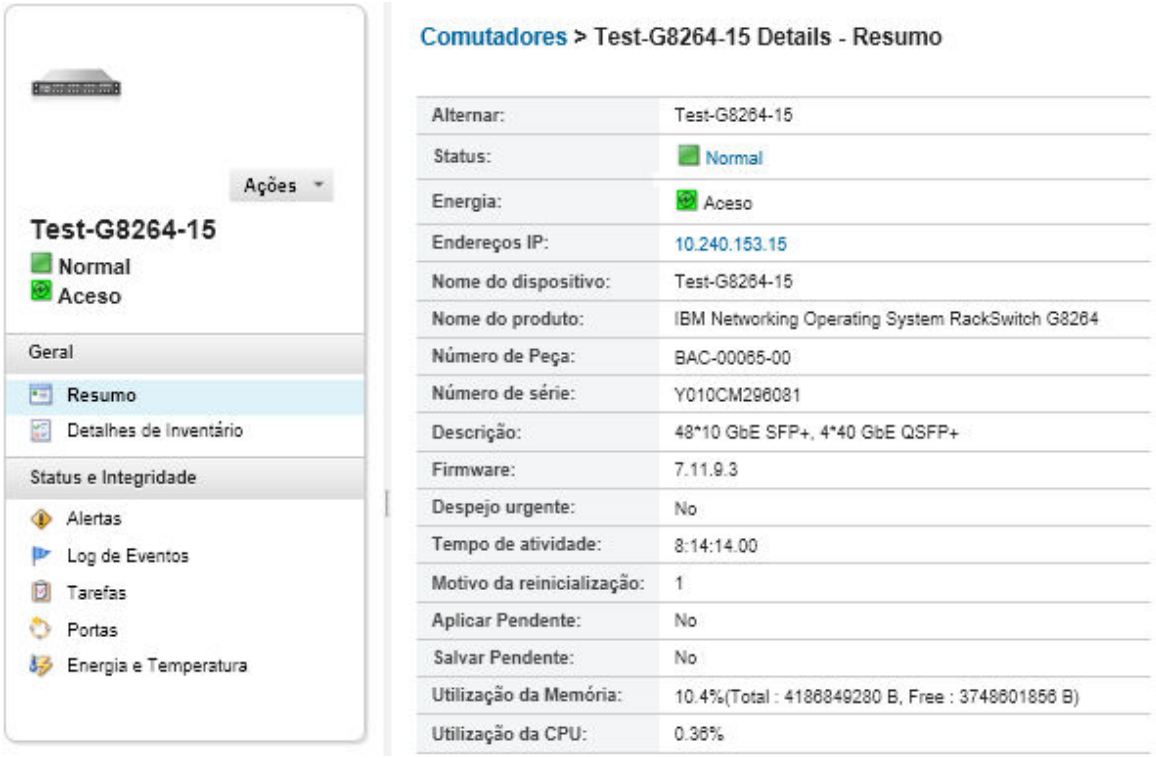
Procedimento

Para restaurar dados de configuração em um comutador gerenciado, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Comutadores**. A página Comutadores é exibida com uma exibição tabular de todos os comutadores que estão instalados no chassi gerenciado.

É possível classificar as colunas da tabela para facilitar a localização dos comutadores que deseja gerenciar. Além disso, digite texto (como um nome ou endereço IP) no campo **Filtro** para filtrar mais comutadores que são exibidos.

Etapa 2. Clique no comutador na coluna **Comutadores**. A página Resumo é exibida, mostrando as propriedades e a lista de componentes instalados no comutador.



Etapa 3. Clique em **Arquivos de Configuração** para exibir os arquivos de configuração do comutador.

Etapa 4. Selecione o arquivo de configuração que você deseja restaurar no comutador e clique no ícone **Restaurar dados de configuração** ( ). A caixa de diálogo Restaurar é exibida.

Etapa 5. (Somente comutadores que executam CNOS) Escolha se deseja reiniciar o comutador depois de concluir a operação de restauração.

Se você optar por não reiniciar o comutador automaticamente, reinicie manualmente o comutador CNOS para ativar os dados da configuração restaurada. Se você esperar demais e uma operação Salvar ocorrer (por exemplo, se uma porta está ativada ou desativada), a operação de restauração será interrompida, e os dados da configuração em execução serão usados.

Etapa 6. Clique em **Restaurar** para restaurar com os dados de configuração no comutador imediatamente ou clique em **Programação** para programar a tarefa de restauração para ser executada posteriormente.

Nota: Tenha cuidado ao programar tarefas de restauração recorrente. Se o comutador for redefinido para uma configuração anterior, verifique a página Tarefas programadas para tarefas de restauração programadas.

Exportando e importando arquivos de configuração do comutador

É possível exportar arquivos de configuração do comutador para seu sistema local e importar arquivos de configuração do comutador para o Lenovo XClarity Administrator.

Procedimento

Para fazer backup dos dados de configuração para um comutador gerenciado, conclua as etapas a seguir.

- Exportar arquivos de configuração do comutador

1. Na barra de menu do XClarity Administrator, clique em **Hardware → Comutadores**. A página Comutadores é exibida com uma exibição tabular de todos os comutadores que estão instalados no chassi gerenciado.

   É possível classificar as colunas da tabela para facilitar a localização dos comutadores que deseja gerenciar. Além disso, digite texto (como um nome ou endereço IP) no campo **Filtro** para filtrar mais comutadores que são exibidos.

2. Clique no comutador na coluna **Comutadores**. A página Resumo é exibida, mostrando as propriedades e a lista de componentes instalados no comutador.
3. Clique em **Configuração** para exibir os arquivos de configuração do comutador.
4. Selecione os arquivos de configuração do comutador a serem exportados.
5. Clique no ícone **Exportar arquivo de configuração** ( ) para fazer backup da configuração do comutador.

- Importar arquivos de configuração do comutador
  1. Na barra de menu do XClarity Administrator, clique em **Hardware → Comutadores**. A página Comutadores é exibida com uma exibição tabular de todos os comutadores que estão instalados no chassi gerenciado.

     É possível classificar as colunas da tabela para facilitar a localização dos comutadores que deseja gerenciar. Além disso, digite texto (como um nome ou endereço IP) no campo **Filtro** para filtrar mais comutadores que são exibidos.

2. Clique no comutador na coluna **Comutadores**. A página Resumo é exibida, mostrando as propriedades e a lista de componentes instalados no comutador.
3. Clique em **Configuração** para exibir os arquivos de configuração do comutador.
4. Clique no ícone **Importar arquivo de configuração** ( ) para fazer backup da configuração do comutador.
5. Digite o nome do arquivo de configuração do comutador ou clique em **Procurar** para encontrar o arquivo de inicialização que você deseja importar.
6. **Opcional:** Digite uma descrição para o arquivo de configuração do comutador.
7. Clique em **Importar**.

   Se você fechar a guia ou a janela do navegador da Web na qual o arquivo está sendo transferido por upload antes do término do processo, ocorrerá falha na importação.

Iniciando a interface do controlador de gerenciamento para um comutador

É possível iniciar a interface da Web do controlador de gerenciamento para um comutador RackSwitch ou Flex System executando ENOS no Lenovo XClarity Administrator.

Procedimento

Conclua as seguintes etapas para iniciar a interface do controlador de gerenciamento para um comutador.

Nota: Iniciar qualquer interface da Web do controlador de gerenciamento do XClarity Administrator usando o navegador da Web Safari não é permitido.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Comutadores**. A página Comutadores é exibida com uma exibição tabular de todos os comutadores que estão instalados no chassi gerenciado.

É possível classificar as colunas da tabela para facilitar a localização dos comutadores que deseja gerenciar. Além disso, digite texto (como um nome ou endereço IP) no campo **Filtro** para filtrar mais comutadores que são exibidos.

Etapa 2. Selecione o comutador e clique em **Todas as Ações → Iniciar → Interface da Web de Gerenciamento**. A interface da Web do controlador de gerenciamento do comutador é exibida.

Dica: também é possível iniciar a interface do controlador de gerenciamento clicando no link do endereço IP na coluna **Endereço IP** e nas páginas de resumo e detalhes do comutador.

Etapa 3. Faça login na interface do controlador de gerenciamento.

Dica: para comutadores Flex, usa suas credenciais de usuário do XClarity Administrator. Para comutadores XClarity Administrator, use as credenciais do comutador.

Iniciando uma sessão remota de SSH de um comutador

Você pode iniciar uma sessão remota de SSH para um comutador gerenciado RackSwitch ou Flex no Lenovo XClarity Administrator. Na sessão remota de SSH, é possível usar a interface da linha de comandos para executar tarefas de gerenciamento que não são fornecidas pelo XClarity Administrator.

Antes de iniciar

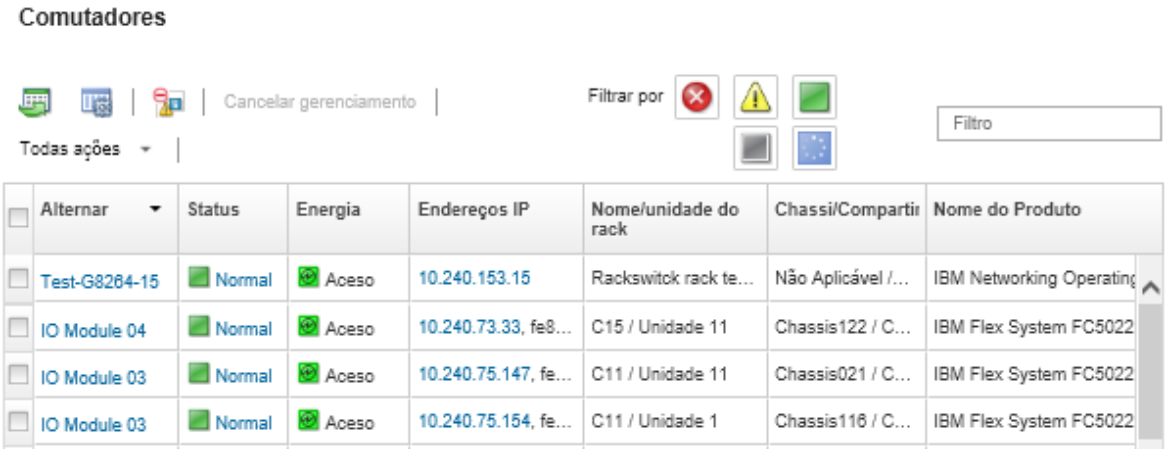
Verifique se o comutador está configurado para ativar SSH. Para comutadores RackSwitch, SSH é ativado quando o comutador é gerenciado pelo XClarity Administrator. Para comutadores Flex, SSH é normalmente ativado por padrão. Se não ativado, SSH deve ser ativado antes que o comutador seja gerenciado por XClarity Administrator.

Procedimento

Conclua as seguintes etapas para iniciar uma sessão remota de SSH para um comutador gerenciado.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Comutadores**. A página Comutadores é exibida com uma exibição tabular de todos os comutadores que estão instalados no chassi gerenciado.

É possível classificar as colunas da tabela para facilitar a localização dos comutadores que deseja gerenciar. Além disso, digite texto (como um nome ou endereço IP) no campo **Filtro** para filtrar mais comutadores que são exibidos.



Etapa 2. Selecione o comutador para iniciar uma sessão de SSH.

Etapa 3. Clique em **Todas as Ações → Iniciar → Console SSH**.

Etapa 4. Se necessário, faça login no comutador usando seu ID de usuário e senha.

Alterando as propriedades do sistema para um comutador

É possível alterar as propriedades do sistema para um determinado comutador Flex System ou RackSwitch.

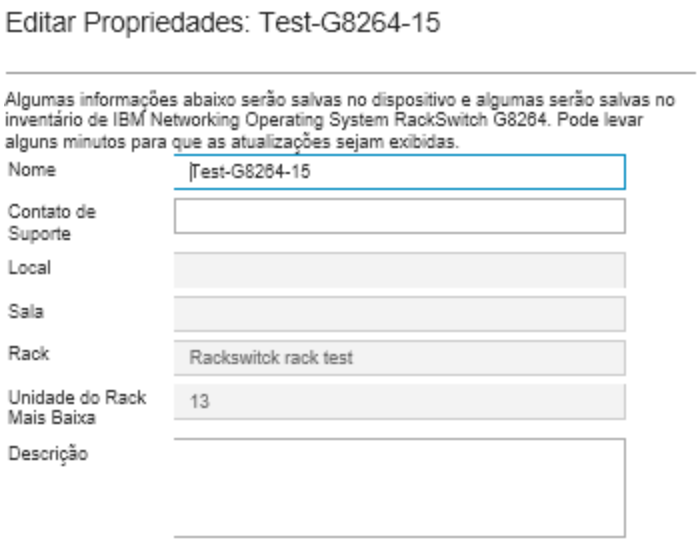
Procedimento

Conclua as etapas a seguir para alterar as propriedades do sistema.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Comutadores** para exibir a página Comutadores.

Etapa 2. Selecione o comutador a ser atualizado.

Etapa 3. Clique em **Todas as Ações → Inventário → Editar Propriedades** para exibir a caixa de diálogo Editar.



Etapa 4. Altere as seguintes informações, conforme necessário.
- Nome do comutador
- Contato de suporte
- Descrição

Nota: As propriedades de local, sala, rack e menor unidade do rack são atualizadas pelo XClarity Administrator ao incluir ou remover dispositivos de um rack na interface da Web (consulte Gerenciando racks).

Etapa 5. Clique em **Salvar**.

Nota: Quando você altera essas propriedades, pode haver um pequeno atraso até as alterações aparecerem na interface da Web do XClarity Administrator.

Resolvendo credenciais armazenadas expiradas ou inválidas para um comutador

Quando uma credencial armazenada expira ou fica inoperante em um dispositivo, o status desse dispositivo é mostrado como "Offline".

Procedimento

Para resolver uma credencial armazenada expirada ou inválida para um comutador, conclua as etapas a seguir.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Comutadores**. A página Comutadores é exibida com uma exibição tabular de todos os comutadores gerenciados.

Etapa 2. Clique no cabeçalho da coluna **Energia** para agrupar todos os comutadores offline na parte superior da tabela.

É possível classificar as colunas da tabela para facilitar a localização dos comutadores que deseja gerenciar. Além disso, é possível digitar texto (como um nome de sistema ou endereço IP) no campo **Filtro** para filtrar mais comutadores que são exibidos.

Etapa 3. Selecione o comutador a ser resolvido.

Etapa 4. Clique em **Todas as Ações → Segurança → Editar Credenciais Armazenadas**.

Etapa 5. Altere a senha para a credencial armazenada ou selecione outra credencial armazenada a ser usada para o dispositivo gerenciado.

Nota: Se você gerenciou mais de um dispositivo usando as mesmas credenciais armazenadas e alterar a senha para as credenciais armazenadas, essa alteração de senha afetará todos os dispositivos que atualmente são usando as credenciais armazenadas.

Recuperando o gerenciamento com um comutador após uma falha no servidor de gerenciamento

É possível recuperar o gerenciamento de um comutador cujo gerenciamento não foi cancelado corretamente (por exemplo, devido a problemas de conectividade durante o cancelamento do gerenciamento ou falha no gerenciamento do Lenovo XClarity Administrator).

Procedimento

- Gerencie o comutador novamente usando a opção **Forçar gerenciamento** (consulte Gerenciando comutadores).
- Para remover permanentemente a configuração específica do XClarity Administrator em um comutador cujo gerenciamento não foi cancelado corretamente e não será gerenciado novamente, conclua estas etapas.
  - Gerencie o comutador novamente usando a opção **Forçar gerenciamento** (consulte Gerenciando comutadores) e, em seguida, cancele o gerenciamento do comutador para apagar a configuração (consulte Cancelando o gerenciamento de um comutador).
  - (ENOS) Faça login no comutador usando a porta do console do comutador ou uma sessão SSH ou telnet, e execute os seguintes comandos de configuração na ordem especificada para apagar a configuração do comutador.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

Cancelando o gerenciamento de um comutador

É possível remover um comutador do gerenciamento do Lenovo XClarity Administrator. Esse processo é chamado de *cancelamento de gerenciamento*.

Antes de iniciar

É possível habilitar o XClarity Administrator para cancelar automaticamente o gerenciamento de dispositivos que estão offline por um período específico. Isso é desativado por padrão. Para habilitar o cancelamento de gerenciamento automático de dispositivos offline, clique em **Hardware → Descobrir e Gerenciar Novos Dispositivos** no menu do XClarity Administrator e, em seguida, clique em **Editar** próximo a **Cancelamento de gerenciamento de dispositivos está desabilitado**. Em seguida, selecione **Habilitar cancelamento de gerenciamento de dispositivos offline** e defina o intervalo de tempo. Por padrão, o gerenciamento dos dispositivos são cancelados após estarem offline por 24 horas.

Antes de cancelar o gerenciamento de um comutador, verifique se não há trabalhos ativos em execução no comutador.

Sobre esta tarefa

Quando o gerenciamento de um comutador é cancelado, o XClarity Administrator retém determinadas informações sobre o comutador. Essa informação é reaplicada ao gerenciar o mesmo comutador novamente.

Dica: todos os dispositivos de demonstração que são incluídos opcionalmente durante a configuração inicial são nós em um chassi. Para cancelar o gerenciamento dos dispositivos da demonstração, cancele o gerenciamento do chassi usando a opção **Forçar cancelamento de gerenciamento mesmo se o dispositivo não estiver acessível**.

Procedimento

Para cancelar o gerenciamento de um comutador, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Hardware → Comutadores** para exibir a página Comutadores.

Etapa 2. Selecione um ou mais comutadores na lista de comutadores gerenciados.

Etapa 3. Clique em **Cancelar Gerenciamento de Comutador**. A caixa de diálogo Cancelar gerenciamento é exibida.

Etapa 4. **Opcional:** selecione **Forçar cancelamento de gerenciamento mesmo se o dispositivo não estiver acessível**.

Importante: Ao cancelar o gerenciamento do hardware da demonstração, selecione essa opção.

Etapa 5. Clique em **Cancelar Gerenciamento**.A caixa de diálogo Cancelar gerenciamento mostra o progresso de cada etapa no processo de cancelamento de gerenciamento.

Etapa 6. Quando esse processo for concluído, clique em **OK**.

Recuperando um comutador cujo gerenciamento não foi cancelado corretamente

Se um comutador estiver sendo gerenciado pelo Lenovo XClarity Administrator e se o XClarity Administrator falhar, será possível recuperar as funções de gerenciamento até que o servidor de gerenciamento seja restaurado ou substituído.

Procedimento

- Gerencie o comutador novamente usando a opção **Forçar gerenciamento** (consulte Gerenciando comutadores).
- Para remover permanentemente a configuração específica do XClarity Administrator em um comutador cujo gerenciamento não foi cancelado corretamente e não será gerenciado novamente, conclua estas etapas.
  - Gerencie o comutador novamente usando a opção **Forçar gerenciamento** (consulte Gerenciando comutadores) e, em seguida, cancele o gerenciamento do comutador para apagar a configuração (consulte Cancelando o gerenciamento de um comutador).
  - (ENOS) Faça login no comutador usando a porta do console do comutador ou uma sessão SSH ou telnet, e execute os seguintes comandos de configuração na ordem especificada para apagar a configuração do comutador.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

Capítulo 11. Configurando servidores com padrões de configuração

Os padrões de servidor são usados para fornecer rapidamente ou fornecer previamente diversos servidores (servidores de rack e em torre e nós de cálculo) de um conjunto único de definições de configurações.

Saiba mais:

- XClarity Administrator: bare metal para cluster
- XClarity Administrator: padrões de configuração

Antes de iniciar

Após o teste gratuito de 90 dias, é possível continuar a usar o XClarity Administrator para gerenciar e monitorar seu hardware gratuitamente; entretanto, você deve comprar licenças de habilitação com funcionalidade completa para cada servidor que ofereça suporte a funções avançadas do XClarity Administrator para continuar a usar a função de configuração do servidor. O Lenovo XClarity Pro fornece direito ao serviço e suporte e a licença de habilitação com funcionalidade completa. Para obter mais informações sobre a aquisição do Lenovo XClarity Pro, entre em contato com seu representante Lenovo ou o parceiro de negócios autorizado. Para obter mais informações, consulte Instalando a licença de habilitação com funcionalidade completa na documentação online do XClarity Administrator.

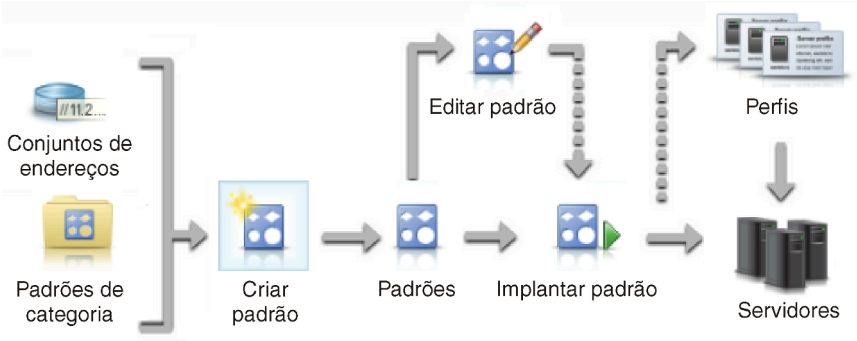
Revise Considerações sobre configuração para obter informações importantes sobre o suporte de configuração para servidores e dispositivos específicos.

Sobre esta tarefa

É possível usar padrões de servidor no XClarity Administrator para configurar o armazenamento local, adaptadores de E/S, ordem de inicialização e outras configurações de Baseboard Management Controller e de Unified Extensible Firmware Interface (UEFI) nos servidores gerenciados. Os padrões de servidor também integram suporte para virtualizar endereços de E/S. Assim, é possível virtualizar conexões de malha do servidor ou redefinir servidores sem interromper a malha. Também é possível iniciar solicitações de alteração de zoneamento de SAN antes de receber o novo hardware, virtualizando endereços de Fibre Channel (pré-configurando).

Procedimento

A figura a seguir ilustra o fluxo de trabalho para configurar servidores gerenciados. As setas contínuas indicam as ações executadas por você. As setas tracejadas indicam as ações que são executadas automaticamente por XClarity Administrator.



Etapa 1. **Criar um conjunto de endereços.**Um *conjunto de endereços* é um conjunto definido de intervalos de endereços. O Lenovo XClarity Administrator usa conjuntos de endereços para atribuir endereços IP e de E/S para servidores individuais quando os padrões de servidor são implantados para esses servidores.

Para obter mais informações sobre criação de conjuntos de endereços, consulte Definindo conjuntos de endereços.

Etapa 2. **Criar padrões de categoria.**

Um *padrão de categoria* agrupa configurações de firmware relacionadas e que podem ser reutilizadas por vários padrões de servidor. É possível criar padrões para as seguintes categorias de firmware:

- Informações do sistema
- Interfaces de gerenciamento
- Dispositivos e portas de E/S
- Destinos de inicialização FC
- Portas do adaptador de E/S

Para obter mais informações sobre esses padrões de categoria, consulte Trabalhando com padrões de servidor.

Etapa 3. **Criar um padrão de servidor.**

Um *padrão de servidor* representa configurações de servidor pré-sistema operacional, incluindo configurações de armazenamento local, configurações de adaptador de E/S, configuração de inicialização e outras configurações do Baseboard Management Controller e de firmware UEFI. Um padrão de servidor é usado como um padrão global para configurar rapidamente vários servidores de uma vez.

É possível definir vários padrões de servidor para representar as diferentes configurações usadas em seu datacenter.

Ao definir um padrão de servidor, selecione padrões de categoria e conjuntos de endereços conforme necessário para construir a configuração desejada para um grupo específico de servidores. Um padrão de categoria agrupa configurações relacionadas que podem ser reutilizadas por vários padrões de servidor.

É possível criar um padrão de servidor do zero para servidores Converged, Flex System, NeXtScale e System x para configurar a configuração desejada antes do hardware chegar. Ou, é possível criar um padrão de servidor em um servidor gerenciado existente. Ao criar um padrão de servidor a partir de um servidor existente, o XClarity Administrator aprende padrões de categoria do servidor selecionado.

Para obter mais informações sobre como criar padrões de servidor, consulte Criando um padrão de servidor.

Etapa 4. **Implantar o padrão de servidor.**

Você pode implantar um padrão de servidor em um ou mais servidores individuais ou em grupos de servidores. Por exemplo, você pode implantar um padrão de servidor em um chassi para que todos os nós de cálculo daquele chassi tenham a mesma configuração. Durante a implantação, o XClarity Administrator cria um perfil de servidor para cada servidor o qual o padrão de servidor foi implementado. Cada *perfil de servidor* representa a configuração específica de um único servidor. Isto herda as configurações do padrão de servidor e também contém informações específicas do servidor (como endereços IP e endereços MAC atribuídos). Como o perfil de servidor herda configurações do padrão de servidor, se você alterar o padrão de servidor, as mudanças são

atualizadas automaticamente no perfil de servidor. Desta forma, é possível manter as configurações comuns em um local.

Nota: As configurações em um servidor poderão ficar fora de conformidade com o perfil de servidor se as configurações forem alteradas sem usar Padrões de Configuração ou se tiver ocorrido um problema durante a implantação, como um problema de firmware ou uma configuração inválida. É possível determinar o status de conformidade de cada servidor na página Padrões de Configuração: Perfis de Servidor.

É possível implantar um padrão de servidor em:

- **Servidores existentes**. Um perfil de servidor é criado para cada servidor. O perfil de servidor é ativado após o servidor associado ser reinicializado.
- **Compartimentos vazios em um chassi existente**. Um perfil de servidor é criado para cada compartimento vazio. O perfil de servidor associado com o compartimento vazio pode, então, ser ativado após o nó de cálculo ser instalado fisicamente.
- **Marcador de um chassi que você ainda não tem**. É possível fornecer nós de cálculo em um chassi que você ainda não tem, definindo um *chassi de marcador* para agir como destino para o padrão de servidor antes do hardware físico chegar. O chassi de marcador reúne todos os perfis de servidor criados para cada compartimento de nó de cálculo vazio. Assim, quando o hardware chega, é possível atribuir os perfis de servidor a todos os nós de cálculo no novo chassi, implantando o chassi de marcador para o novo chassi. Cada perfil de servidor é ativado após o nó de cálculo associado ser reinicializado.

Nota: É possível implantar um padrão de servidor em diversos servidores. Entretanto, diversos padrões não podem ser implantados em um único servidor.

Para obter mais informações sobre a implantação de um padrão de servidor, consulte Implantando um padrão de servidor em um servidor e Implantando um chassi de marcador.

Etapa 5. **Editar o padrão de servidor.**

Você usa os padrões de servidor para controlar uma configuração comum a partir de um único local. Você não precisa mais atualizar as configurações diretamente nos servidores. Ao invés disso, é possível atualizar os padrões de categoria e de servidor, e as alterações serão implantadas automaticamente em todos os perfis associados e em seus servidores.

Para obter mais informações sobre a edição de um padrão de servidor, consulte Alterando um padrão de servidor.

Considerações sobre configuração

Antes de iniciar a configuração dos servidores através do Lenovo XClarity Administrator, revise as seguintes considerações importantes.

- Se um perfil de servidor incluir níveis de firmware anteriores e você atualizar o firmware para níveis mais recentes, o XClarity Administrator vai comparar as configurações de perfil armazenadas com as configurações do servidor e relatar "Não Conforme". Passe o cursor sobre o status "Não Conforme" para determinar o motivo da não conformidade.

  É possível alterar manualmente o status de dispositivos Não Conformes para "Compatíveis" sem reimplantar o perfil selecionando os dispositivos e, em seguida, clicando em **Todas as Ações → Deixar em conformidade**.
- Depois de atualizar o firmware (como UEFI, BMC ou controladores de E/S) em um servidor, algumas configurações podem ser alteradas (por exemplo, ao incluir novos itens, excluir itens existentes ou alterar os comportamentos ou o intervalo de valores de um item). Como resultado, o perfil de servidor pode se tornar não conforme ou a aplicação do padrão de servidor poderá falhar se for criado usando um nível de firmware anterior. Nesse caso, é recomendável escolher aprender um novo padrão com base no firmware atualizado ou editar o padrão com falha para excluir a configuração de itens específicos e, em seguida, aplicar esse padrão ao servidor.
- O adaptador QLogic 8200 2-Port 10 GbE SFP + VFA tem valores inválidos para estas configurações: iSCSIFirstTargetParameters_iSCSIName, iSCSISecondTargetParameters_iSCSIName e IPv6LinkLocalAddress. Você deve corrigir manualmente esses valores na configuração do sistema antes de aprender o padrão de configuração a partir do servidor ou corrigir os valores no padrão de configuração aprendido.
- Para Flex System x240 e x440 Nós de Cálculo com adaptadores RAID integrados, os padrões de servidor que definem as configurações do RAID só podem ser implantados em um ou mais servidores que não têm configurações do RAID. Se um padrão de servidor for implantado em um servidor que tenha uma configuração de RAID existente, as matrizes e os volumes existentes não serão sobrescritos. Para aplicar a configuração do RAID definida no padrão de servidor, primeiro você deverá limpar a configuração do RAID existentes no servidores (consulte Redefinição de adaptadores de armazenamento para os valores padrão) e, em seguida, implemente novamente o perfil de servidor selecionando o servidor e clicando em **Mais → Implantar Perfil de Servidor**.
- Os controladores de armazenamento integrados nos servidores Flex System x220, Flex System x222 e ThinkSystem suportam RAID baseado em software. No entanto, não há suporte para a configuração de RAID de software usando Padrões de Configuração.
- Ao configurar o RAID usando o Padrões de Configuração, se o servidor for desligado, o servidor será iniciado na configuração BIOS/UEFI automaticamente antes de ativar o perfil de servidor.
- Para servidores ThinkServer, o Padrões de Configuração não é suportado.
- Determinados dispositivos de E/S não podem ser configurados usando padrões de servidor. Para obter mais informações, consulte Página da Web Suporte do XClarity Administrator – Compatibilidade.
- Se os recursos avançados (como o SPAR, Easy Connect e pilha) são ativados nos comutadores Flex EN4093R, CN4093, SI4091 ou SI4093, as configurações de rede podem não ser aplicadas corretamente em portas internas.
- Por padrão, o comutador Flex SI4093 é enviado com o SPAR habilitado. Se deseja implantar as configurações de rede usando os padrões da porta nas portas internas nesses comutadores, você precisará remover as portas internas do comutador do SPAR ou remover as configurações do SPAR do comutador.
- É recomendado que *não* use o XClarity Administrator para configurar dispositivos Converged e ThinkAgile usando os Padrões de Configuração.
- Certifique-se de que todas as portas disponíveis sejam ativadas nos adaptadores instalados antes de criar padrões de configuração de um servidor existente, para que todas as portas e configurações disponíveis sejam incluídas no padrão. Em seguida, se necessário, é possível desativar qualquer porta usando as configurações apropriadas definidas no padrão. Se as portas estiverem desativadas quando o padrão for criado, o padrão não poderá ser criado corretamente e implantado com êxito.

Definindo conjuntos de endereços

Um *conjunto de endereços* é um conjunto definido de intervalos de endereços. O Lenovo XClarity Administrator usa conjuntos de endereços para atribuir endereços IP e de E/S para servidores individuais quando os padrões de servidor são implantados para esses servidores.

Sobre esta tarefa

O XClarity Administrator suporta conjuntos de endereços IP e de E/S.

conjuntos de endereços IP

Os *conjuntos de endereços IP* definem intervalos de endereços IP para uso ao configurar a interface de rede do Baseboard Management Controller dos seus servidores. É possível usar ou personalizar conjuntos de endereços predefinidos ou criar novos conjuntos conforme necessário. Ao criar padrões de servidor, é possível escolher qual conjunto de endereços IP a ser usado durante a implantação. Quando o padrão de servidor é implantado, os endereços IP são alocados a partir do conjunto selecionado e atribuídos aos controladores de gerenciamento individuais.

Nota: Se estiver satisfeito com sua configuração de rede do controlador de gerenciamento, não use essa opção.

Atenção:

- Certifique-se de selecionar um subintervalo de endereços IP que não entre em conflito com endereços de E/S existentes em seu datacenter.
- Certifique-se que os endereços IP em intervalos especificados sejam da parte da mesma sub-rede e estejam alcançáveis pelo XClarity Administrator.
- Certifique-se que os endereços IP nos intervalos certificados são exclusivos para cada domínio XClarity Administrator e ferramentas de gerenciamento de IP existentes para evitarem conflitos de endereços.

O intervalo de conjunto de endereços global é derivado do comprimento do prefixo de roteamento e do gateway ou do intervalo inicial. Você pode criar conjuntos de diferentes tamanhos com base no comprimento do prefixo de roteamento específico, mas os intervalos de conjunto globais devem ser exclusivos dentro do domínio XClarity Administrator. Os intervalos são então criados a partir do intervalo de conjunto global.

Os intervalos de endereços também podem ser usados para hosts separados (por exemplo, por tipo de sistema operacional, de carga de trabalho e de negócios). Os intervalos de endereço também podem ser amarrados às regras organizacionais de rede.

conjuntos de endereços Ethernet

Os *conjuntos de endereços Ethernet* são coleções de endereços MAC exclusivos que podem ser atribuídos a adaptadores de rede ao configurar os servidores. É possível usar ou personalizar conjuntos de endereços predefinidos conforme necessário ou criar novos conjuntos. Ao criar padrões de servidor, é possível escolher qual conjunto de endereços Ethernet deverá ser usado durante a implantação. Quando o padrão de servidor é implantado, os endereços são alocados a partir do conjunto selecionado e atribuídos às portas dos adaptadores individuais.

O seguinte conjunto predefinido de endereços MAC está disponível:

- Conjunto de endereços Lenovo MAC

Para uma lista de intervalos de endereços MAC neste conjunto, consulte Conjuntos de endereços Ethernet (MAC).

conjuntos de endereços do Fibre Channel

Os *conjuntos de endereços de Fibre Channel* são coleções de endereços WWNN e WWPN exclusivos que podem ser atribuídos aos adaptadores Fibre Channel ao configurar os servidores. É possível usar ou personalizar conjuntos de endereços predefinidos conforme necessário ou criar novos conjuntos. Ao criar padrões de servidor, é possível escolher qual conjunto de endereços do Fibre Channel deverá ser usado durante a implantação. Quando o padrão de servidor é implantado, os endereços são alocados a partir do conjunto selecionado e atribuídos às portas dos adaptadores individuais.

Os seguintes conjuntos de endereços do Fibre Channel predefinidos estão disponíveis:

- Endereços WWN Lenovo
- Endereços WWN Brocade
- Endereços WWN Emulex
- Endereços WWN QLogic

Para uma lista de intervalos de endereços WWN neste conjunto, consulte Conjuntos de endereços (WWN) do Fibre Channel.

O intervalo de endereços nos conjuntos de endereço devem ser exclusivos dentro do domínio XClarity Administrator. O XClarity Administrator certifica-se de que os intervalos definidos e os endereços atribuídos são exclusivos em seu domínio de gerenciamento.

Importante: Em um ambiente grande com diversas instâncias do XClarity Administrator, certifique-se de que os conjuntos de endereços exclusivos são usados por cada XClarity Administrator para evitar a duplicação de endereço.

Os conjuntos de endereços do Fibre Channel e Ethernet são usados com endereçamento virtual do adaptador de E/S para atribuir endereços organizacionais exclusivos de E/S. Ao criar um padrão de servidor em um nó de cálculo, é possível ativar o endereçamento virtual como parte da configuração de adaptadores de E/S e dispositivos. Quando o endereçamento virtual é ativado, os endereços são atribuídos a partir de conjuntos de endereços do Fibre Channel e Ethernet para evitar conflitos de endereços.

Restrição: o endereçamento virtual é suportado somente para nós de cálculo Flex System. Servidores independentes de rack e em torre não são aceitos.

Para obter informações sobre como criar padrões de servidor, consulte Criando um padrão de servidor.

Criando um conjunto de endereços IP

Um *Conjunto de endereços IP* define um intervalo de endereços IP para uso ao configurar a interface de rede do Baseboard Management Controller dos seus servidores. Quando o padrão de servidor associado é implantado, os endereços IP são alocados a partir do conjunto especificado e atribuídos a servidores individuais.

Sobre esta tarefa

Os dados na tabela de Informações Gerais de Rede na caixa de diálogo Novo Conjunto de Endereços IP são derivados da máscara de sub-rede e gateway especificados ou do intervalo inicial. Você pode criar conjuntos de diferentes tamanhos com base na máscara de sub-rede específica, mas os intervalos de conjunto globais devem ser exclusivos dentro do domínio de gerenciamento. Os intervalos são então criados a partir do intervalo de conjunto global. Todos os intervalos devem fazer parte da mesma sub-rede e são delimitados pelos limites mostrados na tabela Informações Gerais de Rede.

O conjunto e os intervalos têm escopo do Lenovo XClarity Administrator. Em um ambiente grande com diversas instâncias do XClarity Administrator, crie conjuntos e intervalos exclusivos para cada XClarity Administrator para evitar conflitos de endereço com ferramentas de gerenciamento IP existentes. Os

intervalos também podem ser usados para hosts separados (por exemplo, por tipo de sistema operacional, tipo de carga de trabalho e função de negócios) e para vincular as regras organizacionais de rede.

Procedimento

Conclua as seguintes etapas para criar um conjunto de endereços IP:

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Conjuntos de Endereços**. A página Padrões de Configuração: Conjuntos de Endereços é exibida.

Etapa 2. Clique na guia **Conjuntos de endereços IP**.

Etapa 3. Clique no ícone **Criar** ( ). A caixa de diálogo Assistente de Novos Conjuntos de Endereços IP é exibida.

Etapa 4. Preencha as seguintes informações.

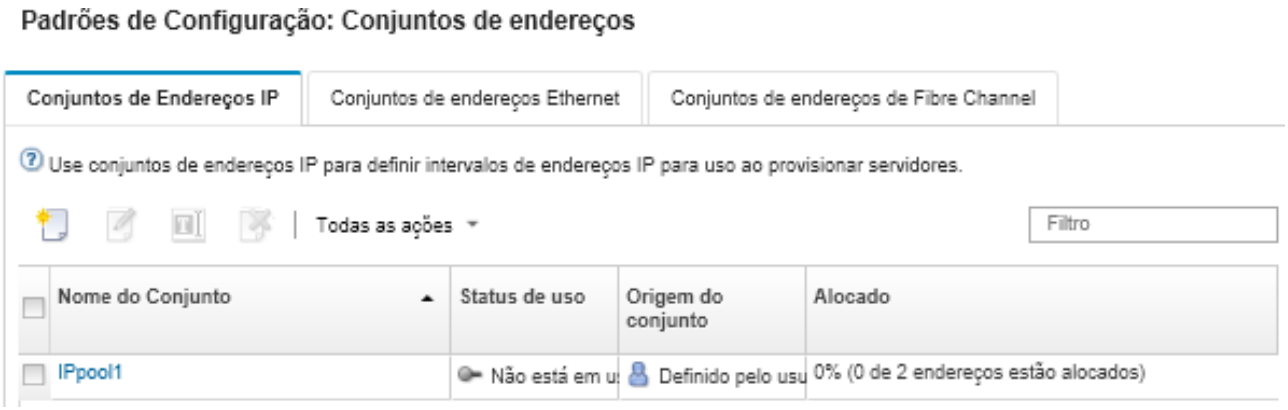
- Nome e descrição do conjunto de endereços.
- Escolha entre usar endereços IPv4 ou IPv6.
- Selecione uma máscara de sub-rede (para IPv4) ou um comprimento de prefixo de roteamento (para IPv6).
- Especifique o endereço do gateway.Os valores das informações de rede são derivados da máscara de sub-rede e gateway especificados ou do intervalo inicial são preenchidos na tabela.
- Adicione um ou mais intervalos de endereços:
  1. Clique em **Adicionar Intervalo** para adicionar um intervalo de endereços. A caixa de diálogo Adicionar Novo Intervalo de Endereços IP é exibida.
  2. Insira um nome do intervalo, primeiro endereço e um tamanho do intervalo.O último endereço é calculado automaticamente.
  3. Clique em **OK**.O intervalo é adicionado à tabela **Definir intervalos do conjunto de endereços IP** e os campos na seção resumida são atualizados automaticamente.

  É possível editar o intervalo clicando no ícone **Editar** ( ) remover o intervalo, clicando no ícone **Remover** ( ).

Etapa 5. Clique em **Criar**.

Depois de concluir

O novo conjunto de endereços IP é listado na tabela na página Conjuntos de Endereços IP:



Nesta página, é possível executar as ações a seguir em um conjunto de endereços selecionado:

- Alterar o conjunto de endereços clicando no ícone **Editar** ( ).
- Renomear o conjunto de endereços clicando no ícone **Renomear**.
- Excluir o conjunto de endereços clicando no ícone **Excluir** ( ).
- Exiba detalhes sobre o conjunto de endereços, incluindo um mapeamento entre os endereços virtuais e as portas do adaptador instalado e os endereços virtuais reservados, clicando no nome de conjunto na coluna **Nome de Conjunto**.

Criando um conjunto de endereços Ethernet

Os *conjuntos de endereços Ethernet* são coleções de endereços exclusivos de controle de acesso de mídia (MAC) que podem ser atribuídos a adaptadores de rede. É possível usar ou personalizar conjuntos de endereços predefinidos conforme necessário ou criar novos conjuntos de endereços. Ao criar um padrão de servidor, se você ativar o endereçamento virtual para adaptadores Ethernet, é possível escolher qual conjunto de endereços Ethernet deve ser usado quando o padrão é implantado. Quando o padrão de servidor associado é implantado, os endereços MAC são alocados a partir do conjunto de endereços selecionado e atribuídos a adaptadores de rede nos servidores.

Procedimento

Conclua as seguintes etapas para criar um conjunto de endereços Ethernet:

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Conjuntos de Endereços**. A página Padrões de Configuração: Conjuntos de Endereços é exibida.

Etapa 2. Clique na guia **Conjuntos de endereços Ethernet**.

Etapa 3. Clique no ícone **Criar** ( ). A caixa de diálogo Novos Conjuntos de Endereços Ethernet (MAC) é exibida.

Etapa 4. Digite um nome e descrição do conjunto de endereços.

Etapa 5. Adicione um ou mais intervalos de endereços:

a. Clique em **Adicionar Intervalo** para adicionar um intervalo de endereços. A caixa de diálogo Intervalo de Endereço Ethernet (MAC) é exibida.

b. Insira um nome do intervalo, endereço MAC primeiro e um tamanho do intervalo.

O último endereço MAC é calculado automaticamente.

c. Clique em **Adicionar**.

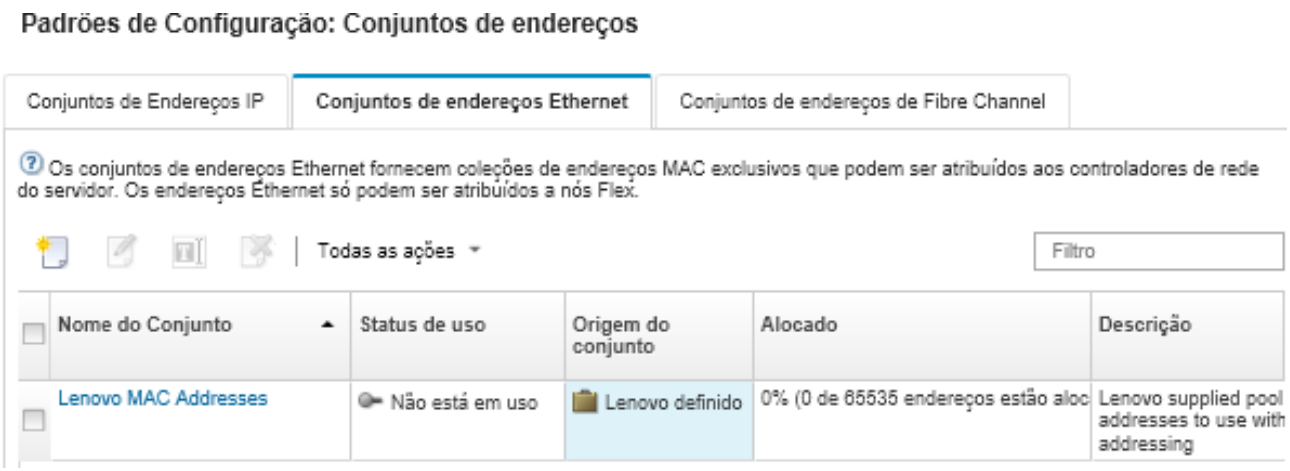
O intervalo é adicionado à tabela **Definir intervalos de conjunto de endereços Ethernet (MAC)** e os campos na seção resumida são atualizados automaticamente.

É possível editar o intervalo clicando no ícone **Editar** ( ) remover o intervalo, clicando no ícone **Remover** ( ).

Etapa 6. Clique em **Salvar**.

Depois de concluir

O novo conjunto de endereços Ethernet é listado na página Conjuntos de Endereços Ethernet.



Nesta página, é possível executar as ações a seguir em um conjunto de endereços selecionado:

- Alterar o conjunto de endereços clicando no ícone **Editar** ( ).
- Renomear o conjunto de endereços clicando no ícone **Renomear**.
- Excluir o conjunto de endereços clicando no ícone **Excluir** ( ).
- Exiba detalhes sobre o conjunto de endereços, incluindo um mapeamento entre os endereços virtuais e as portas do adaptador instalado e os endereços virtuais reservados, clicando no nome de conjunto na coluna **Nome de Conjunto**.

Conjuntos de endereços Ethernet (MAC)

Conjuntos de endereços Ethernet são coleções de endereços exclusivos de controle de acesso de mídia (MAC) que podem ser atribuídos a adaptadores de rede. É possível usar o seguinte conjunto de endereços predefinido nos padrões de servidor.

Tabela 3. Conjunto de endereços Lenovo MAC

Intervalo predefinido	Endereço inicial	Endereço final
Intervalo 1	00:1A:64:76:00:00	00:1A:64:76:1C:70
Intervalo 2	00:1A:64:76:1C:71	00:1A:64:76:38:E1
Intervalo 3	00:1A:64:76:38:E2	00:1A:64:76:55:52
Intervalo 4	00:1A:64:76:55:53	00:1A:64:76:71:C3
Intervalo 5	00:1A:64:76:71:C4	00:1A:64:76:8E:34
Intervalo 6	00:1A:64:76:8E:35	00:1A:64:76:AA:A5
Intervalo 7	00:1A:64:76:AA:A6	00:1A:64:76:C7:16
Intervalo 8	00:1A:64:76:C7:17	00:1A:64:76:E3:87
Intervalo 9	00:1A:64:76:E3:88	00:1A:64:76:FF:F8

Criando um conjunto de endereços do Fibre Channel

Os *conjuntos de endereços do Fibre Channel* são coleções de endereços World Wide Node Name (WWNN) e World Wide Port Name (WWPN) exclusivos que podem ser atribuídos a adaptadores de Fibre Channel. É possível usar ou personalizar conjuntos de endereços predefinidos conforme necessário ou criar novos conjuntos. Ao criar padrões de servidor, se você ativar o endereçamento virtual para adaptadores Ethernet, é possível escolher qual conjunto de endereços do Fibre Channel deve ser usado quando o padrão é implantado. Quando o padrão de servidor associado é implantado, os endereços WWNN e WWPN são alocados a partir do conjunto e atribuídos a servidores individuais.

Procedimento

Conclua as seguintes etapas para criar um conjunto de endereços do Fibre Channel:

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Conjuntos de Endereços**. A página Padrões de Configuração: Conjuntos de Endereços é exibida.

Etapa 2. Clique na guia **Conjuntos de endereços do Fibre Channel**.

Etapa 3. Clique no ícone **Criar** ( ). A caixa de diálogo Conjuntos de Endereços do Fibre Channel é exibida.

Etapa 4. Digite um nome e descrição do conjunto de endereços.

Etapa 5. Adicione um ou mais intervalos de endereços:

a. Clique em **Adicionar Intervalo** para adicionar um intervalo de endereços. A caixa de diálogo Intervalo de Endereços (WWN) do Fibre Channel é exibida.

b. Insira um nome do intervalo, tamanho do intervalo e o primeiro endereço de cada malha.

Os últimos endereços são calculado automaticamente.

c. Clique em **Adicionar**.

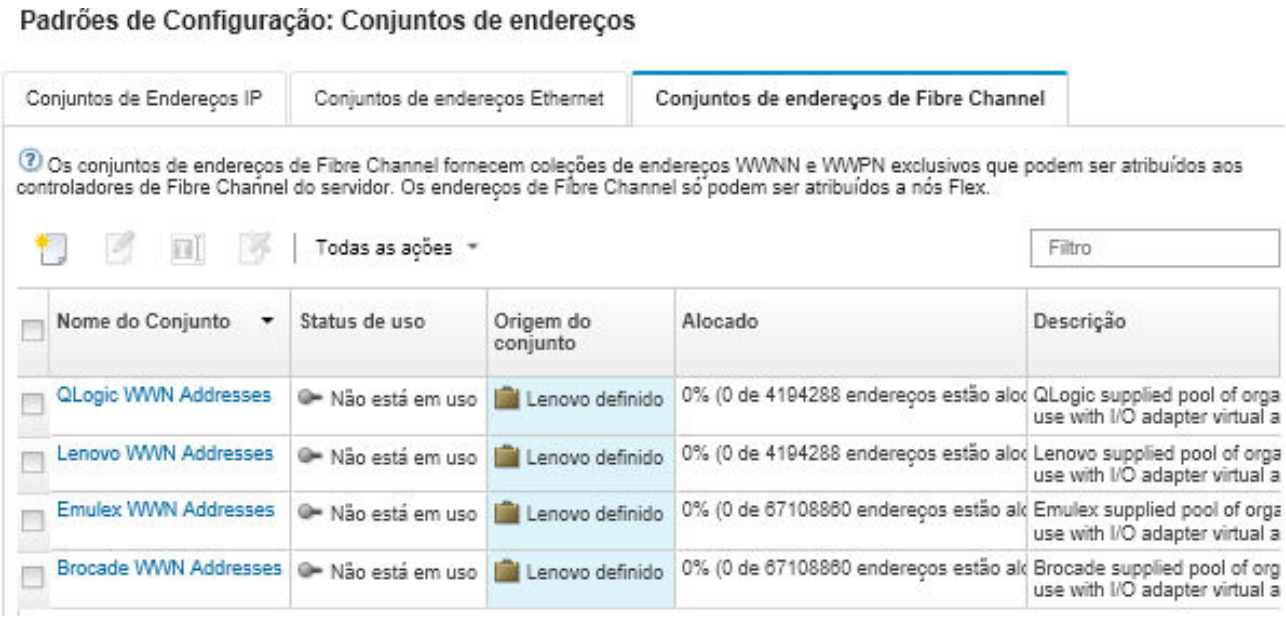
O intervalo é adicionado na tabela **Definir intervalos de conjunto de endereços do Fibre Channel** e os campos na seção resumida são atualizados automaticamente.

É possível editar o intervalo clicando no ícone **Editar** ( ) remover o intervalo, clicando no ícone **Remover** ( ).

Etapa 6. Clique em **Salvar**.

Depois de concluir

O novo conjunto de endereços do Fibre Channel é listado na tabela Conjuntos de Endereços de Fibre Channel.



Nesta página, é possível executar as ações a seguir em um conjunto de endereços selecionado:

- Alterar o conjunto de endereços clicando no ícone **Editar** ( ).

- Excluir o conjunto de endereços clicando no ícone **Excluir** ().
- Exiba detalhes sobre o conjunto de endereços, incluindo um mapeamento entre os endereços virtuais e as portas do adaptador instalado e os endereços virtuais reservados, clicando no nome de conjunto na coluna **Nome de Conjunto**.

Conjuntos de endereços (WWN) do Fibre Channel

Conjuntos de endereços do Fibre Channel são coleções de endereços World Wide Node Name (WWNN) e World Wide Port Name (WWPN) exclusivos que podem ser atribuídos a adaptadores de Fibre Channel. É possível usar os seguintes conjuntos de endereços predefinidos nos padrões de servidor.

Tabela 4 "Conjunto de endereços Brocade WWN" na página 345 lista os conjuntos de endereços World Wide Name (WWN) do Brocade. Cada intervalo de Brocade contém 1.864.135 endereços.

Tabela 5 "Conjunto de endereços Emulex WWN" na página 346 lista os conjuntos de endereços WWN do Emulex. Cada intervalo de Emulex contém 1.864.135 endereços.

Tabela 6 "Conjunto de endereços Lenovo WWN" na página 347 lista os conjuntos de endereços WWN do Lenovo. Cada intervalo de Lenovo WWN contém 116.508 endereços.

Tabela 7 "Conjunto de endereços QLogic WWN" na página 348 lista os conjuntos de endereços WWN do QLogic. Cada intervalo de QLogic WWN contém 116.508 endereços.

Tabela 4. Conjunto de endereços Brocade WWN

Intervalo predefinido	Endereço inicial de WWNN	Endereço final de WWNN	Endereço inicial de WWPN	Endereço final de WWPN
Malha A				
Intervalo 1	2B:FA:00:05:1E:00:00:00	2B:FA:00:05:1E:1C:71:C6	2B:FC:00:05:1E:00:00:00	2B:FC:00:05:1E:1C:71:C6
Intervalo 2	2B:FA:00:05:1E:1C:71:C7	2B:FA:00:05:1E:38:E3:8D	2B:FC:00:05:1E:1C:71:C7	2B:FC:00:05:1E:38:E3:8D
Intervalo 3	2B:FA:00:05:1E:38:E3:8E	2B:FA:00:05:1E:55:55:54	2B:FC:00:05:1E:38:E3:8E	2B:FC:00:05:1E:55:55:54
Intervalo 4	2B:FA:00:05:1E:55:55:55	2B:FA:00:05:1E:71:C7:1B	2B:FC:00:05:1E:55:55:55	2B:FC:00:05:1E:71:C7:1B
Intervalo 5	2B:FA:00:05:1E:71:C7:1C	2B:FA:00:05:1E:8E:38:E2	2B:FC:00:05:1E:71:C7:1C	2B:FC:00:05:1E:8E:38:E2
Intervalo 6	2B:FA:00:05:1E:8E:38:E3	2B:FA:00:05:1E:AA:AA:A9	2B:FC:00:05:1E:8E:38:E3	2B:FC:00:05:1E:AA:AA:A9
Intervalo 7	2B:FA:00:05:1E:AA:AA:AA	2B:FA:00:05:1E:C7:1C:70	2B:FC:00:05:1E:AA:AA:AA	2B:FC:00:05:1E:C7:1C:70
Intervalo 8	2B:FA:00:05:1E:C7:1C:71	2B:FA:00:05:1E:E3:8E:37	2B:FC:00:05:1E:C7:1C:71	2B:FC:00:05:1E:E3:8E:37
Intervalo 9	2B:FA:00:05:1E:E3:8E:38	2B:FA:00:05:1E:FF:FF:FE	2B:FC:00:05:1E:E3:8E:38	2B:FC:00:05:1E:FF:FF:FE
Malha B				
Intervalo 1	2B:FB:00:05:1E:00:00:00	2B:FB:00:05:1E:1C:71:C6	2B:FD:00:05:1E:00:00:00	2B:FD:00:05:1E:1C:71:C6
Intervalo 2	2B:FB:00:05:1E:1C:71:C7	2B:FB:00:05:1E:38:E3:8D	2B:FD:00:05:1E:1C:71:C7	2B:FD:00:05:1E:38:E3:8D

Tabela 4. Conjunto de endereços Brocade WWN (continuação)

Intervalo predefinido	Endereço inicial de WWNN	Endereço final de WWNN	Endereço inicial de WWPN	Endereço final de WWPN
Intervalo 3	2B:FB:00:05:1E:38:E3:8E	2B:FB:00:05:1E:55:55:54	2B:FD:00:05:1E:38:E3:8E	2B:FD:00:05:1E:55:55:54
Intervalo 4	2B:FB:00:05:1E:55:55:55	2B:FB:00:05:1E:71:C7:1B	2B:FD:00:05:1E:55:55:55	2B:FD:00:05:1E:71:C7:1B
Intervalo 5	2B:FB:00:05:1E:71:C7:1C	2B:FB:00:05:1E:8E:38:E2	2B:FD:00:05:1E:71:C7:1C	2B:FD:00:05:1E:8E:38:E2
Intervalo 6	2B:FB:00:05:1E:8E:38:E3	2B:FB:00:05:1E:AA:AA:A9	2B:FD:00:05:1E:8E:38:E3	2B:FD:00:05:1E:AA:AA:A9
Intervalo 7	2B:FB:00:05:1E:AA:AA:AA	2B:FB:00:05:1E:C7:1C:70	2B:FD:00:05:1E:AA:AA:AA	2B:FD:00:05:1E:C7:1C:70
Intervalo 8	2B:FB:00:05:1E:C7:1C:71	2B:FB:00:05:1E:E3:8E:37	2B:FD:00:05:1E:C7:1C:71	2B:FD:00:05:1E:E3:8E:37
Intervalo 9	2B:FB:00:05:1E:E3:8E:38	2B:FB:00:05:1E:FF:FF:FE	2B:FD:00:05:1E:E3:8E:38	2B:FD:00:05:1E:FF:FF:FE

Tabela 5. Conjunto de endereços Emulex WWN

Intervalo predefinido	Endereço inicial de WWNN	Endereço final de WWNN	Endereço inicial de WWPN	Endereço final de WWPN
Malha A				
Intervalo 1	2F:FE:00:00:C9:00:00:00	2F:FE:00:00:C9:1C:71:C6	2F:FC:00:00:C9:00:00:00	2F:FC:00:00:C9:1C:71:C6
Intervalo 2	2F:FE:00:00:C9:1C:71:C7	2F:FE:00:00:C9:38:E3:8D	2F:FC:00:00:C9:1C:71:C7	2F:FC:00:00:C9:38:E3:8D
Intervalo 3	2F:FE:00:00:C9:38:E3:8E	2F:FE:00:00:C9:55:55:54	2F:FC:00:00:C9:38:E3:8E	2F:FC:00:00:C9:55:55:54
Intervalo 4	2F:FE:00:00:C9:55:55:55	2F:FE:00:00:C9:71:C7:1B	2F:FC:00:00:C9:55:55:55	2F:FC:00:00:C9:71:C7:1B
Intervalo 5	2F:FE:00:00:C9:71:C7:1C	2F:FE:00:00:C9:8E:38:E2	2F:FC:00:00:C9:71:C7:1C	2F:FC:00:00:C9:8E:38:E2
Intervalo 6	2F:FE:00:00:C9:8E:38:E3	2F:FE:00:00:C9:AA:AA:A9	2F:FC:00:00:C9:8E:38:E3	2F:FC:00:00:C9:AA:AA:A9
Intervalo 7	2F:FE:00:00:C9:AA:AA:AA	2F:FE:00:00:C9:C7:1C:70	2F:FC:00:00:C9:AA:AA:AA	2F:FC:00:00:C9:C7:1C:70
Intervalo 8	2F:FE:00:00:C9:C7:1C:71	2F:FE:00:00:C9:E3:8E:37	2F:FC:00:00:C9:C7:1C:71	2F:FC:00:00:C9:E3:8E:37
Intervalo 9	2F:FE:00:00:C9:E3:8E:38	2F:FE:00:00:C9:FF:FF:FE	2F:FC:00:00:C9:E3:8E:38	2F:FC:00:00:C9:FF:FF:FE
Malha B				
Intervalo 1	2F:FF:00:00:C9:00:00:00	2F:FF:00:00:C9:1C:71:C6	2F:FD:00:00:C9:00:00:00	2F:FD:00:00:C9:1C:71:C6
Intervalo 2	2F:FF:00:00:C9:1C:71:C7	2F:FF:00:00:C9:38:E3:8D	2F:FD:00:00:C9:1C:71:C7	2F:FD:00:00:C9:38:E3:8D

Tabela 5. Conjunto de endereços Emulex WWN (continuação)

Intervalo predefinido	Endereço inicial de WWNN	Endereço final de WWNN	Endereço inicial de WWPN	Endereço final de WWPN
Intervalo 3	2F:FF:00:00:C9:38:E3:8E	2F:FF:00:00:C9:55:55:54	2F:FD:00:00:C9:38:E3:8E	2F:FD:00:00:C9:55:55:54
Intervalo 4	2F:FF:00:00:C9:55:55:55	2F:FF:00:00:C9:71:C7:1B	2F:FD:00:00:C9:55:55:55	2F:FD:00:00:C9:71:C7:1B
Intervalo 5	2F:FF:00:00:C9:71:C7:1C	2F:FF:00:00:C9:8E:38:E2	2F:FD:00:00:C9:71:C7:1C	2F:FD:00:00:C9:8E:38:E2
Intervalo 6	2F:FF:00:00:C9:8E:38:E3	2F:FF:00:00:C9:AA:AA:A9	2F:FD:00:00:C9:8E:38:E3	2F:FD:00:00:C9:AA:AA:A9
Intervalo 7	2F:FF:00:00:C9:AA:AA:AA	2F:FF:00:00:C9:C7:1C:70	2F:FD:00:00:C9:AA:AA:AA	2F:FD:00:00:C9:C7:1C:70
Intervalo 8	2F:FF:00:00:C9:C7:1C:71	2F:FF:00:00:C9:E3:8E:37	2F:FD:00:00:C9:C7:1C:71	2F:FD:00:00:C9:E3:8E:37
Intervalo 9	2F:FF:00:00:C9:E3:8E:38	2F:FF:00:00:C9:FF:FF:FE	2F:FD:00:00:C9:E3:8E:38	2F:FD:00:00:C9:FF:FF:FE

Tabela 6. Conjunto de endereços Lenovo WWN

Intervalo predefinido	Endereço inicial de WWNN	Endereço final de WWNN	Endereço inicial de WWPN	Endereço final de WWPN
Malha A				
Intervalo 1	20:80:00:50:76:00:00:00	20:80:00:50:76:01:C7:1B	21:80:00:50:76:00:00:00	21:80:00:50:76:01:C7:1B
Intervalo 2	20:80:00:50:76:01:C7:1C	20:80:00:50:76:03:8E:37	21:80:00:50:76:01:C7:1C	21:80:00:50:76:03:8E:37
Intervalo 3	20:80:00:50:76:03:8E:38	20:80:00:50:76:05:55:53	21:80:00:50:76:03:8E:38	21:80:00:50:76:05:55:53
Intervalo 4	20:80:00:50:76:05:55:54	20:80:00:50:76:07:1C:6F	21:80:00:50:76:05:55:54	21:80:00:50:76:07:1C:6F
Intervalo 5	20:80:00:50:76:07:1C:70	20:80:00:50:76:08:E3:8B	21:80:00:50:76:07:1C:70	21:80:00:50:76:08:E3:8B
Intervalo 6	20:80:00:50:76:08:E3:8C	20:80:00:50:76:0A:AA:A7	21:80:00:50:76:08:E3:8C	21:80:00:50:76:0A:AA:A7
Intervalo 7	20:80:00:50:76:0A:AA:A8	20:80:00:50:76:0C:71:C3	21:80:00:50:76:0A:AA:A8	21:80:00:50:76:0C:71:C3
Intervalo 8	20:80:00:50:76:0C:71:C4	20:80:00:50:76:0E:38:DF	21:80:00:50:76:0C:71:C4	21:80:00:50:76:0E:38:DF
Intervalo 9	20:80:00:50:76:0E:38:E0	20:80:00:50:76:0F:FF:FB	21:80:00:50:76:0E:38:E0	21:80:00:50:76:0F:FF:FB
Malha B				
Intervalo 1	20:81:00:50:76:20:00:00	20:81:00:50:76:21:C7:1B	21:81:00:50:76:20:00:00	21:81:00:50:76:21:C7:1B
Intervalo 2	20:81:00:50:76:21:C7:1C	20:81:00:50:76:23:8E:37	21:81:00:50:76:21:C7:1C	21:81:00:50:76:23:8E:37

Tabela 6. Conjunto de endereços Lenovo WWN (continuação)

Intervalo predefinido	Endereço inicial de WWNN	Endereço final de WWNN	Endereço inicial de WWPN	Endereço final de WWPN
Intervalo 3	20:81:00:50:76:23:8E:38	20:81:00:50:76:25:55:53	21:81:00:50:76:23:8E:38	21:81:00:50:76:25:55:53
Intervalo 4	20:81:00:50:76:25:55:54	20:81:00:50:76:27:1C:6F	21:81:00:50:76:25:55:54	21:81:00:50:76:27:1C:6F
Intervalo 5	20:81:00:50:76:27:1C:70	20:81:00:50:76:28:E3:8B	21:81:00:50:76:27:1C:70	21:81:00:50:76:28:E3:8B
Intervalo 6	20:81:00:50:76:28:E3:8C	20:81:00:50:76:2A:AA:A7	21:81:00:50:76:28:E3:8C	21:81:00:50:76:2A:AA:A7
Intervalo 7	20:81:00:50:76:2A:AA:A8	20:81:00:50:76:2C:71:C3	21:81:00:50:76:2A:AA:A8	21:81:00:50:76:2C:71:C3
Intervalo 8	20:81:00:50:76:2C:71:C4	20:81:00:50:76:2E:38:DF	21:81:00:50:76:2C:71:C4	21:81:00:50:76:2E:38:DF
Intervalo 9	20:81:00:50:76:2E:38:E0	20:81:00:50:76:2F:FF:FB	21:81:00:50:76:2E:38:E0	21:81:00:50:76:2F:FF:FB

Tabela 7. Conjunto de endereços QLogic WWN

Intervalo predefinido	Endereço inicial de WWNN	Endereço final de WWNN	Endereço final de WWPN	Endereço final de WWPN
Malha A				
Intervalo 1	20:80:00:E0:8B:00:00:00	20:80:00:E0:8B:01:C7:1B	21:80:00:E0:8B:00:00:00	21:80:00:E0:8B:01:C7:1B
Intervalo 2	20:80:00:E0:8B:01:C7:1C	20:80:00:E0:8B:03:8E:37	21:80:00:E0:8B:01:C7:1C	21:80:00:E0:8B:03:8E:37
Intervalo 3	20:80:00:E0:8B:03:8E:38	20:80:00:E0:8B:05:55:53	21:80:00:E0:8B:03:8E:38	21:80:00:E0:8B:05:55:53
Intervalo 4	20:80:00:E0:8B:05:55:54	20:80:00:E0:8B:07:1C:6F	21:80:00:E0:8B:05:55:54	21:80:00:E0:8B:07:1C:6F
Intervalo 5	20:80:00:E0:8B:07:1C:70	20:80:00:E0:8B:08:E3:8B	21:80:00:E0:8B:07:1C:70	21:80:00:E0:8B:08:E3:8B
Intervalo 6	20:80:00:E0:8B:08:E3:8C	20:80:00:E0:8B:0A:AA:A7	21:80:00:E0:8B:08:E3:8C	21:80:00:E0:8B:0A:AA:A7
Intervalo 7	20:80:00:E0:8B:0A:AA:A8	20:80:00:E0:8B:0C:71:C3	21:80:00:E0:8B:0A:AA:A8	21:80:00:E0:8B:0C:71:C3
Intervalo 8	20:80:00:E0:8B:0C:71:C4	20:80:00:E0:8B:0E:38:DF	21:80:00:E0:8B:0C:71:C4	21:80:00:E0:8B:0E:38:DF
Intervalo 9	20:80:00:E0:8B:0E:38:E0	20:80:00:E0:8B:0F:FF:FB	21:80:00:E0:8B:0E:38:E0	21:80:00:E0:8B:0F:FF:FB
Malha B				
Intervalo 1	20:81:00:E0:8B:20:00:00	20:81:00:E0:8B:21:C7:1B	21:81:00:E0:8B:20:00:00	21:81:00:E0:8B:21:C7:1B
Intervalo 2	20:81:00:E0:8B:21:C7:1C	20:81:00:E0:8B:23:8E:37	21:81:00:E0:8B:21:C7:1C	21:81:00:E0:8B:23:8E:37

Tabela 7. Conjunto de endereços QLogic WWN (continuação)

Intervalo predefinido	Endereço inicial de WWNN	Endereço final de WWNN	Endereço final de WWPN	Endereço final de WWPN
Intervalo 3	20:81:00:E0:8B:23:8E:38	20:81:00:E0:8B:25:55:53	21:81:00:E0:8B:23:8E:38	21:81:00:E0:8B:25:55:53
Intervalo 4	20:81:00:E0:8B:25:55:54	20:81:00:E0:8B:27:1C:6F	21:81:00:E0:8B:25:55:54	21:81:00:E0:8B:27:1C:6F
Intervalo 5	20:81:00:E0:8B:27:1C:70	20:81:00:E0:8B:28:E3:8B	21:81:00:E0:8B:27:1C:70	21:81:00:E0:8B:28:E3:8B
Intervalo 6	20:81:00:E0:8B:28:E3:8C	20:81:00:E0:8B:2A:AA:A7	21:81:00:E0:8B:28:E3:8C	21:81:00:E0:8B:2A:AA:A7
Intervalo 7	20:81:00:E0:8B:2A:AA:A8	20:81:00:E0:8B:2C:71:C3	21:81:00:E0:8B:2A:AA:A8	21:81:00:E0:8B:2C:71:C3
Intervalo 8	20:81:00:E0:8B:2C:71:C4	20:81:00:E0:8B:2E:38:DF	21:81:00:E0:8B:2C:71:C4	21:81:00:E0:8B:2E:38:DF
Intervalo 9	20:81:00:E0:8B:2E:38:E0	20:81:00:E0:8B:2F:FF:FB	21:81:00:E0:8B:2E:38:E0	21:81:00:E0:8B:2F:FF:FB

Trabalhando com padrões de servidor

Um *padrão de servidor* representa uma configuração de servidor pré-sistema operacional, incluindo armazenamento local, adaptador de E/S, inicialização de SAN e outras configurações de Baseboard Management Controller e firmware de UEFI. Os padrões de servidor também integram suporte para virtualizar endereços de E/S. Assim, é possível virtualizar conexões de malha do servidor ou redefinir servidores sem interromper a malha. Um padrão de servidor é usado como um padrão global para configurar rapidamente vários servidores de uma vez.

Sobre esta tarefa

É possível definir vários padrões de servidor para representar as diferentes configurações usadas em seu datacenter.

Ao definir um padrão de servidor, selecione ou crie padrões de categoria e conjuntos de endereços conforme necessário para construir a configuração desejada para um grupo específico de servidores. Um *padrão de categoria* define as configurações de firmware específicas que podem ser reutilizadas por vários padrões de servidor. É possível usar conjuntos de endereços para definir intervalos de endereços e atribuir endereços a servidores individuais ao implantar padrões de servidor. Há conjuntos de endereços IP, conjuntos de endereços Ethernet (MAC) e conjuntos de Endereços (WWN) do Fibre Channel.

Quando um padrão de servidor é implantado em vários servidores, vários perfis de servidor são gerados automaticamente (um perfil para cada servidor). Cada perfil herda configurações do padrão de servidor pai, o que permite controlar uma configuração comum a partir de um único local.

Você pode criar um padrão de servidor a partir do zero, definindo sua configuração desejada antes da chegada do hardware. Se desejar, você pode criar um padrão de servidor a partir de um servidor existente e usar esse padrão para provisionar os outros servidores. Se você criar um padrão de servidor de um servidor existente, os padrões de categoria estendidos serão aprendidos e criados dinamicamente das configurações atuais do servidor. 'Se desejar alterar as configurações de categoria, será possível editá-las diretamente nos padrões do servidor.

Atenção: Ao criar um novo padrão de servidor do zero, será necessário definir as configurações de inicialização dos servidores. Quando você implanta o padrão de servidor nos servidores, a ordem de inicialização existente nos servidores é substituída pelas configurações da ordem de inicialização padrão no padrão de servidor. Se os servidores não iniciarem após você implantar um padrão de servidor neles, o problema poderá ser que as configurações de inicialização originais foram substituídas pelas configurações de ordem de inicialização no novo padrão de servidor. Para restaurar as configurações de inicialização originais nos servidores, consulte Recuperando configurações de inicialização após a implantação do padrão de servidor.

Importante: Ao criar padrões de servidor, certifique-se de criá-los para cada tipo de servidor. Por exemplo, crie um padrão de servidor para todos os Flex System x240 Nós de Cálculo e outro padrão de servidor para todos os Flex System x440 Nós de Cálculo. Não implante um padrão de servidor criado para um tipo do servidor em outro tipo de servidor.

Importante: Se o nó de gerenciamento falhar, você perderá os padrões de servidor. Sempre faça backup do software de gerenciamento após criar ou modificar padrões de servidor (consulte Fazendo backup do Lenovo XClarity Administrator).

Configurações de dispositivos de rede

Alguns dispositivos de rede do Flex System oferecem mais opções de configuração nos padrões de servidor do que outros dispositivos.

Embora os padrões de servidor possam ser aplicados a qualquer dispositivo de rede, alguma funcionalidade desses padrões é limitada a determinados adaptadores de rede. Além disso, algumas configurações avançadas de adaptadores de rede Ethernet (como preferências de compatibilidade do adaptador e porta) não são aceitas atualmente.

Os padrões de servidor podem aprender dados de configuração existentes e as configurações dos adaptadores de rede aceitas e também podem alterar as definições de configuração por meio da implantação de padrão.

Padrões de categoria

As configurações de firmware são organizadas em categorias que agrupam configurações relacionadas. Para cada categoria, é possível criar um *padrão de categoria* que contém configurações comuns de firmware e pode ser reutilizado por vários padrões de servidor. A maioria das configurações de firmware que você pode definir diretamente no Baseboard Management Controller e no UEFI também pode ser configurada por padrões de categoria. As configurações de firmware disponíveis dependem do tipo de servidor, do ambiente do Flex System e do escopo do padrão de servidor.

É possível criar padrões de categoria separadamente dos padrões de servidor.

Os padrões de categoria podem ser predefinidos, aprendidos nos servidores existentes ou definidos pelo usuário.

- **Padrões de categoria estendida**

  Padrões de categoria estendida são padrões para algumas portas de adaptador de E/S, Unified Extensible Firmware Interface (UEFI) avançado e configurações do controlador de gerenciamento do baseboard (BMC) que são aprendidas e criadas dinamicamente de um servidor gerenciado específico. O Lenovo XClarity Administrator cria esses padrões quando você cria um padrão de servidor de um servidor existente. Não é possível criar padrões de categoria estendida manualmente. Entretanto, é possível editar os padrões depois de criados.

Os seguintes padrões de UEFI Estendida estão predefinidos pelo XClarity Administrator para otimizar servidores para ambientes específicos.
  - **Opções de instalação do ESXi**
  - **Eficiência - Desempenho Favorável**
  - **Energia a Favor da Eficiência**
  - **Desempenho Máximo**
  - **Energia Mínima**
- **Padrões de categoria definidos pelo usuário**

  Padrões de categoria definidos pelo usuário são padrões que você pode criar, incluindo informações de sistema, interfaces de gerenciamento, dispositivos e portas de E/S, destinos de inicialização do Fibre Channel, portas e adaptador de E/S. É possível criar os seguintes padrões de categoria:

  - **Informações do sistema**. As configurações incluem nome do sistema gerado automaticamente, local e contatos.
  - **Interface de gerenciamento**. As configurações incluem o nome do host gerado automaticamente, endereço IP, espaço de nome de domínio (DNS), velocidade da interface e atribuições de porta para a interface de gerenciamento.As configurações duplex não são suportadas pelos padrões de servidor.
  - **Dispositivo e portas de E/S**. As configurações incluem o redirecionamento do console e portas COM. É possível usar os padrões de servidor para ativar serial over LAN na área de Redirecionamento do Console. No entanto, quando serial over LAN estiver ativado, a única configuração de modo de acesso à porta serial aceita pelos padrões de servidor é **Dedicado**; as configurações de IPMI **Compartilhado** e **Pré-Inicialização** para o modo de acesso da porta serial não estão disponíveis nos padrões de servidor.

    Importante: Se você criar um padrão de servidor a partir de um servidor existente, e esse servidor possuir a configuração de modo de acesso à porta serial **Compartilhado** ou **Pré-Inicialização**, o padrão de dispositivo e portas de E/S que é conhecido a partir do servidor terá a configuração de modo de acesso à porta serial **Dedicado**.
  - **Destinos de Inicialização do Fibre Channel**. As configurações incluem destinos primário e secundário específicos de inicialização WWN do Fibre Channel.
  - **Portas**. As configurações incluem adaptadores de E/S e portas para configurar interconexões de malha.

Criando um padrão de servidor

Ao criar um padrão de servidor, você define as característica de configuração para um tipo de servidor específico. É possível criar um padrão de servidor do zero usando as configurações padrão ou usando as configurações de um servidor existente.

Sobre esta tarefa

Antes de criar um padrão de servidor, considere as seguintes sugestões.

- A primeira vez que criar um padrão de servidor, considere criá-lo de um servidor existente. Ao criar um padrão de servidor a partir de um servidor existente, o Lenovo XClarity Administrator aprende e cria padrões de categoria estendidos para algumas portas de adaptadores de E/S, UEFI, e configurações do Baseboard Management Controller. Em seguida, esses padrões de categoria estão disponíveis para uso de qualquer padrão de servidor criado posteriormente. Para obter mais informações sobre padrões de categoria, consulte Definindo configurações de firmware.
- Identifique os grupos de servidores que têm as mesmas opções de hardware e que você deseja que configurem da mesma maneira. É possível usar um padrão de servidor para aplicar as mesmas definições de configuração em diversos servidores, com isso, controlando uma configuração comum de um local.

- Identifique os aspectos de configuração que deseja customizar para o padrão do servidor (por exemplo, armazenamento local, adaptadores de rede, configurações de inicialização, configurações do controlador de gerenciamento, configurações UEFI).
- Não é possível gerenciar contas de usuário locais nem configurar o servidor LDAP usando padrões de configuração.

Importante: Se o nó de gerenciamento falhar, você perderá os padrões de servidor. Sempre faça backup do software de gerenciamento após criar ou modificar padrões de servidor (consulte Fazendo backup do Lenovo XClarity Administrator).

Procedimento

Para criar um padrão de servidor, conclua as seguintes etapas.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Padrões de Configuração de Servidor**. A página Padrões de Configuração de Servidor é exibida.

Etapa 2. Clique na guia **Padrões de Servidor**.

Etapa 3. Clique no ícone **Criar** ( ). O Assistente dos Novos Padrões de Servidor é exibido.

Etapa 4. Para criar um padrão de servidor, execute uma das seguintes ações.

- Clique em **Criar um novo padrão a partir de um servidor existente** para usar as configurações de um servidor existente. Em seguida, selecione o servidor gerenciado o qual o novo padrão deve ser baseado a partir da lista exibida.

  Quando você criar um padrão de servidor a partir de um servidor existente, o XClarity Administrator aprende as configurações de um servidor gerenciado especificado (incluindo a porta estendida, UEFI e configurações do controlador de gerenciamento) e cria dinamicamente padrões de categoria para essas configurações. Se o servidor for novo, o Lenovo XClarity Administrator aprende as configurações de fábrica. Se o XClarity Administrator está gerenciando o servidor, o XClarity Administrator usa as configurações personalizadas. É possível personalizar as configurações especificamente para os servidores os quais esse padrão deve ser implantado.
- Clique em **Criar um novo padrão a partir do zero** para usar as configurações padrão. Em seguida, selecione o tipo do servidor no campo **Fator Forma**.

Nota: As opções apresentadas nas guias restantes podem diferir dependendo do tipo de servidor para o qual você está criando um padrão.

Etapa 5. Insira o nome do novo padrão e uma descrição.

Etapa 6. Personalize o nome do perfil de servidor, selecionando o botão de alternância **Personalizar** e, em seguida, selecionando um ou mais elementos para incluir no esquema de nomenclatura (como texto personalizado, nome do servidor e incremento numérico) e a ordem.

Etapa 7. Clique em **Avançar**

Etapa 8. Escolha a configuração de armazenamento local a ser aplicada quando esse padrão é implantado em um servidor e clique em **Avançar**.

Para obter informações sobre as configurações de armazenamento local, consulte Definindo o armazenamento local.

Etapa 9. **Opcional:** Modifique o endereçamento do adaptador de E/S e defina adaptadores de E/S adicionais para corresponderem ao hardware que você espera configurar com este padrão, e clique em **Avançar**.

Para obter informações sobre as configurações de adaptadores de E/S, consulte Definindo adaptadores de E/S.

Etapa 10. Defina a ordem de inicialização a ser aplicada quando esse padrão é implantado em um servidor e clique em **Avançar**.

Para obter informações sobre as configurações de destino de inicialização de SAN, consulte Definindo opções de inicialização.

Etapa 11. Selecione as configurações de firmware na lista de padrões de categoria existentes.

É possível criar novos padrões de categoria clicando no ícone **Criar** ( ).

Para obter informações sobre as configurações de firmware, consulte Definindo configurações de firmware.

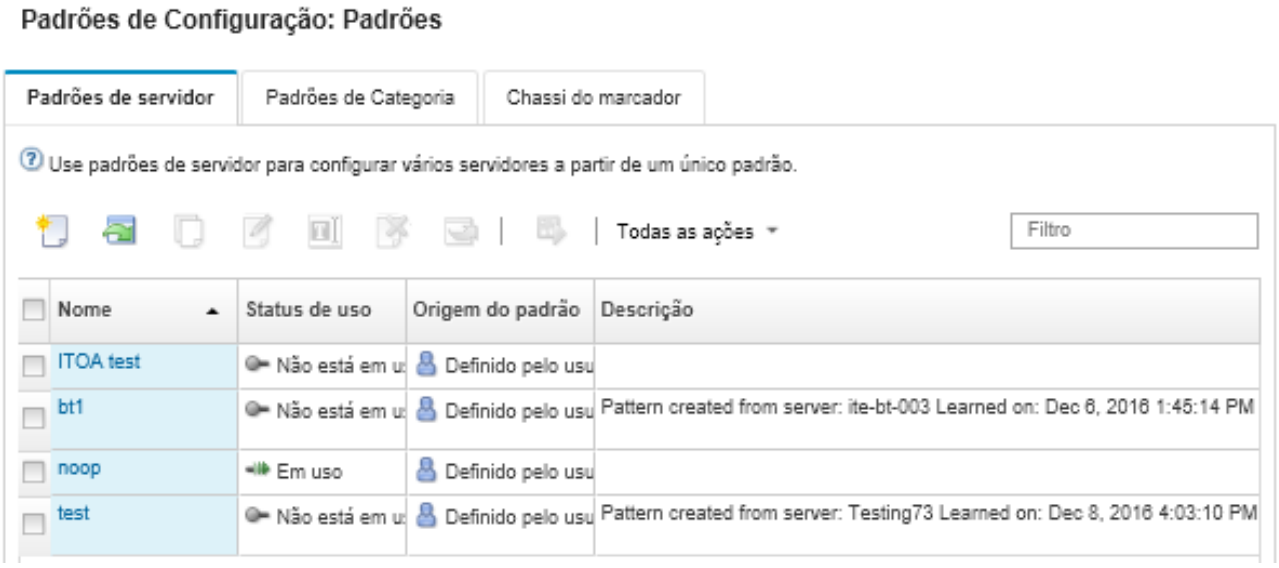
Etapa 12. Clique em **Salvar** para salvar o padrão ou clique em **Salvar e Implantar** para salvar e implantar imediatamente o padrão em um ou mais servidores.

Para obter informações sobre a implantação de um padrão de servidor, consulte Implantando um padrão de servidor em um servidor.

Depois de concluir

Se você clicou em **Salvar e Implantar**, a página Implantar Padrão de Servidor é exibida. Nesta página, é possível implantar o padrão de servidor para servidores específicos.

Se você clicou em **Salvar**, p padrão de servidor e todos os padrões de categoria serão salvos na página Padrões de Servidor.



Nesta página, é possível executar as ações a seguir nos padrões de servidor selecionados:

- Exibir detalhes sobre o padrão clicando nele na coluna **Nome**.
- Implante o padrão (consulte Implantando um padrão de servidor em um servidor).
- Copie o padrão clicando no ícone **Copiar** ( ).
- Edite o padrão (consulte Alterando um padrão de servidor).
- Renomeie o padrão clicando no ícone **Renomear** ( ).
- Exclua o padrão clicando no ícone **Excluir** ( ).
- Exporte e importe padrões de servidor (consulte Exportando e importando padrões de servidor e de categoria).

Definindo o armazenamento local

É possível definir a configuração de armazenamento local a ser aplicada aos servidores de destino quando esse padrão é implantado.

Sobre esta tarefa

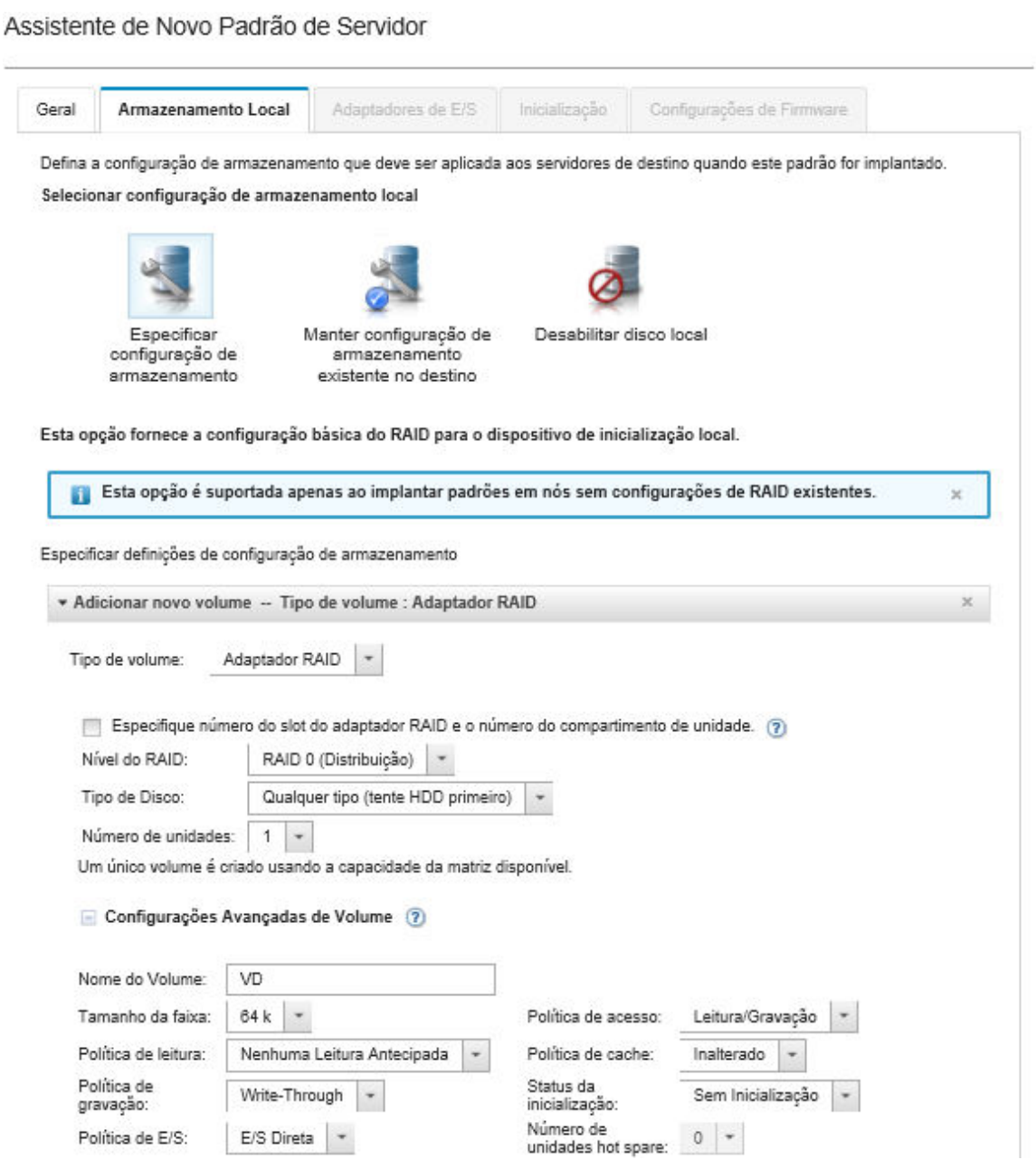
Notas:

- Os controladores de armazenamento integrados nos servidores Flex System x220, Flex System x222 e ThinkSystem suportam RAID baseado em software. No entanto, não há suporte para a configuração de RAID de software usando Padrões de Configuração.
- Ao configurar o RAID usando o Padrões de Configuração, se o servidor for desligado, o servidor será iniciado na configuração BIOS/UEFI automaticamente antes de ativar o perfil de servidor.

Procedimento

Para definir a configuração de armazenamento local, conclua as etapas a seguir.

Etapa 1. No Assistente do Novo Padrão de Servidor, clique na guia **Armazenamento Local**.



Etapa 2. Para definir configurações de armazenamento local, escolha uma destas opções.

- **Especificar configuração de armazenamento**. (Somente dispositivos sem sair das configurações de RAID) As configurações básicas de RAID estão definidas no dispositivo de inicialização local durante a implantação

  Especifique a configuração de armazenamento com base na opção de armazenamento. Você pode adicionar opções de armazenamento adicionais clicando em **Adicionar** ( ).

  – **Adaptador RAID**. Escolha o nível de RAID, as características e o número de unidades instaladas no servidor. Há suporte para RAID 0, 1, 5. Além disso, é possível escolher as configurações de volume avançadas, como tamanho da faixa, políticas e número de unidades hot spare.

    Servidores ThinkSystem com XCC versão 2.1 e posterior (ThinkSystem SR950 requer XCC versão 1.4 ou posterior); também é possível especificar o número de slot do adaptador RAID

e os números de compartimento de unidade para criar um único volume usando a capacidade da matriz disponível. Nesse caso, há suporte para o nível de RAID 0, 1, 5, 6, 10, 50, 60 e 00. Além disso, é possível escolher as configurações de volume avançadas, como tamanho da faixa, políticas e unidades hot spare.

Nota: No servidor de destino, verifique se há unidades suficientes disponíveis do tipo especificado e se o status de RAID das unidades é "Não Configurado Válido", conforme relatado na seção **Unidades** na página Detalhes de Inventário dos servidores (consulte Visualizando os detalhes de um servidor gerenciado).

- **Adaptador de mídia SD da Lenovo**. Escolha o local onde o volume deve ser criado e o tamanho do volume. Você também pode escolher as configurações avançadas de volume, como tipo de mídia e política de acesso.
- **ThinkSystem M.2 com espelhamento**. Escolha o slot PCI, nível de RAID, o nome do volume e o tamanho da faixa para criar um único volume usando a capacidade da matriz disponível.
  - É possível definir vários ThinkSystem M.2 com adaptadores de armazenamento de espelhamento, cada um em um slot PCI diferente.
  - Para servidores de borda ThinkSystem, você deve especificar um número de slot PCI específico. Para outros servidores ThinkSystem que tenham apenas um adaptador RAID M.2 instalado, é possível escolher o primeiro correspondente (valor padrão) ou especificar um número de slot PCI específico.
- **Memória persistente Intel Optane DC**. Escolha o tipo de memória persistente, o limite de aviso para a porcentagem de capacidade restante e a porcentagem de capacidade total a ser usada como memória. (A memória restante é usada como armazenamento persistente).

  Atenção:
  - Para configurar DIMMs de memória persistente Intel Optane DC, a segurança deve estar desabilitada e não deve ser criado um namespace.
  - O recurso Habilitar Segurança é suportado apenas quando o estado de segurança é "desativado" para todos os DIMMs de memória persistente Intel Optane DC no servidor.
  - Os recursos Desabilitar Segurança e Apagar com Segurança são suportados apenas quando o estado de segurança é "Bloqueado" e a senha é igual para todos os DIMMs de memória persistente Intel Optane DC no servidor.
  - O estado de segurança Intel Optane DC PMEM não está incluído no inventário do XClarity Administrator. Você pode verificar manualmente o estado de segurança em UEFI.

- **Manter configuração de armazenamento existente no destino**. A configuração de armazenamento existente não é alterada durante a implantação. Escolha essa opção para usar a configuração de armazenamento que já está em vigor no servidor de destino.
- **Desabilitar disco local**. (Somente Nó de Cálculo do Flex System x240) O controlador de armazenamento integrado e a ROM de opção de armazenamento (UEFI e legado) são exibidos durante a implantação. Desativar a unidade de disco local diminui o tempo total de inicialização ao inicializar de SAN.

Definindo adaptadores de E/S

É possível definir as configurações de porta de E/S e o modo de resolução a serem aplicados aos servidores de destino quando esse padrão é implantado.

Sobre esta tarefa

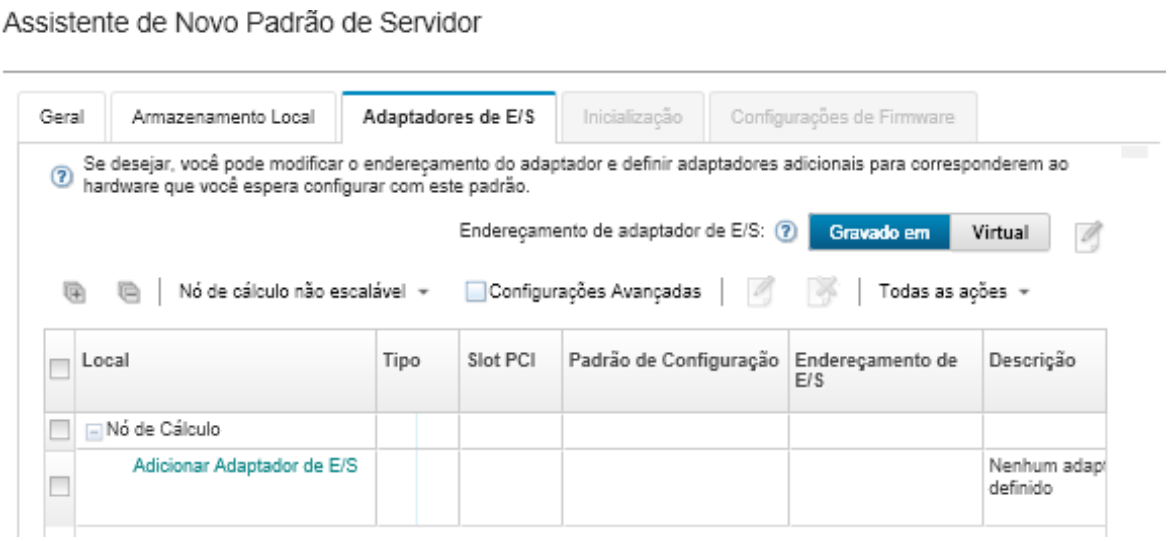
Se você pretender virtualizar ou reatribuir seus endereços de adaptador de E/S, poderá configurar este padrão para usar o endereçamento de adaptador de E/S virtual.

Se estiver criando um padrão a partir de um servidor existente, algumas informações do adaptador podem ser aprendidas automaticamente. É possível definir padrões adicionais de adaptador de E/S para corresponder ao hardware que você espera ter nos servidores quando esse padrão é implantado. Definindo padrões de adaptador de E/S, é possível definir configurações de porta para seu adaptador compatível. Se você estiver usando endereços virtuais de adaptador de E/S, também poderá definir destinos de inicialização de SAN para os adaptadores de Fibre Channel adicionados (consulte Definindo opções de inicialização).

Procedimento

Para definir as configurações de adaptador de E/S, conclua as seguintes etapas.

Etapa 1. No Assistente do Novo Padrão de Servidor, clique na guia **Adaptadores de E/S**.



Nota: Para exibir informações adicionais sobre adaptadores de E/S, clique em **Configurações Avançadas**.

Etapa 2. Se você estiver criando um padrão de servidor para um servidor em um chassi do Flex System, escolha o tipo de modo de resolução do adaptador de E/S:

- **Gravado em**. Use os endereços World Wide Name (WWN) e Media Access Control (MAC) existentes fornecidos com o adaptador de fábrica.
- **Virtual**. Use o endereçamento de adaptador de E/S virtual para simplificar o gerenciamento de conexões LAN e SAN. A virtualização de endereços de E/S designa novamente os endereços de hardware gravados com endereços WWN Fibre e MAC Ethernet virtualizados. Isso pode agilizar a implantação configurando previamente a afiliação de zonas SAN e facilitar o failover eliminando a necessidade de reconfigurar atribuições de zoneamento de SAN e mascaramento de LUN ao substituir o hardware.

  Quando o endereçamento virtual está habilitado, os endereços Ethernet e Fibre Channel são alocados, por padrão, independentemente dos adaptadores definidos. É possível escolher o conjunto do qual os endereços Ethernet e Fibre Channel são alocados.

  Também é possível editar as configurações de endereço virtual clicando no ícone **Editar** ( ) próximo aos modos de endereço.

  Restrição: o endereçamento virtual tem suporte apenas em servidores no chassi do Flex System. Servidores de rack e em torre não são aceitos.

Etapa 3. Se você estiver criando um padrão de servidor para um servidor em um chassi do Flex System, selecione uma das seguintes opções de escalabilidade. As linhas na tabela mudam com base no que é selecionado.
- Flex System não escalável
- Flex System escalável de 2 nós
- Flex System escalável de 4 nós

Etapa 4. Escolha os adaptadores de E/S que devem estar instalados nos servidores em que o padrão deve ser implantado. Para adicionar um adaptador:

a. Clique no link **Adicionar Adaptador de E/S** na tabela para exibir a caixa de diálogo Adicionar Adaptador de E/S 1 ou LOM.

b. Selecione o slot PCI para o adaptador.

c. Selecione o tipo de adaptador na tabela.

Nota: Por padrão, a tabela lista apenas os adaptadores de E/S que estão instalados atualmente nos servidores gerenciados. Para listar todos os adaptadores de E/S permitidos, clique em **Todos os Adaptadores Suportados**.

d. Selecione o padrão de porta inicial a ser atribuído a todas as portas no grupo de portas quando um padrão é implantado.

Padrões de porta são usados para alterar as configurações de porta obtidas no servidor. Esses padrões de porta iniciais são atribuídos quando o adaptador é adicionado pela primeira vez. Após a adição do adaptador, é possível designar padrões diferentes para portas individuais na página Adaptador de E/S.

É possível criar um padrão de porta clicando no ícone **Criar** (). É possível criar um padrão de porta com base em um padrão existente clicando no ícone **Editar** ().

Para obter mais informações sobre padrões de porta, consulte Definindo configurações da porta.

e. Clique em **Adicionar** para adicionar o padrão de porta à tabela na página Adaptador de E/S.

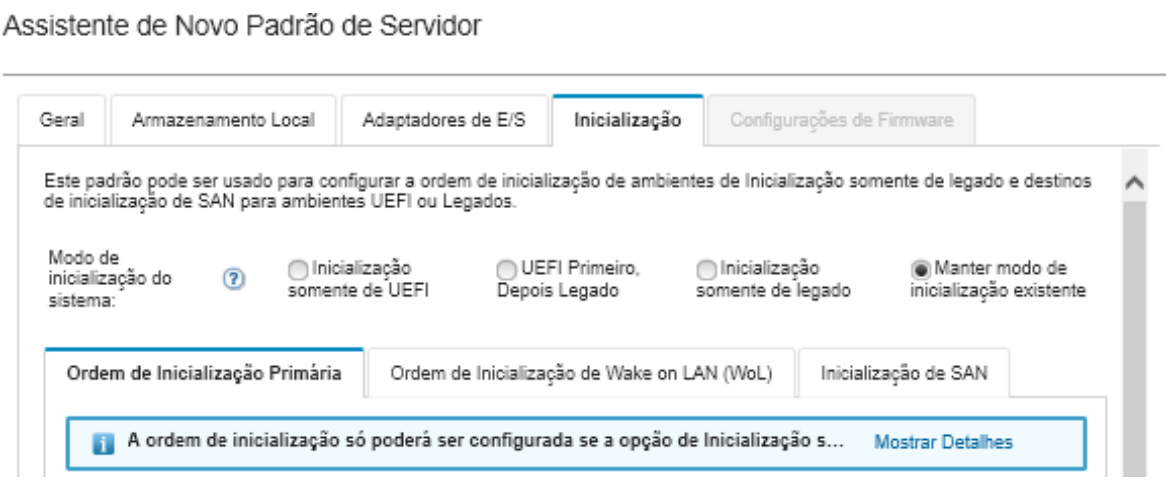
Definindo opções de inicialização

É possível definir a ordem de inicialização a ser aplicada aos servidores de destino quando esse padrão é implantado.

Procedimento

Conclua as seguintes etapas para criar um padrão de opções de inicialização.

Etapa 1. No Assistente do Novo Padrão de Servidor, clique na guia **Boot**.



Etapa 2. Selecione um dos modos de inicialização do sistema a seguir:

- **Inicialização somente de UEFI**. Selecione esta opção para configurar um servidor que suporta Unified Extensible Firmware Interface (UEFI). Se você estiver inicializando sistemas operacionais habilitados para UEFI, esta opção pode reduzir o tempo de inicialização desabilitando ROMs de opção de legado.

  Se o padrão for aprendido em um servidor Thinksystem, você poderá clicar na guia **Ordem de inicialização primária** para especificar a ordem de inicialização. É possível manter a ordem de inicialização especificada no servidor no qual o padrão deve ser implantado ou configurar a ordem de inicialização para especificar a ordem na qual as opções de inicialização devem ser aplicadas. No entanto, a prioridade de inicialização dos dispositivos de inicialização em um grupo de dispositivos (opção de inicialização) não é permitida.

- **UEFI primeiro, depois legado**. Selecione esta opção para configurar um servidor para tentar inicializar usando UEFI primeiro. Se houver um problema, o servidor tenta inicializar em modo legado.

  Se o padrão for aprendido em um servidor Thinksystem, você poderá clicar na guia **Ordem de inicialização primária** para especificar a ordem de inicialização. É possível manter a ordem de inicialização especificada no servidor no qual o padrão deve ser implantado ou configurar a ordem de inicialização para especificar a ordem na qual as opções de inicialização devem ser aplicadas. No entanto, a prioridade de inicialização dos dispositivos de inicialização em um grupo de dispositivos (opção de inicialização) não é permitida.

- **Inicialização somente de legado**. Selecione essa opção se estiver configurando um servidor para inicializar um sistema operacional que requer o firmware de legado (BIOS). Selecione esta opção apenas se estiver inicializando sistemas operacionais habilitados para não UEFI.

  Dica: Se você selecionar o modo de inicialização apenas legado (que torna o tempo de inicialização muito mais rápido), não será possível ativar nenhuma chave do Features on Demand (FoD).

  Se você escolher essa opção, poderá especificar:

  – **Ordem de inicialização primária**. Escolha manter a ordem de inicialização especificado no servidor o qual o padrão deve ser implantado. É possível também escolher configurar a ordem de Inicialização Somente de Legado para especificar apenas a ordem a qual a opção de inicialização a ser aplicada.

  – **Ordem de inicialização de Wake on LAN (WoL)**. Escolha manter a ordem de inicialização WoL atual especificada no servidor o qual o padrão deve ser implantado. É possível também escolher configurar a ordem de Inicialização Somente de Legado para especificar apenas a ordem a qual a opção de inicialização WoL a ser aplicada.

- **Manter modo de inicialização existente**. Selecione esta opção para manter as configurações existentes no servidor de destino. Nenhuma alteração na ordem de inicialização será feita quando um padrão é implantado.

Etapa 3. Selecione a guia **Inicialização de SAN** para escolher um padrão de destino de inicialização e especificar destinos de dispositivo de inicialização.

Nota: Se você definiu os Fibre Channel e ativou o endereçamento virtual ao definir os adaptadores de E/S, é possível definir os destinos de inicialização primários e secundários de SAN para os adaptadores Fibre Channel. É possível especificar diversos identificadores de nome da porta universal (WWPN) e número de unidade lógica (LUN) para os armazenamentos de destino.

Definindo configurações de firmware

É possível especificar as configurações de firmware UEFI e Baseboard Management Controller que devem ser aplicadas aos servidores de destino quando esse padrão é implantado.

Sobre esta tarefa

As configurações de firmware são organizadas em categorias que agrupam configurações relacionadas. Para cada categoria, é possível criar um *padrão de categoria* que contém configurações comuns de firmware e pode ser reutilizado por vários padrões de servidor. A maioria das configurações de firmware que você pode definir diretamente no Baseboard Management Controller e no UEFI também pode ser configurada por padrões de categoria. As configurações de firmware disponíveis dependem do tipo de servidor, do ambiente do Flex System e do escopo do padrão de servidor.

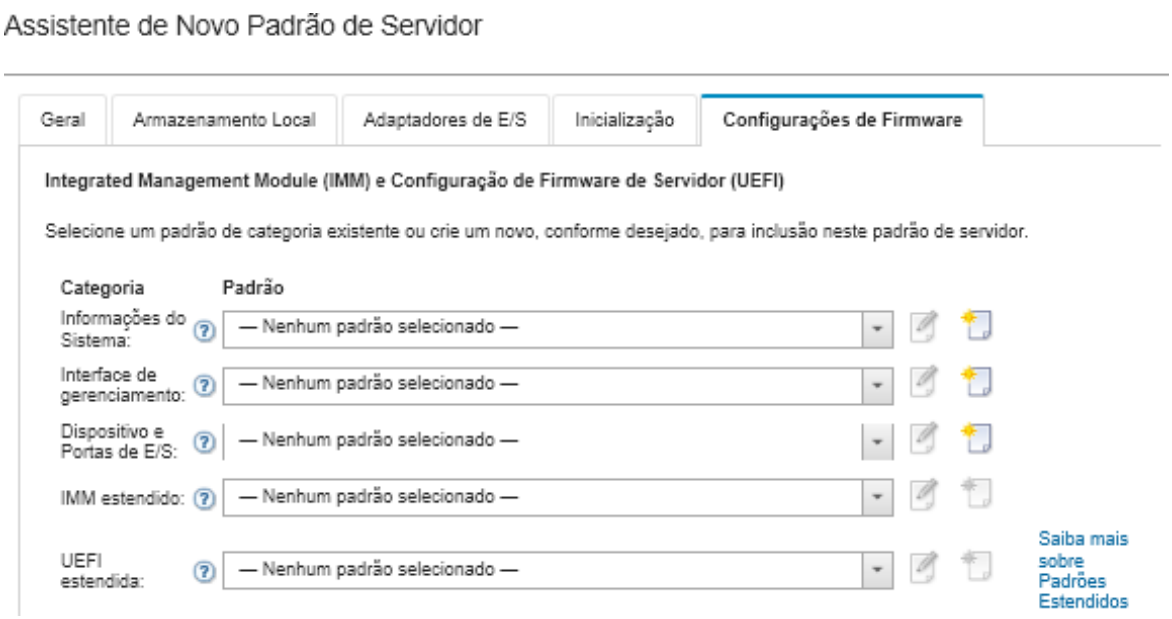
Os padrões de categoria podem ser predefinidos, definidos pelo usuário ou aprendidos nos servidores existentes:

- *Padrões de categoria estendida* são padrões para algumas portas de adaptador de E/S, Unified Extensible Firmware Interface (UEFI) avançado e configurações do controlador de gerenciamento do baseboard (BMC) que são aprendidas e criadas dinamicamente de um servidor gerenciado específico. O Lenovo XClarity Administrator cria esses padrões quando você cria um padrão de servidor de um servidor existente. Não é possível criar padrões de categoria estendida manualmente. Entretanto, é possível editar os padrões depois de criados.
- *Padrões de categoria definidos pelo usuário* são padrões que você pode criar, incluindo informações de sistema, interfaces de gerenciamento, dispositivos e portas de E/S, destinos de inicialização do Fibre Channel, portas e adaptador de E/S.

Procedimento

Conclua as seguintes etapas para definir as configurações de firmware.

Etapa 1. No Assistente do Novo Padrão de Servidor, clique na guia **Configurações de Firmware**.



Etapa 2. Escolha o tipo de padrão de categoria com as configurações que deseja definir.

- **Informações do sistema**. Use esse padrão de categoria para definir a geração automática de nome do sistema, nomes de contato e locais. Para obter mais informações sobre padrões de informações do sistema, consulte Definindo configurações de informações do sistema.
- **Interfaces de gerenciamento**. Use esse padrão de categoria para definir a geração automática de nome do host, atribuições de endereço IP de gerenciamento, configurações de Sistema de Nomes de Domínio (DNS) e configurações de velocidade da Internet. Para obter mais informações sobre padrões de interface de gerenciamento, consulte Definindo configurações de interface de gerenciamento.
- **Dispositivo e portas de E/S**. Use esse padrão de categoria para configurar o redirecionamento de console e portas COM, velocidade de PCIe, dispositivos integrados, ROM opcional do adaptador e ordem de execução de ROM opcional. Para obter mais informações sobre padrões de dispositivo e portas de E/S, consulte Definindo configurações de dispositivos e portas de E/S.
- **BMC estendido**. Use esse padrão de categoria para definir outras configurações do Baseboard Management Controller. Os padrões estendidos do controlador de gerenciamento são criados automaticamente quando um padrão de servidor é criado em um servidor existente. Não é possível criar manualmente um padrão estendido do controlador de gerenciamento. Para obter mais informações sobre padrões de interface de gerenciamento, consulte Definindo configurações estendidas do controlador de gerenciamento.
- **UEFI estendida**. Use esse padrão de categoria para definir outras configurações de Unified Extensible Firmware Interface (UEFI). Os padrões de UEFI estendida são criados automaticamente quando um padrão de servidor é criado em um servidor existente. Não é possível criar manualmente um padrão de UEFI estendida. Para obter mais informações sobre padrões de interface de gerenciamento, consulte Definindo configurações UEFI estendidas.

Etapa 3. Crie novos padrões de categoria clicando no ícone **Criar** ( ) próximo a esse tipo de padrão de categoria.

Também é possível editar um padrão de categoria existente selecionando um padrão específico na lista suspensa e clicando no ícone **Editar** ( ) próximo a esse tipo de padrão de categoria. Também é possível copiar um padrão de categoria existente editando o padrão e clicando em **Salvar como** para salvá-lo com um novo nome.

Definindo configurações de informações do sistema

É possível definir informações do nome do sistema, contato e local, criando um padrão de informações do sistema.

Procedimento

Conclua as seguintes etapas para criar um padrão de informações do sistema:

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Padrões**. A página Padrões de Configuração: Padrões é exibida.

Etapa 2. Clique na guia **Padrões de Categoria**.

Etapa 3. Clique na guia vertical **Padrões de Informações do Sistema** e, em seguida, clique no ícone **Criar** ().

Dica: É possível criar também um novo padrão de informações do sistema da página Configurações de Firmware do assistente do Novo Padrão de Servidor, clicando no ícone **Criar** próximo da seleção **Informações do Sistema**.

Etapa 4. Na caixa de diálogo Novo Padrão de Informações do Sistema, especifique as seguintes informações.

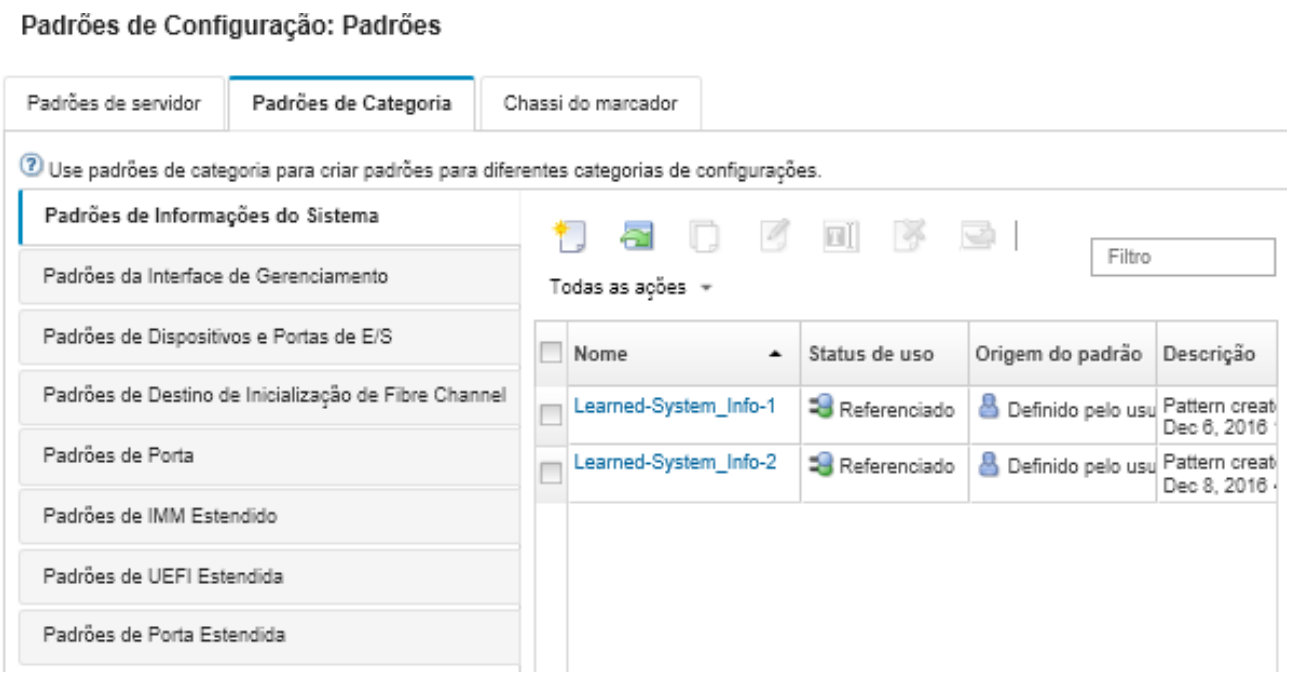
- Insira um nome e uma descrição para o padrão.
- Escolha se irá gerar automaticamente os nomes do sistema. Se clicar em **Personalizar**, é possível especificar como os nomes devem ser gerados quando o padrão é implantado. Se clicar em **Desabilitar**, o nome do sistema permanecerá inalterado em cada servidor quando o padrão é implantado. Para a maioria dos dispositivos, o nome está limitado a 256 caracteres em inglês pelo Baseboard Management Controller. Os nomes gerados automaticamente serão truncados para 256 caracteres.
- Especifique a pessoa a ser contatada por este servidor e o local do servidor.

  Nota: Se SNMP for habilitado, especifique um local do sistema e contato.

Etapa 5. Clique em **Criar**.

Resultados

O novo padrão de categoria é listado na guia **Padrões de Informações do Sistema** na página Padrões de Configuração: Padrões de Categoria:



Dessa página, também é possível executar as seguintes ações em um padrão de categoria selecionado:

- Modificar as configurações do padrão atual clicando no ícone **Editar** ( ).
- Copiar um padrão existente clicando no ícone **Copiar** ( ).
- Excluir um padrão clicando no ícone **Excluir** ( ).
- Renomear um padrão clicando no ícone **Renomear** ( ).
- Importe ou exporte padrões (consulte Exportando e importando padrões de servidor e de categoria).

Definindo configurações de interface de gerenciamento

É possível definir nomes de host, endereço IP, sistema de nomes de domínio (DNS), velocidade da interface e atribuições de porta para a interface de gerenciamento, criando um padrão de interface de gerenciamento.

Procedimento

Conclua as seguintes etapas para criar um padrão de interface de gerenciamento.

Nota: As configurações duplex não são suportadas pelos padrões de servidor.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Padrões**. A página Padrões de Configuração: Padrões é exibida.

Etapa 2. Clique na guia **Padrões de Categoria**.

Etapa 3. Clique na guia vertical **Padrões de Interface de Gerenciamento** e, em seguida, clique no ícone **Criar** ( ).

Dica: É possível criar também um novo padrão de interface de gerenciamento da página Configurações de firmware do assistente do Novo Padrão de Servidor, clicando no ícone **Criar** ( ) próximo da seleção **Interface de Gerenciamento**.

Etapa 4. Na caixa de diálogo Novo Padrão de Interface de Gerenciamento, especifique as seguintes informações.

- Insira um nome e uma descrição para o padrão.

- Clique na guia **Nome de host** e se escolha se irá gerar automaticamente os nomes de host. Se clicar em **Personalizar**, é possível especificar como os nomes devem ser gerados quando o padrão é implantado. Se você clicar em **Desabilitar**, o nome do host permanecerá inalterado em cada servidor quando o padrão for implantado.

  Os nomes de host são limitadas a 63 caracteres em inglês pelo Baseboard Management Controller. Os nomes gerados automaticamente serão truncados para 63 caracteres.
- Clique na guia **Endereços IP de Gerenciamento** e defina as configurações de endereços do IPv4 e IPv6.

  Para endereços **IPv4**, é possível escolher uma ou mais das seguintes opções:
  - **Obtenha o endereço IP dinâmico no servidor DHCP**.
  - **Primeiro por DHCP**. Se não for bem-sucedido, obtenha um endereço IP estático a partir do conjunto de endereços.
  - **Obtenha um endereço IP estático do conjunto de endereços.**

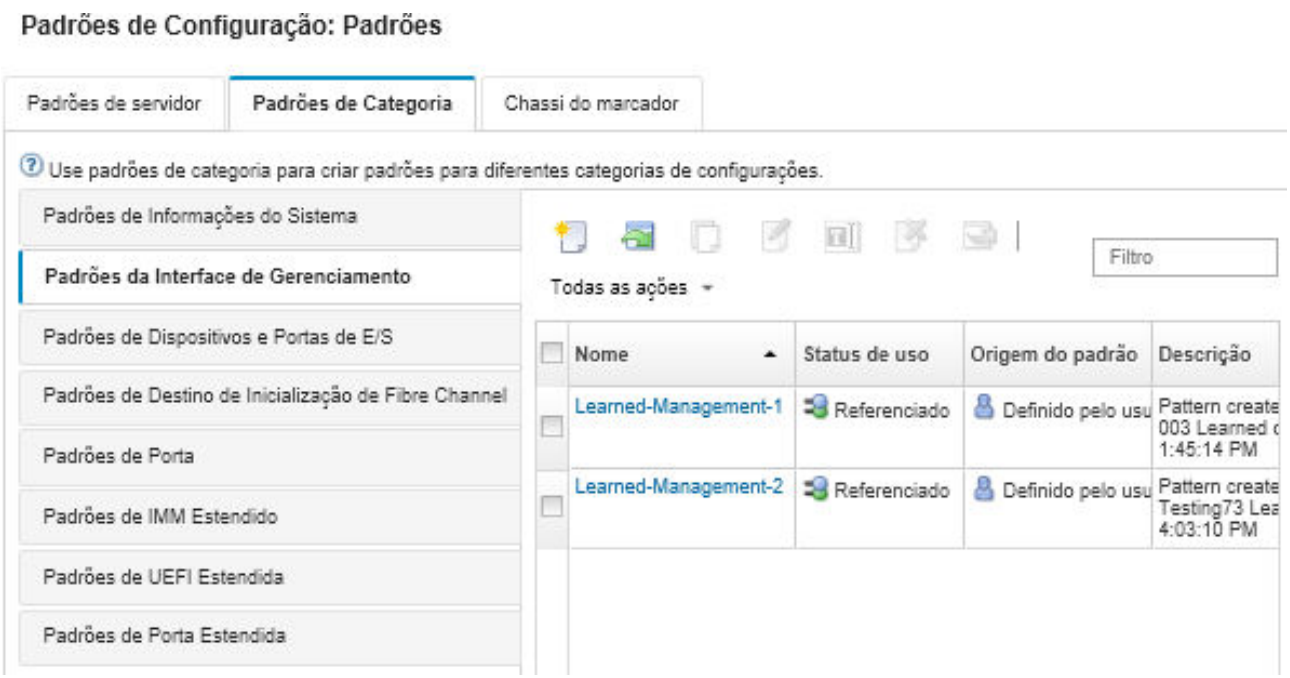
  Para endereços **IPv6**, é possível escolher:
  - **Use a configuração automática de endereço sem estado**.
  - **Obtenha um endereço IP dinâmico a partir de um servidor DHCP**.
  - **Obtenha um endereço IP estático do conjunto de endereços**.

  Na guia **Sistema de Nomes de Domínio (DNS)**, escolha habilitar ou desabilitar o Serviço do Sistema de Nomes de Domínio Dinâmico (DDNS). Se habilitar o DDNS, é possível escolher uma das opções a seguir:
  - Obtenha o nome de domínio de servidor DHCP.
  - Especifique um nome de domínio.
- Clique na guia **Configurações de Interface** e especifique a Unidade de Transmissão Máxima (MTU). O padrão é 1500.
- Clique na guia **Atribuições de Porta** e especifique os números usados para as seguintes portas:
  - HTTP
  - HTTPS
  - CLI Telnet
  - CLI SSH
  - Agente do SNMP
  - Traps SNMP
  - Console de controle remoto
  - CIM sobre HTTP
  - CIM sobre HTTPS

Etapa 5. Clique em **Criar**.

Resultados

O novo padrão de categoria é listado na guia **Padrões de Interface de Gerenciamento** na página Padrões de Configuração: Padrões de Categoria:



Dessa página, também é possível executar as seguintes ações em um padrão de categoria selecionado:

- Modificar as configurações do padrão atual clicando no ícone **Editar** ( ).
- Copiar um padrão existente clicando no ícone **Copiar** ( ).
- Excluir um padrão clicando no ícone **Excluir** ( ).
- Renomear um padrão clicando no ícone **Renomear** ( ).
- Importe ou exporte padrões (consulte Exportando e importando padrões de servidor e de categoria).

Definindo configurações de dispositivos e portas de E/S

É possível habilitar o redirecionamento do console e habilitar e definir as características da porta COM 1, criando um padrão de dispositivos e portas de E/S.

Procedimento

Para criar um padrão de dispositivos e portas de E/S, conclua as seguintes etapas.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Padrões**. A página Padrões de Configuração: Padrões é exibida.

Etapa 2. Clique na guia **Padrões de Categoria**.

Etapa 3. Clique na guia vertical **Padrões de Dispositivos e Portas de E/S** e, em seguida, clique no ícone **Criar** ( ).

Dica: é possível criar também um padrão de dispositivos e portas de E/S da página Configurações de f\Firmware do assistente do Novo Padrão de Servidor clicando no ícone **Criar** ( ) próximo da seleção **Dispositivos e Portas de E/S**.

Etapa 4. Na caixa de diálogo Novo Padrão de Dispositivos e Portas de E/S, especifique as seguintes informações.

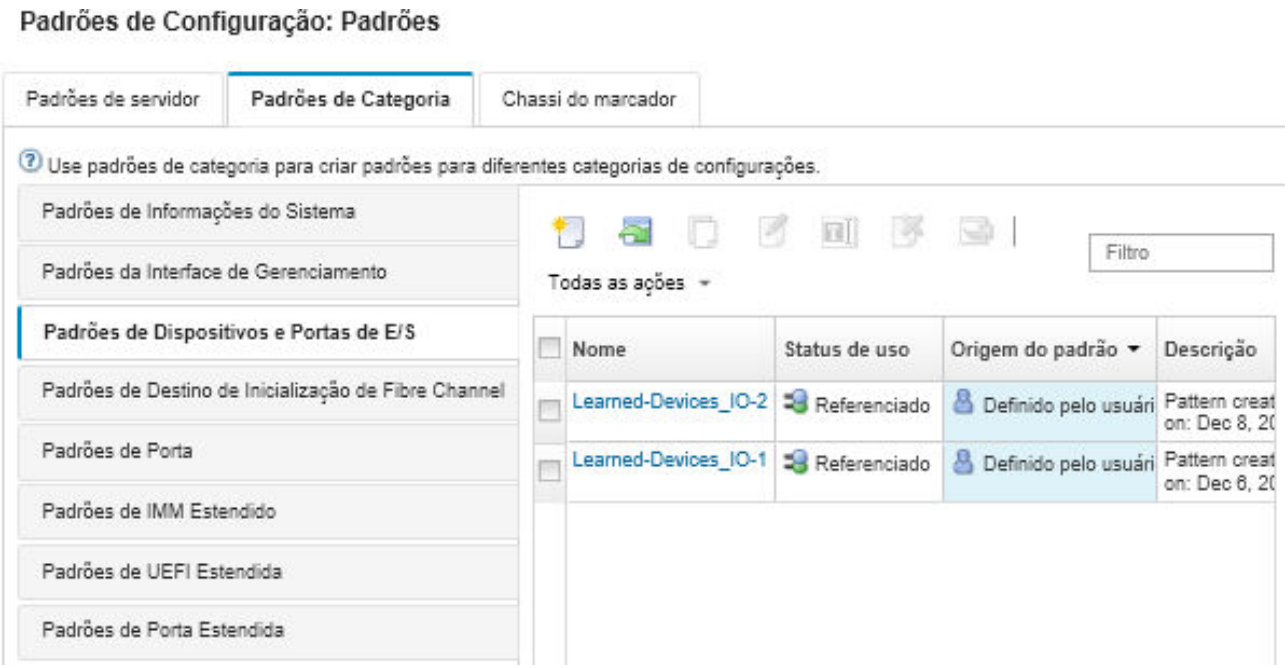
- Insira um nome e uma descrição para o padrão.
- Escolha entre habilitar ou desabilitar o redirecionamento do console. Se habilitar o redirecionamento do console, é possível escolher ativar ou desativar os itens a seguir:

  - **Serial over LAN**.
  - **Redirecionamento do processador de serviços**. Se você ativar o redirecionamento de processador de serviço, será possível usar a porta COM 1 ou 2 para a parta de dados seriais opcional. Observe que se for desabilitada, a porta COM 1 sempre será usada.Também é possível escolher um dos modos CLI a seguir:
    - Desativar
    - Habilitar com a sequência de pressionamento de tecla definida pelo usuário
    - Habilitar com a sequência de pressionamento de tecla compatível com EMS
- Escolher habilitar ou desabilitar portas 1 e 2 COM. Se escolher ativar as portas COM, especifique as seguintes configurações:
  - Taxa de bauds
  - Bits de dados
  - Paridade
  - Bits de parada
  - Emulação de texto
  - Ativo após reinicialização
  - Controle de fluxo

Etapa 5. Clique em **Criar**.

Resultados

O novo padrão de categoria é listado na guia **Padrões de Dispositivos e Portas de E/S** na página Padrões de Configuração: Padrões de Categoria:



Dessa página, também é possível executar as seguintes ações em um padrão de categoria selecionado:

- Modificar as configurações do padrão atual clicando no ícone **Editar** ( ).
- Copiar um padrão existente clicando no ícone **Copiar** ( ).
- Excluir um padrão clicando no ícone **Excluir** ( ).
- Renomear um padrão clicando no ícone **Renomear** ( ).
- Importe ou exporte padrões (consulte Exportando e importando padrões de servidor e de categoria).

Definindo configurações de destino de inicialização do Fibre Channel

É possível configurar o servidor para inicializar a partir de um dispositivo da rede de área de armazenamento (SAN) ao invés de inicializar a partir da unidade de disco local, criando um padrão de destino de inicialização do Fibre Channel.

Procedimento

Conclua as seguintes etapas para criar um padrão de destino de inicialização do Fibre Channel.

Restrição: os destinos de inicialização do Fibre Channel são suportados somente para nós de cálculo Flex. Servidores independentes de rack e em torre não são aceitos.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Padrões**. A página Padrões de Configuração: Padrões é exibida.

Etapa 2. Clique na guia **Padrões de Categoria**.

Etapa 3. Clique na guia vertical **Padrão de Destino de Inicialização do Fibre Channel** e, em seguida, clique no ícone **Criar** ( ).

Etapa 4. Na caixa de diálogo Novo Padrão de Destino de Inicialização do Fibre Channel, especifique as seguintes informações.

- Insira um nome e uma descrição para o padrão.
- Especifique um ou mais endereços WWPNs e identificadores LUN a serem usados como destinos de inicialização primários. Além disso, é possível especificar opcionalmente um ou mais endereços WWPN e identificadores LUN a serem usados como destinos de inicialização secundários.

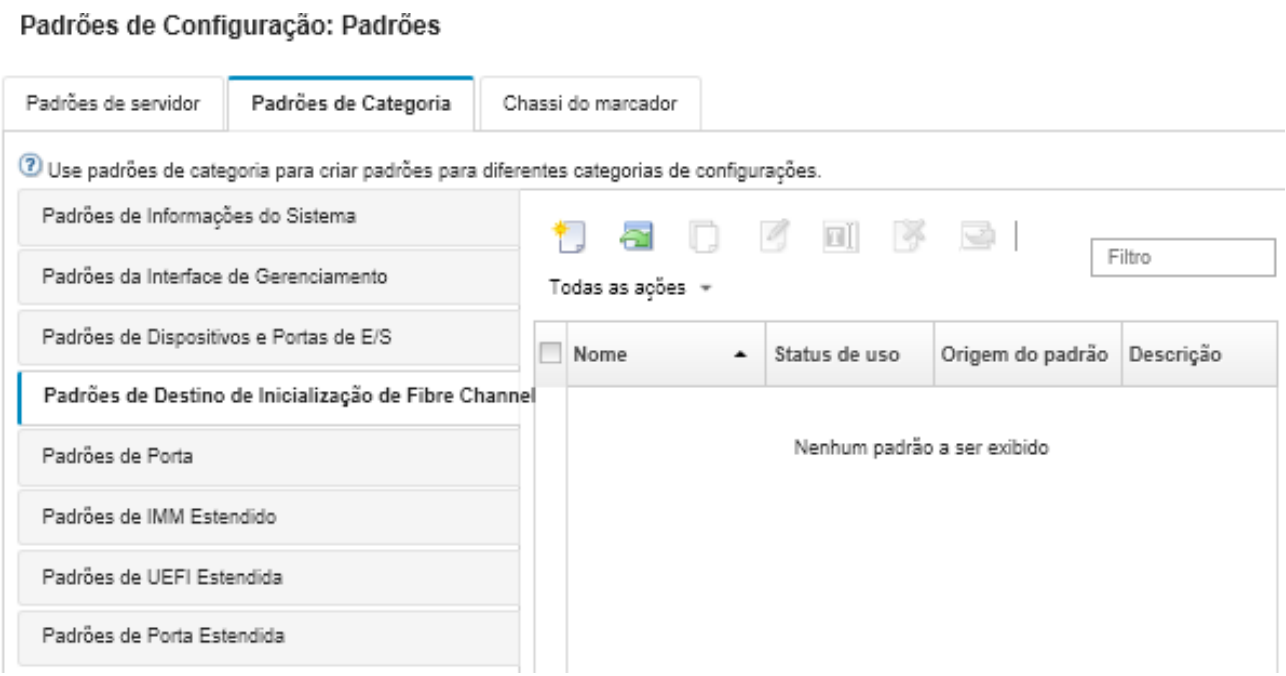
  Por exemplo, você pode adicionar os caminhos primários de armazenamento como destinos primários e os caminhos secundários de armazenamento como destinos secundários. Usando diferentes grupos de destino em diferentes padrões de servidor, você pode balancear a carga de armazenamento durante solicitações simultâneas de inicialização de vários hosts.

  Dica: se você especificar `00:00:00:00:00:00:00:00` do WWPN, o XClarity Administrator tentará inicializar a partir do destino descoberto primeiro.

Etapa 5. Clique em **Criar**.

Resultados

O novo padrão de categoria é listado na guia **Padrões de Destino de Inicialização do Fibre Channel** na página Padrões de Configuração: Padrões de Categoria:



Dessa página, também é possível executar as seguintes ações em um padrão de categoria selecionado:

- Modificar as configurações do padrão atual clicando no ícone **Editar** ( ).
- Copiar um padrão existente clicando no ícone **Copiar** ( ).
- Excluir um padrão clicando no ícone **Excluir** ( ).
- Renomear um padrão clicando no ícone **Renomear** ( ).
- Importe ou exporte padrões (consulte Exportando e importando padrões de servidor e de categoria).

Definindo configurações da porta

É possível definir as configurações típicas da porta para um tipo de adaptador de E/S específico criando um padrão de porta.

Sobre esta tarefa

É possível usar as configurações de rede em padrões de porta para configurar as portas internas do comutador. Entretanto, não é possível usar padrões de porta para definir as configurações globais do comutador, como os IDs de VLAN, modo UFP global, modo CEE, e os FIPs globais. Você precisará definir manualmente as configurações globais usando as seguintes regras compatíveis com configurações de portas internas, que pretende implantar antes de implantar os padrões de porta. Também não é possível usar padrões de porta para configurar a marcação do PVID. Consulte a documentação fornecida com seu comutador para determinar as verificações de compatibilidade entre as configurações globais e configurações de porta interna, e como definir essas configurações para esse comutador.

- Assegure-se de que o **globalCEEState** está "Ligado" quando o PFC está configurado.
- Certifique-se de que o **globalCEEState** esteja "Ligado" quando o vport estiver configurado no modo "FCoE".
- Certifique-se de que o **globalCEEState** esteja "Ligado" e o **globalFIPsState** esteja "Ligado" quando os FIPs estão configurados.
- Certifique-se de que o **globalUFPMode** esteja "Habilitado" quando o modo da porta interna do comutador estiver configurada no modo "UFP".

- Certifique-se de que o ID de VLAN está criado antes de adicionar uma porta ao VLAN específico.

Procedimento

Conclua as seguintes etapas para criar um padrão de porta do adaptador de E/S.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Padrões**. A página Padrões de Configuração: Padrões é exibida.

Etapa 2. Clique na guia **Padrões de Categoria**.

Etapa 3. Clique na guia vertical **Padrão de Porta** e, em seguida, clique no ícone **Criar** ( ).

Dica: Também é possível criar um novo padrão de porta na página Adicionar Adaptador de E/S, clicando no ícone **Criar** ( ) ao lado da seleção **Padrão de porta inicial**.

Etapa 4. Na caixa de diálogo Novo Padrão de Porta, especifique as seguintes informações.

- Insira um nome e uma descrição para o padrão.
- Especifique as seguintes configurações de compatibilidade de porta e adaptador. Ao atribuir padrões aos adaptadores e portas, as configurações de padrões são filtradas com base na compatibilidade com o adaptador ou porta de destino.
  - Tipo do adaptador de destino
  - Modo operacional de porta de destino, incluindo:
    - Modo pNIC
    - Modo vNIC com malha virtual
    - Modo de comutador independente vNIC
    - Modo vNIC com protocolo de malha unificada

    Essas configurações habilitam a virtualização do NIC. Para obter mais informações, consulte Virtualização NIC no Flex System Fabric Solutions.
  - Protocolos de porta de destino, incluindo:
    - Apenas Ethernet
    - Ethernet e FCoE
    - Ethernet e iSCSI
  - O padrão de configurações estendidas de porta, o qual é usado para definir configurações adicionais que são aprendidas no servidor.
- Se você configurar o modo operacional da porta de destino como **modo pNIC**, escolha aplicar as configurações correspondentes às portas internas do comutador Flex, onde aplicável. Se selecionado, é possível configurar VLAN adicionais e configurações avançadas:
  - Especifique o protocolo de porta de destino.
  - Se configurar o protocolo da porta de destino para **Ethernet e FCoE**, selecione e especifique o ID de prioridade 2 opcionalmente.
- Se você configurar o modo operacional da porta de destino como **modo vNIC com malha virtual**, defina as configurações de função física, incluindo o tipo e a marcação VLAN para cada função.
- Se você configurar o modo operacional da porta de destino como **modo vNIC independente de comutador**, especifique o tipo, a largura de banda mínima e a VLAN para cada função habilitada. Você também pode optar por aplicar as configurações correspondentes às portas internas do comutador Flex quando aplicável. Se selecionado, é possível configurar uma porta interna do comutador adicional e configurações avançadas:
  - Especifique a LAN padrão, que é usado somente pelo sistema operacional enquanto o ele envia pacotes não marcados.
  - Especifique uma lista de VLANs separadas por vírgula.

- Escolha configurar o controle manual e especifique os acionadores.
- Escolha configurar o tipo do controle de fluxo, incluindo
  - Manter o controle de fluxo existente
  - Controle de fluxo baseado em prioridade
  - Controle de fluxo em nível de link

  Para obter mais informações sobre estes tipos de controle de fluxo, consulte a documentação fornecida com seu comutador Flex.

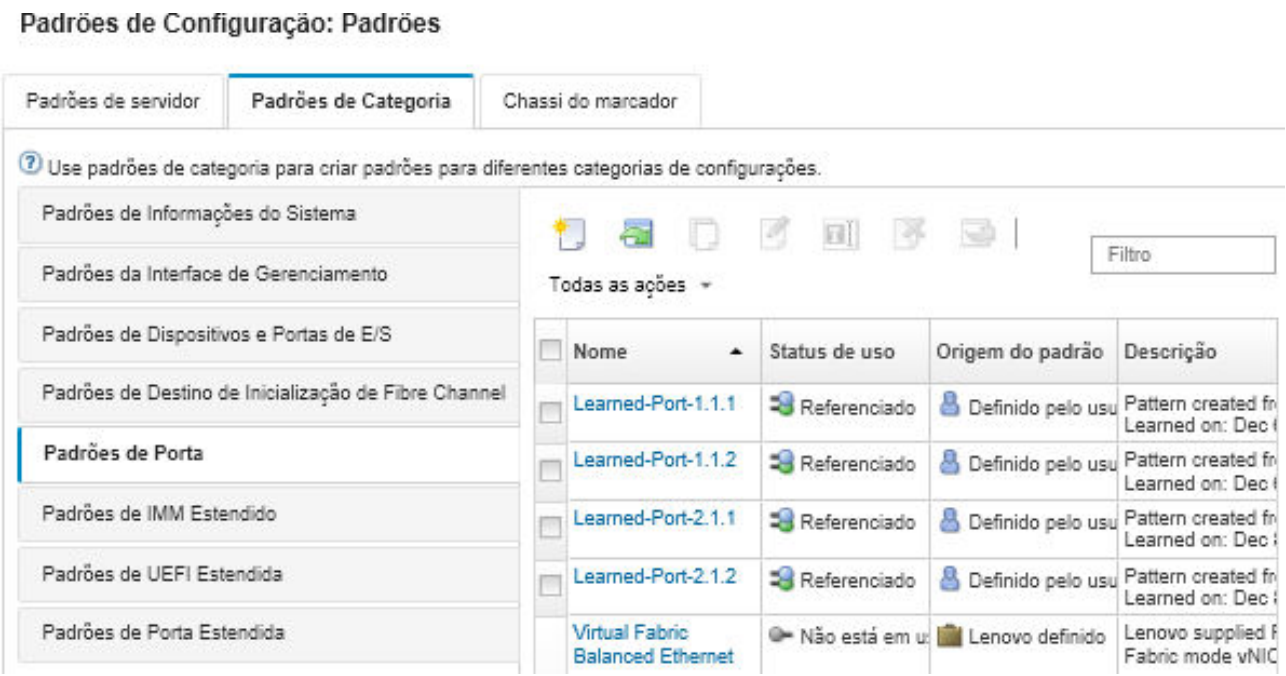
- Se você configurar o modo operacional da porta de destino como **modo vNIC de protocolo com malha unificada**, escolha aplicar as configurações correspondentes às portas internas do comutador Flex, onde aplicável. Se selecionado, é possível configurar funções UFP adicionais e configurações avançadas:
  - Especifique o modo de QoS (largura de banda ou prioridade).
  - Escolha habilitar a marcação de ID da VLAN padrão e especifique o modo, a largura de banda mínima e a marcação de VLAN para cada função habilitada.
  - Escolha configurar a falha layer 2 e especifique o número de acionadores para cada função.
  - Para o modo de largura de banda QoS, especifique o tipo de controle de fluxo (com base em prioridade, no nível de link ou controle de fluxo existente).
  - Para o modo de largura de banda QoS, escolha se a prioridade 4 está habilitada quando iSCSI é selecionado.

  Nota: Certifique-se de que o failover global esteja "Ligado" ao configurar os acionadores de failover.

Etapa 5. Clique em **Criar**.

Resultados

O novo padrão de categoria é listado na guia **Padrões de Porta** na página Padrões de Configuração: Padrões de Categoria:



Dessa página, também é possível executar as seguintes ações em um padrão de categoria selecionado:

- Modificar as configurações do padrão atual clicando no ícone **Editar** ( ).

- Copiar um padrão existente clicando no ícone **Copiar** ().
- Excluir um padrão clicando no ícone **Excluir** ().
- Renomear um padrão clicando no ícone **Renomear** ().
- Importe ou exporte padrões (consulte Exportando e importando padrões de servidor e de categoria).

Definindo configurações estendidas do controlador de gerenciamento

As configurações estendidas do Baseboard Management Controller são aprendidas e criadas dinamicamente de um servidor gerenciado específico. O Lenovo XClarity Administrator cria esses padrões ao criar um padrão de servidor de um servidor existente. Não é possível criar padrões estendidos do controlador de gerenciamento manualmente. Entretanto, é possível copiar e modificar os padrões que já foram criados.

Antes de iniciar

Nota: Configuração do IMM térmica pode entrar em conflito com a configuração do modo operacional UEFI. Se estiverem em conflito, as configurações de UEFI substitui a configuração do IMM quando o dispositivo é reinicializado, e as configurações térmicas que você define em um padrão de controlador de gerenciamento baseboard estendido estarão fora de conformidade. Para resolver o problema de não conformidade, remova a configuração do padrão do controlador de gerenciamento baseboard estendido de ou selecione uma configuração que não entre em conflito com a configuração atual do modo operacional UEFI.

Procedimento

Conclua as seguintes etapas para modificar padrões estendidos do controlador de gerenciamento.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Padrões**. A página Padrões de Configuração: Padrões é exibida.

Etapa 2. Clique na guia **Padrões de Categoria**.

Etapa 3. Clique na guia vertical **Padrões de BMC Estendido**.

Etapa 4. Selecione o padrão a ser alterado e clique no ícone **Editar** ().

Etapa 5. Modifique os campos apropriados.

É possível selecionar as configurações que deseja incluir no padrão de categoria clicando nas configurações **Incluir/Excluir**.

- Para definir as configurações de DNS, clique em **Interface de Configurações de Rede → Configuração de DNS**. É possível habilitar o DNS, selecionar o protocolo IP, especificar até três endereços IPv4 ou IPv6 e ativar a descoberta de endereços IP XClarity Administrator.

  Nota: Para dispositivos Flex System, é possível configurar somente o endereço IP a ser usado para descobrir o servidor XClarity Administrator.

- Para definir as configurações de NTP, clique em **Interface de Configurações de Rede → Configuração de NTP do módulo integrado**. É possível especificar o nome do host para até 4 servidores NTP e a frequência.

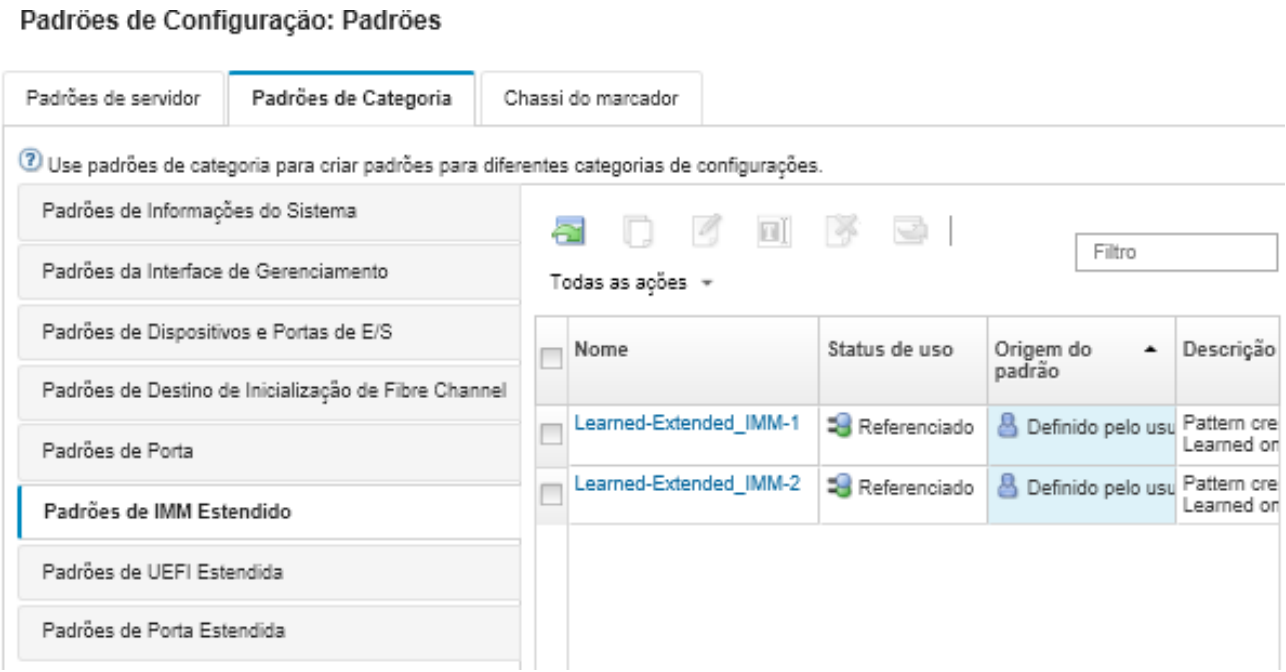
  Nota: Para dispositivos Flex System, não é possível definir as configurações de NTP.

- (Somente servidores em rack) Para configurar dados e tempo, clique em **Configurações gerais → Configurações integradas do relógio do módulo**. É possível especificar o fuso horário (deslocamento UTC), ativar ou desativar o horário de verão (DST) e escolher se deve usar UTC ou a hora local no host.
- Para alterar as configurações de segurança da conta do usuário, clique em **Configuração de segurança da conta**.

Etapa 6. Clique em **Salvar** para salvar as alterações no padrão de categoria atual ou clique em **Salvar como** para salvar as alterações em um novo padrão de categoria.

Resultados

O padrão de categoria modificado é listado na guia **Padrões de BMC Estendido** na página Padrões de Configuração: Padrões de Categoria:



Dessa página, também é possível executar as seguintes ações em um padrão de categoria selecionado:

- Copiar um padrão existente clicando no ícone **Copiar** ( ).
- Excluir um padrão clicando no ícone **Excluir** ( ).
- Renomear um padrão clicando no ícone **Renomear** ( ).
- Importe ou exporte padrões (consulte Exportando e importando padrões de servidor e de categoria).

Definindo configurações UEFI estendidas

As configurações Unified Extensible Firmware Interface (UEFI) estendidas são aprendidas e criadas dinamicamente de um servidor gerenciado específico. O Lenovo XClarity Administrator cria esses padrões ao criar um padrão de servidor de um servidor existente. Não é possível criar padrões de UEFI estendida manualmente. Entretanto, é possível copiar e modificar os padrões que já foram criados.

Sobre esta tarefa

Os seguintes padrões de UEFI Estendida estão predefinidos pelo Lenovo XClarity Administrator para otimizar servidores para ambientes específicos.

- **Opções de instalação do ESXi**
- **Eficiência - Desempenho Favorável**
- **Energia a Favor da Eficiência**
- **Desempenho Máximo**
- **Energia Mínima**

Notas:

- A mudança de configurações de segurança de UEFI (incluindo inicialização segura, Trusted Platform Module [TPM] e configuração de política de presença física) não é aceita usando padrões de UEFI estendida.
- É possível modificar a senha do administrador UEFI para os servidores ThinkSystem e ThinkAgile selecionados na página Servidores clicando em **Todas as Ações → Segurança → Senha do administrador UEFI**. O firmware Lenovo XClarity Controller nível 20A é necessário.

Procedimento

Conclua as seguintes etapas para modificar padrões de UEFI estendida.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Padrões**. A página Padrões de Configuração: Padrões é exibida.

Etapa 2. Clique na guia **Padrões de Categoria**.

Etapa 3. Clique na guia vertical **Padrões de UEFI Estendida**.

Etapa 4. Selecione o padrão a ser alterado e clique no ícone **Editar** ( ).

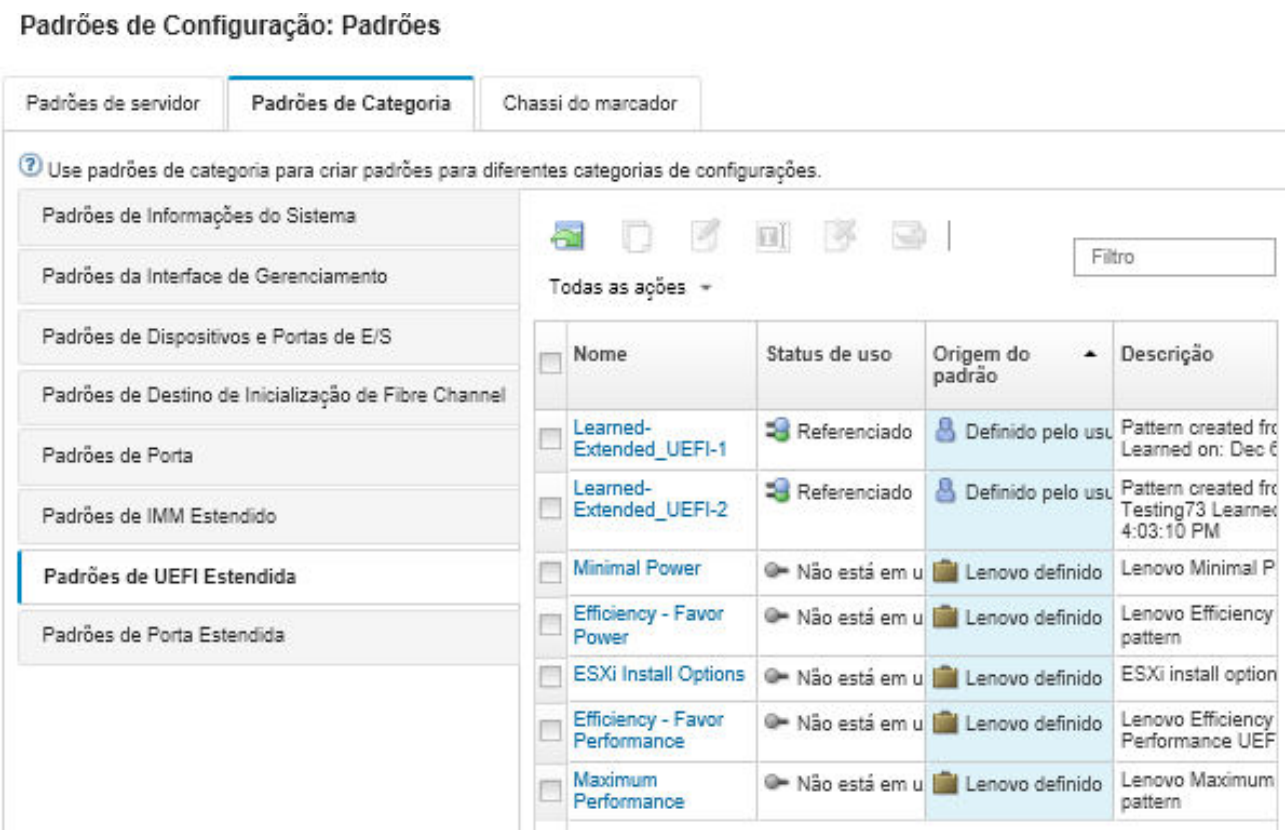
Etapa 5. Modifique os campos apropriados.

É possível selecionar as configurações que deseja incluir no padrão de categoria clicando nas configurações **Incluir/Excluir**.

Etapa 6. Clique em **Salvar** para salvar as alterações no padrão de categoria atual ou clique em **Salvar como** para salvar as alterações em um novo padrão de categoria.

Resultados

O padrão de categoria modificado é listado na guia **Padrões de UEFI Estendida** na página Padrões de Configuração: Padrões de Categoria:



Dessa página, também é possível executar as seguintes ações em um padrão de categoria selecionado:

- Copiar um padrão existente clicando no ícone **Copiar** ( ).
- Excluir um padrão clicando no ícone **Excluir** ( ).
- Renomear um padrão clicando no ícone **Renomear** ( ).
- Importe ou exporte padrões (consulte Exportando e importando padrões de servidor e de categoria).

Definindo configurações de porta estendidas

As configurações de porta estendidas são aprendidas e criadas dinamicamente de um servidor gerenciado específico. O Lenovo XClarity Administrator cria esses padrões ao criar um padrão de servidor de um servidor existente. Não é possível criar padrões de porta estendida manualmente. Entretanto, é possível copiar e modificar os padrões que já foram criados.

Sobre esta tarefa

O XClarity Administrator fornece o seguinte padrão predefinido de porta estendida:

- **Ethernet Balanceada de Virtual Fabric**. Padrão de porta fornecido pela Lenovo para o modo vNIC com malha virtual, Ethernet apenas

Algumas configurações no nível de dispositivo em adaptadores de E/S Mellanox e Broadcom devem ser definidas com o mesmo valor em todas as portas. Se as configurações forem definidas com valores diferentes em portas diferentes, as configurações de uma porta serão usadas, e as configurações de outras portas ficarão fora de conformidade. Para resolver o problema de não conformidade, selecione o mesmo valor para essas configurações de nível de dispositivo.

Para adaptadores de E/S Mellanox, as configurações a seguir devem ser definidas com o mesmo valor em todas as portas.

- Configurações de energia avançadas
- Funções virtuais PCI anunciadas
- Limitador de energia do slot
- Modo de virtualização

Para adaptadores de E/S Broadcom, as configurações a seguir devem ser definidas com o mesmo valor em todas as portas.
- Tempo limite de mensagem de faixa
- Limite de BW
- Limite de BW válido
- Reserva de BW
- Reserva de BW válido
- Habilitar recurso PME
- Número máximo de vetores PF MSI-X
- Modo de várias funções
- Número de vetores MSI-X por VF
- Número de VFs por PF
- ROM opcional
- SR-IOV
- Suporte a RDMA

Procedimento

Conclua as seguintes etapas para modificar padrões de porta estendida.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Padrões**. A página Padrões de Configuração: Padrões é exibida.

Etapa 2. Clique na guia **Padrões de Categoria**.

Etapa 3. Clique na guia vertical **Padrões de Porta Estendida**.

Etapa 4. Selecione o padrão a ser alterado e clique no ícone **Editar** ( ).

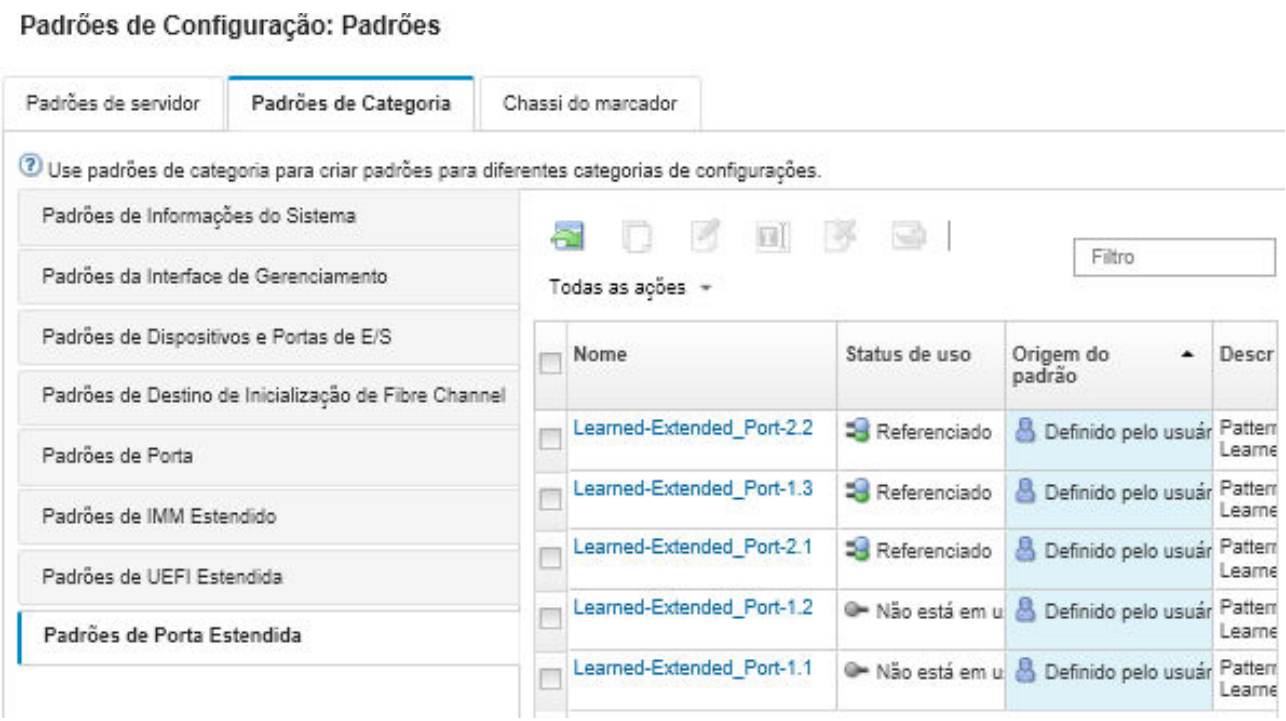
Etapa 5. Modifique os campos apropriados.

É possível selecionar as configurações que deseja incluir no padrão de categoria clicando nas configurações **Incluir/Excluir**.

Etapa 6. Clique em **Salvar** para salvar as alterações no padrão de categoria atual ou clique em **Salvar como** para salvar as alterações em um novo padrão de categoria.

Resultados

O padrão de categoria modificado é listado na guia **Padrões de Porta Estendida** na página Padrões de Configuração: Padrões de Categoria:



Dessa página, também é possível executar as seguintes ações em um padrão de categoria selecionado:

- Copiar um padrão existente clicando no ícone **Copiar** ( ).
- Excluir um padrão clicando no ícone **Excluir** ( ).
- Renomear um padrão clicando no ícone **Renomear** ( ).
- Importe ou exporte padrões (consulte Exportando e importando padrões de servidor e de categoria).

Definindo configurações estendidas do BIOS para SR635/SR655

As configurações do BIOS para SR635/SR655 estendidas são aprendidas e criadas dinamicamente em um servidor gerenciado específico. O Lenovo XClarity Administrator cria esses padrões ao criar um padrão de servidor a partir de um servidor ThinkSystem SR635 ou SR655 existente. Não é possível criar padrões estendidos de BIOS para SR635/SR655 manualmente. Entretanto, é possível copiar e modificar os padrões que já foram criados.

Procedimento

Conclua as seguintes etapas para modificar padrões estendidos de BIOS para SR635/SR655.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Padrões**. A página Padrões de Configuração: Padrões é exibida.

Etapa 2. Clique na guia **Padrões de Categoria**.

Etapa 3. Clique na guia vertical **Padrões estendidos de BIOS para SR635/SR655**.

Etapa 4. Selecione o padrão a ser alterado e clique no ícone **Editar** ( ).

Etapa 5. Modifique os campos apropriados.

É possível selecionar as configurações que deseja incluir no padrão de categoria clicando nas configurações **Incluir/Excluir**.

Etapa 6. Clique em **Salvar** para salvar as alterações no padrão de categoria atual ou clique em **Salvar como** para salvar as alterações em um novo padrão de categoria.

Resultados

O padrão de categoria modificado é listado na guia **Padrões estendidos de BIOS para SR635/SR655** na página Configuration Patterns: Category Patterns (Padrões de configuração: Padrões de categoria):

Dessa página, também é possível executar as seguintes ações em um padrão de categoria selecionado:

- Copiar um padrão existente clicando no ícone **Copiar** ( ).
- Excluir um padrão clicando no ícone **Excluir** ( ).
- Renomear um padrão clicando no ícone **Renomear** ( ).
- Importe ou exporte padrões (consulte Exportando e importando padrões de servidor e de categoria).

Definindo configurações estendidas do ThinkServer CPlus BIOS

As configurações do ThinkServer CPlus BIOS estendidas são aprendidas e criadas dinamicamente em um servidor gerenciado específico. O Lenovo XClarity Administrator cria esses padrões ao criar um padrão de servidor a partir de um servidor ThinkServer CPlus existente. Não é possível criar padrões de ThinkServer CPlus BIOS estendidos manualmente. Entretanto, é possível copiar e modificar os padrões que já foram criados.

Procedimento

Conclua as seguintes etapas para modificar padrões estendidos do ThinkServer CPlus BIOS.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Padrões**. A página Padrões de Configuração: Padrões é exibida.

Etapa 2. Clique na guia **Padrões de Categoria**.

Etapa 3. Clique na guia vertical **Padrões estendidos do ThinkServer CPlus BIOS**.

Etapa 4. Selecione o padrão a ser alterado e clique no ícone **Editar** ( ).

Etapa 5. Modifique os campos apropriados.

É possível selecionar as configurações que deseja incluir no padrão de categoria clicando nas configurações **Incluir/Excluir**.

Etapa 6. Clique em **Salvar** para salvar as alterações no padrão de categoria atual ou clique em **Salvar como** para salvar as alterações em um novo padrão de categoria.

Resultados

O padrão de categoria modificado é listado na guia **Padrões estendidos do ThinkServer CPlus BIOS** na página Padrões de Configuração: Padrões de Categoria:

Dessa página, também é possível executar as seguintes ações em um padrão de categoria selecionado:

- Copiar um padrão existente clicando no ícone **Copiar** ( ).
- Excluir um padrão clicando no ícone **Excluir** ( ).
- Renomear um padrão clicando no ícone **Renomear** ( ).
- Importe ou exporte padrões (consulte Exportando e importando padrões de servidor e de categoria).

Implantando um padrão de servidor em um servidor

É possível implantar um padrão de servidor em um ou mais servidores gerenciados. Também é possível implantar um padrão de servidor em um ou mais compartimentos vazios em um chassi gerenciado pelo Lenovo XClarity Administrator ou em um chassi de marcador. Implantar um padrão de servidor antes de instalar o servidor reserva endereços IP de gerenciamento, reserva endereços virtuais Ethernet ou Fibre Channel e envia por push a configuração de rede para as portas internas do comutador relacionado.

Antes de iniciar

Leia as considerações de configuração do servidor antes de tentar aplicar um padrão de servidor aos dispositivos gerenciados (consulte Implantando um padrão de servidor em um servidor).

Procedimento

Para implantar um padrão de servidor em um servidor gerenciado, conclua as seguintes etapas.

Etapa 1. Na barra de menus do Lenovo XClarity Administrator, clique em **Fornecimento → Padrões de Configuração de Servidor**. A página Padrões de Configuração de Servidor é exibida.

Etapa 2. Clique na guia **Padrões de Servidor**.

Etapa 3. Selecione o padrão de servidor a ser implantado e clique no ícone **Implantar** ( ).

A caixa de diálogo Implantar Padrão de Servidor é exibida com o padrão de servidor selecionado listado na lista **Padrão para implantação**.

Etapa 4. Escolha quando ativar as configurações:

- **Completo**. Liga ou reinicia imediatamente o servidor para ativar as configurações de servidor, Baseboard Management Controller e Unified Extensible Firmware Interface (UEFI).
- **Parcial**. (padrão) Ativa imediatamente as configurações do controlador de gerenciamento, mas adia a ativação das configurações de servidor e UEFI até a próxima reinicialização do servidor. O servidor deve ser ligado ou reiniciado manualmente para que o perfil seja totalmente ativado.

  Nota: Ao implantar os padrões de servidor que incluíam apenas as configurações do IMM (incluindo informações do sistema, interface de gerenciamento e padrões de categoria estendida do BMC), o servidor não precisará ser reiniciado.
- **Adiado**. Gera um perfil para as configurações de servidor, controlador de gerenciamento e UEFI, mas não ativa as configurações no servidor. Você deve ativar manualmente o perfil de servidor reiniciando o servidor antes que o perfil seja totalmente ativado.

Nota: As configurações de rede em portas internas do comutador relacionado são enviadas por push para o comutador imediatamente após a implantação, independentemente da configuração de ativação.

Etapa 5. Escolha um ou mais servidores ou compartimentos de chassi vazios nos quais deseja implantar o padrão de servidor.

Nota: Para exibir uma lista de compartimentos de chassi vazios, selecione **Mostrar Compartimentos Vazios**.

Etapa 6. Clique em **Implantar**. Uma caixa de diálogo é exibida e lista o status de implantação de cada compartimento selecionado.

Etapa 7. Clique em **Implantar** novamente para iniciar o processo de implantação.

Nota: A implantação pode levar vários minutos para ser concluída. Durante a implantação, um perfil de servidor é criado e designado a cada compartimento de chassi ou servidor selecionado.

Etapa 8. Clique em **Fechar**.

Depois de concluir

Você pode monitorar o progresso da implantação clicando em **Monitoramento → Trabalhos** na barra de menu do XClarity Administrator. Você também pode monitorar a criação do perfil de servidor clicando em **Fornecimento → Perfis de Servidor**. Após a conclusão da implantação, revise os perfis de servidor gerados e anote o endereço IP de gerenciamento e os endereços Ethernet ou Fibre Channel virtualizados.

Se você tiver implantado um padrão de servidor em um servidor existente e selecionado:

- Modo de ativação **Completo**, um perfil de servidor será criado para cada servidor, a configuração será propagada para cada servidor e cada servidor será reinicializado para ativar as alterações de configuração.
- Modo de ativação **Parcial**, um perfil de servidor será criado para cada servidor e a configuração será propagada para cada servidor. Para ativar totalmente as alterações de configuração, você deve ligar ou reiniciar manualmente cada servidor (consulte Ligando e desligando um servidor).
- Modo de ativação **Adiado**, um perfil de servidor será criado para cada servidor. Você deve ativar manualmente o perfil de servidor no servidor (consulte Ativando um perfil de servidor).

Se você tiver implantado um padrão de servidor em um compartimento vazio em um chassi gerenciado ou chassi de marcador, após os nós de cálculo serem fisicamente instalados nos compartimentos de chassi apropriados e então descobertos e gerenciados pelo Lenovo XClarity Administrator, você deverá implantar e ativar o perfil de servidor nos nós de cálculo instalados recentemente (consulte Ativando um perfil de servidor).

Se um ou mais servidores não iniciarem após você ter implantado um novo padrão de servidor neles, o problema poderá ser que as configurações de inicialização foram substituídas pelas configurações de inicialização do padrão de servidor. Para sistemas operacionais instalados no modo UEFI, restaurar as configurações padrão pode requerer etapas de configuração adicionais para restaurar a configuração de inicialização. Para ver exemplos de recuperação das configurações de inicialização nos servidores que estão em execução no Windows ou Linux, consulte Recuperando configurações de inicialização após a implantação do padrão de servidor.

Alterando um padrão de servidor

É possível fazer alterações de configuração subsequentes em um padrão de servidor existente. Se o padrão de servidor original for implantado em servidores (se estiver em uso), será possível reimplantar o padrão de servidor alterado em todos os servidores ou em um subconjunto de servidores.

Sobre esta tarefa

Nota: Se você optar por não reimplantar o padrão de servidor alterado em um conjunto de servidores, esses servidores permanecerão associados com o padrão de servidor inalterado original.

Ao editar o padrão de servidor, você pode controlar uma configuração comum de um único local e manter o conjunto original de atribuições de endereço virtual.

Procedimento

Conclua as etapas a seguir para modificar um padrão de servidor.

Etapa 1. Na barra de menus do Lenovo XClarity Administrator, clique em **Fornecimento → Padrões de Configuração de Servidor**. A página Padrões de Configuração de Servidor é exibida.

Etapa 2. Clique na guia **Padrões de Servidor**.

Etapa 3. Selecione o padrão de servidor a ser editado e clique no ícone **Editar** (). A opção Editar Assistente de Padrões do Servidor é exibida.

Etapa 4. Insira o nome do novo padrão e uma descrição.

Etapa 5. Escolha a configuração de armazenamento local a ser aplicada quando esse padrão é implantado em um servidor e clique em **Avançar**.

Para obter informações sobre as configurações de armazenamento local, consulte Definindo o armazenamento local.

Etapa 6. **Opcional:** Modifique o endereçamento do adaptador de E/S e defina adaptadores de E/S adicionais para corresponderem ao hardware que você espera configurar com este padrão, e clique em **Avançar**.

Para obter informações sobre as configurações de adaptadores de E/S, consulte Definindo adaptadores de E/S.

Etapa 7. Defina a ordem de inicialização a ser aplicada quando esse padrão é implantado em um servidor e clique em **Avançar**.

Para obter informações sobre as configurações de destino de inicialização de SAN, consulte Definindo opções de inicialização.

Etapa 8. Selecione as configurações de firmware na lista de padrões de categoria existentes.

É possível criar novos padrões de categoria clicando no ícone **Criar** ( ).

Para obter informações sobre as configurações de firmware, consulte Definindo configurações de firmware.

Etapa 9. Clique em **Salvar** para salvar as alterações de configuração no padrão de servidor atual ou clique em **Salvar como** para salvar as alterações de configuração em um novo padrão de servidor.

Etapa 10. Escolha essa opção para salvar as alterações no padrão de servidor atual ou em um novo padrão de servidor.

- Clique em **Salvar** para salvar as alterações no padrão de servidor atual. Na caixa de diálogo Salvar e Reimplantar Padrão, execute estas etapas:
  1. Escolha quando ativar as configurações.
     - **Completo**. Liga ou reinicia imediatamente o servidor para ativar as configurações de servidor, Baseboard Management Controller e Unified Extensible Firmware Interface (UEFI).
     - **Parcial**. (padrão) Ativa imediatamente as configurações do controlador de gerenciamento, mas adia a ativação das configurações de servidor e UEFI até a próxima reinicialização do servidor. O servidor deve ser ligado ou reiniciado manualmente para que o perfil seja totalmente ativado.

       Nota: Ao implantar os padrões de servidor que incluíam apenas as configurações do IMM (incluindo informações do sistema, interface de gerenciamento e padrões de categoria estendida do BMC), o servidor não precisará ser reiniciado.

     Nota: As configurações de rede em portas internas do comutador relacionado são enviadas por push para o comutador imediatamente após a implantação, independentemente da configuração de ativação.
  2. Selecione os servidores de destino nos quais você deseja reimplantar as alterações de configuração. É possível escolher todos os servidores nos quais o padrão de servidor original foi implantado ou um subconjunto desses servidores.
  3. Clique em **Reimplantar**
- Clique em **Salvar como** para salvar as alterações em um novo padrão de servidor. Para implantar o novo padrão, consulte Implantando um padrão de servidor em um servidor.

Exportando e importando padrões de servidor e de categoria

Se você tiver várias instâncias do Lenovo XClarity Administrator, poderá exportar padrões de servidor e de categoria de uma instância do XClarity Administrator e importá-los para outra instância do XClarity Administrator.

Sobre esta tarefa

É possível exportar somente padrões de servidor e de categoria. Políticas, conjuntos de endereços e perfis não podem ser exportados. Os padrões exportados são separados de todos os conjuntos de endereços de referência. Para aproveitar os conjuntos de endereços em um padrão importado, edite um padrão e reassocie o padrão aos conjuntos do XClarity Administrator em que são importados.

Nota: Quando você exporta um padrão de servidor, os padrões de categoria associados também são exportados.

Procedimento

- Para exportar um ou mais padrões:
  1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Padrões de Configuração de Servidor**. A página Padrões de Configuração de Servidor é exibida.
  2. Clique na guia **Padrões de Servidor** ou **Padrões de Categoria**.
  3. Selecione um ou mais padrões a serem exportados.
  4. Clique no ícone **Exportar** ( ).
  5. Clique em **Exportar** para exportar os padrões.
  6. Salve o arquivo de dados do padrão no sistema local.

     Nota: Se um padrão exportado fizer referência a conjuntos de endereços, essa referência será removida do padrão exportado para evitar conflitos quando o padrão for importado para outra instância do XClarity Administrator. Quando o padrão for importado novamente, será possível editar o padrão importado e atribuir os conjuntos de endereços desejados.
- Para importar um ou mais padrões:
  1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Padrões de Configuração de Servidor**. A página Padrões de Configuração de Servidor é exibida.
  2. Clique no ícone **Importar** ( ) para importar os padrões. A caixa de diálogo Importar Padrões é exibida.
  3. Clique em **Selecionar Arquivo** e selecione um arquivo de dados do padrão a ser importado. Repita para outros arquivos de dados do padrão.
  4. Clique em **Importar** para importar os arquivos selecionados.

     Um relatório de resumo é exibido com uma lista de padrões que foram importados, padrões que foram renomeados devido a conflitos de nomenclatura e padrões que foram ignorados porque já existem.

Trabalhando com perfis de servidor

Um *perfil de servidor* é uma instância de um padrão de servidor que é aplicada a um determinado servidor. Os perfis de servidor são gerados e atribuídos automaticamente quando um padrão de servidor é implantado em um ou mais servidores. Um perfil de servidor é criado para cada servidor de destino. Cada perfil de servidor contém a configuração específica de um único servidor e contém informações (como nome, endereços IP e endereços MAC atribuídos) que são exclusivas para esse servidor específico.

Sobre esta tarefa

O perfil de servidor é ativado durante o processo de inicialização do Baseboard Management Controller. É possível optar por:
- Reinicializar o servidor quando o padrão é implantado para ativar o perfil de servidor imediatamente.

- Adiar a ativação até a próxima reinicialização.
- Adiar a ativação até você ativar manualmente o perfil de servidor.

Vários perfis de servidor podem herdar um único padrão de servidor. Depois que um padrão de servidor é implantado em um ou mais servidores, é possível implantar rapidamente alterações de configuração em vários servidores editando os padrões de servidor e categoria pai. Os perfis de servidor dependentes são atualizados e reimplantados automaticamente em seus servidores associados. Editando o padrão de servidor, você pode controlar uma configuração comum de um único local.

Se você substituir um servidor existente ou instalar um servidor fornecido anteriormente em um compartimento vazio em um chassi, deverá ativar o perfil de servidor para que esse novo servidor forneça as alterações de configuração no novo servidor.

Nota: É possível implantar um padrão de servidor em diversos servidores. Entretanto, diversos padrões não podem ser implantados em um único servidor.

Você pode alterar o perfil de servidor associado a um servidor de várias maneiras, dependendo do motivo para a alteração.

- Se desejar mover ou realocar um servidor:
  1. Desative o perfil de servidor atual no servidor atual (consulte Desativando um perfil de servidor).
  2. Implante o novo padrão de servidor no novo servidor (consulte Implantando um padrão de servidor em um servidor).
- Se o servidor falhar e você quiser usar um servidor de reposição no lugar:
  1. Desative o perfil de servidor atual no servidor com falha (consulte Desativando um perfil de servidor).
  2. Ative o mesmo perfil de servidor no servidor de reposição (consulte Ativando um perfil de servidor).
  3. Quando o servidor com falha for corrigido, repita essas etapas para alternar novamente o perfil.
- Se o servidor falhar e você quiser substituir o hardware:
  1. Desative o perfil de servidor atual no servidor com falha (consulte Desativando um perfil de servidor).
  2. Substitua o servidor com falha.
  3. Ative o mesmo perfil de servidor no novo servidor (consulte Ativando um perfil de servidor).

Importante:

- Ao usar a virtualização de endereços, um servidor mantém seu endereço MAC ou WWN virtual designado até ser desligado. Para desativar um perfil que tenha a virtualização de endereços ativada, a caixa de seleção **Desligar o servidor** é marcada por padrão. Certifique-se de que o servidor original esteja desligado antes de ativar o perfil inativo em um servidor diferente para evitar conflitos de endereço.
- Se você excluir um perfil que não é o criado mais recentemente, os endereços MAC e WWN virtuais *não são* liberados do conjunto de endereços. Para obter mais informações, consulte Excluindo um perfil de servidor.
- As configurações em um servidor poderão ficar fora de conformidade com o perfil de servidor se as configurações forem alteradas sem usar Padrões de Configuração ou se tiver ocorrido um problema durante a implantação, como um problema de firmware ou uma configuração inválida. É possível determinar o status de conformidade de cada servidor na página Padrões de Configuração: Perfis de Servidor.

Ativando um perfil de servidor

É possível ativar um perfil do servidor em um servidor gerenciado substituído, reatribuído ou instalado recentemente.

Sobre esta tarefa

Se você substituir um servidor existente ou instalar um servidor fornecido anteriormente em um compartimento vazio em um chassi, deverá ativar o perfil de servidor para que esse novo servidor forneça as alterações de configuração no novo servidor.

Importante:

- Ao usar a virtualização de endereços, um servidor mantém seu endereço MAC ou WWN virtual designado até ser desligado. Para desativar um perfil que tenha a virtualização de endereços ativada, a caixa de seleção **Desligar o servidor** é marcada por padrão. Certifique-se de que o servidor original esteja desligado antes de ativar o perfil inativo em um servidor diferente para evitar conflitos de endereço.
- Se você excluir um perfil que não é o criado mais recentemente, os endereços MAC e WWN virtuais *não são* liberados do conjunto de endereços. Para obter mais informações, consulte Excluindo um perfil de servidor.
- As configurações em um servidor poderão ficar fora de conformidade com o perfil de servidor se as configurações forem alteradas sem usar Padrões de Configuração ou se tiver ocorrido um problema durante a implantação, como um problema de firmware ou uma configuração inválida. É possível determinar o status de conformidade de cada servidor na página Padrões de Configuração: Perfis de Servidor.

Procedimento

Para ativar um perfil de servidor, conclua as seguintes etapas.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Perfis de Servidor**. A página Padrões de Configuração: Perfis de Servidor é exibida.

Etapa 2. Selecione o perfil de servidor para ativar.

Dicas: o estado atual dos perfis de servidor está listado na coluna **Status do Perfil**. É possível ativar o perfil de servidor que apresenta um estado Inativo ou Ativação pendente.

Etapa 3. Clique no ícone **Ativar Perfil de Servidor** ().

Etapa 4. Clique em **Ativar**.

Se o perfil estiver no estado pendente, ativo ou com falha ativa, você poderá escolher quando ativar a implantação:

- **Completo**. Liga ou reinicia imediatamente o servidor para ativar as configurações de servidor, Baseboard Management Controller e Unified Extensible Firmware Interface (UEFI).
- **Parcial**. (padrão) Ativa imediatamente as configurações do controlador de gerenciamento, mas adia a ativação das configurações de servidor e UEFI até a próxima reinicialização do servidor. O servidor deve ser ligado ou reiniciado manualmente para que o perfil seja totalmente ativado.

  Nota: Ao implantar os padrões de servidor que incluíam apenas as configurações do IMM (incluindo informações do sistema, interface de gerenciamento e padrões de categoria estendida do BMC), o servidor não precisará ser reiniciado.

Quando o perfil de servidor é ativado pela primeira vez, o status do perfil muda para "Ativo." Depois que a conformidade é verificada, o status muda para "Compatível" ou "Não compatível."

Resultados

O estado do perfil de servidor na página Padrão de Configuração: Perfis de Servidor altera para Ativo.

Desativando um perfil de servidor

É possível cancelar a atribuição de um perfil de servidor de um servidor ou compartimento de chassi desativando o perfil.

Procedimento

Para desativar um perfil de servidor, conclua as seguintes etapas.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Perfis de Servidor**. A página Padrões de Configuração: Perfis de Servidor é exibida.

Etapa 2. Selecione o perfil de servidor para desativar.

Dica: o estado atual dos perfis de servidor está listado na coluna **Status de Perfil**.

Etapa 3. Clique no ícone **Desativar Perfil de Servidor** ( ).

Etapa 4. Escolha uma das opções de desativação a seguir:

- **Redefinir Configurações de Identidade do IMM**. Redefinir as configurações de identidade configuradas por perfil (incluindo o nome do host, o nome do dispositivo ou os endereços IP estáticos atribuídos da interface de gerenciamento do Baseboard Management Controller). Apenas as configurações definidas por meio do padrão do servidor associado são redefinidas.

  Nota: Para servidores com endereços IP atribuídos estaticamente, essa opção ativa o modo DHCP. Se não houver um servidor DHCP ativado na rede, o servidor deverá ser reconfigurado manualmente com um endereço IP estático válido. Os servidores de rack e em torre Converged, NeXtScale e System x devem, então, ser gerenciado novamente usando o XClarity Administrator.

- **Desligar o servidor**. Desliga o servidor. Quando o servidor é ligado novamente, as atribuições de endereço virtual são revertidas para os padrões gravados.
- **Forçar desativação**. Desativa o perfil do servidor mesmo se o servidor foi removido ou não está acessível.
- **Redefinir configurações de porta interna do comutador**. Redefine as configurações de porta interna do comutador configuradas por perfil para valores padrão, incluindo desativação do modo UFP e remoção de portas de membros associados das definições de VLAN. Apenas as configurações definidas por meio do padrão do servidor associado são redefinidas.

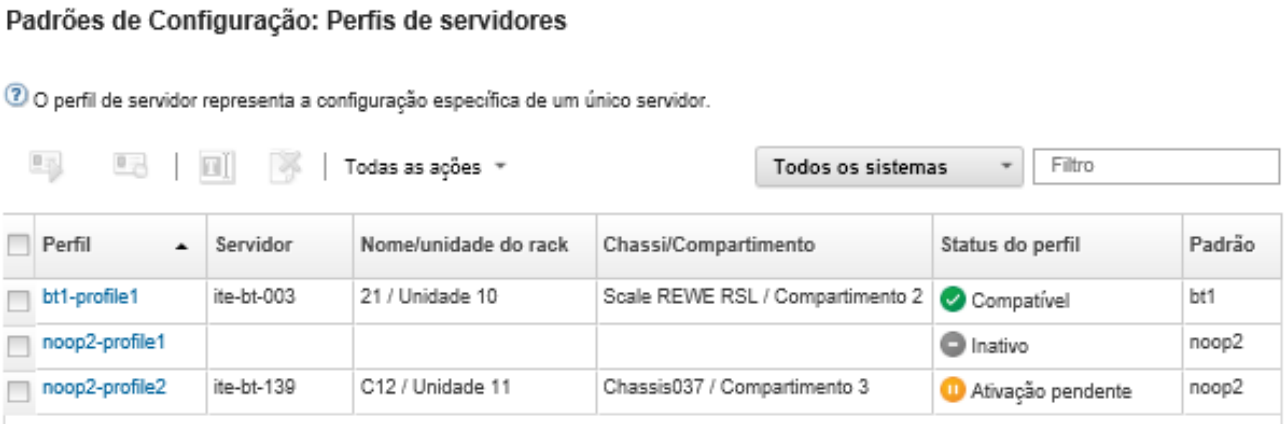
  Essa opção é desativada por padrão.

Escolha essa opção para deixe as portas do comutador em um estado em que o perfil de servidor possam ser implantado em outro servidor sem configurações que entrem em conflito com a configuração de porta do comutador anterior.

Etapa 5. Clique em **Desativar**.

Resultados

O estado do perfil de servidor na página Padrão de Configuração: Perfis de Servidor altera para Inativo.



Nota: Se o XClarity Administrator não puder se comunicar com controlador de gerenciamento (por exemplo, se o controlador de gerenciamento está em um estado de erro ou está reiniciando), a desativação do perfil do servidor falha e o perfil de servidor não é desligado. Se isto ocorrer, tente novamente a desativação e selecione a opção de forçar desativação para desativar o perfil. O servidor atribuído anteriormente é configurado ainda com as atribuições de endereço e identidade atribuídos ao perfil. O servidor precisará ser desligado e removido da infraestrutura para evitar conflitos de endereço.

Excluindo um perfil de servidor

É possível excluir apenas os perfis de servidor que foram desativados.

Antes de iniciar

Certifique-se de que os perfis de servidor a serem excluídos estejam desativados (consulte Desativando um perfil de servidor).

Procedimento

Para excluir um perfil de servidor, conclua as seguintes etapas

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Perfis de Servidor**. A página Padrões de Configuração: Perfis de Servidor é exibida.

Etapa 2. Selecione o perfil de servidor que está no estado Desativado.

Dica: o estado atual dos perfis de servidor está listado na coluna **Status de Perfil**.

Etapa 3. Clique no ícone **Excluir** ( ).

Nota: Quando você exclui o perfil criado mais recentemente, nenhum endereço MAC ou WWN virtual é liberado do conjunto de endereços. Se você excluir um perfil que não é o criado mais recentemente, os endereços MAC e WWN virtuais *não são* liberados do conjunto de endereços.

Trabalhando com chassi de marcador

É possível pré-provisionar servidores que serão instalados em um chassi do Flex System posteriormente configurando um *chassi de marcador* para agir como destino para o padrão de servidor até o hardware físico chegar.

Sobre esta tarefa

Quando você implanta um padrão de servidor em um chassi de marcador, o, Lenovo XClarity Administrator cria um perfil de servidor para os 14 compartimentos do servidor no chassi do Flex System e reserva os endereços IP de gerenciamento e endereços virtuais Ethernet ou Fibre Channel para os servidores.

O chassi de marcador reúne todos os perfis de servidor para que, quando o hardware chegar, seja possível implantar o chassi de marcador para ativar os perfis de servidor em servidores físicos em vez de implantar os 14 perfis de servidor individualmente. Cada servidor deve ser reinicializado para ativar totalmente o perfil de servidor.

Criando um chassi de marcador

É possível criar um chassi de marcador que pode ser fornecido antes do hardware ser instalado. O fornecimento de nós de cálculo no chassi reserva endereços IP de gerenciamento e endereços virtuais Ethernet ou Fibre Channel.

Procedimento

Conclua as seguintes etapas para criar um chassi de marcador.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Padrões**. A página Padrões de Configuração: Padrões é exibida.

Etapa 2. Clique na guia **Chassi de Marcador**.

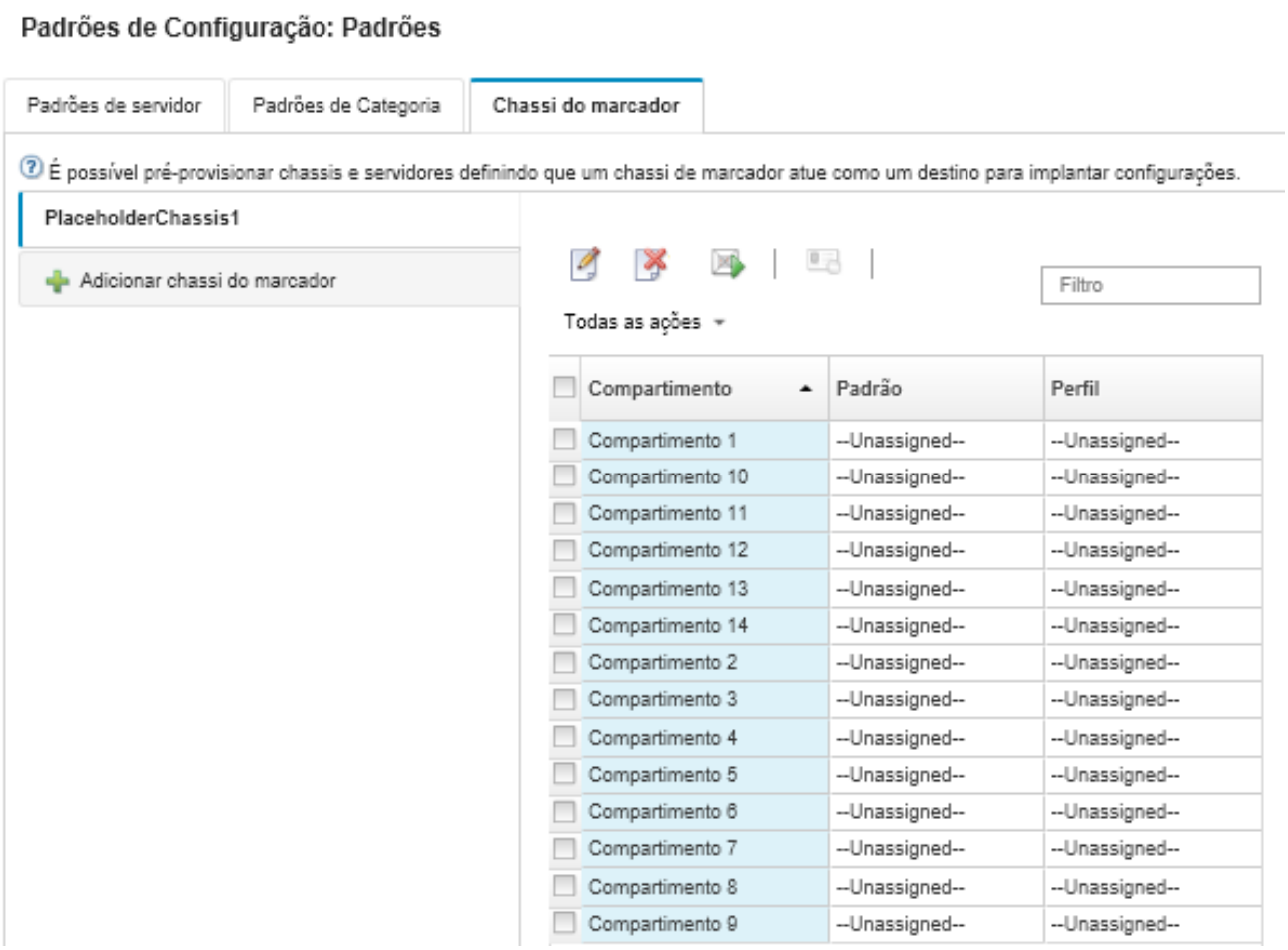
Etapa 3. Clique na guia vertical **Adicionar Chassi de Marcador**.

Etapa 4. Insira um nome e descrição para o chassi de marcador.

Etapa 5. Clique em **Adicionar**.

Depois de concluir

Uma guia vertical é adicionada para o novo chassi de marcador na página Padrões de Configuração: Chassi de Marcador.



Nesta página, é possível executar as ações a seguir em um chassi de marcador selecionado:

- Implante o chassi de marcador clicando no ícone **Implantar** ( ).
- Modifique o nome e a descrição do chassi de marcador clicando no ícone **Editar** ( ).
- Implante um padrão de servidor ao chassi de marcador (consulte Implantando um padrão de servidor em um chassi de marcador).
- Desative o perfil de servidor de um chassi de marcador (consulte Desativando um perfil de servidor).
- Exclua o chassi de marcador clicando no ícone **Excluir** ( ).

Implantando um padrão de servidor em um chassi de marcador

É possível implantar um padrão de servidor em cada compartimento em um chassi de marcador. Implantar um padrão de servidor antes da instalação dos servidores no chassi do Flex System cria um perfil de servidor para cada compartimento do servidor no chassi e reserva endereços IP de gerenciamento e endereços virtuais Ethernet ou Fibre Channel.

Procedimento

Conclua as seguintes etapas para implantar um padrão de servidor em um chassi de marcador.

Etapa 1. Na barra de menus do Lenovo XClarity Administrator, clique em **Fornecimento → Padrões de Configuração de Servidor**. A página Padrões de Configuração de Servidor é exibida.

Etapa 2. Clique na guia **Padrões de Servidor**.

Etapa 3. Selecione o padrão de servidor que deseja implantar no chassis de marcador.

Etapa 4. Clique no ícone **Implantar** (). A caixa de diálogo Implantar Padrão de Servidor é exibida com uma lista de chassis e chassis de marcador disponíveis.

Etapa 5. Selecione **Adiado** na lista **Ativação**.

Etapa 6. Clique em **Mostrar Compartimentos Vazios**.

Etapa 7. Escolha um ou mais compartimentos de chassi de marcador nos quais deseja implantar o padrão de servidor.

Etapa 8. Clique em **Implantar**. Uma caixa de diálogo é exibida e lista o status de implantação de cada compartimento selecionado.

Etapa 9. Clique em **Implantar** novamente para iniciar o processo de implantação.

Um perfil de servidor é criado e designado a cada compartimento selecionado no chassi de marcador.

Nota: A implantação pode levar vários minutos para ser concluída.

Etapa 10. Clique em **Fechar**.

Depois de concluir

Você pode monitorar o progresso da implantação clicando em **Monitoramento → Trabalhos** na barra de menu do XClarity Administrator. Você também pode monitorar a criação do perfil de servidor clicando em **Fornecimento → Perfis de Servidor**. Após a conclusão da implantação, revise os perfis de servidor gerados e anote o endereço IP de gerenciamento e os endereços Ethernet ou Fibre Channel virtualizados.

Após o chassi do Flex System ser fisicamente instalado no rack e então descoberto e gerenciado pelo XClarity Administrator, é possível implantar o chassi de marcador para fornecer todos os servidores no chassi (consulte Implantando um padrão de servidor em um chassi de marcador).

Implantando um chassi de marcador

Depois de configurar previamente um chassi de marcador implantando um padrão de servidor nesse chassi de marcador, e então descobrir e gerenciar o chassi real, é possível implantar o chassis de marcador para configurar os nós de cálculo reais.

Procedimento

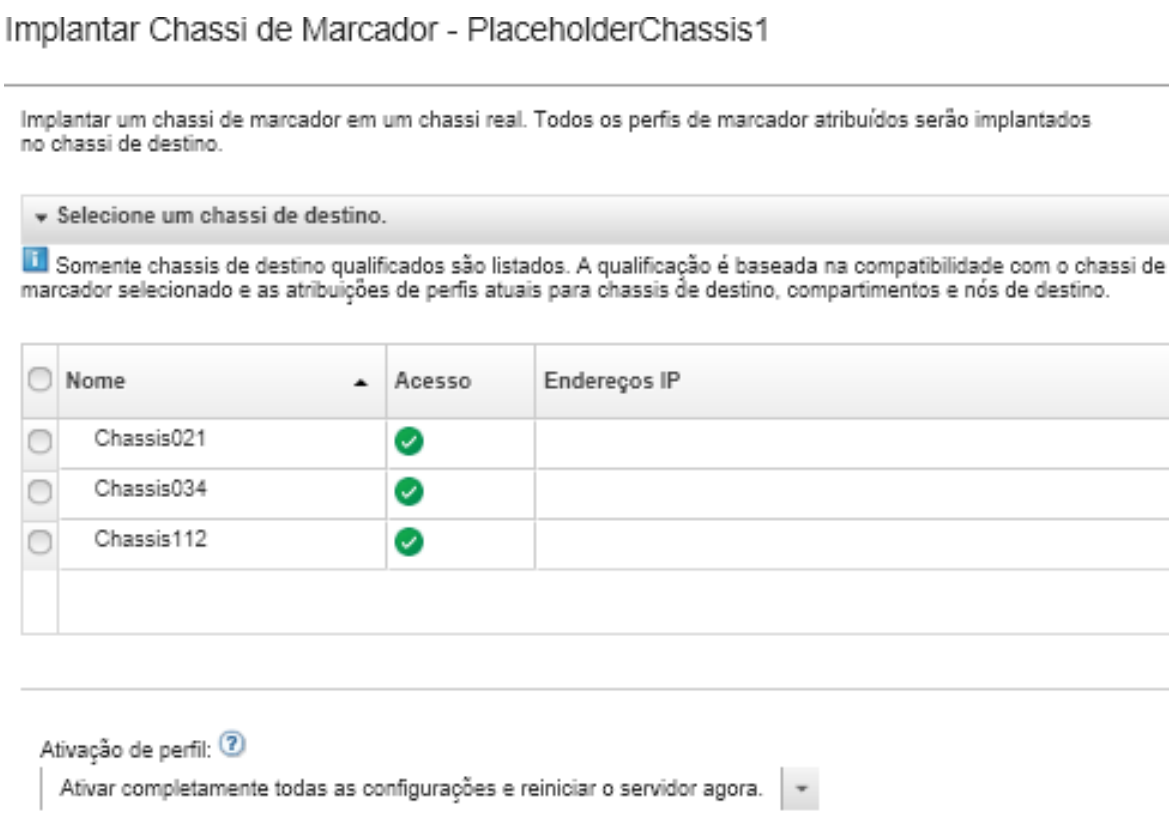
Conclua as seguintes etapas para implantar um chassi de marcador.

Etapa 1. Na barra de menus do Lenovo XClarity Administrator, clique em **Fornecimento → Padrões de Configuração de Servidor**. A página Padrões de Configuração de Servidor é exibida.

Etapa 2. Clique na guia **Chassi de Marcador**.

Etapa 3. Selecione a guia vertical do chassi de marcador que deseja implantar.

Etapa 4. Clique no ícone **Implantar chassi de marcador** () para exibir a caixa de diálogo Implantar chassi de marcador.



Etapa 5. Escolha quando ativar as configurações:

Nota: As configurações de rede em portas internas do comutador relacionado são enviadas por push para o comutador imediatamente após a implantação, independentemente da configuração de ativação.

- **Completo**. Liga ou reinicia imediatamente o servidor para ativar as configurações de servidor, Baseboard Management Controller e Unified Extensible Firmware Interface (UEFI).
- **Parcial**. (padrão) Ativa imediatamente as configurações do controlador de gerenciamento, mas adia a ativação das configurações de servidor e UEFI até a próxima reinicialização do servidor. O servidor deve ser ligado ou reiniciado manualmente para que o perfil seja totalmente ativado.

  Nota: Ao implantar os padrões de servidor que incluíam apenas as configurações do IMM (incluindo informações do sistema, interface de gerenciamento e padrões de categoria estendida do BMC), o servidor não precisará ser reiniciado.

Etapa 6. Clique em **Ativar**.

Redefinição de adaptadores de armazenamento para os valores padrão

Você pode redefinir os adaptadores de armazenamento local para as configurações de fabricação padrão para um ou mais servidores.

Sobre esta tarefa

Atenção: Essa ação apaga todos os dados nos adaptadores de armazenamento local.

Se o servidor for desligado e o link RAID for suportado, o servidor será inicializado na configuração do sistema para redefinir os adaptadores HDD e SSD locais.

Procedimento

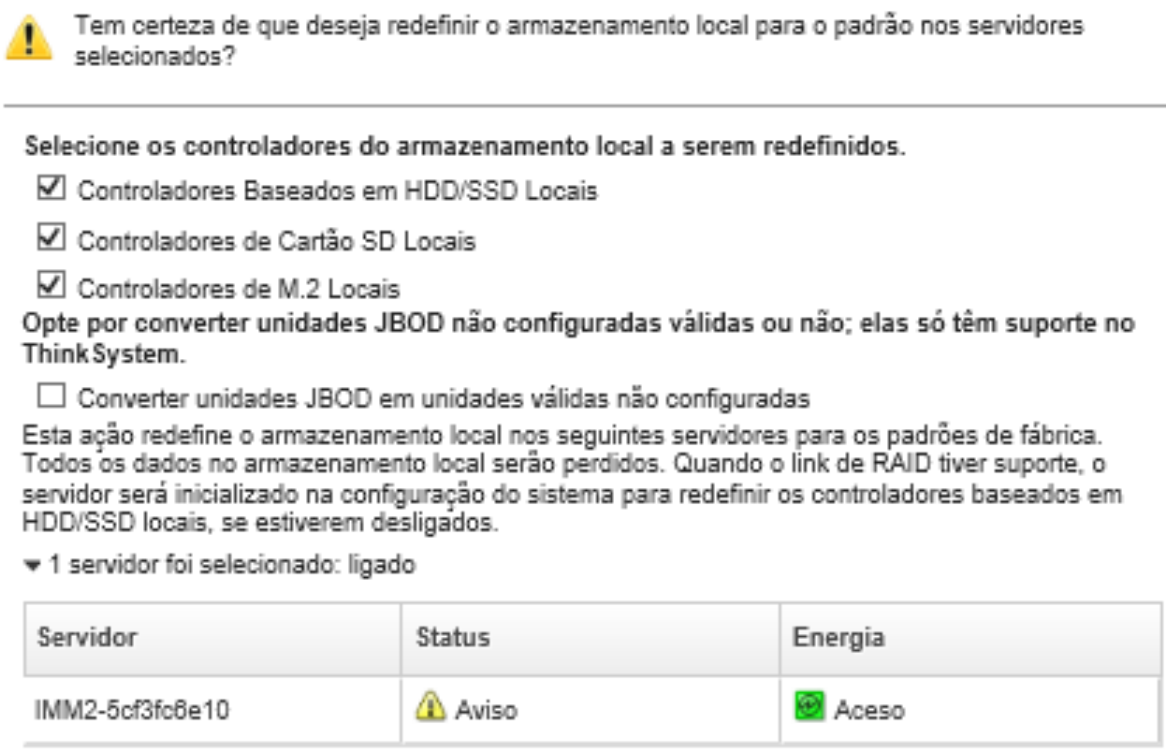
Conclua estas etapas para limpar a configuração do RAID para um ou mais servidores.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados (servidores de rack e nós de cálculo).

É possível classificar as colunas da tabela para facilitar a localização do servidor que deseja gerenciar. Além disso, é possível selecionar um tipo de servidor na lista suspensa **Todos os Sistemas** e inserir texto (como nome ou endereço IP) no campo **Filtro** para filtrar mais os servidores que são exibidos.

Etapa 2. Selecione um ou mais servidores

Etapa 3. Selecione **Todas as Ações → Serviço → Redefinir Armazenamento Local para Padrões**. Uma caixa de diálogo é exibida e solicita informações adicionais.



Etapa 4. Selecione os adaptadores de armazenamento local a serem redefinidos.

Etapa 5. : (Somente servidores ThinkSystem) Opte por converter unidades JBOD em boa não configurada.

Etapa 6. Clique em **Redefinir Armazenamento**.

Configurando a memória

Você pode criptografar e descriptografar a memória persistente para DIMMs de memória persistente Intel® Optane™ DC.

Procedimento

Conclua o procedimento a seguir para criptografar e descriptografar a memória persistente.

Etapa 1. No menu XClarity Administrator, clique em **Hardware → Servidores**. A página Servidores é exibida com uma exibição tabular de todos os servidores gerenciados (servidores de rack e nós de cálculo).

Etapa 2. Selecione um ou mais servidores que você deseja configurar.

Etapa 3. Clique em **Todas as Ações → Segurança → Operação de Segurança do Intel Optane** para exibir a caixa de diálogo Operação do Intel Optane PMEM.

Etapa 4. Selecione a operação de segurança que você deseja executar.

- **Habilitar segurança**. Os dados que são gravados na região de memória persistente são criptografados com a senha especificada.

  Importante: Registre a senha de criptografia. A senha é necessária para autorizar a desativação da segurança ou o apagamento da senha de criptografia.

- **Desabilitar segurança**. Os dados gravados na região de memória persistente não são criptografados.

  Os dados que já estão armazenados na região de memória persistente permanecem criptografados e ainda acessíveis.

Nota: Essa ação está disponível somente quando a segurança está habilitada e a senha definida. Você deve autorizar essa operação usando a senha atual. Será possível desativar a segurança para vários DIMMs no dispositivo apenas se todos os DIMMs compartilharem a mesma senha.

- **Apagar com segurança**. Apaga a senha de criptografia que é usada para criptografar os dados armazenados na região de memória persistente para garantir que os dados sejam irrecuperáveis.

  Nota: Essa ação está disponível somente quando a segurança está habilitada e a senha definida. Você deve autorizar essa operação usando a senha atual.

- **Apagar com segurança sem senha** Apaga com segurança todos os dados armazenados na memória persistente dos DIMMs especificados no dispositivo. Depois do apagamento seguro, todos os dados são irrecuperáveis.

  Nota: Essa ação está disponível somente quando a segurança está desabilitada e a senha não é necessária.

Etapa 5. Se necessário, especifique e confirme a senha.

Etapa 6. Clique em **OK**.

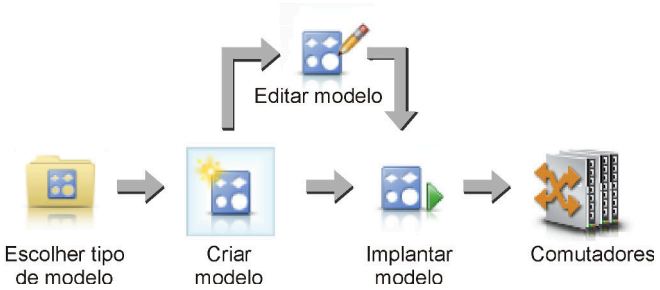
Capítulo 12. Configurando comutadores com modelos de configuração

É possível usar modelos para fornecer rapidamente vários comutadores de rack de CNOS de um conjunto único de configurações definidas.

Sobre esta tarefa

Você pode usar modelos de configuração de comutador em XClarity Administrator para definir configurações globais, canais de porta, LANs virtuais, grupos de agregação de links virtuais e topologias de lateral da folha em comutadores gerenciados. Atualmente, apenas os comutadores de rack que executam o CNOS são suportados.

A figura a seguir ilustra o fluxo de trabalho para configurar comutadores de rack gerenciados.



1. **Escolha um tipo de modelo.**

   Um *modelo de configuração de comutador* agrupa configurações de comutador relacionadas. É possível criar os seguintes tipos de modelos de configuração de comutador.
   - **Globais**. Define as configurações globais, incluindo a propriedade do sistema, as tags de VLAN nativas e interfaces L2.
   - **Canal de porta**. Define configurações de canal de porta básicas e avançadas, remove portas e exclui um canal de porta.
   - **Lateral da folha**. Implanta uma configuração de lateral da folha em uma topologia existente.
   - **LAN Virtual (VLAN)**. Define as propriedades e configurações de VLAN e exclui uma VLAN.
   - **Grupo de agregação de links virtuais (VLAG)**. Define configurações de pares de VLAG, básicas e avançadas e cria e exclui uma instância de VLAG.
2. **Crie um modelo.**

   É possível criar vários modelos de configuração de comutador para representar as diferentes configurações usadas em seu datacenter. Você usa modelos de configuração de comutador para controlar uma configuração comum de comutador de um único local.

   Para obter mais informações sobre como criar modelos de configuração do comutador, consulte Criando um modelo de configuração de comutador.
3. **Implante o modelo em um ou mais comutadores.**

   É possível implantar um padrão de servidor em um ou mais comutadores de rack individuais que executam o CNOS.

   Para obter mais informações sobre como implantar uma configuração do comutador, consulte Implantando modelos de configuração de comutador em um comutador de destino.
4. **Edite um modelo.**

Editar um modelo de configuração de comutador não implanta automaticamente as configurações atualizadas em todos os comutadores nos quais o modelo inicial foi implantado. Você precisa reimplantar manualmente os modelos alterados. A página Histórico controla as configurações para cada implantação.

Configurando preferências padrão de configuração do servidor

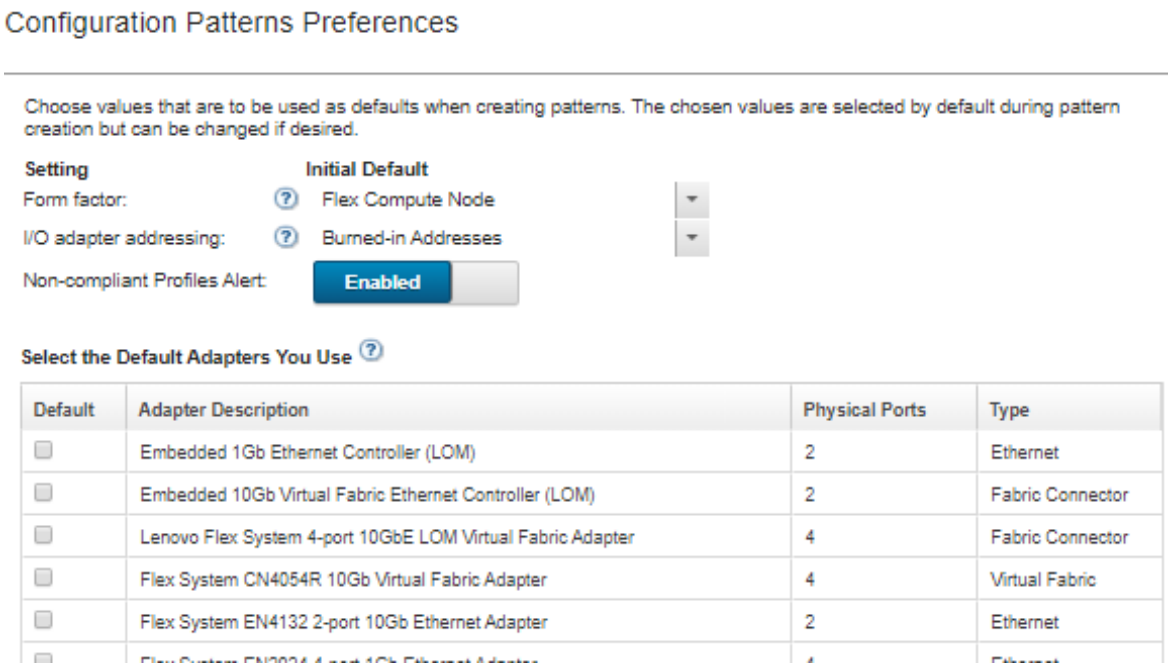
É possível configurar valores a serem selecionados pelo padrão ao criar os padrões de configurações do servidor. Os valores podem ser alterados durante a criação do padrão de servidor.

Procedimento

Para definir configurações padrão do servidor, conclua as etapas a seguir.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento** e, em seguida, clique no ícone de ajuda (?) ao lado de **Padrões de Configuração** para exibir a página Padrões de Configuração: Introdução.

Etapa 2. Clique em **Definir Preferência do Padrão de Configuração** para exibir a caixa de diálogo Preferência do Padrão de Configuração.



Etapa 3. Selecione o fator de forma de servidor padrão.

Etapa 4. Selecione o modo de endereçamento do adaptador de E/S padrão.

- **Gravado em**. Use os endereços World Wide Name (WWN) e Media Access Control (MAC) existentes fornecidos com o adaptador de fábrica.
- **Virtual**. Use o endereçamento de adaptador de E/S virtual para simplificar o gerenciamento de conexões LAN e SAN. A virtualização de endereços de E/S designa novamente os endereços de hardware gravados com endereços WWN Fibre e MAC Ethernet virtualizados. Isso pode agilizar a implantação configurando previamente a afiliação de zonas SAN e facilitar o failover eliminando a necessidade de reconfigurar atribuições de zoneamento de SAN e mascaramento de LUN ao substituir o hardware.

  Quando o endereçamento virtual está habilitado, os endereços Ethernet e Fibre Channel são alocados, por padrão, independentemente dos adaptadores definidos. É possível escolher o conjunto do qual os endereços Ethernet e Fibre Channel são alocados.

Também é possível editar as configurações de endereço virtual clicando no ícone **Editar** ( ) próximo aos modos de endereço.

Restrição: o endereçamento virtual tem suporte apenas em servidores no chassi do Flex System. Servidores de rack e em torre não são aceitos.

Etapa 5. Escolha entre habilitar ou desabilitar o acionamento de um alerta quando as opções de configuração do servidor não corresponderem ao perfil de configuração do servidor atribuído

Os alertas são gerados apenas para não conformidade com um perfil ativo (no estado ASSIGNED ou ERROR_ACTIVATING).

Quando a configuração do servidor se tornar compatível ou se o perfil do servidor não for atribuído, o alerta de perfil não compatível será excluído.

Etapa 6. Selecione um ou mais adaptadores de E/S padrão que você deseja usar como adaptadores preferenciais nas listas de seleção.

Etapa 7. Clique em **Salvar**.

Criando um modelo de configuração de comutador

Ao criar um modelo de configuração de comutador, você define as configurações de um tipo específico.

Antes de iniciar

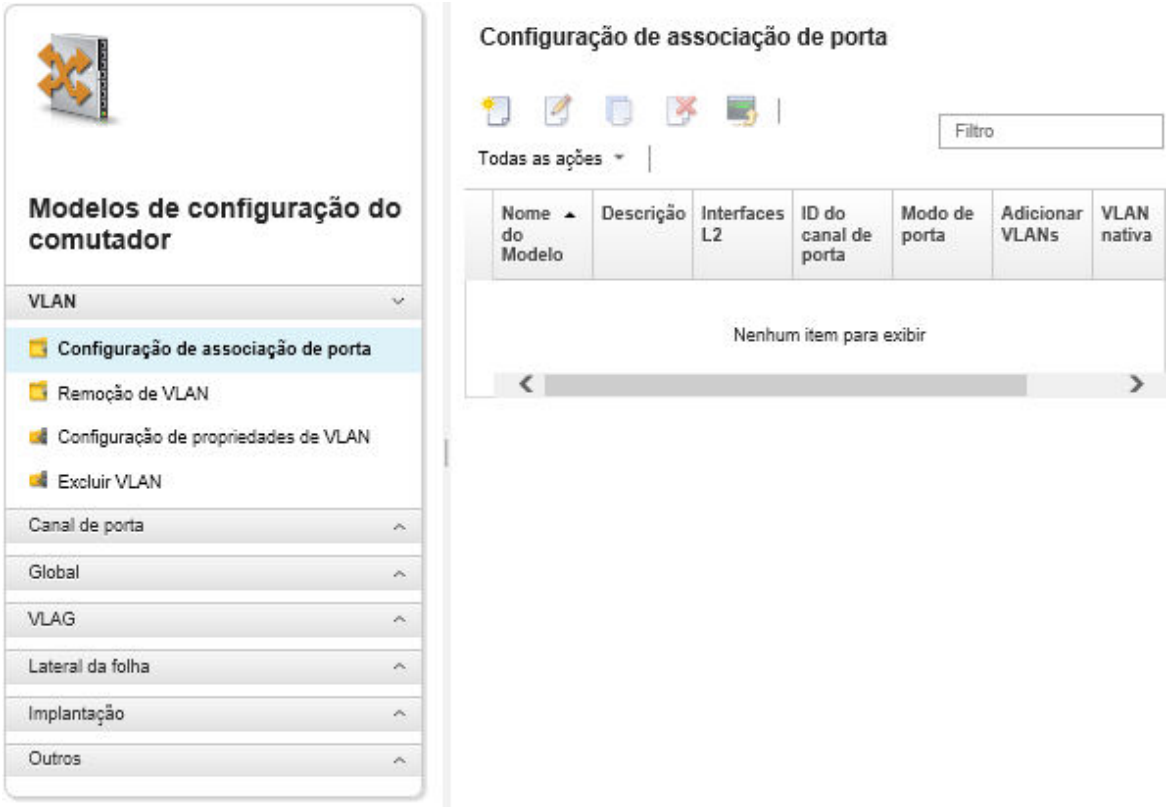
Antes de criar um modelo de configuração do comutador, considere as seguintes sugestões:

- Identifique os grupos de comutadores que têm as mesmas opções de hardware e que você deseja configurar da mesma maneira. É possível usar um modelo de configuração de comutador para aplicar as mesmas configurações em diversos comutadores, controlando, dessa forma, uma configuração comum de um local.
- Identifique os aspectos da configuração que você deseja personalizar (por exemplo, configurações globais, de canais de porta ou VLAN).

Procedimento

Execute as seguintes etapas para criar um modelo de configuração de comutador.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.



Etapa 2. Selecione o tipo de modelo que você deseja criar na navegação esquerda.

Etapa 3. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Criar novo modelo.

Os campos que estão listados nessa caixa de diálogo variam dependendo do tipo de modelo.

Etapa 4. Clique em **Salvar** para salvar o modelo ou clique em **Salvar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino.

Depois de concluir

Se você clicou em **Salvar e Implantar**, a página Implantar modelo de comutador é exibida. Nesta página, é possível implantar o modelo de configuração de comutador em comutadores específicos.

Se você clicou em **salvar**, o modelo de configuração do comutador será salvo na página Modelos de configuração do comutador. Nesta página, é possível executar as ações a seguir nos padrões de servidor selecionados:

- Exibir detalhes sobre o modelo clicando nele na coluna Nome.
- Exibir uma lista agregada de todos os modelos clicando em **Outros → Todos os modelos**.
- Implantar o modelo (consulte Implantando modelos de configuração de comutador em um comutador de destino).
- Copiar e modificar um modelo clicando no ícone **Copiar** ( ).
- Edite o modelo clicando no ícone **Editar** ( ).

Nota: As alterações no modelo não *são reimplantadas automaticamente* nos comutadores em que o modelo original foi implantado.

- Renomeie o padrão clicando no ícone **Renomear** ().
- Exclua o padrão clicando no ícone **Excluir** ().

Definindo configurações de associação de porta de VLAN

É possível adicionar portas físicas e canais de porta a uma ou mais VLANs (para troncos) usando o modelo de configuração de associação de porta de VLAN.

Procedimento

Execute as seguintes etapas para criar um modelo de configuração de associação de porta.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **VLAN → Configuração de associação de porta** na navegação esquerda e, em seguida, clique no ícone **Criar** ().

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

Importante: Você deve especificar uma ou mais interfaces L2 físicas ou IDs de canal de porta.

- Insira um nome e uma descrição para o modelo.
- Especifique uma ou mais interfaces físicas L2 válidas. É possível especificar uma lista de interfaces separados por vírgula, um intervalo de IDs separados por um hífen ou uma combinação de ambos, por exemplo:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Especifique um ou mais IDs do canal de porta (interfaces de agregador de porta). É possível especificar uma lista de números separados por uma vírgula, um intervalo de números separados por um hífen ou uma combinação de ambos. Os valores e intervalos podem ser números de 1 – 4096, por exemplo:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13
- Escolha se a porta aceita tráfego marcado ou não marcado. Este pode ser um dos valores a seguir.
  - **acesso**. A porta transporta o tráfego para uma única VLAN.
  - **trunk**. (padrão) A porta transporta o tráfego de todas as VLANs que são acessíveis ao comutador.
- Especifique um ou mais IDs de VLAN a serem adicionados à lista de associação VLAN da porta. É possível especificar uma lista de números separados por uma vírgula, um intervalo de números separados por um hífen ou uma combinação de ambos. Os valores e intervalos podem ser números de 1 – 4096, por exemplo:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Notas:

  - Se o modo da porta estiver configurado como "acesso," apenas o primeiro ID de VLAN será usado. Por exemplo, no intervalo `2-4,5,10-20`, apenas `2` é usado.
  - O CNOS reserva IDs de VLAN 4000 – 4095 por padrão. O uso de IDs de VLAN reservados (pelo CNOS ou por outro usuário) pode fazer com que a implantação de configuração do comutador falhe.
- Especifique um ID de VLAN nativo com o qual o tráfego não marcado é marcado. Pode ser um número de 1 – 4096.

  Notas:
  - Esse campo é válido somente quando o modo de porta é definido como "trunk."
  - Se não for especificado, ou se o ID estiver fora das VLANs de estado final em uma porta, a porta efetivamente não permitirá tráfego não marcado.
- Selecione **Criar VLANs** para criar IDs de VLAN que estão atualmente ausentes no comutador de destino.

  Se uma porta pertencer a uma VLAN que não está criada, a porta continuará a ser um membro dessa VLAN, mas qualquer tráfego marcado com esse ID de VLAN e que atingir a porta não terá permissão para passar.

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Definindo as propriedades de VLAN

É possível configurar as propriedades avançadas de VLAN usando o modelo de configuração de propriedades de VLAN.

Procedimento

Execute as seguintes etapas para criar um modelo de configuração de propriedades de VLAN.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **VLAN → Configuração de propriedades de VLAN** na navegação esquerda e, em seguida, clique no ícone **Criar** ( ).

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

- Insira um nome e uma descrição para o modelo.
- Especifique um ID de VLAN no qual aplicar as alterações. Pode ser um número de 1 – 4095.

  Nota: O CNOS reserva IDs de VLAN 4000 – 4095 por padrão. O uso de IDs de VLAN reservados (pelo CNOS ou por outro usuário) pode fazer com que a implantação de configuração do comutador falhe.
- Especifique um nome personalizado para a VLAN.
- Escolha se a VLAN está ativa (habilitada) ou suspensa (desativada).
- Escolha se o fluxo de multicast IP (IPMC) na VLAN de destino é controlado (habilitado) em interfaces IPv4 ou IPv6. Este pode ser um dos valores a seguir.
  - **Desabilitar**. IPv4 e IPv6 estão desativados.
  - **Habilitar**. IPv4 e IPv6 estão ativados.
  - **Desabilitar IPv4**.

- **Habilitar IPv4**
- **Desabilitar IPv6**
- **Habilitar IPv6**

  Essa ação é aditiva, indicando que "Habilitar IPv4" implantado sobre "Desabilitar" resulta em "Desabilitar IPv4", mas implantar sobre "Habilitar IPv6" resulta em " "Habilitar". O inverso é verdadeiro para as opções de desativação.

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Removendo configurações de VLAN

É possível remover interfaces de VLANs usando o modelo de remoção de VLAN.

Procedimento

Execute as seguintes etapas para criar um modelo de remoção de VLAN.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **VLAN → Remoção de VLAN** na navegação esquerda e, em seguida, clique no ícone **Criar** ( ).

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

Importante: Você deve especificar uma ou mais interfaces L2 físicas ou IDs de canal de porta.

- Insira um nome e uma descrição para o modelo.
- Especifique uma ou mais interfaces físicas L2 válidas. É possível especificar uma lista de interfaces separados por vírgula, um intervalo de IDs separados por um hífen ou uma combinação de ambos, por exemplo:
  - Ethernet1/10
  - Ethernet1/1,3,5,7
  - Ethernet1/1-10,21-30
  - Ethernet2/1-5,7,9,11-13
- Especifique um ou mais IDs do canal de porta (interfaces de agregador de porta). É possível especificar uma lista de números separados por uma vírgula, um intervalo de números separados por um hífen ou uma combinação de ambos. Os valores e intervalos podem ser números de 1 – 4096, por exemplo:
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13
- Especifique um ou mais IDs de VLAN a serem removidos da lista de associação VLAN da porta. É possível especificar uma lista de números separados por uma vírgula, um intervalo de números separados por um hífen ou uma combinação de ambos. Os valores e intervalos podem ser números de 1 – 4096, por exemplo:
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13

Nota: Se o modo de porta for configurado como "acesso", a remoção da VLAN fará com que a porta entre na VLAN 1.

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Excluindo VLANs

É possível remover as configurações de VLAN do comutador usando o modelo Excluir VLAN.

Procedimento

Execute as seguintes etapas para criar um modelo de exclusão de VLAN.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **VLAN → Excluir VLAN** na navegação esquerda e, em seguida, clique no ícone **Criar** ( ).

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

- Insira um nome e uma descrição para o modelo.
- Especifique um ou mais IDs de VLAN a serem removidos da lista de associação VLAN da porta. É possível especificar uma lista de números separados por uma vírgula, um intervalo de números separados por um hífen ou uma combinação de ambos. Os valores e intervalos podem ser números de 1 – 4096, por exemplo:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Nota: Não é possível excluir IDs de VLAN reservados.

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Definindo configurações básicas de canais de porta

É possível criar agregadores de porta e adicionar portas aos agregadores usando um modelo de configuração básica do canal de porta.

Se o canal da porta tiver portas nele, e algumas dessas portas fizerem parte do modelo, as propriedades (prioridade de porta, modo e tempo limite) serão atualizadas com as configurações do modelo quando o modelo for implantado.

Procedimento

Execute as seguintes etapas para criar um modelo de configuração básica de canais de porta.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **Canal de porta → Configuração básica** na navegação esquerda e, em seguida, clique no ícone **Criar** ( ).

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

- Insira um nome e uma descrição para o modelo.
- Especifique uma ou mais interfaces físicas L2 válidas. É possível especificar uma lista de interfaces separados por vírgula, um intervalo de IDs separados por um hífen ou uma combinação de ambos, por exemplo:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Especifique o ID do canal de porta (interface de agregador de porta) a ser criado ou atualizado. Pode ser um número de 1 – 4095.
- Especifique o modo de porta Link Aggregation Control Protocol (LACP). Este pode ser um dos valores a seguir.
  - **Ativo**. (padrão) Habilita o LACP incondicionalmente
  - **Passivo**. Habilita o LACP apenas quando um dispositivo LCAP é detectado.
  - **Static**. Desabilita LCAP.

  Nota: Ativo e Passivo podem ser combinados no mesmo agregador, mas Estático não pode.
- Especifique a prioridade da porta LACP. Pode ser um número de 1 – 65535.

  Nota: A prioridade da porta de LACP é usada com o número da porta para formar o do ID da porta de LACP.
- Especifique o modo de tempo limite LACP para que o LCAP vá para o modo individual. Este pode ser um dos valores a seguir.
  - **Longo**. (padrão) 90 segundos
  - **Curto**. 3 segundos

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Definindo configurações avançadas de canais de porta

É possível configurar as propriedades avançadas de canais de porta usando o modelo de configuração avançada de canais de porta.

Procedimento

Execute as seguintes etapas para criar um modelo de configuração avançada de canais de porta.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **Canal de porta → Configuração avançada** na navegação esquerda e, em seguida, clique no ícone **Criar** ( ).

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

- Insira um nome e uma descrição para o modelo.
- Especifique um ID do canal de porta (interface de agregador de porta) a ser atualizado. Pode ser um número de 1 – 4095.

- Escolha se as portas individuais permanecem ou não ativas quando ocorre uma falha no LACP. Este pode ser um dos valores a seguir.
  - **Ativar**. (padrão) Habilita o LACP incondicionalmente.
  - **Suspender**. Desabilita LACP.
- Especifique o número mínimo de links que deve estar ativos para o canal de porta ser considerado ativo. Pode ser um número de 1 – 32.

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Excluindo canais de porta

É possível remover canais de porta do comutador usando o modelo Excluir canal de porta.

Procedimento

Execute as seguintes etapas para criar um modelo de exclusão de canais de porta.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **Canal de porta → Excluir canal de porta** na navegação esquerda e, em seguida, clique no ícone **Criar** ( ).

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

- Insira um nome e uma descrição para o modelo.
- Especifique um ou mais IDs do canal de porta (interfaces de agregador de porta) a ser excluído. É possível especificar uma lista de números separados por uma vírgula, um intervalo de números separados por uma vírgula ou uma combinação de ambos. Os valores e intervalos podem ser números de 1 – 4096, por exemplo:
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Definindo configurações gerais do comutador

É possível configurar as propriedades gerais do comutador usando o modelo global de configuração genérica.

Procedimento

Execute as seguintes etapas para criar um modelo global de configuração genérica do comutador.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **Global → Configuração Genérica** na navegação esquerda e, em seguida, clique no ícone **Criar** ( ).

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

- Insira um nome e uma descrição para o modelo.
- Especifique a prioridade do sistema LACP usada para gerar o ID do sistema LACP. Pode ser um número de 1 – 65535.
- Escolha onde habilitar a marcação de VLAN nativa. Este pode ser um dos valores a seguir.
  - **Entrada e saída**
  - **Somente saída**

  Nota: Essa propriedade é suportada pelo CNOS 10.10.1 e posterior.

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Definindo configurações globais da interface L2

É possível configurar as propriedades de marcação de VLAN em interfaces L2 usando o modelo de configuração de interface L2.

Procedimento

Execute as seguintes etapas para criar um modelo de configuração da interface L2.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **Global → Configuração da interface L2** na navegação esquerda e, em seguida, clique no ícone **Criar** ( ).

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

- Insira um nome e uma descrição para o modelo.
- Especifique uma ou mais interfaces físicas L2 válidas. É possível especificar uma lista de interfaces separados por vírgula, um intervalo de IDs separados por um hífen ou uma combinação de ambos, por exemplo:
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Escolha onde habilitar a marcação de VLAN nativa. Este pode ser um dos valores a seguir.
  - **Entrada e saída**
  - **Somente saída**

  Nota: Essa propriedade é suportada pelo CNOS 10.10.1 e posterior.
- Escolha entre habilitar ou desabilitar o suporte a tunelamento (QinQ).

  Nota: Essa propriedade é suportada pelo CNOS 10.10.1 e posterior.

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Definindo configurações de pares de VLAG

É possível configurar um par de VLAGs usando o modelo de Configuração de Pares do VLAG.

Procedimento

Execute as seguintes etapas para criar um modelo de Configuração de Pares do VLAG.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **VLAG → Configuração de pares** na navegação esquerda e, em seguida, clique no ícone **Criar** ( ).

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

- Insira um nome e uma descrição para o modelo.
- Escolha entre habilitar ou desabilitar o VLAG.
- Para os pares 1 e 2, preencha os campos a seguir. Os campos dos dois pares devem ser preenchidos.
  - Especifique o endereço IPv4 ou IPv6 do par de VLAG a ser usado para verificação de integridade.
  - Especifique o ID do canal de porta usado entre os dois pares. Pode ser um número de 1 – 4095.
  - Especifique o VRF usado para verificação de integridade (por exemplo, gerenciamento, padrão ou customVRF).

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Definindo configurações da instância do VLAG

É possível criar ou atualizar uma instância do VLAG usando o modelo de configuração instância do VLAG. Uma instância do VLAG é um dispositivo conectado aos dois comutadores (geralmente por meio de uma agregação de porta) ao qual o VLAG aparece como um único dispositivo.

Procedimento

Execute as seguintes etapas para criar um modelo de Configuração de Instância de VLAG.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **VLAG → Configuração de instância** na navegação esquerda e, em seguida, clique no ícone **Criar** ( ).

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

- Insira um nome e uma descrição para o modelo.
- Especifique o ID de VLAG. Pode ser um número de 1 – 64.
- Especifique o ID do canal de porta que está conectado ao Par 1 e a Par 2. Pode ser um número de 1 – 4095.
- Escolha entre habilitar ou desabilitar a instância do VLAG.

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Definindo configurações avançadas do VLAG

É possível configurar as propriedades avançadas de VLAG usando o modelo de configuração avançada de VLAG.

Procedimento

Execute as seguintes etapas para criar um modelo de Configuração Avançada de VLAG.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **VLAG → Configuração avançada** na navegação esquerda e, em seguida, clique no ícone **Criar** ( ).

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

- Insira um nome e uma descrição para o modelo.
- Especifique a prioridade que é usada para controlar qual par é principal. Pode ser um número de 1 – 65535.

  Se não for especificado, a prioridade padrão do comutador será usada. Para CNOS, o padrão é 0.
- Especifique o período de cortesia, em segundos, para que o VLAG fique online após uma reinicialização simultânea. Pode ser um número de 240 – 3600.

  Se não for especificado, o padrão do comutador será usado. Para CNOS, o padrão é 300.
- Especifique o ID da camada que é usada para diferenciar configurações de VLAG na mesma rede. Pode ser um número de 1 – 512.
- Especifique o intervalo de atraso de inicialização do VLAG, em segundos, que é usado para atrasar a ativação de portas após o recarregamento de um par. Pode ser um número de 0 – 3600.

  Se não for especificado, o padrão do comutador será usado. Para CNOS, o padrão é 120.
- Especifique o número de tentativas de Keep-Alive do VLAG (mensagens de saudação não respondidas) antes da falha do VLAG. Pode ser um número de 1 – 24.

  Se não for especificado, o padrão do comutador será usado. Para CNOS, o padrão é 3.
- Especifique o intervalo, em segundos, entre tentativas de manutenção ativa do VLAG. Pode ser um número de 2 – 300.

  Se não for especificado, o padrão do comutador será usado. Para CNOS, o padrão é 5.
- Especifique o intervalo, em segundos, entre novas tentativas de manutenção ativa do VLAG. Pode ser um número de 1 – 300.

  Se não for especificado, o padrão do comutador será usado. Para CNOS, o padrão é 30.

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Excluindo uma instância do VLAG

É possível excluir uma instância do VLAG usando o modelo de Exclusão de Instâncias do VLAG.

Procedimento

Execute as seguintes etapas para criar um modelo de Exclusão de Instâncias do VLAG.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **VLAG → Excluir instância** na navegação esquerda e, em seguida, clique no ícone **Criar** ( ).

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

- Insira um nome e uma descrição para o modelo.
- Especifique o ID exclusivo da instância do VLAG. Pode ser um número de 1 – 64.

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Definindo uma topologia de lateral da folha

É possível verificar a topologia física e implantar uma configuração de SpineLeaf (malha L3) em comutadores gerenciados usando o modelo do assistente de topologia de lateral da folha.

Procedimento

Execute as seguintes etapas para criar um modelo do assistente de topologia de lateral da folha.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Clique em **Lateral da folha → Assistente de topologia** na navegação esquerda e, em seguida, clique no ícone **Criar** ( ).

Etapa 3. Na caixa de diálogo Criar Novo Modelo, especifique as seguintes informações.

- Insira um nome e uma descrição para o modelo.
- Especifique o número do sistema autônomo (AS) para o protocolo BGP (Border Gateway Protocol) em execução no comutador. Pode ser um número de 1 – 4294967295.

  Nota: Isso é suportado pelo CNOS 10.9.3 e posterior.
- Escolha se deseja permitir links únicos entre comutadores.

  Em geral, a implantação falhará se não houver pelo menos dois links entre um comutador de lateral e de folha.

Etapa 4. Clique em **Criar** para salvar o modelo ou clique em **Criar e implantar** para salvar e implantar imediatamente o modelo em um ou mais comutadores de rack gerenciados.

Para obter informações sobre a implantação de um modelo, consulte Implantando modelos de configuração de comutador em um comutador de destino

Implantando modelos de configuração de comutador em um comutador de destino

É possível definir as configurações de porta VLAN criando um modelo de configuração de porta VLAN.

Sobre esta tarefa

Há três tipos de implantações:

- **Normal**. Implanta as configurações de comutador em um ou mais comutadores de rack em uma arquitetura em camadas básica.
- **VLAG**. Implanta as configurações do comutador em exatamente dois comutadores que oferecem suporte a uma arquitetura de grupo de agregação de link virtual (VLAG). Os comutadores devem ter a mesma versão de software e modelo.
- **Lateral da folha**. Modelos de implantação em um ou mais comutadores laterais e de folha.

Procedimento

Para implantar um modelo de configuração de computador em um ou mais comutadores gerenciados, execute as seguintes etapas.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Selecione um ou mais modelos de configuração de comutador que você deseja implantar.

Etapa 3. Clique no ícone **Implantar** ( ) para exibir a caixa de diálogo Implantar modelo.

Etapa 4. Selecione um ou mais comutadores nos quais você deseja implantar os modelos.

Somente os comutadores que são compatíveis com os modelos selecionados são listados.

Etapa 5. Clique em **Implantar**. Uma caixa de diálogo é exibida e lista o status de implantação de cada comutador selecionado.

Etapa 6. Clique em **Implantar** novamente para iniciar o processo de implantação.

Nota: A implantação pode levar vários minutos para ser concluída.

Depois de concluir

É possível exibir o histórico de implantação (consulte Exibindo o histórico de implantação da configuração do comutador).

Exibindo o histórico de implantação da configuração do comutador

É possível exibir informações sobre os modelos de configuração do comutador que foram implantados nos comutadores gerenciados, incluindo o nome e o tipo do modelo, o carimbo de data e hora e os comutadores que foram implantados. Cada implantação contém uma captura de tela do modelo de quando ele foi implantado.

Procedimento

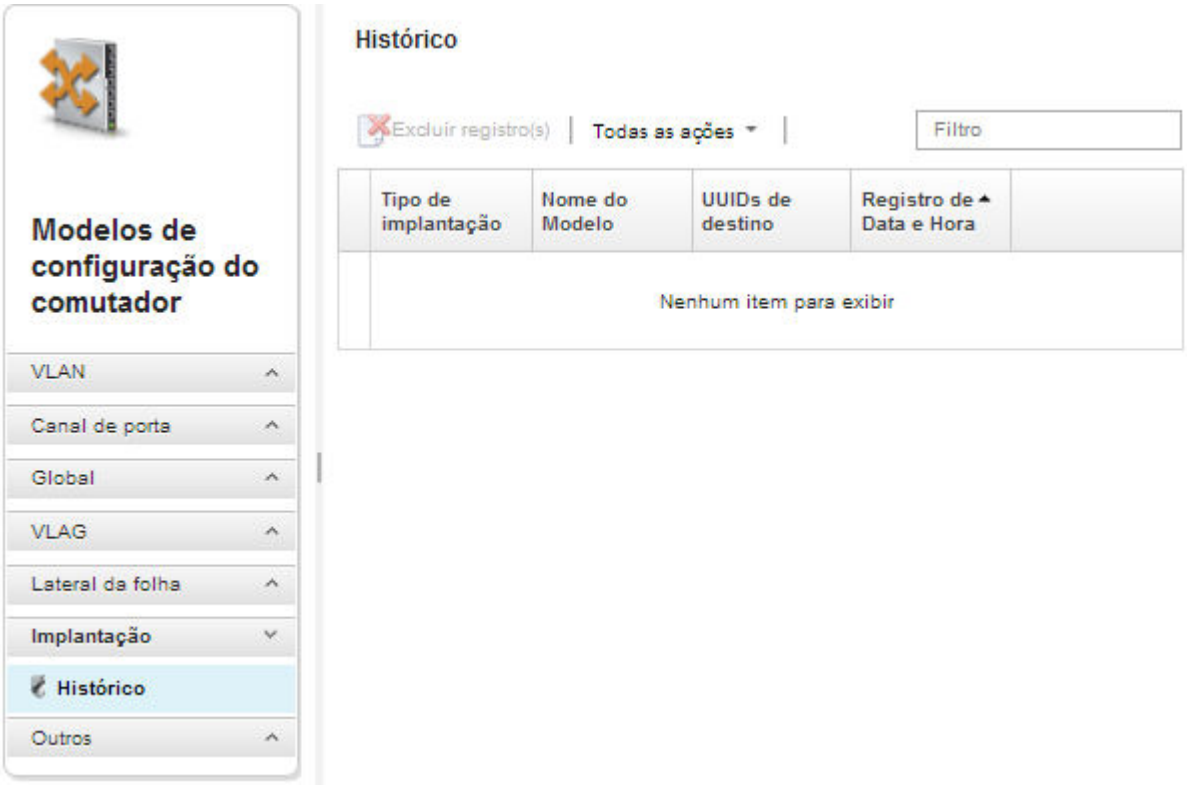
Execute as seguintes etapas para exibir um histórico de implantação da configuração do comutador.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Modelos de configuração do comutador**. A página Modelos de configuração de comutador é exibida.

Etapa 2. Expanda **Implantação** e clique em **Histórico** na navegação esquerda para exibir uma tabela dos modelos implantados.

A coluna **Status** indica se a implantação da configuração foi bem-sucedida. Pode ser um dos estados a seguir:

- **Bem-sucedida**. A implantação da configuração em todos os comutadores de destino foi concluída com êxito.
- **Aviso**. A implantação da configuração em um ou mais comutadores de destino foi concluída com avisos.
- **Com falha**. A implantação da configuração em um ou mais comutadores de destino falhou.



Depois de concluir

- Exiba as informações sobre cada modelo implantado, incluindo o que foi implantado e o que foi bem-sucedido ou teve falha clicando no nome do modelo na tabela.
- Limpe o histórico de implantação selecionando uma implantação e clicando no ícone **Excluir** ( ).

Capítulo 13. Atualizando firmware em dispositivos gerenciados

Na interface da Web do Lenovo XClarity Administrator, você pode baixar, instalar e gerenciar atualizações de firmware para dispositivos gerenciados, incluindo chassis, servidores, sistemas de armazenamento e comutadores. É possível atribuir políticas de conformidade de firmware aos dispositivos gerenciados para assegurar que o firmware nesses dispositivos permaneça compatível. Também é possível criar e editar políticas de conformidade de firmware quando níveis de firmware validados não correspondem às políticas predefinidas sugeridas.

Saiba mais:

- XClarity Administrator: aumentando a eficiência ao atualizar o firmware
- Melhores práticas nas atualizações de firmware e drivers do Lenovo ThinkSystem
- XClarity Administrator: bare metal para cluster
- XClarity Administrator: atualizações de firmware
- XClarity Administrator: fornecimento de atualizações de segurança de firmware

Antes de iniciar

A atualização do firmware e a atualização dos drivers de dispositivo são processos separados no XClarity Administrator. Não há conexão entre esses processos. O XClarity Administrator não mantém a conformidade entre o firmware e os drivers de dispositivo em dispositivos gerenciados, mesmo que seja recomendado que você atualize os drivers de dispositivos ao mesmo tempo que o firmware.

Sobre esta tarefa

Nota: Não é necessário ter um sistema operacional para atualizar o firmware. Para servidores bare metal, certifique-se de que o servidor esteja desligado antes de atualizar o firmware.

Você pode gerenciar e aplicar atualizações de firmware para os dispositivos gerenciados a seguir.

- **Chassi**. Atualizações do CMM
- **Servidores ThinkAgile, ThinkSystem, System x, Converged, Flex System e NeXtScale**. Atualizações de Baseboard Management Controller, UEFI, DSA, mezanino e adaptador
- **Comutadores RackSwitch e Flex System**
- **Dispositivos de armazenamento Lenovo Storage e ThinkSystem DM**
- **Dispositivos de biblioteca de fitas IBM TS4300**

O firmware para os dispositivos a seguir não pode ser atualizado com o XClarity Administrator.

- **Servidores ThinkServer**. Consulte a documentação fornecida com o servidor para obter informações sobre como atualizar o firmware.
- **Nós de cálculo Flex Power Systems**. Vários métodos estão disponíveis para atualizar o firmware para nós de cálculo Flex Power Systems. Para obter mais informações, consulte Documentação online dos Nós de Cálculo do IBM Flex System p260/p460. O processo é semelhante para outros nós de cálculo Flex Power Systems.
- **Comutadores Flex que estejam no modo empilhado ou no modo protegido**. *Não é possível* atualizar o firmware em comutadores empilhados. A atualização do firmware é desabilitada para todos os comutadores que estiverem empilhados.
- **Comutadores Flex**. Se você estiver usando o comutador a seguir, consulte a documentação fornecida com o comutador para obter informações sobre como atualizar o firmware.

– Extensor de Malha B22 Cisco Nexus

Procedimento

A figura a seguir ilustra o fluxo de trabalho para atualizar o firmware em dispositivos gerenciados.

Etapa 1. **Gerenciar o repositório das atualizações de firmware**

O *repositório de atualizações de firmware* contém um catálogo de atualizações disponíveis e os pacotes de atualização que podem ser aplicados aos dispositivos gerenciados.

O *catálogo* contém informações sobre as atualizações de firmware que estão disponíveis atualmente para todos os dispositivos compatíveis com o XClarity Administrator. O catálogo organiza as atualizações de firmware por tipo de dispositivo. Quando você atualiza o catálogo, o XClarity Administrator recupera informações sobre as atualizações de firmware mais recentes disponíveis do site da Lenovo (inclusive os arquivos de metadados xml. ou .json e leiame .txt) e armazena as informações no repositório das atualizações de firmware. O arquivo de carga útil (. exe) não foi baixado. Para obter mais informações sobre como atualizar o catálogo, consulte Atualizando o catálogo de produtos.

Se novas atualizações de firmware estiverem disponíveis, você deverá primeiro baixar os pacotes de atualização antes de atualizar esse firmware nos dispositivos gerenciados. A atualização do catálogo não baixa automaticamente os pacotes de atualização. A tabela do **Catálogo de Produtos** na página Repositório das Atualizações de Firmware identifica quais pacotes de atualização são baixados e quais estão disponíveis para download.

Você pode baixar atualizações de firmware de algumas maneiras diferentes:

- **Pacotes do repositório de atualizações de firmware**

  Os pacotes do repositório de atualização de firmware são coleções do firmware mais recente disponível no mesmo momento do lançamento do XClarity Administrator para a maioria dos dispositivos compatíveis e uma política de conformidade de firmware padrão atualizada. Esses pacotes de repositório são importados e, depois, aplicados da página Atualizar Servidor de Gerenciamento. Quando você aplica um pacote do repositório de atualizações de firmware, cada pacote de atualização é adicionado ao repositório das atualizações de firmware, e uma política de conformidade de firmware padrão é criada automaticamente para todos os dispositivos gerenciáveis. É possível copiar essa política predefinida, mas não é possível alterá-la.

  Os pacotes do repositório a seguir estão disponíveis.

  – **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os CMMs e comutadores Flex System.
  – **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os comutadores RackSwitch e dispositivos Lenovo Storage.
  – **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos Converged HX Series, Flex System, NeXtScale e Servidores System x.
  – **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os servidores ThinkAgile e ThinkSystem.

  - **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os servidores ThinkAgile e ThinkSystem V2.
  - **lnvgy_sw_lxca_thinksystemv3repo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os servidores ThinkAgile e ThinkSystem V3.

  É possível determinar se os pacotes do repositório de atualizações de firmware estão armazenados no repositório na coluna **Status de Download** da página Atualizar Servidor de Gerenciamento. Essa coluna contém os seguintes valores:

  - **Baixado**. O pacote do repositório de atualizações de firmware é armazenado no repositório.
  - **Não Baixado**. O pacote do repositório de atualizações de firmware está disponível, mas não armazenado no repositório.

- **UpdateXpress System Packs (UXSPs)**

  Nota: Para servidores com XCC2, esses pacotes são chamados de pacotes de firmware. O *pacote* é usado nos nomes de pacote e nomes de política predefinidos.

  Os UXSPs contêm as atualizações mais recentes disponíveis de drivers de dispositivo e firmware, organizadas por sistema operacional. Quando você baixa UXSPs, o XClarity Administrator baixa o UXSP com base na versão que está relacionada no catálogo e armazena os pacotes de atualizações no repositório de atualizações de firmware. Quando você baixa um UXSP, cada atualização de firmware no UXSP é adicionada ao repositório das atualizações de firmware e listada na guia **Atualizações Individuais**, e uma política de conformidade de firmware padrão é criada automaticamente para todos os dispositivos gerenciáveis usando os seguintes nomes. É possível copiar essa política predefinida, mas não é possível alterá-la.
  - *{uxsp-version}-{date}-{server-short-name}***-UXSP** (por exemplo, `v1.50-2017-11-22-SD530-UXSP`)
  - *{uxsp-version}-{buildnumber}-{server-short-name}***-bundle** (por exemplo, `22a.0-kaj92va-SR650V3-bundle`)

  Nota: Quando os UXSPs são baixados ou importados da página Atualizações de Firmware: Repositório, somente atualizações de firmware são baixadas e armazenadas no repositório. Atualizações de driver de dispositivo são descartadas. Para obter informações sobre o download ou a importação de atualizações de driver de dispositivo do Windows usando os UXSPs, consulte Gerenciando o repositório de drivers de dispositivo do SO.

  É possível determinar se os UXSPs estão armazenados no repositório das atualizações de firmware na coluna **Estado de Download** na guia **Atualizações Individuais** da página Atualizações de Firmware: Repositório. Essa coluna contém os seguintes valores:

  - **Baixado**. O pacote de atualização inteiro ou a atualização de firmware individual são armazenados no repositório.
  - *x* **de** *y* **Baixado**. Algumas atualizações de firmware (não todas) no pacote de atualização estão armazenadas no repositório. Os números entre parênteses indicam o número de atualizações disponíveis e o número de atualizações armazenadas, ou não há atualizações para o tipo de dispositivo específico.
  - **Não Baixado**. O pacote de atualização inteiro ou a atualização de firmware individual estão disponíveis, mas não armazenados no repositório.

- **Atualizações individuais de firmware**

  Também é possível baixar pacotes de atualização de firmware individuais de uma vez. Quando você baixa pacotes de atualização de firmware, o XClarity Administrator baixa a atualização, com base na versão que é listada no catálogo, e armazena os pacotes de atualizações no

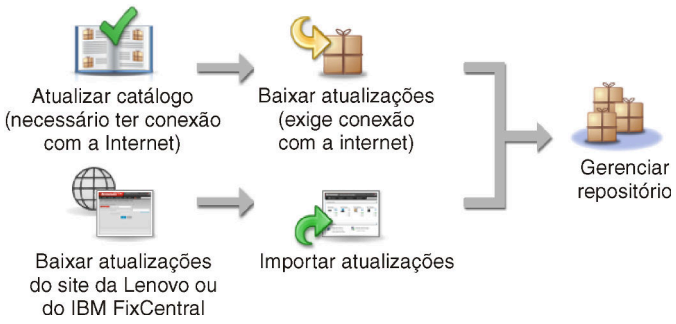
repositório das atualizações de firmware. Você pode então criar políticas de conformidade de firmware usando esses pacotes de atualização para cada um dos dispositivos gerenciados.

Nota: As principais atualizações de firmware (como controlador de gerenciamento, UEFI e pDSA) são independentes do sistema operacional. Os pacotes de atualização de firmware para os sistemas operacionais RHEL 6 ou SLES 11 são usados para atualizar nós de cálculo e servidores de rack. Para obter mais informações sobre quais pacotes de atualização de firmware usar para servidores gerenciados, consulte Baixando atualizações de firmware.

É possível determinar se *atualizações de firmware* específicas estão armazenadas no repositório de atualizações de firmware na coluna **Status de Download** na guia **Atualizações Individuais** na página Atualizações de Firmware: Repositório. Essa coluna contém os seguintes valores.

- **Baixado**. O pacote de atualização inteiro ou a atualização de firmware individual são armazenados no repositório.
- *x* **de** *y* **Baixado**. Algumas atualizações de firmware (não todas) no pacote de atualização estão armazenadas no repositório. Os números entre parênteses indicam o número de atualizações disponíveis e o número de atualizações armazenadas, ou não há atualizações para o tipo de dispositivo específico.
- **Não Baixado**. O pacote de atualização inteiro ou a atualização de firmware individual estão disponíveis, mas não armazenados no repositório.

O XClarity Administrator deve estar conectado à Internet para atualizar o catálogo e baixar as atualizações de firmware. Se ele não estiver conectado à Internet, será possível baixar manualmente os arquivos para uma estação de trabalho que tenha acesso host do XClarity Administrator usando um navegador da Web e, em seguida, importar os arquivos para o repositório das atualizações de firmware.



Ao importar manualmente atualizações de firmware para o XClarity Administrator, você deve incluir os seguintes arquivos necessários: carga útil (imagem e MIB), metadados, histórico de alterações e leiame. Exemplo:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Atenção:

- Importe somente esses arquivos necessários. Não importe outros arquivos que possam ser encontrados nos sites de download de firmware.
- Se você não incluir o arquivo XML no pacote de atualização, a atualização não será importada.

- Se você não incluir todos os arquivos necessários à atualização, o repositório mostrará que a atualização não foi baixada, indicando que ela foi parcialmente importada. Você poderá então importar os arquivos ausentes. Basta selecionar os arquivos e importá-los.
- As principais atualizações de firmware (como controlador de gerenciamento, UEFI e pDSA) são independentes do sistema operacional. Os pacotes de atualização de firmware para os sistemas operacionais RHEL 6 ou SLES 11 são usados para atualizar nós de cálculo e servidores de rack. Para obter mais informações sobre quais pacotes de atualização de firmware usar para servidores gerenciados, consulte Baixando atualizações de firmware.

Para obter mais informações sobre as atualizações de firmware, consulte Gerenciando o repositório das atualizações de firmware.

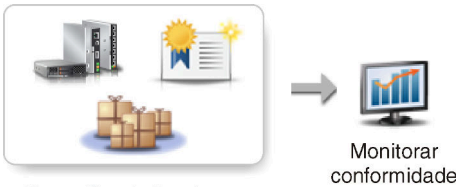
Etapa 2. **(Opcional) Criar e atribuir políticas de conformidade de firmware**

As políticas de conformidade de firmware garantem que o firmware em determinados dispositivos gerenciados esteja no nível atual ou específico sinalizando os dispositivos que precisam de atenção. Cada política de conformidade de firmware identifica quais dispositivos são monitorados e qual nível de firmware deve ser instalado para manter os dispositivos em conformidade. Você pode definir a conformidade no nível do componente do dispositivo ou do firmware. O XClarity Administrator, em seguida, usa essas políticas para verificar o status dos dispositivos gerenciados e identificar dispositivos que estão fora de conformidade.

Ao criar uma política de conformidade de firmware, você pode optar para que o XClarity Administrator sinalize um dispositivo quando:
- O firmware no dispositivo estiver em um nível inferior
- O firmware no dispositivo não corresponder exatamente à versão do destino de conformidade

O XClarity Administrator é fornecido com uma política de conformidade de firmware predefinida chamada **Firmware mais recente no repositório**. Quando um novo firmware é baixado ou importado para o repositório, essa política é atualizada para incluir as versões mais recentes disponíveis do firmware no repositório.

Depois que uma política de conformidade de firmware é atribuída a um dispositivo, o XClarity Administrator verifica o status de conformidade de cada dispositivo quando há alterações no inventário do dispositivo ou no repositório das atualizações de firmware. Quando o firmware em um dispositivo não está em conformidade com a política atribuída, o XClarity Administrator identifica esse dispositivo como incompatível na página na Atualizações de Firmware: Aplicar/Ativar, com base na regra especificada na política de conformidade de firmware



Por exemplo, é possível criar uma política de conformidade de firmware que defina o nível da linha de base do firmware instalado em todos os dispositivos ThinkSystem SR850 e atribuir essa política de conformidade de firmware a todos os dispositivos ThinkSystem SR850 gerenciados. Quando o repositório das atualizações de firmware é atualizado e uma nova atualização de firmware é adicionada, esses nós de cálculo podem ficar fora de conformidade. Quando isso acontece, o XClarity Administrator atualiza a página Atualizações de Firmware: Aplicar/Ativar para mostrar que os dispositivos não estão em conformidade e gerar um alerta.

Nota: É possível optar por mostrar ou ocultar alertas de dispositivos que não atendem aos requisitos de suas políticas de conformidade de firmware atribuídas (consulte Definir configurações globais de atualização de firmware). Os alertas são ocultos por padrão.

Para obter mais informações sobre as políticas de conformidade de firmware, consulte Criando e atribuindo políticas de conformidade de firmware.

Etapa 3. **Aplicando e ativando atualizações**

O XClarity Administrator não aplica atualizações de firmware em dispositivos gerenciados automaticamente. Para atualizar o firmware, você deve aplicar e ativar manualmente a atualização em dispositivos selecionados. É possível aplicar o firmware de uma das maneiras a seguir.

- **Aplicar atualizações de firmware em um pacote usando políticas de conformidade**

  Você pode aplicar atualizações de firmware a *todos* os componentes dos dispositivos selecionados de acordo com a política de conformidade de firmware atribuída usando uma imagem de pacote que contenha os pacotes de atualização de firmware aplicáveis.

  O processo de atualização em pacote atualiza primeiro o Baseboard Management Controller e o UEFI fora da banda. Quando essas atualizações são concluídas, o processo cria uma imagem em pacote do firmware restante na política de conformidade com base no tipo de máquina. Em seguida, o processo monta a imagem no dispositivo selecionado e reinicia o dispositivo para inicializar a imagem. A imagem é executada automaticamente para executar as atualizações restantes.

  Atenção: Os dispositivos selecionados são desligados antes de iniciar o processo de atualização. Certifique-se de que as cargas de trabalho em execução tenham sido interrompidas ou, se você estiver trabalhando em um ambiente virtualizado, tenham sido movidas para outro servidor. Se houver trabalhos em execução, o trabalho de atualização será enfileirado até que todos os outros trabalhos sejam concluídos. Para ver uma lista de trabalhos ativos, clique em **Monitoramento → Trabalhos**.

  Notas:

  – A aplicação de atualizações de firmware em pacote são compatíveis apenas com servidores ThinkSystem SR635 e SR655.

  – A aplicação de atualizações de firmware empacotadas é suportada apenas para endereço IPv4. Endereços IPv6 não têm suporte.

  – Certifique-se de que cada dispositivo de destino tenha sido inicializado no SO pelo menos uma vez para recuperar as informações completas do inventário.

  – O firmware do Baseboard Management Controller v2.94 ou posterior é necessário para usar a função de atualização em pacote.

  – Apenas atualizações de firmware de pacotes de repositórios ou atualizações de firmware individuais são usadas. UpdateXpress System Packs (UXSPs) não são compatíveis.

  – Somente as atualizações de firmware baixadas são aplicadas. Atualize o catálogo de produtos e faça download das atualizações de firmware apropriadas (consulte Atualizando o catálogo de produtos e Baixando atualizações de firmware).

    Nota: Quando o XClarity Administrator é inicialmente instalado, o catálogo de produtos e o repositório estão vazios.

  – A verificação de conformidade é suportada apenas para o Baseboard Management Controller e UEFI nos servidores ThinkSystem SR635 e SR655; no entanto, o XClarity Administrator tenta aplicar atualizações de firmware a todos os componentes de hardware disponíveis.

- As atualizações são aplicadas de acordo com a política de conformidade de firmware atribuída. Não é possível optar por atualizar um subconjunto de componentes.
- O XClarity Administrator v 3.2 ou posterior é necessário para aplicar atualizações de firmware para o Lenovo XClarity Provisioning Manager (LXPM), drivers do LXPM Windows drivers ou drivers do LXPM Linux para servidores ThinkSystem SR635 e SR655.
- O Baseboard Management Controller e as atualizações do UEFI serão ignoradas se a versão instalada atualmente for mais recente do que a política de conformidade atribuída.
- As políticas de conformidade de firmware devem ser criadas e atribuídas aos dispositivos em que você pretende aplicar atualizações de firmware. Para obter mais informações, consulte Criando e atribuindo políticas de conformidade de firmware.
- Os dispositivos selecionados são desligados antes de iniciar o processo de atualização. Certifique-se de que as cargas de trabalho em execução tenham sido interrompidas ou, se você estiver trabalhando em um ambiente virtualizado, tenham sido movidas para outro servidor.

- **Aplicar atualizações de firmware selecionadas com ou sem políticas de conformidade**

  Você pode aplicar atualizações de firmware a componentes e dispositivos selecionados de acordo com a política de conformidade de firmware atribuída usando pacotes de atualização de firmware aplicáveis. Você também pode optar por aplicar atualizações de firmware mais recentes do que o firmware instalado atualmente em componentes e dispositivos selecionados sem usar políticas de conformidade.

  É possível optar por aplicar atualizações para todos os componentes em um dispositivo específico. Entretanto, também é possível optar por atualizar apenas um subconjunto de componentes nos dispositivos selecionados, como Baseboard Management Controller ou UEFI.

  Para ativar as atualizações de firmware, os dispositivos devem ser reiniciados. (Lembre-se de que reiniciar um dispositivo causa interrupção.) Você pode optar por reiniciar os dispositivos como parte do processo de atualização (chamado de *ativação imediata*) ou aguardar até uma janela de manutenção estar disponível para reiniciar os dispositivos (chamado de *ativação atrasada*). Nesse caso, você deverá reiniciar manualmente o dispositivo para que a atualização tenha efeito.

  Quando você opta por atualizar o firmware de um dispositivo gerenciado, ocorrem as etapas a seguir.

  1. O XClarity Administrator envia as atualizações de firmware (por exemplo, para o controlador de gerenciamento, a UEFI e a DSA) ao dispositivo.
  2. Quando o dispositivo é reiniciado, as atualizações de firmware são ativadas no dispositivo.
  3. Para servidores, o XClarity Administrator envia atualizações para dispositivos opcionais, como atualizações de adaptador de rede e unidade de disco rígido. O XClarity Administrator aplica essas atualizações e o servidor é reiniciado.
  4. Quando você reinicia o dispositivo ou escolhe a ativação imediata, as atualizações para os dispositivos opcionais são ativadas.

  Notas:

  - Ao aplicar atualizações usando políticas de conformidade, uma política de conformidade de firmware deve ser criada e atribuída a cada dispositivo de destino. Para obter mais informações, consulte Criando e atribuindo políticas de conformidade de firmware.
  - Se você optar por instalar um pacote de atualização de firmware que contenha atualizações para vários componentes, todos os componentes aos quais o pacote de atualização se aplica serão atualizados.

– As atualizações para CMMs e comutadores Flex são sempre ativadas imediatamente, mesmo que você selecione a ativação atrasada.

Quando você executa atualizações em um conjunto de dispositivos, o XClarity Administrator executa as atualizações na ordem a seguir.

- CMM do chassi
- Comutadores RackSwitch e Flex System
- Nós de cálculo Flex, rack e servidores em torre
- Dispositivos de armazenamento Lenovo

Atenção: Antes de tentar aplicar atualizações de firmware em dispositivos gerenciados, certifique-se de ter concluído as ações a seguir.

- Leia as considerações sobre a atualização de firmware antes de tentar atualizar o firmware em seus dispositivos gerenciados (consulte Considerações de atualização de firmware).
- Inicialmente, os dispositivos sem suporte para atualizações são ocultos na exibição. Os dispositivos sem suporte não podem ser selecionados para atualizações.
- Por padrão, todos componentes detectados são listados como disponíveis para aplicação de atualizações; entretanto, o firmware de nível inferior pode impedir um componente de aparecer no inventário ou fazer o relatório de informações da versão completa. Para listar todos os pacotes baseados em política que estão disponíveis para você aplicar atualizações, clique em **Todas as Ações → Configurações Globais** e selecione **Suporte Aprimorado para Dispositivos de Nível Inferior**. Quando essa opção é selecionada, "Outro Software Disponível" é listado na coluna Versão Instalada para dispositivos não detectados. Para obter mais informações, consulte Definir configurações globais de atualização de firmware.

  Notas:

  – As configurações globais não podem ser alteradas quando há atualizações em andamento em dispositivos gerenciados.

  – Leva alguns minutos para gerar as opções adicionais. Depois de alguns momentos, talvez você precise clicar no ícone **Atualizar** ( ) para atualizar a tabela.
- Certifique-se de que nenhum trabalho esteja em execução atualmente no servidor de destino. Se houver trabalhos em execução, o trabalho de atualização será enfileirado até que todos os outros trabalhos sejam concluídos. Para ver uma lista de trabalhos ativos, clique em **Monitoramento → Trabalhos**.
- Verifique se o repositório das atualizações de firmware contém os pacotes de firmware que você pretende implantar. Se não contiver, atualize o catálogo de produtos e baixe as atualizações de firmware apropriadas (consulte Atualizando o catálogo de produtos e Baixando atualizações de firmware).

  Nota: Quando o XClarity Administrator é inicialmente instalado, o catálogo de produtos e o repositório estão vazios.

  Se você pretende instalar firmware de pré-requisito, certifique-se de que o firmware de pré-requisito também seja baixado no repositório.

  Em alguns casos, várias versões podem ser necessárias para atualizar o firmware, e todas as versões precisam ser baixadas para o repositório. Por exemplo, para atualizar o comutador escalável IBM FC5022 SAN de v7.4.0a para v8.2.0a, você deve primeiro instalar a v8.0.1-pha, em seguida, v8.1.1 e, em seguida, v8.2.0a. Todas as três versões devem estar no repositório para atualizar o comutador para v8.2.0a.
- Normalmente, os dispositivos devem ser reiniciados para ativar a atualização de firmware. Se você optar por reiniciar o dispositivo durante o processo de atualização (*ativação imediata*),

certifique-se de que as cargas de trabalho em execução sejam interrompidas ou, se estiverem funcionando em um ambiente virtualizado, sejam movidas para um servidor diferente.

Para obter mais informações sobre como instalar atualizações, consulte Aplicando e ativando atualizações de firmware.

Considerações de atualização de firmware

Antes de começar a atualizar o firmware para dispositivos gerenciados usando o Lenovo XClarity Administrator, revise as considerações importantes a seguir.

- Considerações gerais
- Considerações sobre CMM
- Considerações sobre o Baseboard Management Controller
- Considerações sobre o dispositivo ThinkSystem
- Considerações sobre o dispositivo Flex System
- Considerações sobre armazenamento

Considerações gerais

- **Níveis mínimos de firmware necessários.**

  Certifique-se de que o firmware instalado em cada dispositivo gerenciado esteja no nível mínimo necessário antes de usar o XClarity Administrator para atualizar o firmware nesses dispositivos. É possível localizar os níveis mínimos de firmware necessários em Página da Web Suporte do XClarity Administrator – Compatibilidade clicando na guia **Compatibilidade** e, em seguida, clicando no link para os tipos de dispositivo apropriados.

  Nota: Para obter informações sobre o suporte a dispositivos de E/S e as limitações conhecidas, consulte Página da Web Suporte do XClarity Administrator – Compatibilidade.

- **Atualize todos os componentes para o nível que está incluído no repositório das atualizações de firmware.**

  Como as atualizações de firmware para componentes Flex System são testadas e liberadas juntas, é recomendável manter o mesmo nível de firmware em todos os componentes em um chassi do Flex System. Portanto, é importante atualizar o firmware em todos os componentes do chassi na mesma janela de manutenção. O XClarity Administrator aplica as atualizações selecionadas na sequência correta automaticamente.

- **Drivers LXPM Linux e drivers LXPM Windows não são incluídos durante o download de UXSPs**

  Lenovo XClarity Provisioning Manager (LXPM) Drivers Linux e Windows não estão incluídos no UpdateXpress System Packs (UXSPs). Para aplicar esses pacotes de atualização aos dispositivos, faça download dos pacotes do repositório de atualizações de firmware mais recentes ou faça download manualmente dos pacotes individuais e crie uma política de conformidade de firmware para incluir esses pacotes.

- **Algumas atualizações de firmware são codependentes em um nível mínimo de driver de dispositivo.**

  Antes de aplicar atualizações de adaptador e firmware de E/S em um servidor, pode ser necessário atualizar o driver de dispositivo para um nível mínimo. Em geral, as atualizações de firmware não são dependentes de níveis específicos de drivers de dispositivo. Consulte o readme de atualização de firmware para ver essas codependências e atualize os drivers de dispositivo no sistema operacional antes de atualizar o firmware. O XClarity Administrator não atualiza drivers de dispositivo no seu sistema operacional.

- **Reinicie o XClarity Administrator antes de atualizar o firmware**

  Se ocorrer falha nas tentativas anteriores de atualizar o firmware, reinicie XClarity Administrator antes de atualizar o firmware. A reinicialização do servidor de gerenciamento garante que a conta reservada do sistema usada para atualizar o firmware esteja sincronizada nos dispositivos gerenciados.

- **Atualizações de firmware causam transtornos e requerem que as cargas de trabalho sejam encerradas em dispositivos.**

  As atualizações de firmware em dispositivos gerenciados causam transtornos quando você opta por ativar imediatamente a atualização. Você deve desligar os dispositivos antes de atualizar o firmware usando a ativação imediata.

  Na atualização do firmware em servidores, os servidores são desligados e colocados em um sistema operacional de manutenção para atualizar os drivers de dispositivo para adaptadores, unidades de disco e unidades de estado sólido.

  Os Comutadores Flex em um determinado chassi são atualizados em sequência e reiniciados durante o processo de atualização de firmware. A implementação de caminhos de dados redundantes diminui o transtorno, mas ainda pode haver uma interrupção rápida na conectividade de rede durante a atualização de firmware.

- **Não use o XClarity Administrator para atualizar o firmware no servidor em que o XClarity Administrator está sendo executado.**

  Se o XClarity Administrator estiver em execução em um host do hipervisor executado em um servidor que ele está gerenciando, não use o XClarity Administrator para atualizar o firmware nesse servidor. Quando são aplicadas atualizações de firmwares com ativação imediata, o XClarity Administrator força o servidor de destino a reiniciar, o que também reinicia o host do hipervisor e o XClarity Administrator. Quando aplicada com ativação adiada, somente parte do firmware é aplicada até o sistema de destino ser reiniciado

Considerações sobre CMM

- **Reposicione virtualmente os CMMs antes de atualizar firmware.**

  Se você estiver atualizando CMMs que executam a versão da pilha do nível de firmware 1.3.2.1 2PET12K até 2PET12Q, que são executados há mais de três semanas e têm uma configuração dupla do CMM, você deverá reposicionar virtualmente os CMMs primário e de espera antes de atualizar o firmware (consulte Reposicionando virtualmente um CMM).

Considerações sobre o Baseboard Management Controller

- **Níveis mínimos de BMC necessários para status de ativação pendente**

  Para ver o status de ativação pendente, a versão do firmware a seguir deve estar instalada no Baseboard Management Controller no servidor.
  - **IMM2**: TCOO46F, TCOO46E ou posterior (dependendo da plataforma)
  - **XCC**: CDI328M, PSI316N, TEI334I ou posterior (dependendo da plataforma)

- **Atualizações aplicadas às partições primárias de firmware do controlador de gerenciamento e da UEFI.**

  As atualizações de Baseboard Management Controller (BMC) e UEFI podem ser aplicadas às partições primárias e de backup do firmware para o controlador de gerenciamento e a UEFI de modo independente.

  Também é possível aplicar atualizações de controlador de gerenciamento e UEFI apenas às partições primárias do firmware no servidor. Por padrão, o controlador de gerenciamento é configurado para sincronizar a partição de backup do controlador de gerenciamento com a partição primária do controlador de gerenciamento após o controlador de gerenciamento primário ter sido executado satisfatoriamente e o novo nível estar pronto para ser promovido a backup. Entretanto, o controlador de

gerenciamento não está configurado para sincronizar a partição de backup da UEFI por padrão. Portanto, considere uma das seguintes opções no controlador de gerenciamento:

– Habilitar a sincronização automática da partição de backup da UEFI.

  Isso assegura que as partições primária e de backup estejam executando o mesmo nível de firmware (e que o firmware UEFI de backup seja compatível com o firmware do controlador de gerenciamento).

– Desabilitar a sincronização automática da partição de backup do controlador de gerenciamento.

  Embora não seja recomendado, isso oferece a você controle total sobre os níveis de firmware do controlador de gerenciamento e da UEFI. Entretanto, você deverá atualizar manualmente o controlador de gerenciamento e o firmware UEFI para ambas as partições.

Você usa as políticas de conformidade de firmware para determinar quais atualizações são aplicadas a cada dispositivo. Para obter mais informações sobre políticas de conformidade de firmware, consulte Criando e atribuindo políticas de conformidade de firmware.

Nota: Se o controlador de gerenciamento e a UEFI estiverem configurados para sincronizar automaticamente o firmware de backup a partir do primário, não será necessário que o XClarity Administrator atualize os bancos de backup. Nesse caso, você pode limpar as atualizações de banco de backup ao aplicar atualizações em um servidor ou remover os bancos de backup da política de conformidade de firmware.

- **Possibilidade de falha do sistema VMware vSphere ESXi (tela de diagnóstico do host na cor púrpura) quando um controlador de gerenciamento é redefinido.**

  Se você estiver executando o VMware vSphere ESXi em algum servidor, certifique-se de que os seguintes níveis mínimos VMware ESXi sejam instalados antes de atualizar o firmware no servidor:

  – Se estiver executando o VMware vSphere ESXi 5.0, instale um nível mínimo 5.0u2 (atualização 2)
  – Se estiver executando o VMware vSphere ESXi 5.1, instale um nível mínimo 5.1u1 (atualização 1)

  Se você não instalar esses níveis mínimos, poderá ocorrer uma falha do sistema VMware vSphere ESXi (tela de diagnóstico do host na cor púrpura) sempre que o controlador de gerenciamento for redefinido, inclusive quando o firmware do controlador de gerenciamento for aplicado e ativado.

  Nota: Esse problema não afeta o ESXi v5.5.

Considerações sobre o dispositivo ThinkSystem

- **Para servidores ThinkSystem SE350 que executam a versão de firmware XCC anterior a 20A, o IPMI sobre acesso via KCS deve ser ativado manualmente no Baseboard Management Controller para assegurar que o controlador de gerenciamento possa se comunicar com o XClarity Administrator.**

  Para servidores ThinkSystem SE350, o IPMI sobre KCS é desativado por padrão. Para servidores ThinkSystem SE350 que executam o firmware XCC versão 20A ou posterior, o XClarity Administrator ativa automaticamente o IPMI sobre KCS durante uma atualização de firmware e, em seguida, desativa-o após a atualização de firmware ser concluída. No entanto, para os servidores ThinkSystem SE350 executando a versão de firmware XCC anterior a 20A, você deve habilitar manualmente essa opção na interface do Lenovo XClarity Controller clicando em **Configuração BMC → Segurança → IPMI sobre acesso via KCS**.

- Para servidores ThinkSystem SR635 e SR655, as limitações a seguir se aplicam.

  – Somente a ativação imediata é compatível. Não há suporte para ativação atrasada e ativação prioritária.
  – Para XClarity Administrator v3.1.1 e posterior, você pode usar a função de atualização de pacote para atualizar todos os componentes nos servidores ThinkSystem SR635 e SR655, incluindo o Baseboard Management Controller, UEFI, unidades de disco e opções de E/S.

Atenção: Os dispositivos selecionados são desligados antes de iniciar o processo de atualização. Certifique-se de que as cargas de trabalho em execução tenham sido interrompidas ou, se você estiver trabalhando em um ambiente virtualizado, tenham sido movidas para outro servidor. Se houver trabalhos em execução, o trabalho de atualização será enfileirado até que todos os outros trabalhos sejam concluídos. Para ver uma lista de trabalhos ativos, clique em **Monitoramento → Trabalhos**.

Notas:

- A aplicação de atualizações de firmware em pacote são compatíveis apenas com servidores ThinkSystem SR635 e SR655.
- A aplicação de atualizações de firmware empacotadas é suportada apenas para endereço IPv4. Endereços IPv6 não têm suporte.
- Certifique-se de que cada dispositivo de destino tenha sido inicializado no SO pelo menos uma vez para recuperar as informações completas do inventário.
- O firmware do Baseboard Management Controller v2.94 ou posterior é necessário para usar a função de atualização em pacote.
- Apenas atualizações de firmware de pacotes de repositórios ou atualizações de firmware individuais são usadas. UpdateXpress System Packs (UXSPs) não são compatíveis.
- Somente as atualizações de firmware baixadas são aplicadas. Atualize o catálogo de produtos e faça download das atualizações de firmware apropriadas (consulte Atualizando o catálogo de produtos e Baixando atualizações de firmware).

  Nota: Quando o XClarity Administrator é inicialmente instalado, o catálogo de produtos e o repositório estão vazios.
- A verificação de conformidade é suportada apenas para o Baseboard Management Controller e UEFI nos servidores ThinkSystem SR635 e SR655; no entanto, o XClarity Administrator tenta aplicar atualizações de firmware a todos os componentes de hardware disponíveis.
- As atualizações são aplicadas de acordo com a política de conformidade de firmware atribuída. Não é possível optar por atualizar um subconjunto de componentes.
- O XClarity Administrator v 3.2 ou posterior é necessário para aplicar atualizações de firmware para o Lenovo XClarity Provisioning Manager (LXPM), drivers do LXPM Windows drivers ou drivers do LXPM Linux para servidores ThinkSystem SR635 e SR655.
- O Baseboard Management Controller e as atualizações do UEFI serão ignoradas se a versão instalada atualmente for mais recente do que a política de conformidade atribuída.
- As políticas de conformidade de firmware devem ser criadas e atribuídas aos dispositivos em que você pretende aplicar atualizações de firmware. Para obter mais informações, consulte Criando e atribuindo políticas de conformidade de firmware.
- Os dispositivos selecionados são desligados antes de iniciar o processo de atualização. Certifique-se de que as cargas de trabalho em execução tenham sido interrompidas ou, se você estiver trabalhando em um ambiente virtualizado, tenham sido movidas para outro servidor.

Também é possível usar a função de atualização tradicional para aplicar atualizações de firmware apenas ao Baseboard Management Controller e ao UEFI.

- Para XClarity Administrator v3.0:
  - Os dados de gerenciamento não são atualizados corretamente ao atualizar o firmware do 20A para o 20B ou 20C. Para resolver esse problema, cancele o gerenciamento e, em seguida, gerencie o dispositivo novamente ou reinicie o XClarity Administrator.
  - O downgrade de atualizações de firmware não é compatível.

- **As atualizações de firmware não são permitidas em servidores ThinkSystem usando DHCPv6 ou endereços IPv6 atribuídos estaticamente**

Ao usar o endereçamento IPv6 em servidores ThinkSystem, as atualizações de firmware são aceitas apenas em endereços de link local (LLA) e endereços sem estado do IPv6.

- **Ao atualizar o firmware para a versão 20D, você deve atualizar o UEFI e o XCC juntos.**

  O UEFI e o Lenovo XClarity Controller (XCC) devem ser atualizados juntos para a versão 20D. Atualizar o XCC e não o UEFI, e vice-versa, causará problemas.

Considerações sobre o dispositivo Flex System

- **Verifique se os comutadores Flex que estão sendo atualizados estão ligados,**
- **Selecione Ativação Imediata ao atualizar nós de cálculo que estiverem nos níveis de firmware do controlador de gerenciamento anteriores ao Flex System 1.3.2.**

  Ao aplicar a versão de ciclo de vida Flex System 1.3.2, 2nd Quarter a um nó de cálculo, você deve escolher *Ativação Imediata* para atualizar o nó de cálculo. A ativação imediata força o nó de cálculo a reiniciar durante o processo de atualização.
- **Os Comutadores Flex devem ser configurados com um endereço IP que seja acessível no XClarity Administrator.**

  Deve ser atribuído ao Comutador Flex de destino um endereço IP que possa se comunicar com o XClarity Administrator, para que o XClarity Administrator possa baixar e aplicar a atualização de firmware.
- **Suporte para atualização em complexos escaláveis, como os nós x480 X6 e x880 X6.**

  O suporte para atualização em nós escaláveis como o Flex System x480 X6 e os nós de Cálculo x880 X6 está limitado às configurações onde complexo está configurado como uma *única partição* que inclui todos os nós de cálculo que fazem parte do complexo com vários nós. Não é possível usar o XClarity Administrator para atualizar um complexo que consiste em diversas partições.

  Se você atribuir uma política de conformidade de firmware a uma partição que inclua vários servidores em um complexo escalável (como Flex System x480 X6 e x880 X6 Nós de Cálculo), o XClarity Administrator atualizará o firmware em todos os controladores de gerenciamento e UEFIs para cada servidor da partição por padrão. Entretanto, se você selecionar um subconjunto de componentes da partição, o XClarity Administrator atualizará o firmware somente nos componentes selecionados da partição.
- **Antes de atualizar o CMM2 para v1.30 (1AON06C) ou posterior, os comutadores Flex devem estar executando a versão Nível 3 do protocolo Enhanced Configuration and Management (EHCM L3)**

  O CMM2 e os comutadores Flex se comunicam usando o protocolo EHCM. Esse protocolo é necessário para que o XClarity Administrator atualize os comutadores Flex. Quando você atualiza um CMM2 para a v1.30 (1AON06C) ou posterior, o XClarity Administrator verifica se os comutadores Flex estão executando o EHCM L3 e, se não estiverem, cancela a atualização do CMM com um aviso de que os comutadores Flex devem ser atualizados primeiro para uma versão que ofereça suporte ao EHCM-L3. É possível substituir essa verificação selecionando **Tentar atualizar componentes já em conformidade** ao atualizar o firmware do CMM.

  Atenção: Atualmente não há nenhuma versão de firmware para Comutadores Ethernet EN6131 Flex System e Comutador InfiniBand IB6131 com suporte para EHCM L3. Isso significa que, depois de atualizar o CMM2 para o firmware v1.30 (1AON06C) ou posterior, você não pode mais usar o XClarity Administrator para atualizar esses comutadores. A alternativa é usar a interface da Web do controlador de gerenciamento ou a interface da linha de comandos do chassi para atualizar o comutador.

Comutador Flex System	Versão	Data de liberação
CN4093	7.8.4.0	Junho de 2014
EN4023	6.0.0	Abril de 2015
EN4093	7.8.4.0	Junho de 2014

Comutador Flex System	Versão	Data de liberação
EN4093R	7.8.4.0	Junho de 2014
EN6132	Não disponível	Não disponível
FC3171	9.1.3.02.00	Junho de 2014
FC5022	7.4.0b1	Março de 2016
IB6132	Não disponível	Não disponível
SI4091	7.8.4.0	Junho de 2014
SI4093	7.8.4.0	Junho de 2014

Nota: O Comutador Escalável Ethernet de 1 Gb EN2092 não requer o EHCM L3 e não tem essa restrição.

Considerações sobre armazenamento

- **Considerações sobre dispositivos de armazenamento ThinkSystem DM**

  Para atualizar o firmware em dispositivos de armazenamento ThinkSystem DM, os dispositivos devem estar executando a v9.7 ou posterior.

  O downgrade é compatível apenas com versões secundárias. Por exemplo, é possível fazer downgrade da 9.7P11 para a 9.7P9; no entanto, não é possível fazer downgrade da 9.8 para 9.7.

  Para fazer download do firmware para dispositivos de armazenamento ThinkSystem série DM:

  - Um ou mais dispositivos de armazenamento ThinkSystem série DM devem ser gerenciados pelo XClarity Administrator.
  - Cada dispositivo de armazenamento ThinkSystem série DM deve ter direito a serviço e suporte de hardware.
  - Você deve especificar o país em que os dispositivos de armazenamento ThinkSystem série DM estão localizados na página Atualizações de Firmware: Repositório. Somente o firmware criptografado pode ser baixado para dispositivos nos seguintes países: Armênia, Bielorrússia, China, Cuba, Irã, Casaquistão, Kyrgyzstão, Coreia do Norte, Rússia, Sudão, Síria.
- **As unidades de disco devem estar no estado JBOD, online, pronto ou não configurado (bom).**

  Para atualizar o firmware nas unidades de disco, o estado RAID deve ser JBOD, online, pronto ou não configurado (bom). Outras estados não são suportados. Para determinar o estado do RAID para uma unidade de disco, acesse a página Inventário do dispositivo, expanda a seção **Unidades** e verifique a coluna **Estado do RAID** dessa unidade de disco (consulte Visualizando os detalhes de um servidor gerenciado).
- **A versão do firmware não detecta unidades de disco e unidades de estado sólido.**

  O XClarity Administrator detecta somente a versão do firmware instalado e executa uma verificação de conformidade para unidades de disco e unidades de estado sólido (SSDs) que estão conectadas a um adaptador MegaRAID ou NVMe. Outras unidades conectadas podem ter um nível de firmware que não seja aceito ou podem não oferecer suporte ao relatório de versão do firmware. Entretanto, as atualizações de firmware são aplicadas a essas unidades quando selecionadas.
- **O firmware NVMe é aplicado mesmo que não seja identificado com um componente de destino**

  Na página Aplicar/Ativar, a versão de firmware de NVMe é listada para unidades de estado sólido (SSDs). Como nenhuma atualização de firmware de destino é identificada para os dispositivos NVMe descobertos, uma mensagem de aviso é exibida quando você tenta atualizar o sistema de destino. Entretanto, a atualização de HDD/SSD é aplicada mesmo que não ele não seja identificado com um componente de destino, para que o firmware de NVMe ainda seja atualizado.

- **Aplicar o pacote de atualização ServeRAID M5115 PSoC3 do XClarity Administrator requer um nível mínimo 68 instalado.**

  A atualização ServeRAID M5115 PSoC3 (Programmable System-on-Chip) de versão anterior à 68 deve ser feita de uma maneira controlada.

  Dica: Você pode exibir a versão do código do ServeRAID M5115 PSoC3 fazendo login na interface da Web do CMM e selecionando a guia **Firmware** do nó de cálculo de destino. Em seguida, selecione a placa de expansão para o adaptador ServeRAID M5115. A versão do código PSoc3 é o tipo de firmware GENÉRICO.

  Para as versões instaladas anteriores à 68, você não pode atualizar usando o XClarity Administrator. Em vez disso, você deve executar as seguintes etapas na interface da Web do Chassis Management Module (CMM) ou na interface da linha de comandos (CLI):

  – **Usando a interface da Web do CMM:**
    1. Faça login na interface da Web do Chassis Management Module (CMM).
    2. No menu principal, clique em **Serviço e Suporte → Avançado**.
    3. Clique na guia **Redefinição de Serviços**.
    4. Selecione o nó de cálculo apropriado clicando no botão de opção.
    5. No menu suspenso **Redefinir**, clique em **Reposicionamento Virtual**.
    6. Clique em **OK** para confirmar.
  – **Usando a CLI do CMM**:
    – Faça login na interface do CMM Secure Shell (SSH).
    – Insira o seguinte comando para executar um reposicionamento virtual:
      `'service -vr -T blade[x]`

      em que *x* é o número de compartimento do nó de cálculo a ser reposicionado.

  Depois que o sistema for novamente ligado, inicialize o sistema operacional e atualize o ServeRAID M5115 PSoC3 usando o pacote de atualização integrado extraído. Conclua as etapas a seguir para extrair o pacote integrado.

  – **Usando o Microsoft Windows:**

    Abra o pacote de atualização (lnvgy_fw_psoc3_m5115-70_windows_32-64.exe) e selecione Extrair para Disco Rígido. Em seguida, selecione o caminho em que o pacote integrado deve ser extraído.
  – **Usando o Linux:**

    Execute o seguinte comando:

    `lnvgy_fw_psoc3_m5115-70_linux_32-64.bin -x`

    em que *x* é o local onde o pacote integrado deve ser extraído.

Gerenciando o repositório das atualizações de firmware

O *repositório de atualizações de firmware* contém um catálogo de atualizações disponíveis e os pacotes de atualização que podem ser aplicados aos dispositivos gerenciados.

Sobre esta tarefa

O *catálogo* contém informações sobre as atualizações de firmware que estão disponíveis atualmente para todos os dispositivos compatíveis com o XClarity Administrator. O catálogo organiza as atualizações de firmware por tipo de dispositivo. Quando você atualiza o catálogo, o XClarity Administrator recupera informações sobre as atualizações de firmware mais recentes disponíveis do site da Lenovo (inclusive os

arquivos de metadados xml. ou .json e leiame .txt) e armazena as informações no repositório das atualizações de firmware. O arquivo de carga útil (.exe) não foi baixado. Para obter mais informações sobre como atualizar o catálogo, consulte Atualizando o catálogo de produtos.

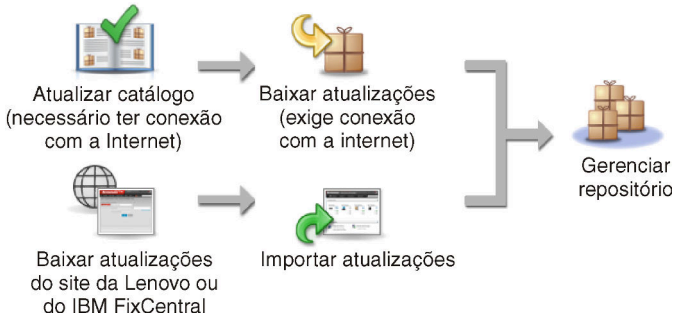
Se novas atualizações de firmware estiverem disponíveis, você deverá primeiro baixar os pacotes de atualização antes de atualizar esse firmware nos dispositivos gerenciados. A atualização do catálogo não baixa automaticamente os pacotes de atualização. A tabela do **Catálogo de Produtos** na página Repositório das Atualizações de Firmware identifica quais pacotes de atualização são baixados e quais estão disponíveis para download.

Você pode baixar atualizações de firmware de algumas maneiras diferentes:

- **Pacotes do repositório de atualizações de firmware**. Os pacotes do repositório contêm as mais recentes atualizações de firmware disponíveis para todos os dispositivos compatíveis e uma política de conformidade de firmware padrão atualizada. Esses pacotes de repositório são importados e, depois, aplicados da página Atualizar Servidor de Gerenciamento.
- **UpdateXpress System Packs (UXSPs)**. Os UXSPs contêm as atualizações mais recentes disponíveis de drivers de dispositivo e firmware, organizadas por sistema operacional. Quando os UXSPs são baixados da página Atualizações de Firmware: Repositório, somente atualizações de firmware são baixadas e armazenadas no repositório. Atualizações de driver de dispositivo são excluídas.

  Nota: Para servidores com XCC2, esses pacotes são chamados de *pacotes* de firmware.
- **Atualizações individuais de firmware**. Você pode baixar pacotes de atualização de firmware individuais ao mesmo tempo, com base na versão listada no catálogo.

O XClarity Administrator deve estar conectado à Internet para atualizar o catálogo e baixar as atualizações de firmware. Se ele não estiver conectado à Internet, será possível baixar manualmente os arquivos para uma estação de trabalho que tenha acesso host do XClarity Administrator usando um navegador da Web e, em seguida, importar os arquivos para o repositório das atualizações de firmware.



Ao importar manualmente atualizações de firmware para o XClarity Administrator, você deve incluir os seguintes arquivos necessários: carga útil (imagem e MIB), metadados, histórico de alterações e leiame. Exemplo:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Atenção:

- Importe somente esses arquivos necessários. Não importe outros arquivos que possam ser encontrados nos sites de download de firmware.
- Se você não incluir o arquivo XML no pacote de atualização, a atualização não será importada.

- Se você não incluir todos os arquivos necessários à atualização, o repositório mostrará que a atualização não foi baixada, indicando que ela foi parcialmente importada. Você poderá então importar os arquivos ausentes. Basta selecionar os arquivos e importá-los.
- As principais atualizações de firmware (como controlador de gerenciamento, UEFI e pDSA) são independentes do sistema operacional. Os pacotes de atualização de firmware para os sistemas operacionais RHEL 6 ou SLES 11 são usados para atualizar nós de cálculo e servidores de rack. Para obter mais informações sobre quais pacotes de atualização de firmware usar para servidores gerenciados, consulte Baixando atualizações de firmware.

Depois que as atualizações de firmware são baixadas no repositório, são fornecidas informações sobre cada atualização, incluindo a data de liberação, o tamanho, o uso de política e a severidade. A severidade indica o impacto e a necessidade de aplicar a atualização para ajudar a avaliar como seu ambiente pode ser afetado.
- **Versão Inicial**. Esta é a primeira versão do firmware.
- **Crítico**. A versão do firmware contém correções urgentes para problemas de dados corrompidos, segurança ou estabilidade.
- **Sugerido**. A versão do firmware contém correções significativas para problemas que você poderá encontrar.
- **Não Crítico**. A versão de firmware contém pequenas correções, melhorias de desempenho e alterações textuais.

Notas:

- A severidade está relacionada à versão anteriormente liberada da atualização. Por exemplo, se o firmware instalado é v1.01, e a atualização v1.02 é Crítica e a atualização v1.03 é Recomendada, isso significa que a atualização de 1.02 para 1.03 é recomendada, mas a atualização de v1.01 para v1.03 é crítica porque é cumulativa (a v1.03 inclui problemas críticos da v1.02).
- Podem surgir casos especiais em que uma atualização seja crítica ou recomendada apenas para um tipo de máquina ou um sistema operacional específicos. Consulte as Notas de Versão para obter as informações adicionais.

Procedimento

Para ver as atualizações de firmware disponíveis no catálogo de produtos, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Repositório**. A página Repositório das Atualizações de Firmware é exibida com uma lista de pacotes de atualização de firmware disponíveis, organizados por tipo de dispositivo.

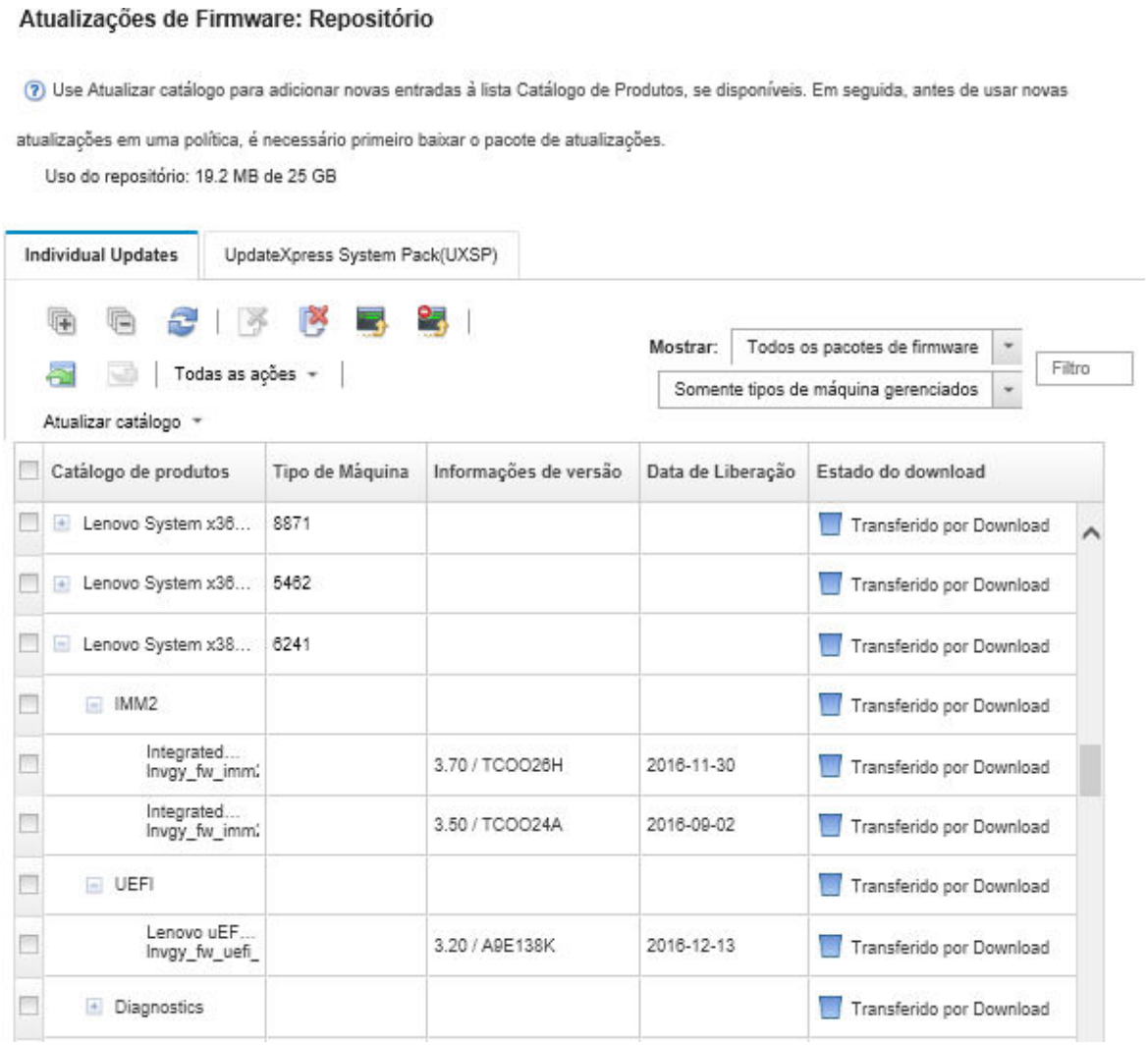
Etapa 2. Clique na guia **Atualizações Individuais** para exibir informações sobre os pacotes de atualização de firmware disponíveis ou clique na guia **UpdateXpress System Packs (UXSPs)** para exibir informações sobre UXSPs disponíveis.

Etapa 3. Expanda um dispositivo e componentes do dispositivo para listar os pacotes de atualização e as atualizações de firmware para esse dispositivo.

Você pode classificar as colunas da tabela e clicar no ícone **Expandir tudo** () e no ícone **Reduzir tudo** () para facilitar a localização de atualizações específicas de firmware. Além disso, é possível filtrar a lista de dispositivos e as atualizações de firmware exibidos selecionando uma opção no menu **Mostrar** para listar somente as atualizações de firmware de uma idade específica, atualizações de firmware de todos os tipos de servidor ou somente de tipos de servidor gerenciado ou inserindo texto no campo **Filtro**. Observe que se você pesquisar dispositivos específicos, somente os dispositivos são listados; as atualizações de firmware não são listadas sob o nome do dispositivo.

Nota: Para os servidores, estão disponíveis pacotes de atualização específicos baseados no tipo de servidor. Por exemplo, se você expandir um servidor, como o Nó de Cálculo do Flex System

x240, os pacotes de atualização disponíveis especificamente para esse nó de cálculo serão exibidos.



Resultados

Nesta página, é possível executar as ações a seguir:

- Atualizar esta página com as informações atuais de atualização de firmware do catálogo clicando no ícone **Atualizar** ( ).
- Recuperar as informações mais recentes sobre atualizações disponíveis clicando em **Atualizar Catálogo**. A recuperação dessas informações pode levar vários minutos para ser concluída. Para obter mais informações, consulte Atualizando o catálogo de produtos.
- Adicionar as atualizações de firmware ao repositório selecionando um ou mais pacotes de atualização ou atualizações no catálogo de produtos e clicando no ícone **Baixar** ( ). Quando as atualizações de firmware são baixadas e adicionadas ao repositório, o status muda para "Baixado".

  Nota: O XClarity Administrator deve ser conectado à Internet para adquirir atualizações pela interface do usuário do XClarity Administrator. Se não estiver conectado à Internet, você não poderá importar as atualizações anteriormente baixadas.

Para obter mais informações sobre o download de atualizações, consulte Baixando atualizações de firmware.

- Importar as atualizações de firmware baixadas manualmente para uma estação de trabalho que tenha acesso à rede no XClarity Administrator selecionando uma ou mais atualizações e clicando no ícone **Importar** ().Para obter mais informações sobre a importação de atualizações, consulte Baixando atualizações de firmware.
- Pare os downloads de firmware que estejam atualmente em andamento selecionando uma ou mais atualizações e, em seguida, clicando no ícone **Cancelar Downloads** ().Cancelar os downloads cancela *todos* os downloads de firmware que estão em andamento. É possível monitorar o andamento detalhado e interromper um download de firmware específico do log de trabalhos (consulte Monitorando trabalhos).
- Excluir pacotes de atualização ou atualizações individuais do repositório (consulte Excluindo atualizações de firmware).
- Exportar atualizações de firmware existentes no repositório de atualizações de firmware para um sistema local (consulte Exportando e importando atualizações de firmware).

Usando um repositório remoto para atualizações de firmware

Por padrão, o Lenovo XClarity Administrator usa um repositório local (interno) para armazenar atualizações de firmware. É possível liberar o espaço em disco que está disponível para o repositório local do XClarity Administrator usando um compartilhamento remoto montado no SSH File System (SSHFS) como repositório remoto. É possível então usar arquivos de atualização de firmware diretamente do repositório remoto para manter a conformidade de firmware em seus dispositivos.

Antes de iniciar

Somente atualizações de firmware podem ser armazenadas no compartilhamento remoto. Drivers de dispositivo Windows e atualizações do XClarity Administrator podem ser armazenados apenas no repositório de atualizações local.

Verifique se o serviço SFTP na porta 22 está aberto no servidor de compartilhamento remoto. Os Baseboard Management Controllers devem ter acesso a essa porta.

O compartilhamento remoto é usado como um servidor SFTP quando é usado como um repositório de firmware. Não desabilite o SFTP ao atualizar a configuração do SSHD.

Sobre esta tarefa

Ao alterar o local do repositório de atualizações de firmware, é possível optar por copiar todas as atualizações de firmware do repositório original no novo repositório.

Os arquivos de atualização de firmware no repositório original *não* são limpos automaticamente depois de alternar locais.

Se o XClarity Administrator tiver permissões de gravação e leitura no repositório remoto, o comportamento será o mesmo que usar o repositório local. Entretanto, se o XClarity Administrator tiver permissões somente leitura, não será possível atualizar o catálogo nem baixar ou importar atualizações para o repositório.

O mesmo repositório remoto pode ser compartilhado por várias instâncias do XClarity Administrator; entretanto, se uma instância do XClarity Administrator mudar o repositório, as outras instâncias do XClarity Administrator não serão notificadas automaticamente. Você deve atualizar o repositório para obter os detalhes mais recentes. Para atualizar o repositório, clique em **Todas as Ações → Atualizar repositório** na página Atualizações de Firmware: Repositório.

Nota: Tome cuidado ao excluir atualizações de firmware e UXSPs se o repositório das atualizações de firmware estiver localizado em um compartilhamento remoto usado por várias instâncias do XClarity Administrator.

Procedimento

Para usar um repositório de atualizações de firmware, conclua as etapas a seguir.

Etapa 1. Adicione um compartilhamento remoto ao XClarity Administrator (consulte Gerenciando o compartilhamentos remotos).

Etapa 2. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Repositório**. A página Repositório das Atualizações de Firmware é exibida.

Etapa 3. Clique em **Todas as Ações → Trocar local do repositório** para exibir a caixa de diálogo Trocar local do repositório.

Etapa 4. Selecione o compartilhamento remoto que você acabou de criar na lista suspensa **Local do repositório**.

Etapa 5. Opcionalmente, selecione **Limpar repositório atual** para excluir arquivos de atualização de firmware do local atual do repositório.

Etapa 6. Opcionalmente, selecione **Copiar pacotes de atualização do repositório atual no novo repositório** para copiar arquivos de atualização de firmware para o novo local do repositório antes de alternar o local do repositório.

Por padrão, os arquivos de atualização de firmware existentes no novo local não são copiados (são ignorados). É possível substituir quaisquer arquivos existentes ou substituir apenas o arquivo existente com um tamanho ou data de modificação diferente na lista suspensa **Substituir regras**.

Etapa 7. Clique em **OK**.

Um trabalho é criado para copiar pacotes de atualização de firmware para o novo repositório. Você pode monitorar o andamento do trabalho clicando em **Monitoramento → Trabalhos** na barra de menus do XClarity Administrator.

Atualizando o catálogo de produtos

O catálogo de produtos contém informações sobre todas as atualizações de firmware que estão disponíveis para todos os dispositivos compatíveis com o Lenovo XClarity Administrator, incluindo chassis, servidores e Comutadores Flex.

Antes de iniciar

Uma conexão com a Internet é necessária para atualizar o catálogo de produtos.

A atualização do catálogo pode levar vários minutos para ser concluída.

Sobre esta tarefa

Quando você atualiza o catálogo, o XClarity Administrator recupera informações sobre as atualizações de firmware mais recentes disponíveis do Site de suporte do Lenovo XClarity e armazena as informações no repositório das atualizações de firmware.

A atualização do catálogo apenas adiciona informações sobre as atualizações de firmware disponíveis no repositório. Ela não baixa os pacotes de atualização. Você deve baixar as atualizações de firmware para tornar as atualizações disponíveis para instalação. Para obter mais informações sobre o download de atualizações, consulte Baixando atualizações de firmware.

Procedimento

Para atualizar o catálogo de produtos, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Repositório**. A página Repositório das Atualizações de Firmware é exibida.

Etapa 2. Clique na guia **Atualizações Individuais** para recuperar informações sobre os pacotes de atualização de firmware individuais ou clique na guia **UpdateXpress System Pack (UXSP)** para recuperar informações sobre UXSPs.

Etapa 3. Clique em **Atualizar Catálogo** e clique em uma das opções a seguir para obter informações sobre as atualizações de firmware mais recentes disponíveis.

- **Atualizar Selecionado - Somente Mais Recente**. Recupera informações sobre a versão mais atual das atualizações de firmware disponíveis apenas para os dispositivos selecionados.
- **Atualizar Tudo - Somente Mais Recente**. Recupera informações sobre a versão mais atual de todas as atualizações de firmware para os dispositivos com suporte.
- **Atualizar Selecionado**. Recupera informações sobre todas as versões de atualizações de firmware disponíveis apenas para os dispositivos selecionados.
- **Atualizar Tudo**. Recupera informações sobre todas as versões de todas as atualizações de firmware disponíveis para todos os dispositivos com suporte.

Dica: é possível atualizar o catálogo de produtos e fazer download do firmware mais recente em uma etapa clicando em **Todas as Ações → Atualizar e fazer download do mais recente para todos os dispositivos gerenciados** ou **Todas as Ações → Atualizar e fazer download do mais recente para os dispositivos selecionados**.

Baixando atualizações de firmware

É possível baixar ou importar atualizações de firmware no repositório das atualizações de firmware, dependendo do seu acesso à Internet. As atualizações de firmware devem estar disponíveis no repositório das atualizações de firmware para que você possa atualizar o firmware em dispositivos de gerenciamento.

Antes de iniciar

Verifique se todas as portas e o endereço de Internet que o Lenovo XClarity Administrator exige estão disponíveis antes de tentar baixar o firmware. Para obter mais informações sobre portas, consulte Disponibilidade de porta e Firewalls e servidores proxy na documentação online do XClarity Administrator.

Se um tipo de dispositivo não estiver listado no repositório das atualizações de firmware, você deverá primeiro gerenciar um dispositivo desse tipo antes de baixar ou importar atualizações de firmware individuais para esse tipo de dispositivo.

Importante:

- Para o XClarity Administrator v1.1.1 e versões anteriores, você deve baixar e importar manualmente as atualização de firmware para Lenovo Hardware na Site de Suporte a data center da Lenovo.
- O XClarity Administrator não pode fazer download de atualizações para comutadores RackSwitch e dispositivos de armazenamento Lenovo séries DE, DX e SS do site da Lenovo para o repositório das atualizações de firmware; em vez disso, você deve fazer download e importar manualmente essas atualizações do site da Lenovo para uma estação de trabalho que tenha acesso ao host do XClarity Administrator ou fazer download e aplicar os *pacotes do repositório de atualizações de firmware*, que contêm todas as atualizações de firmware disponíveis.
- Os navegadores da Web Internet Explorer e Microsoft Edge têm um limite de upload de 4 GB. Se o arquivo que você está importando for maior que 4 GB, considere usar outro navegador da Web (como o Chrome ou o Firefox).

- Para fazer download do firmware para dispositivos de armazenamento ThinkSystem série DM:
  - Um ou mais dispositivos de armazenamento ThinkSystem série DM devem ser gerenciados pelo XClarity Administrator.
  - Cada dispositivo de armazenamento ThinkSystem série DM deve ter direito a serviço e suporte de hardware.
  - Você deve especificar o país em que os dispositivos de armazenamento ThinkSystem série DM estão localizados na página Atualizações de Firmware: Repositório. Somente o firmware criptografado pode ser baixado para dispositivos nos seguintes países: Armênia, Bielorrússia, China, Cuba, Irã, Casaquistão, Kyrgyzstão, Coreia do Norte, Rússia, Sudão, Síria.

Sobre esta tarefa

Você pode baixar atualizações de firmware de algumas maneiras diferentes:

- **Pacotes do repositório de atualizações de firmware**

  Os pacotes do repositório de atualização de firmware são coleções do firmware mais recente disponível no mesmo momento do lançamento do XClarity Administrator para a maioria dos dispositivos compatíveis e uma política de conformidade de firmware padrão atualizada. Esses pacotes de repositório são importados e, depois, aplicados da página Atualizar Servidor de Gerenciamento. Quando você aplica um pacote do repositório de atualizações de firmware, cada pacote de atualização é adicionado ao repositório das atualizações de firmware, e uma política de conformidade de firmware padrão é criada automaticamente para todos os dispositivos gerenciáveis. É possível copiar essa política predefinida, mas não é possível alterá-la.

  Os pacotes do repositório a seguir estão disponíveis.

  - **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os CMMs e comutadores Flex System.
  - **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os comutadores RackSwitch e dispositivos Lenovo Storage.
  - **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos Converged HX Series, Flex System, NeXtScale e Servidores System x.
  - **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os servidores ThinkAgile e ThinkSystem.
  - **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os servidores ThinkAgile e ThinkSystem V2.
  - **lnvgy_sw_lxca_thinksystemv3repo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os servidores ThinkAgile e ThinkSystem V3.

  É possível determinar se os pacotes do repositório de atualizações de firmware estão armazenados no repositório na coluna **Status de Download** da página Atualizar Servidor de Gerenciamento. Essa coluna contém os seguintes valores:

  - **Baixado**. O pacote do repositório de atualizações de firmware é armazenado no repositório.
  - **Não Baixado**. O pacote do repositório de atualizações de firmware está disponível, mas não armazenado no repositório.

- **UpdateXpress System Packs (UXSPs)**

  Nota: Para servidores com XCC2, esses pacotes são chamados de pacotes de firmware. O *pacote* é usado nos nomes de pacote e nomes de política predefinidos.

  Os UXSPs contêm as atualizações mais recentes disponíveis de drivers de dispositivo e firmware, organizadas por sistema operacional. Quando você baixa UXSPs, o XClarity Administrator baixa o UXSP

com base na versão que está relacionada no catálogo e armazena os pacotes de atualizações no repositório de atualizações de firmware. Quando você baixa um UXSP, cada atualização de firmware no UXSP é adicionada ao repositório das atualizações de firmware e listada na guia **Atualizações Individuais**, e uma política de conformidade de firmware padrão é criada automaticamente para todos os dispositivos gerenciáveis usando os seguintes nomes. É possível copiar essa política predefinida, mas não é possível alterá-la.

– *{uxsp-version}-{date}-{server-short-name}*-**UXSP** (por exemplo, `v1.50-2017-11-22- SD530-UXSP`)
– *{uxsp-version}-{buildnumber}-{server-short-name}*-**bundle** (por exemplo, `22a.0-kaj92va-SR650V3-bundle`)

Nota: Quando os UXSPs são baixados ou importados da página Atualizações de Firmware: Repositório, somente atualizações de firmware são baixadas e armazenadas no repositório. Atualizações de driver de dispositivo são descartadas. Para obter informações sobre o download ou a importação de atualizações de driver de dispositivo do Windows usando os UXSPs, consulte Gerenciando o repositório de drivers de dispositivo do SO.

É possível determinar se os UXSPs estão armazenados no repositório das atualizações de firmware na coluna **Estado de Download** na guia **Atualizações Individuais** da página Atualizações de Firmware: Repositório. Essa coluna contém os seguintes valores:

– **Baixado**. O pacote de atualização inteiro ou a atualização de firmware individual são armazenados no repositório.
– *x* **de** *y* **Baixado**. Algumas atualizações de firmware (não todas) no pacote de atualização estão armazenadas no repositório. Os números entre parênteses indicam o número de atualizações disponíveis e o número de atualizações armazenadas, ou não há atualizações para o tipo de dispositivo específico.
– **Não Baixado**. O pacote de atualização inteiro ou a atualização de firmware individual estão disponíveis, mas não armazenados no repositório.

- **Atualizações individuais de firmware**

  Também é possível baixar pacotes de atualização de firmware individuais de uma vez. Quando você baixa pacotes de atualização de firmware, o XClarity Administrator baixa a atualização, com base na versão que é listada no catálogo, e armazena os pacotes de atualizações no repositório das atualizações de firmware. Você pode então criar políticas de conformidade de firmware usando esses pacotes de atualização para cada um dos dispositivos gerenciados.

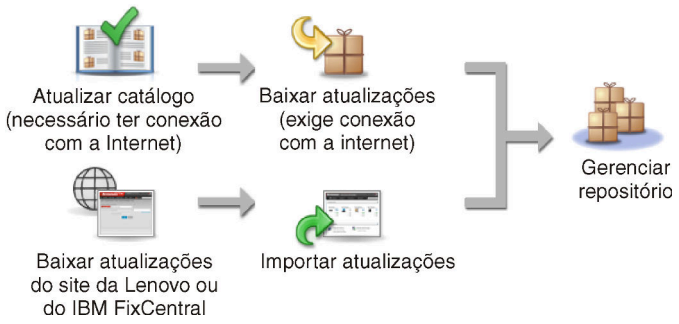
  Nota: As principais atualizações de firmware (como controlador de gerenciamento, UEFI e pDSA) são independentes do sistema operacional. Os pacotes de atualização de firmware para os sistemas operacionais RHEL 6 ou SLES 11 são usados para atualizar nós de cálculo e servidores de rack. Para obter mais informações sobre quais pacotes de atualização de firmware usar para servidores gerenciados, consulte Baixando atualizações de firmware.

  É possível determinar se *atualizações de firmware* específicas estão armazenadas no repositório de atualizações de firmware na coluna **Status de Download** na guia **Atualizações Individuais** na página Atualizações de Firmware: Repositório. Essa coluna contém os seguintes valores.

  – **Baixado**. O pacote de atualização inteiro ou a atualização de firmware individual são armazenados no repositório.
  – *x* **de** *y* **Baixado**. Algumas atualizações de firmware (não todas) no pacote de atualização estão armazenadas no repositório. Os números entre parênteses indicam o número de atualizações disponíveis e o número de atualizações armazenadas, ou não há atualizações para o tipo de dispositivo específico.
  – **Não Baixado**. O pacote de atualização inteiro ou a atualização de firmware individual estão disponíveis, mas não armazenados no repositório.

Ao instalar o XClarity Administrator ou atualizar para uma nova versão, é recomendável baixar o pacote do repositório mais recente para garantir que você tenha as atualizações de firmware mais recentes. Em seguida, é possível agendar um trabalho recorrente para atualizar o catálogo para localizar atualizações individuais que foram lançadas na Web desde o último pacote do repositório e, em seguida, baixar eletronicamente essas atualizações, uma por vez.

O XClarity Administrator deve estar conectado à Internet para atualizar o catálogo e baixar as atualizações de firmware. Se ele não estiver conectado à Internet, será possível baixar manualmente os arquivos para uma estação de trabalho que tenha acesso host do XClarity Administrator usando um navegador da Web e, em seguida, importar os arquivos para o repositório das atualizações de firmware.



Ao importar manualmente atualizações de firmware para o XClarity Administrator, você deve incluir os seguintes arquivos necessários: carga útil (imagem e MIB), metadados, histórico de alterações e leiame. Exemplo:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Nota: As principais atualizações de firmware (como controlador de gerenciamento, UEFI e pDSA) são independentes do sistema operacional. Os pacotes de atualização de firmware para os sistemas operacionais RHEL 6 ou SLES 11 são usados para atualizar nós de cálculo e servidores de rack.

Uma mensagem é exibida na página quando o repositório está mais de 50% completo. Uma outra mensagem é exibida na página quando o repositório está mais de 85% completo. Para reduzir o espaço usado no repositório, é possível remover os arquivos de imagens e políticas não usados. Para remover as políticas de conformidade de firmware não usadas e os pacotes de firmware associados, clique em **Fornecimento → Políticas de conformidade**, selecione uma ou mais políticas a serem excluídas e clique em **Ações → Excluir todos os pacotes de políticas e firmware**.

A tabela a seguir resume as diferenças entre adquirir pacotes do repositório de atualização de firmware, UXSPs e pacotes de atualização de firmware individuais.

Pacote de atualização	Página da interface do usuário para baixar e importar arquivos	Página da Web para baixar arquivos manualmente	O repositório das atualizações de firmware está atualizado?	A política de conformidade de firmware é atualizada automaticamente?
Pacotes do repositório de atualizações de firmware	Página Atualizar Servidor de Gerenciamento **Nota:** Você deve importar e depois aplicar o pacote do repositório.	Página da Web de download do XClarity Administrator	Sim	Sim
UpdateXpress System Packs	Atualizações de Firmware: página Repositório, guia **UpdateXpress System Packs (UXSPs)**	Web site do Lenovo XClarity Essentials UpdateXpress	Sim	Sim
Atualizações de firmware	Atualizações de firmware: página Repositório, guia **Atualizações Individuais**	Site de Suporte a data center da Lenovo **Notas:** Use o Website do Fix Central para os seguintes dispositivos: • Flex System x220 Tipo 2585, 7906 • Flex System x222 Compute Nod Tipo 2589, 7916 • Flex System x240 Tipo 7863, 8737, 8738, 8956 • Flex System x280 / x480 / x880 X6 Tipo 4259, 7903 • Flex System x440 Tipo 2584, 7917	Sim	Não

Procedimento

Para baixar uma ou mais atualizações de firmware, conclua as etapas a seguir.

- Para importar um ou mais *pacotes do repositório de atualizações de firmware*:
  1. Na barra de menus XClarity Administrator, clique em **Administração → Atualizar Servidor de Gerenciamento** para exibir a página Atualização do Servidor de Gerenciamento.
  2. Baixe os pacotes de repositório mais recentes:
     - Se o XClarity Administrator estiver conectado à Internet:
       a. Recupere informações sobre as atualizações mais recentes clicando em **Atualizar catálogo → Atualizar Todos Os Gerenciados – apenas os Mais Recentes**). As novas atualizações do servidor de gerenciamento e os pacotes do repositório de atualizações de firmware são listados na tabela da página "Atualização do Servidor de Gerenciamento".

          A atualização do repositório pode levar vários minutos para ser concluída.

Nota: A atualização do repositório não baixa automaticamente os arquivos de carga útil. Apenas os arquivos de metadados e leiame são baixados.

b. Selecione os pacotes do repositório de atualizações de firmware que deseja baixar.

Dica: certifique-se de que os pacotes selecionado tenham "Pacote Complementar" na coluna **Tipo**.

c. Clique no ícone **Baixar Selecionado** (). Quando o download estiver concluído, o **Status de Download** dessa atualização de software será alterado para "Baixado".

– Se o XClarity Administrator não estiver conectado à Internet:

a. Baixe os pacotes do repositório de atualizações de firmware do Página da Web de download do XClarity Administrator para uma estação de trabalho que tenha uma conexão de rede com o host do XClarity Administrator.

b. Na página Atualização do Servidor de Gerenciamento, clique no ícone **Importar** ().

c. Clique em **Selecionar Arquivos** e navegue até o local dos pacotes do repositório de atualizações de firmware na estação de trabalho.

d. Selecione todos os arquivos do pacote e clique em **Abrir**.

Você deve importar o arquivo de metadados (.xml ou .json), bem como o arquivo de imagem ou carga útil (.zip, .bin, .uxz ou .tgz), o arquivo de histórico de alterações (.chg) e o arquivo leiame (.txt) para a atualização. Os arquivos que estiverem selecionados, mas não especificados no arquivo de metadados, serão descartados. Se você não incluir o arquivo de metadados, a atualização não será importada.

e. Clique em **Importar**.

Quando a importação estiver concluída, os pacotes do repositório de atualizações de firmware serão listados na tabela da página Atualização do Servidor de Gerenciamento, e o **Status de Download** de cada atualização será "Baixado".

3. Selecione os pacotes do repositório de atualizações de firmware que você deseja instalar para o repositório das atualizações de firmware.

Nota: Verifique se o **Status de Download** é "Baixado" e o **Tipo** é "Patch."

4. Clique no ícone **Realizar Atualização** () para adicionar os pacotes de atualizações de firmware ao repositório.
5. Aguarde alguns minutos para concluir a atualização e o XClarity Administrator ser reiniciado.
6. Determine se a atualização está concluída atualizando o navegador da Web.

Quando estiver concluída, a página Atualização do Servidor de Gerenciamento será exibida e a coluna **Status Aplicado** será alterada para "Aplicado."

7. Limpe o cache do navegador da Web.

- Para baixar um ou mais *UXSPs*.

1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Repositório** para exibir a página Repositório das Atualizações de Firmware.
2. Clique na guia **UpdateXpress System Packs (UXSPs)**.
3. Baixe os UXSPs mais recentes:

– Se o XClarity Administrator estiver conectado à Internet:

Para atualizar o catálogo e fazer download do UXSPs mais recente para todos os dispositivos gerenciados, clique em **Todas as Ações → Atualizar e fazer download do mais recente para todos os dispositivos gerenciados**.

Para atualizar o catálogo e fazer download dos UXSPs mais recentes somente para dispositivos selecionados:

a. Expanda o dispositivo para exibir a lista de UXSPs disponíveis.

b. Selecione um ou mais UXSPs dos quais você deseja fazer download.

c. Clique em **Todas as Ações → Atualizar e fazer download do mais recente para dispositivos selecionados**.

Quando o download estiver concluído, o **Status de download** dos UXSPs selecionados será alterado para "Baixado."

– Se o XClarity Administrator não estiver conectado à Internet:

a. Baixe os UXSPs do Web site do Lenovo XClarity Essentials UpdateXpress para uma estação de trabalho que tenha uma conexão de rede com o host do XClarity Administrator

b. No XClarity Administrator, clique no ícone **Importar** ( ).

c. Clique em **Selecionar Arquivos** e navegue até o local do UXSPs na estação de trabalho.

d. Selecione todos os arquivos do pacote e clique em **Abrir**.

Você deve importar o arquivo de metadados (.xml ou .json), bem como o arquivo de imagem ou carga útil (.zip, .bin, .uxz ou .tgz), o arquivo de histórico de alterações (.chg) e o arquivo leiame (.txt) para a atualização. Os arquivos que estiverem selecionados, mas não especificados no arquivo de metadados, serão descartados. Se você não incluir o arquivo de metadados, a atualização não será importada.

e. Clique em **Importar**.

Quando a importação estiver concluída, os pacotes do repositório de atualizações de firmware serão relacionados na tabela da página Atualização do Servidor de Gerenciamento, e o Status de Download de cada atualização será "Baixado."

- Para baixar um ou mais *pacotes de atualização de firmware* individuais.

1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Repositório** para exibir a página Repositório das Atualizações de Firmware.
2. Se você fizer download do firmware para dispositivos de armazenamento ThinkSystem série DM, selecione o país onde os dispositivos de armazenamento estão localizados.
3. Clique na guia **Atualizações Individuais**.
4. Baixe as atualizações de firmware individuais mais recentes:

– Se o XClarity Administrator estiver conectado à Internet:

Para atualizar o catálogo e fazer download do firmware mais recente para todos os dispositivos gerenciados, clique em **Todas as Ações → Atualizar e fazer download do mais recente para todos os dispositivos gerenciados**.

Para atualizar o catálogo e fazer download do firmware mais recente somente para dispositivos selecionados:

a. Expanda o dispositivo para exibir a lista de atualizações de firmware disponíveis.

b. Selecione uma ou mais atualizações de firmware das quais você deseja fazer download.

Dica: Um pacote de atualização pode consistir em várias atualizações de firmware. Ao baixar uma atualização de firmware, você pode optar por baixar o pacote de atualização inteiro ou somente atualizações específicas. É possível também optar por baixar vários pacotes ao mesmo tempo.

c. Clique em **Todas as Ações → Atualizar e fazer download do mais recente para dispositivos selecionados**.

Quando o download estiver concluído, o **Status de download** das atualizações de firmware selecionadas será alterado para "Baixado".

- Se o XClarity Administrator não estiver conectado à Internet:
  a. Baixe os pacotes de atualização de firmware do Site de Suporte a data center da Lenovo para uma estação de trabalho que tenha uma conexão de rede com o host do XClarity Administrator.

     Para os servidores a seguir, baixe atualizações de firmware para o sistema operacional SLES 11 do Website do Fix Central:

     - Flex System x220 Tipo 2585, 7906
     - Flex System x222 Compute Nod Tipo 2589, 7916
     - Flex System x240 Tipo 7863, 8737, 8738, 8956
     - Flex System x280 / x480 / x880 X6 Tipo 4259, 7903
     - Flex System x440 Tipo 2584, 7917

     Para todos os outros servidores, baixe atualizações de firmware para o sistema operacional RHEL 6 do Site de suporte do Lenovo XClarity:

  b. No XClarity Administrator, clique no ícone **Importar** ().
  c. Clique em **Selecionar Arquivos** e navegue até o local das atualizações de firmware na estação de trabalho.
  d. Selecione todos os arquivos do pacote e clique em **Abrir**.

     Você deve importar o arquivo de metadados (.xml ou .json), bem como o arquivo de imagem ou carga útil (.zip, .bin, .uxz ou .tgz), o arquivo de histórico de alterações (.chg) e o arquivo leiame (.txt) para a atualização. Os arquivos que estiverem selecionados, mas não especificados no arquivo de metadados, serão descartados.

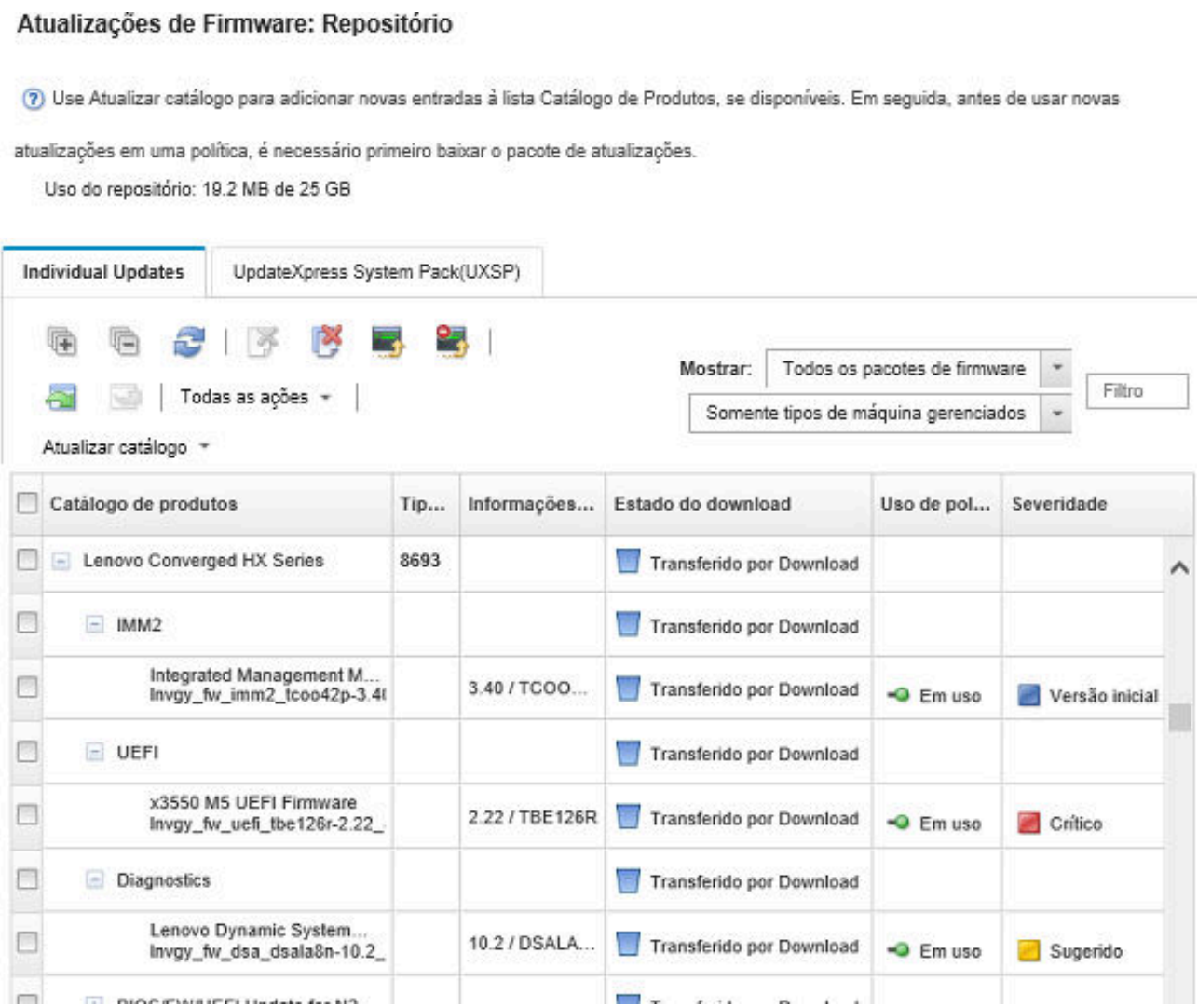
     Atenção:

     - Importe somente esses arquivos necessários. Não importe outros arquivos que possam ser encontrados nos sites de download de firmware.
     - Se você não incluir o arquivo XML no pacote de atualização, a atualização não será importada.
     - Se você não incluir todos os arquivos necessários à atualização, o repositório mostrará que a atualização não foi baixada, indicando que ela foi parcialmente importada. Você poderá então importar os arquivos ausentes. Basta selecionar os arquivos e importá-los.
     - As principais atualizações de firmware (como controlador de gerenciamento, UEFI e pDSA) são independentes do sistema operacional. Os pacotes de atualização de firmware para os sistemas operacionais RHEL 6 ou SLES 11 são usados para atualizar nós de cálculo e servidores de rack. Para obter mais informações sobre quais pacotes de atualização de firmware usar para servidores gerenciados, consulte Baixando atualizações de firmware.

  e. Clique em **Importar**.

A atualização do catálogo e o download das atualizações de firmware podem levar alguns minutos. Quando as atualizações tiverem sido baixadas e armazenadas no repositório, a linha será destacada no catálogo de produtos, e a coluna **Status de Download** será alterada para "Baixado."

Nota: O tipo de máquina para alguns comutadores pode aparecer como um número hexadecimal.



Depois de concluir

Você pode configurar o tamanho máximo do repositório de atualizações (incluindo firmware, drivers de dispositivo do sistema operacional e atualizações de servidores de gerenciamento) na página Repositório de firmware clicando em **Todas as Ações → Configurações Globais**. O tamanho mínimo é de 50 GB. O tamanho máximo depende da quantidade de espaço em disco no sistema local.

Exportando e importando atualizações de firmware

Você pode exportar atualizações de firmware individuais e UpdateXpress System Packs (UXSPs) existentes no repositório para o sistema local.

Sobre esta tarefa

Somente atualizações de firmware existentes no repositório são exportadas. Verifique se o status de download das atualizações de firmware selecionadas é "Baixado."

Todos os arquivos que estão associados com a atualização de firmware são exportados, incluindo a imagem de atualização ou o arquivo de carga útil (.zip, .bin, .uxz ou .tgz), o arquivo de metadados (.xml ou .json), o arquivo de histórico de alterações (.chg) e o arquivo leiame (.txt).

Atenção: Não altere o nome dos arquivos de atualização de firmware.

Procedimento

- Para exportar atualizações de firmware:
  1. Clique na guia **Atualizações Individuais** ou na guia **UpdateXpress System Packs (UXSPs)**.
  2. Selecione uma ou mais atualizações de firmware.
  3. Clique no ícone **Exportar** ( ).
- Para importar atualizações de firmware:

  É possível importar arquivos manualmente exportados do Lenovo XClarity Administrator e os arquivos baixados manualmente da web. Para obter mais informações, consulte Baixando atualizações de firmware.

Excluindo atualizações de firmware

É possível excluir atualizações de firmware e UpdateXpress System Packs (UXSPs) do repositório das atualizações de firmware.

Antes de iniciar

Certifique-se de que todos os trabalhos de atualização em execução ou planejados, que usam uma política de conformidade de firmware contendo atualizações de firmware a serem excluídas, sejam concluídos ou cancelados (consulte Monitorando trabalhos).

Certifique-se de que a atualização não esteja sendo usada em uma política de conformidade de firmware antes de excluir a atualização. Você não pode excluir pacotes de atualização de firmware que sejam atualmente usados em uma ou mais políticas de conformidade de firmware.

Excluir um UXSP também exclui a política de conformidade de firmware que foi criada automaticamente para o UXSP.

Nota: Tome cuidado ao excluir atualizações de firmware e UXSPs se o repositório das atualizações de firmware for um compartilhamento remoto usado por várias instâncias do XClarity Administrator.

Procedimento

Para excluir uma ou mais atualizações de firmware do repositório, conclua as etapas a seguir.

Etapa 1. Cancele a atribuição de todas as políticas de conformidade de firmware que contêm as atualizações de firmware a serem excluídas de todos os dispositivos gerenciados.

a. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Aplicar/Ativar**. A página Aplicar/Ativar Atualizações de Firmware é exibida.

b. Selecione "Sem atribuição" ou outra política de conformidade de firmware na coluna **Política Atribuída** para os dispositivos gerenciados que usam a política de conformidade de firmware.

Etapa 2. Exclua todas as políticas de conformidade de firmware definidas pelo usuário que contêm as atualizações de firmware a serem excluídas ou edite as políticas para remover as atualizações de firmware a serem excluídas.

a. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Políticas de Conformidade**. A página Política de Conformidade das Atualizações de Firmware é exibida.

b. Selecione a política de conformidade de firmware e, em seguida, selecione o ícone **Excluir** ( ) para excluir a política, ou clique no ícone **Editar** ( ) para remover as atualizações de firmware da política.

Etapa 3. Exclua as atualizações de firmware.

- **Atualizações individuais de firmware**
  1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Repositório**. A página Repositório das Atualizações de Firmware é exibida.
  2. Clique na guia **Atualizações Individuais**.
  3. Selecione uma ou mais atualizações de firmware a serem excluídas.
  4. Clique no ícone **Excluir imagens apenas** ( ) para excluir a imagem ou o arquivo de carga útil (.zip, .bin, .uxz ou .tgz). Informações sobre a atualização são mantidas, para que você possa baixar novamente a atualização com facilidade. Ou, clique no ícone **Excluir pacotes de atualização inteiros** ( ) para excluir os pacotes de atualização inteiros, incluindo o arquivo de imagem ou carga útil, o arquivo de histórico de alterações (.chg), o arquivo leiame (.txt) e o arquivo de metadados (.xml ou j.son).

  Quando você exclui uma atualização de firmware, os arquivos de carga útil são removidos; entretanto, o arquivo de metadados, que contém informações sobre a atualização, é mantido de forma que você possa baixar novamente a atualização com facilidade, se necessário, e o **Estado de Download** será alterado para "Não baixado".
- **UXSPs**
  1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Repositório**. A página Repositório das Atualizações de Firmware é exibida.
  2. Clique na guia **UpdateXpress System Pack (UXSP)**.
  3. Selecione um ou mais UXSPs a serem excluídos.
  4. Clique no ícone **Excluir UXSP e política associada** ( ) para excluir os UXSPs inteiros, incluindo o arquivo de imagem ou carga útil, o arquivo de histórico de alterações (.chg), o arquivo leiame (.txt), o arquivo de metadados (.xml ou j.son) e todas as políticas de conformidade de firmware associadas.

  Se os UXSPs selecionado estiverem associados às políticas em uso (atribuído para dispositivos), a caixa de diálogo Excluir UXSP, Política e Pacotes de Atualização será exibida. Escolha se deseja excluir as políticas atribuídas além do UXSP e das políticas não atribuídas e clique em **Ok**.

Criando e atribuindo políticas de conformidade de firmware

As políticas de conformidade de firmware garantem que o firmware em determinados dispositivos gerenciados esteja no nível atual ou específico sinalizando os dispositivos que precisam de atenção. Cada política de conformidade de firmware identifica quais dispositivos são monitorados e qual nível de firmware deve ser instalado para manter os dispositivos em conformidade. Você pode definir a conformidade no nível do componente do dispositivo ou do firmware. O XClarity Administrator, em seguida, usa essas políticas para verificar o status dos dispositivos gerenciados e identificar dispositivos que estão fora de conformidade.

Antes de iniciar

Ao criar uma política de conformidade de firmware, selecione a versão de atualização de destino a ser aplicada aos dispositivos que serão atribuídos à política. Certifique-se de que as atualizações de firmware da versão de destino estejam no repositório de atualizações antes de criar a política (consulte Baixando atualizações de firmware).

Se um tipo de dispositivo não estiver listado no repositório das atualizações de firmware, você deverá primeiro gerenciar um dispositivo desse tipo e, em seguida, baixar ou importar o conjunto completo de atualizações de firmware antes de criar políticas de conformidade para dispositivos desse tipo.

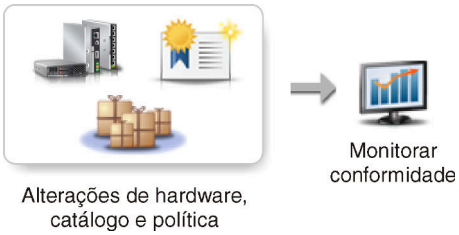
Sobre esta tarefa

Ao criar uma política de conformidade de firmware, você pode optar para que o XClarity Administrator sinalize um dispositivo quando:

- O firmware no dispositivo estiver em um nível inferior
- O firmware no dispositivo não corresponder exatamente à versão do destino de conformidade

O XClarity Administrator é fornecido com uma política de conformidade de firmware predefinida chamada **Firmware mais recente no repositório**. Quando um novo firmware é baixado ou importado para o repositório, essa política é atualizada para incluir as versões mais recentes disponíveis do firmware no repositório.

Depois que uma política de conformidade de firmware é atribuída a um dispositivo, o XClarity Administrator verifica o status de conformidade de cada dispositivo quando há alterações no inventário do dispositivo ou no repositório das atualizações de firmware. Quando o firmware em um dispositivo não está em conformidade com a política atribuída, o XClarity Administrator identifica esse dispositivo como incompatível na página na Atualizações de Firmware: Aplicar/Ativar, com base na regra especificada na política de conformidade de firmware



Por exemplo, é possível criar uma política de conformidade de firmware que defina o nível da linha de base do firmware instalado em todos os dispositivos ThinkSystem SR850 e atribuir essa política de conformidade de firmware a todos os dispositivos ThinkSystem SR850 gerenciados. Quando o repositório das atualizações de firmware é atualizado e uma nova atualização de firmware é adicionada, esses nós de cálculo podem ficar fora de conformidade. Quando isso acontece, o XClarity Administrator atualiza a página Atualizações de Firmware: Aplicar/Ativar para mostrar que os dispositivos não estão em conformidade e gerar um alerta.

Nota: É possível optar por mostrar ou ocultar alertas de dispositivos que não atendem aos requisitos de suas políticas de conformidade de firmware atribuídas (consulte Definir configurações globais de atualização de firmware). Os alertas são ocultos por padrão.

Procedimento

Para criar e atribuir uma política de conformidade de firmware, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Políticas de Conformidade**. A página Política de Conformidade é exibida com uma lista de todas as políticas de conformidade de firmware existentes.

Etapa 2. Crie uma política de conformidade de firmware.

1. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Criar uma Nova Política.

2. Preencha o nome e a descrição da política de conformidade de firmware.
3. Preencha a tabela com base nos seguintes critérios para cada dispositivo.
   - **Tipo de dispositivo**. Escolha um tipo de dispositivo ou componente para o qual esta política deve ser aplicada.

     Dica: Se você escolher um servidor, o nível de conformidade será feito no nível de UXSP. Entretanto, também é possível expandir o servidor para definir níveis de firmware específicos para cada componente, como Baseboard Management Controller ou UEFI.
   - **Destino de Conformidade**. Especifique o destino de conformidade para dispositivos e subcomponentes aplicáveis.

     Em servidores, é possível escolher um dos valores a seguir.

     – **Padrão**. Altera o destino de conformidade de cada subcomponente para o valor padrão (como o conjunto mais recente de firmware no repositório desse dispositivo).

– **Não atualizar**. Altera o destino de conformidade de cada subcomponente para "Não atualizar."

Para dispositivos sem subcomponentes (como CMMs, comutadores ou dispositivos de armazenamento) ou subcomponentes em um servidor, é possível escolher um dos valores a seguir.

– <*firmware_level*>. Especifica o nível de firmware da linha de base.

– **Não atualizar**. Especifica que o firmware não será atualizado. Observe que o firmware no controlador de gerenciamento de backup não é atualizado por padrão.

Nota: Quando você altera os valores padrão para qualquer subcomponente em um servidor, o destino de conformidade do servidor muda para **Personalizar**.

- **Regra de Conformidade**. Especifique quando um dispositivo é sinalizado como não conforme na coluna **Versão Instalada** de Atualizações de Firmware: Aplicar/Ativar.

  – **Sinalizar se for de nível inferior**. Se o nível de firmware que estiver instalado em um dispositivo for anterior ao nível especificado na política de conformidade de firmware, o dispositivo será sinalizado como não conforme. Por exemplo, se você substituir um adaptador de rede em um nó de cálculo, e o firmware nesse adaptador de rede for anterior ao nível identificado na política de conformidade de firmware, o nó de cálculo será sinalizado como não conforme.

  – **Sinalizar se a correspondência não for exata**. Se o nível de firmware que estiver instalado em um dispositivo não for uma correspondência exata com a política de conformidade de firmware, o dispositivo será sinalizado como não conforme. Por exemplo, se você substituir um adaptador de rede em um nó de cálculo, e o firmware nesse adaptador de rede for diferente do nível identificado na política de conformidade de firmware, o nó de cálculo será sinalizado como não conforme.

  – **Sem sinalizador**. Dispositivos que estão fora de conformidade não são sinalizados.

4. **Opcional:** Expanda o tipo de sistema para exibir cada atualização do pacote, e selecione o nível de firmware a ser usado como destino de conformidade, ou selecione "Não atualizar" para evitar que o firmware seja atualizado nesse dispositivo.
5. Clique em **Criar**.

   A política de conformidade de firmware está listada na tabela da página Atualizações de Firmware: Política de Conformidade. A tabela mostra o status de uso, a origem da política (se é definida pelo usuário ou predefinida), e a data da última modificação.

Etapa 3. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Aplicar/Ativar**. A página Atualizações de Firmware: Aplicar/Ativar é exibida com uma lista de dispositivos gerenciados.

Etapa 4. Atribua a política de conformidade de firmware a dispositivos.

- **Para um único dispositivo**

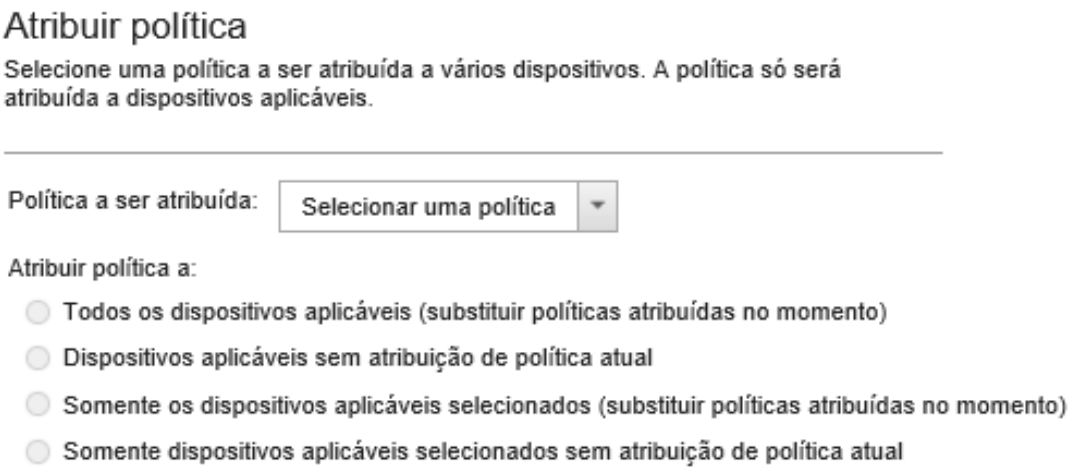
  Para cada dispositivo, selecione uma política no menu suspenso na coluna **Política de Conformidade Atribuída**.

  Você pode selecionar uma opção em uma lista de políticas de conformidade de firmware aplicáveis a cada dispositivo. Se não houver uma política atualmente atribuída ao dispositivo, a política atribuída será definida como **Sem atribuição**. Se nenhuma política for aplicável ao dispositivo, a política atribuída será definida como **Sem políticas aplicáveis**.

- **Para vários dispositivos**

  1. **Opcional:** Selecione um ou mais dispositivos aos quais deseja atribuir uma política de conformidade de firmware.

2. Clique no ícone **Atribuir política** ( ) para exibir a caixa de diálogo Atribuir política.



3. Selecione uma política de conformidade de firmware no menu suspenso **Política para atribuição**.

   Você pode selecionar uma opção em uma lista de políticas de conformidade de firmware aplicáveis a todos os dispositivos selecionados. Se os dispositivos não foram selecionados antes de abrir a caixa de diálogo, todas as políticas serão listadas.

   Para cancelar a atribuição de uma política, selecione **Sem atribuição**.
4. Selecione um dos seguintes escopos para a atribuição de política.
   - **Todos os dispositivos aplicáveis que são...**
   - **Somente dispositivos aplicáveis selecionados que são...**
5. Selecione um ou mais critérios de dispositivo.
   - **Sem uma política atribuída**
   - **Não compatível (substituir política atribuída atual)**
   - **Compatível (substituir política atribuída atual)**
   - **Não monitorado (substituir política atribuída atual)**
   - **Outro (substituir política atribuída atual)**. Isso se aplica a dispositivos em outros estados, como o estado pendente, com dados ausentes ou não compatíveis com atualizações. Passe o mouse sobre o ícone de ajuda ( ) para ver uma lista de dispositivos aplicáveis.

   Nota: Não monitorado e **Outros** critérios são listados apenas quando há dispositivos nesses estados.
6. Clique em **OK**.

   A política listada na coluna **Política Atribuída** na página Atualizações de Firmware: Repositório altera o nome da política de conformidade de firmware selecionada.

Depois de concluir

Depois de criar uma política de conformidade de firmware, você executa as seguintes ações em uma política de conformidade de firmware selecionada:

- Exiba detalhes de política, incluindo uma lista de dispositivos atribuídos, clicando no nome da política na tabela.

- Crie uma duplicata de uma política selecionada clicando no ícone **Copiar** ().
- Defina outro nome ou modifique uma política selecionada clicando no ícone **Editar** ().Não é possível editar uma política de conformidade de firmware predefinida ou uma política atribuída a um dispositivo gerenciado.

  Se você modificar uma política atribuída de forma que não se aplique mais a determinados dispositivos atribuídos, a atribuição da política será automaticamente cancelada nesses dispositivos.

  Não é possível definir outro nome nem modificar a política **Firmware mais recente** predefinida.
- Exclua uma política de conformidade de firmware selecionada clicando no ícone **Excluir política** () ou exclua a política de conformidade de firmware selecionada e todas as atualizações de firmware associadas usadas apenas por essa política clicando no ícone **Excluir todos os pacotes de políticas e firmware** ().Você pode optar por excluir a política mesmo que ela esteja atribuída a um dispositivo.

  Ao excluir uma política atribuída a um dispositivo, a atribuição da política será cancelada antes de ser excluída.

  Não é possível excluir a política **Firmware mais recente** predefinida; entretanto, é possível desabilitar a política clicando no ícone **Configurações globais** () e, em seguida, selecionando **Desabilitar política de firmware mais recente**. Quando essa opção é selecionada, a atribuição da política Firmware mais recente é cancelada dos dispositivos gerenciados e a política não é mais atualizada para incluir as versões mais recentes disponíveis do firmware no repositório.
- Exporte uma política selecionada para um sistema local selecionando as políticas e clicando no ícone **Exportar** (). Você poderá então importar as políticas para outra instância do XClarity Administrator clicando no ícone **Importar** ().

Depois de criar uma política de conformidade de firmware, você pode atribuir a política a um dispositivo específico (consulte Criando e atribuindo políticas de conformidade de firmware) e aplicar e ativar as atualizações para esse dispositivo (consulte Aplicando e ativando atualizações de firmware).

Identificando dispositivos que não são compatíveis

Se uma política de conformidade de firmware tiver sido atribuída a um dispositivo gerenciado, você poderá determinar se o firmware nesse dispositivo está em conformidade com a política.

Procedimento

Para determinar se o firmware em um dispositivo é compatível com a política de conformidade de firmware, clique em **Fornecimento → Atualizações de firmware: Aplicar/Ativar** na barra de menus do Lenovo XClarity Administrator para exibir a página Atualização de Firmware: Política de Conformidade e verifique a coluna **Versões instaladas** desse dispositivo.

A coluna **Versões Instaladas** contém um dos seguintes valores:

- **Versão do firmware**. A versão do firmware instalada no dispositivo é compatível com a política atribuída.
- **Compatível**. O firmware instalado no dispositivo está em conformidade com a política atribuída.
- **Não Conforme**. O firmware instalado no dispositivo não está em conformidade com a política atribuída.
- **Sem Conjunto de Políticas de Conformidade**. Uma política de conformidade de firmware não foi atribuída ao dispositivo.

É possível clicar no ícone **Atualizar** () para atualizar o conteúdo na coluna **Versão Instalada**.

Definir configurações globais de atualização de firmware

Configurações globais servem como as configurações padrão quando as atualizações de firmware forem aplicadas.

Sobre esta tarefa

Na página Configurações Globais, é possível definir as seguintes configurações:
- Suporte aprimorado para dispositivos de nível inferior
- Alertas de dispositivos que não são compatíveis com as políticas atribuídas
- Atribuição automática de uma política de conformidade de firmware a um dispositivo sem política atribuída
- Status de não conformidade para dispositivos com um componente de firmware que não tem destino associado na política de conformidade de firmware

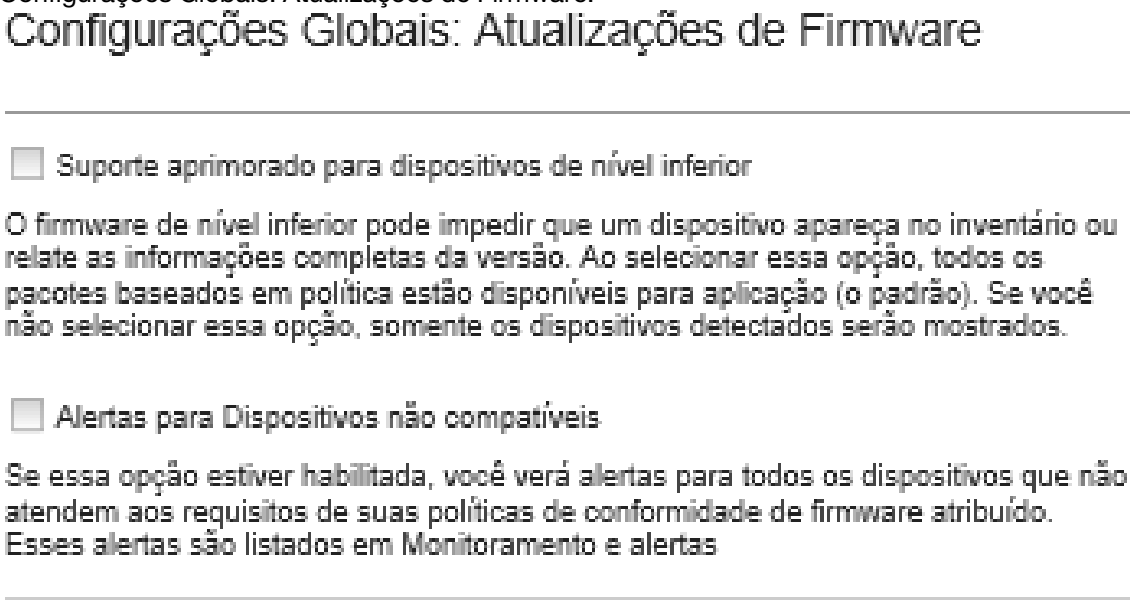
Procedimento

Para definir as configurações globais a serem usadas para todos os servidores, conclua as etapas a seguir.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Aplicar/Ativar**. A página Atualizações de Firmware: Aplicar/Ativar é exibida.

Etapa 2. Clique na guia **Atualização com Política** ou **Atualização sem Política**.

Etapa 3. Clique em **Todas as Ações → Configurações Globais** para exibir a caixa de diálogo Configurações Globais: Atualizações de Firmware.



Etapa 4. Selecione, opcionalmente, uma das opções a seguir.

- Selecione **Suporte Aprimorado para Dispositivos de Nível Inferior** para exibir o inventário e informações da versão completa para todos os dispositivos, mesmo que o firmware esteja em um nível inferior ou que o dispositivo esteja ausente do inventário.
- Selecione **Alertas de Dispositivos Mão Compatíveis** para exibir os alertas na página de Alertas para dispositivos que não atendem aos requisitos de suas políticas de conformidade de firmware atribuídas. Os alertas são ocultos na página Alertas por padrão. Para obter mais informações, consulte Visualizando alertas ativos.
- Selecione **Desabilitar atribuição de política automática** para desabilitar a atribuição automática de uma política de conformidade de firmware a um dispositivo sem política

atribuída. Se essa opção não estiver selecionada, as políticas de conformidade de firmware serão atribuídas a dispositivos sem uma política quando o XClarity Administrator for reiniciado ou quando você gerenciar um novo dispositivo.

- Selecione **Relatar não conformidade para firmware sem destino** para sinalizar dispositivos como não conformes quando um componente de firmware não tem destino associado na política de conformidade de firmware. Se essa opção não for selecionada, os dispositivos sem destinos serão marcados como conformes.

Etapa 5. Clique em **OK** para fechar a caixa de diálogo.

Aplicando e ativando atualizações de firmware

O Lenovo XClarity Administrator não aplica atualizações de firmware em dispositivos gerenciados automaticamente. Você pode optar por aplicar atualizações de firmware com ou sem políticas de conformidade.

Antes de iniciar

Ao usar políticas de conformidade, você pode planejar atualizações em vários dispositivos ao mesmo tempo. O XClarity Administrator atualiza dispositivos na sequência correta automaticamente. O CMM é atualizado primeiro, seguido por comutadores, servidores e, depois, dispositivos de armazenamento.

Somente as atualizações de firmware baixadas podem ser aplicadas.

Quando você executa uma atualização de firmware, o XClarity Administrator inicia um ou mais trabalhos para realizar a atualização.

Enquanto a atualização de firmware estiver em andamento, o dispositivo de destino ficará bloqueado. Não é possível iniciar outras tarefas de gerenciamento no dispositivo de destino até o processo de atualização ser concluído.

Após uma atualização de firmware ser aplicada a um dispositivo, uma ou mais reinicializações podem ser necessárias para ativar totalmente a atualização de firmware. Você pode optar por reiniciar o dispositivo imediatamente, atrasar a ativação ou priorizar a ativação. Se você optar por reiniciar imediatamente, o XClarity Administrator minimizará o número de reinicializações necessárias. Se optar por atrasar a ativação, as atualizações serão ativadas na próxima vez que o dispositivo for reiniciado. Se você escolher a ativação priorizada, as atualizações serão ativadas imediatamente no Baseboard Management Controller e todas as outras atualizações de firmware serão ativadas na próxima vez em que o dispositivo for reiniciado.

É possível atualizar o firmware selecionado em, no máximo, 50 dispositivos ao mesmo tempo. Se você optar por atualizar o firmware selecionado em mais de 50 dispositivos, os dispositivos restantes serão colocados na fila. Um dispositivo na fila é tirado da fila de "atualização de firmware selecionado" quando a ativação é concluída em um dispositivo atualizado ou um dispositivo atualizado é colocado no estado Modo de Manutenção Pendente (se uma reinicialização for necessária nesse dispositivo). Quando um dispositivo no estado Modo de Manutenção Pendente for reiniciado, o dispositivo será inicializado no Modo de Manutenção e continuará o processo de atualização, mesmo se o número máximo de atualizações de firmware já estiver em andamento.

É possível atualizar o firmware em pacote, no máximo, em 10 dispositivos ao mesmo tempo. Se você optar por atualizar o firmware em pacote em mais de 10 dispositivos, os dispositivos restantes serão colocados na fila. Um dispositivo colocado na fila é retirado da fila de "atualização de firmware em pacote" quando a ativação é concluída em um dispositivo no qual uma atualização de firmware em pacote foi realizada.

Atenção: Para o Red Hat® Enterprise Linux (RHEL) v7 e posterior, reiniciar o sistema operacional de um modo gráfico suspende o servidor por padrão. Antes de executar as ações **Reiniciar normalmente** ou

Reiniciar imediatamente no XClarity Administrator, você deverá configurar manualmente o sistema operacional para alterar o comportamento do botão liga/desliga para desligar. Para obter instruções, consulte Guia de administração e migração de dados Red Hat: Mudar o comportamento ao pressionar o botão de ligar no modo de destino gráfico .

Nota: O XClarity Administrator habilita automaticamente a interface LAN sobre USB.

Aplicando atualizações de firmware em pacote usando políticas de conformidade

Depois que o Lenovo XClarity Administrator identificar um dispositivo gerenciado como não compatível, você poderá aplicar manualmente atualizações de firmware a *todos* os componentes dos servidores ThinkSystem SR635 e SR655 selecionados que não estão em conformidade com a política de conformidade de firmware atribuída usando uma imagem em pacote que contenha os pacotes de atualização de firmware aplicáveis. A *imagem em pacote* é criada durante o processo de atualização coletando todos os pacotes de atualização de firmware da política de conformidade.

Antes de iniciar

- Leia as considerações sobre a atualização de firmware antes de tentar atualizar o firmware em seus dispositivos gerenciados (consulte Considerações de atualização de firmware).
- Inicialmente, os dispositivos sem suporte para atualizações são ocultos na exibição. Os dispositivos sem suporte não podem ser selecionados para atualizações.
- Por padrão, todos componentes detectados são listados como disponíveis para aplicação de atualizações; entretanto, o firmware de nível inferior pode impedir um componente de aparecer no inventário ou fazer o relatório de informações da versão completa. Para listar todos os pacotes baseados em política que estão disponíveis para você aplicar atualizações, clique em **Todas as Ações → Configurações Globais** e selecione **Suporte Aprimorado para Dispositivos de Nível Inferior**. Quando essa opção é selecionada, "Outro Software Disponível" é listado na coluna Versão Instalada para dispositivos não detectados. Para obter mais informações, consulte Definir configurações globais de atualização de firmware.

  Notas:

  – As configurações globais não podem ser alteradas quando há atualizações em andamento em dispositivos gerenciados.

  – Leva alguns minutos para gerar as opções adicionais. Depois de alguns momentos, talvez você precise clicar no ícone **Atualizar** ( ) para atualizar a tabela.
- Certifique-se de que nenhum trabalho esteja em execução atualmente no servidor de destino. Se houver trabalhos em execução, o trabalho de atualização será enfileirado até que todos os outros trabalhos sejam concluídos. Para ver uma lista de trabalhos ativos, clique em **Monitoramento → Trabalhos**.
- A aplicação de atualizações de firmware em pacote são compatíveis apenas com servidores ThinkSystem SR635 e SR655.
- A aplicação de atualizações de firmware empacotadas é suportada apenas para endereço IPv4. Endereços IPv6 não têm suporte.
- Certifique-se de que cada dispositivo de destino tenha sido inicializado no SO pelo menos uma vez para recuperar as informações completas do inventário.
- O firmware do Baseboard Management Controller v2.94 ou posterior é necessário para usar a função de atualização em pacote.
- Apenas atualizações de firmware de pacotes de repositórios ou atualizações de firmware individuais são usadas. UpdateXpress System Packs (UXSPs) não são compatíveis.

- Somente as atualizações de firmware baixadas são aplicadas. Atualize o catálogo de produtos e faça download das atualizações de firmware apropriadas (consulte Atualizando o catálogo de produtos e Baixando atualizações de firmware).

  Nota: Quando o XClarity Administrator é inicialmente instalado, o catálogo de produtos e o repositório estão vazios.
- A verificação de conformidade é suportada apenas para o Baseboard Management Controller e UEFI nos servidores ThinkSystem SR635 e SR655; no entanto, o XClarity Administrator tenta aplicar atualizações de firmware a todos os componentes de hardware disponíveis.
- As atualizações são aplicadas de acordo com a política de conformidade de firmware atribuída. Não é possível optar por atualizar um subconjunto de componentes.
- O XClarity Administrator v 3.2 ou posterior é necessário para aplicar atualizações de firmware para o Lenovo XClarity Provisioning Manager (LXPM), drivers do LXPM Windows drivers ou drivers do LXPM Linux para servidores ThinkSystem SR635 e SR655.
- O Baseboard Management Controller e as atualizações do UEFI serão ignoradas se a versão instalada atualmente for mais recente do que a política de conformidade atribuída.
- As políticas de conformidade de firmware devem ser criadas e atribuídas aos dispositivos em que você pretende aplicar atualizações de firmware. Para obter mais informações, consulte Criando e atribuindo políticas de conformidade de firmware.
- Os dispositivos selecionados são desligados antes de iniciar o processo de atualização. Certifique-se de que as cargas de trabalho em execução tenham sido interrompidas ou, se você estiver trabalhando em um ambiente virtualizado, tenham sido movidas para outro servidor.

Atenção: Os dispositivos selecionados são desligados antes de iniciar o processo de atualização. Certifique-se de que as cargas de trabalho em execução tenham sido interrompidas ou, se você estiver trabalhando em um ambiente virtualizado, tenham sido movidas para outro servidor. Se houver trabalhos em execução, o trabalho de atualização será enfileirado até que todos os outros trabalhos sejam concluídos. Para ver uma lista de trabalhos ativos, clique em **Monitoramento → Trabalhos**.

Sobre esta tarefa

O processo de atualização em pacote atualiza primeiro o Baseboard Management Controller e o UEFI fora da banda. Quando essas atualizações são concluídas, o processo cria uma imagem em pacote do firmware restante na política de conformidade com base no tipo de máquina. Em seguida, o processo monta a imagem no dispositivo selecionado e reinicia o dispositivo para inicializar a imagem. A imagem é executada automaticamente para executar as atualizações restantes.

É possível atualizar o firmware em pacote, no máximo, em 10 dispositivos ao mesmo tempo. Se você optar por atualizar o firmware em pacote em mais de 10 dispositivos, os dispositivos restantes serão colocados na fila. Um dispositivo colocado na fila é retirado da fila de "atualização de firmware em pacote" quando a ativação é concluída em um dispositivo no qual uma atualização de firmware em pacote foi realizada.

Se ocorrer um erro ao atualizar qualquer um componente no dispositivo, o processo de atualização de firmware não atualizará o firmware desse componente específico; entretanto, o processo de atualização de firmware continuará a atualizar os outros componentes no dispositivo e todos os outros dispositivos no trabalho de atualização de firmware atual.

Procedimento

Para aplicar atualizações de firmware na forma de uma imagem em pacote em dispositivos gerenciados, execute as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Aplicar/Ativar**. A página Atualizações de Firmware: Aplicar/Ativar é exibida.

Etapa 2. Clique na guia **Atualização com Política**.

Etapa 3. Selecione um ou mais dispositivos e componentes aos quais as atualizações de firmware devem ser aplicadas.

É possível classificar as colunas da tabela para facilitar a localização dos dispositivos específicos. Além disso, é possível filtrar a lista de dispositivos exibidos, selecionando uma opção no menu **Mostrar** para listar somente os dispositivos em um chassi, rack ou grupo específico, inserindo texto (como um nome ou endereço IP) no campo **Filtro** ou clicando nos ícones a seguir para listar somente os dispositivos com um status específico.

- Ícone **Ocultar dispositivos não conformes** ()
- Ícone **Ocultar status de dispositivos não conformes** ()
- Ícone **Ocultar dispositivos sem uma política de conformidade atribuída** ()
- Ícone **Ocultar dispositivos que não estão sendo monitorados** ()
- Ícone **Ocultar dispositivos com ativação pendente de firmware** ()
- Ícone **Ocultar dispositivos com erros de conformidade** ()
- Ícone **Ocultar dispositivos não compatíveis com atualizações** ()
- Ícone **Ocultar dispositivos submetidos a atualizações de firmware** ()
- Ícone **Ocultar dispositivos com firmware não simulado** ()

A coluna **Grupos** indica os grupos dos quais cada dispositivo é membro. Você pode passar o mouse sobre a coluna **Grupos** para obter uma lista completa de grupos por tipo de grupos

A coluna **Versão Instalada** indica a versão do firmware instalada, o status de conformidade ou o status do dispositivo.

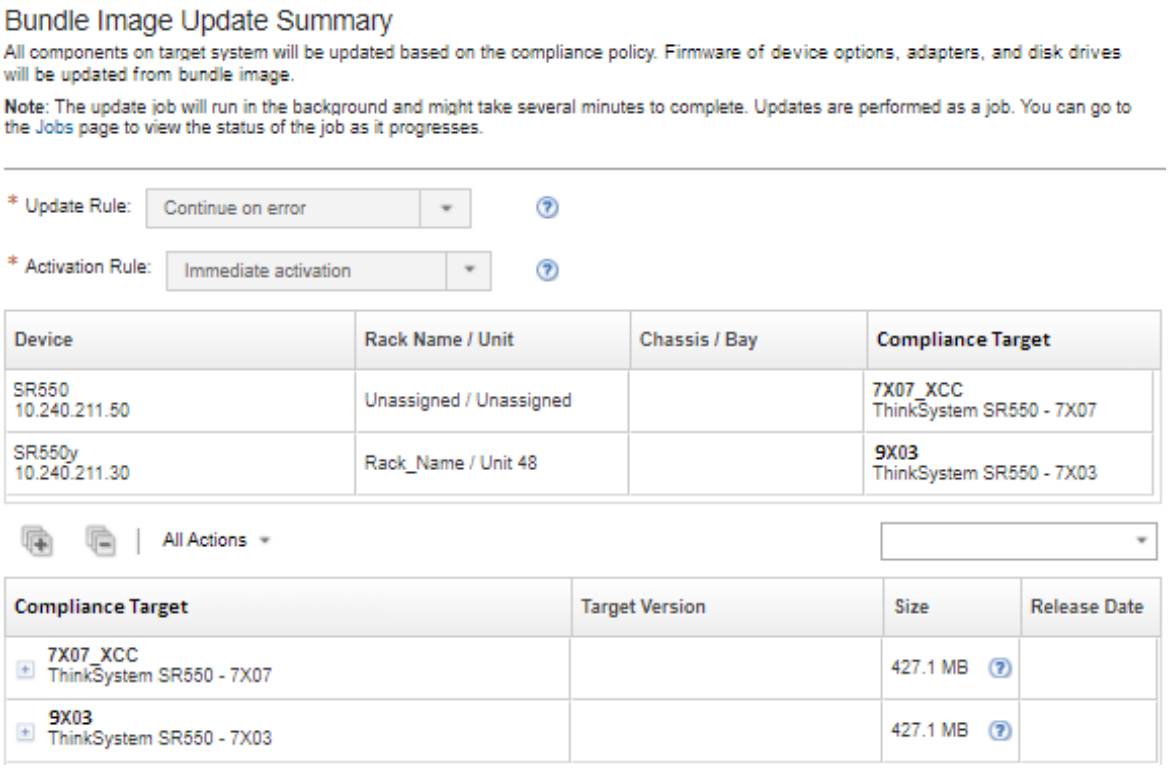
O status de conformidade pode ser um dos seguintes:

-  **Conforme**
-  **Erro de conformidade**
-  **Não Conforme**
-  **Sem Conjunto de Políticas de Conformidade**
-  **Não monitorado**

O status do dispositivo pode ser um dos seguintes:

-  **Sem Suporte para Atualizações**
-  **Atualização em Andamento**

Etapa 4. Clique no ícone **Executar atualização a partir da imagem do pacote** ( ). A caixa de diálogo Resumo de atualização da imagem do pacote é exibida. Essa caixa de diálogo lista os dispositivos selecionados e as atualizações de firmware que estão incluídas na imagem em pacote.



Etapa 5. Clique em **Realizar atualização da imagem do pacote** para atualizar imediatamente ou clique em **Programar** para programar a execução dessa atualização para mais tarde.

Depois de concluir

Ao aplicar uma atualização de firmware, se o servidor não entrar no modo de manutenção, tente aplicar a atualização novamente.

Se as atualizações não forem concluídas com êxito, consulte Problemas de repositório e atualização de firmware na documentação online do XClarity Administrator para conhecer as ações de solução de problemas e correção.

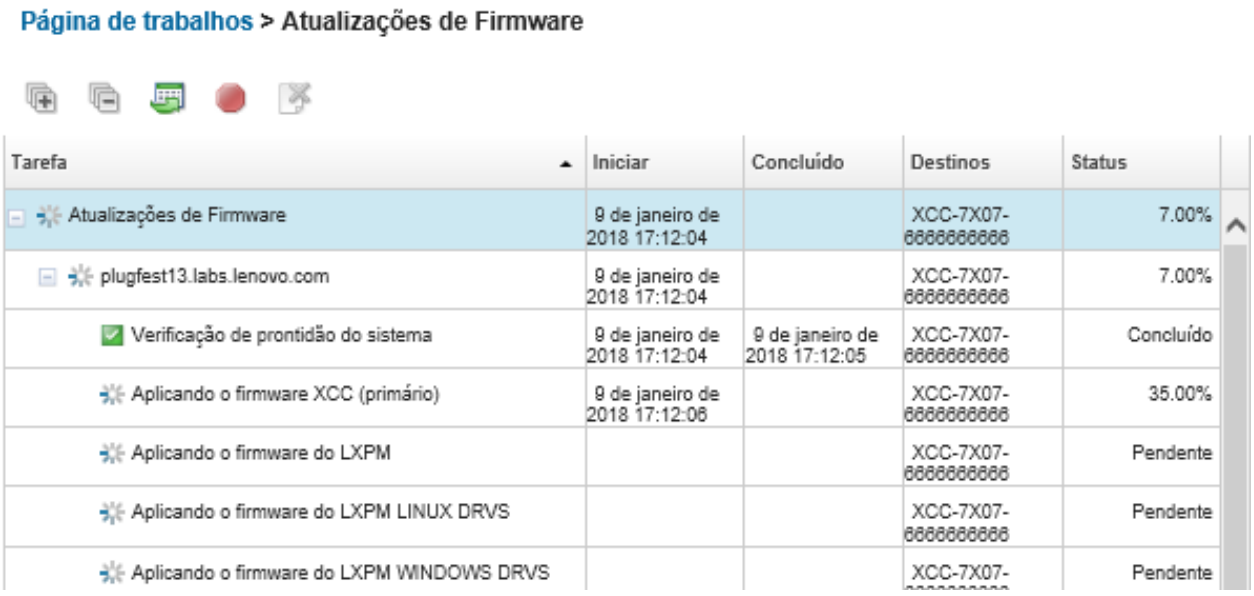
Na página Atualizações de Firmware: Aplicar/Ativar, é possível realizar as ações a seguir.

- Exportar informações de firmware e de conformidade para cada dispositivo gerenciado clicando em **Todas as Ações → Exportar Exibição como CSV**.

  Nota: O arquivo CSV contém apenas informações filtradas na exibição atual. Informações que são filtradas da exibição e informações em colunas ocultas não estão incluídas.
- Cancele uma atualização que está sendo aplicada a um dispositivo selecionando o dispositivo e clicando no ícone **Cancelar Atualização** ( ).

  Nota: Você pode cancelar atualizações de firmware que estão na fila para iniciar. Após o início do processo de atualização, a atualização de firmware pode ser cancelada somente quando o processo de atualização está executando uma tarefa diferente de aplicar a atualização, como alterar para modo de manutenção ou reiniciar o dispositivo.
- Exiba o status da atualização do firmware diretamente na página Aplicar/Ativar na coluna **Status**.
- Monitore o status do processo de atualização no log de trabalhos. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Trabalhos**.

  Para obter mais informações sobre o log de trabalhos, consulte Monitorando trabalhos.



Quando os trabalhos de atualização de firmware estiverem concluídos, você poderá verificar se os dispositivos estão em conformidade clicando em **Fornecimento → Atualizações de Firmware: Aplicar/Ativar** para voltar à página Atualizações de Firmware: Aplicar/Ativar e, em seguida, clica no ícone **Atualizar** ( ). A versão atual do firmware que está ativa em cada dispositivo é listada na coluna **Versão Instalada**.

Aplicando atualizações de firmware selecionadas usando políticas de conformidade

Depois que o Lenovo XClarity Administrator identifica um dispositivo como não conforme, é possível aplicar e ativar manualmente as atualizações de firmware nesses dispositivos gerenciados. Você pode optar por aplicar e ativar todas as atualizações de firmware que se aplicam à política de conformidade de firmware ou somente atualizações específicas em uma política. Somente as atualizações de firmware baixadas são aplicadas.

Saiba mais:

- XClarity Administrator: aumentando a eficiência ao atualizar o firmware
- Melhores práticas nas atualizações de firmware e drivers do Lenovo ThinkSystem
- XClarity Administrator: bare metal para cluster
- XClarity Administrator: atualizações de firmware
- XClarity Administrator: fornecimento de atualizações de segurança de firmware

Antes de iniciar

- Leia as considerações sobre a atualização de firmware antes de tentar atualizar o firmware em seus dispositivos gerenciados (consulte Considerações de atualização de firmware).
- Inicialmente, os dispositivos sem suporte para atualizações são ocultos na exibição. Os dispositivos sem suporte não podem ser selecionados para atualizações.
- Por padrão, todos componentes detectados são listados como disponíveis para aplicação de atualizações; entretanto, o firmware de nível inferior pode impedir um componente de aparecer no inventário ou fazer o relatório de informações da versão completa. Para listar todos os pacotes baseados em política que estão disponíveis para você aplicar atualizações, clique em **Todas as Ações → Configurações Globais** e selecione **Suporte Aprimorado para Dispositivos de Nível Inferior**. Quando essa opção é selecionada, "Outro Software Disponível" é listado na coluna Versão Instalada para dispositivos não detectados. Para obter mais informações, consulte Definir configurações globais de atualização de firmware.

  Notas:

  – As configurações globais não podem ser alteradas quando há atualizações em andamento em dispositivos gerenciados.

  – Leva alguns minutos para gerar as opções adicionais. Depois de alguns momentos, talvez você precise clicar no ícone **Atualizar** ( ) para atualizar a tabela.
- Certifique-se de que nenhum trabalho esteja em execução atualmente no servidor de destino. Se houver trabalhos em execução, o trabalho de atualização será enfileirado até que todos os outros trabalhos sejam concluídos. Para ver uma lista de trabalhos ativos, clique em **Monitoramento → Trabalhos**.
- Verifique se o repositório das atualizações de firmware contém os pacotes de firmware que você pretende implantar. Se não contiver, atualize o catálogo de produtos e baixe as atualizações de firmware apropriadas (consulte Atualizando o catálogo de produtos e Baixando atualizações de firmware).

  Nota: Quando o XClarity Administrator é inicialmente instalado, o catálogo de produtos e o repositório estão vazios.

  Se você pretende instalar firmware de pré-requisito, certifique-se de que o firmware de pré-requisito também seja baixado no repositório.

  Em alguns casos, várias versões podem ser necessárias para atualizar o firmware, e todas as versões precisam ser baixadas para o repositório. Por exemplo, para atualizar o comutador escalável IBM FC5022 SAN de v7.4.0a para v8.2.0a, você deve primeiro instalar a v8.0.1-pha, em seguida, v8.1.1 e, em seguida, v8.2.0a. Todas as três versões devem estar no repositório para atualizar o comutador para v8.2.0a.

- Normalmente, os dispositivos devem ser reiniciados para ativar a atualização de firmware. Se você optar por reiniciar o dispositivo durante o processo de atualização (*ativação imediata*), certifique-se de que as cargas de trabalho em execução sejam interrompidas ou, se estiverem funcionando em um ambiente virtualizado, sejam movidas para um servidor diferente.
- Para servidores ThinkSystem SR635 e SR655, você pode usar esta função de atualização tradicional para aplicar apenas atualizações do Baseboard Management Controller e do firmware UEFI. É necessário ter a versão de firmware do Management Controller AMBT10M ou posterior e a versão de firmware UEFI CFE114L ou posterior. Para atualizar todos os componentes (incluindo o Management Controller, UEFI, unidades de disco e opções de E/S), use a função de atualização do pacote (consulte Aplicando atualizações de firmware em pacote usando políticas de conformidade).

Sobre esta tarefa

- É possível atualizar o firmware selecionado em, no máximo, 50 dispositivos ao mesmo tempo. Se você optar por atualizar o firmware selecionado em mais de 50 dispositivos, os dispositivos restantes serão colocados na fila. Um dispositivo na fila é tirado da fila de "atualização de firmware selecionado" quando a ativação é concluída em um dispositivo atualizado ou um dispositivo atualizado é colocado no estado Modo de Manutenção Pendente (se uma reinicialização for necessária nesse dispositivo). Quando um dispositivo no estado Modo de Manutenção Pendente for reiniciado, o dispositivo será inicializado no Modo de Manutenção e continuará o processo de atualização, mesmo se o número máximo de atualizações de firmware já estiver em andamento.
- Você pode aplicar e ativar um firmware que seja mais recente do que o atualmente instalado.
- É possível optar por aplicar todas as atualizações para um dispositivo específico. Entretanto, também é possível optar por expandir um dispositivo para especificar atualizações para componentes específicos, como Baseboard Management Controller ou UEFI.
- Se você optar por instalar um pacote de atualização de firmware que contenha atualizações para vários componentes, todos os componentes aos quais o pacote de atualização se aplica serão atualizados.

Procedimento

Para aplicar e ativar atualizações em dispositivos gerenciados, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Aplicar/Ativar**. A página Atualizações de Firmware: Aplicar/Ativar é exibida.

Etapa 2. Clique na guia **Atualização com Política**.

Etapa 3. Selecione um ou mais dispositivos aos quais as atualizações de firmware devem ser aplicadas.

É possível classificar as colunas da tabela para facilitar a localização dos servidores específicos. Além disso, é possível filtrar a lista de dispositivos exibidos, selecionando uma opção no menu **Mostrar** para listar somente os dispositivos em um chassi, rack ou grupo específico, inserindo texto (como um nome ou endereço IP) no campo **Filtro** ou clicando nos ícones a seguir para listar somente os dispositivos com um status específico.

- Ícone **Ocultar dispositivos não conformes** ()
- Ícone **Ocultar status de dispositivos não conformes** ()
- Ícone **Ocultar dispositivos sem uma política de conformidade atribuída** ()
- Ícone **Ocultar dispositivos que não estão sendo monitorados** ()
- Ícone **Ocultar dispositivos com ativação pendente de firmware** ()
- Ícone **Ocultar dispositivos com erros de conformidade** ()

- Ícone **Ocultar dispositivos não compatíveis com atualizações** ( )
- Ícone **Ocultar dispositivos submetidos a atualizações de firmware** ( )
- Ícone **Ocultar dispositivos com firmware não simulado** ( )

A coluna **Grupos** indica os grupos dos quais cada dispositivo é membro. Você pode passar o mouse sobre a coluna **Grupos** para obter uma lista completa de grupos por tipo de grupos

A coluna **Versão Instalada** indica a versão do firmware instalada, o status de conformidade ou o status do dispositivo.

O status de conformidade pode ser um dos seguintes:

- **Conforme**
- **Erro de conformidade**
- **Não Conforme**
- **Sem Conjunto de Políticas de Conformidade**
- **Não monitorado**

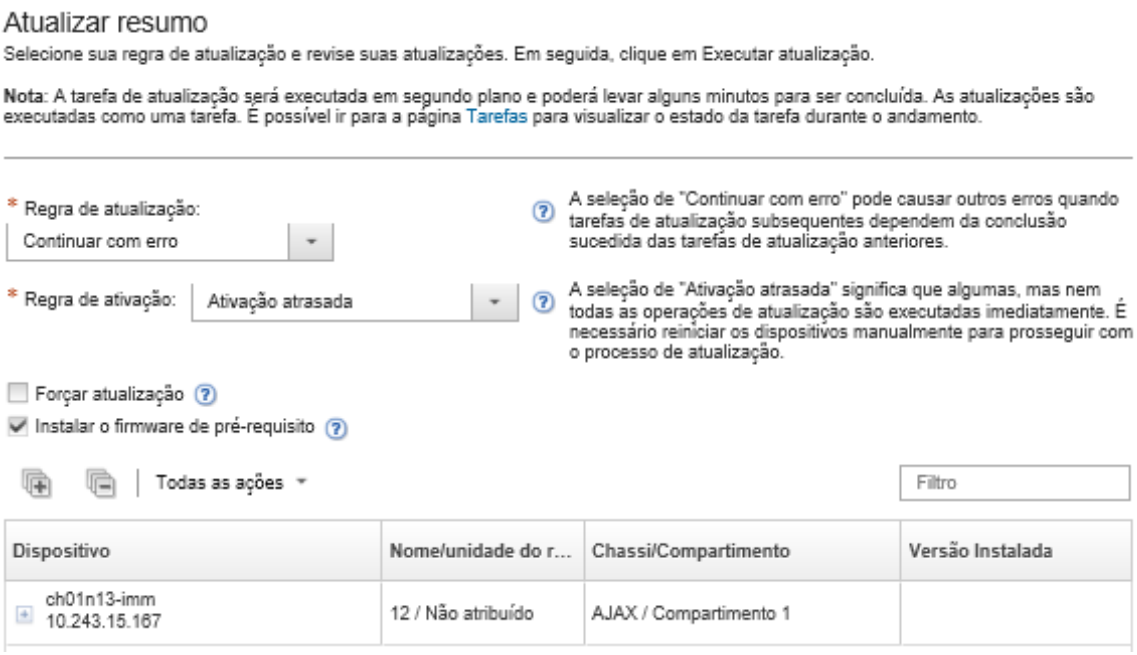
O status do dispositivo pode ser um dos seguintes:

- **Sem Suporte para Atualizações**
- **Atualização em Andamento**

Notas: Se a versão do firmware instalada for ativação pendente, "(Ativação pendente)" será anexada à versão do firmware instalada ou status de conformidade de cada dispositivo aplicável, por exemplo "2.20 / A9E12EUS (Ativação pendente)." Para ver o status de ativação pendente, a versão do firmware a seguir deve estar instalada no Baseboard Management Controller no servidor.

- **IMM2**: TCOO46F, TCOO46E ou posterior (dependendo da plataforma)
- **XCC**: CDI328M, PSI316N, TEI334I ou posterior (dependendo da plataforma)

Etapa 4. Clique no ícone **Realizar Atualizações** ( ). A caixa de diálogo Resumo de Atualização é exibida.



Etapa 5. Selecione uma das regras de atualização a seguir

- **Interromper todas as atualizações em caso de erro**. Se ocorrer um erro ao atualizar qualquer um dos componentes (como um adaptador ou controlador de gerenciamento) no dispositivo de destino, o processo de atualização de firmware será interrompido para todos os dispositivos selecionados no trabalho de atualização de firmware atual. Nesse caso, nenhuma das atualizações no pacote de atualização do dispositivo é aplicada. O firmware que estiver instalado em todos os sistemas selecionados permanecerá em vigor.
- **Continuar em caso de erro**. Se ocorrer um erro ao atualizar qualquer um dos dispositivos no dispositivo, o processo de atualização de firmware não atualizará o firmware desse dispositivo específico; entretanto, o processo de atualização de firmware continuará a atualizar os outros dispositivos no dispositivo e todos os outros dispositivos no trabalho de atualização de firmware atual.
- **Continuar para o próximo sistema em caso de erro**. Se ocorrer um erro ao atualizar qualquer um dos dispositivos no dispositivo, o processo de atualização de firmware interromperá todas as tentativas de atualizar o firmware desse dispositivo específico; portanto, o firmware atual que estiver instalado nesse dispositivo permanecerá em vigor. O processo de atualização continuará a atualizar todos os outros dispositivos no trabalho de atualização de firmware atual.

Etapa 6. Selecione uma das regras de ativação a seguir:

- **Ativação imediata**. Durante o processo de atualização, o dispositivo poderá ser reiniciado automaticamente várias vezes até a conclusão de todo o processo de atualização. Certifique-se de fechar todos os aplicativos no dispositivo antes de continuar.
- **Ativação atrasada**. Algumas, mas nem todas as operações de atualização, são executadas. Os dispositivos devem ser reiniciados para continuar o processo de atualização. Em seguida, as reinicializações adicionais são executadas até o término do processo de atualização.

  Um evento é gerado quando o status muda para o **Modo de Manutenção de Firmware Pendente** para notificar você quando o servidor precisa ser reiniciado.

  Se um dispositivo reiniciar por algum motivo, o processo de atualização atrasado será concluído.

Essa regra de ativação tem suporte apenas em servidores e comutadores de rack. Os CMMs e comutadores Flex são ativados de imediato, independentemente dessa configuração.

Um evento é gerado quando o status muda para o **Modo de Manutenção de Firmware Pendente** para notificar você quando o servidor precisa ser reiniciado.

O processo de atualização atrasada é concluído quando o dispositivo é reiniciado por qualquer motivo (inclusive uma reinicialização manual). Não há limite de tempo em que o servidor deve ser reiniciado.

O XClarity Administrator pode aplicar atualizações com ativação atrasada para até 50 dispositivos ao mesmo tempo. Se você tentar aplicar atualizações com ativação atrasada para mais de 50 dispositivos, os dispositivos restantes serão colocados em fila. Um dispositivo sai da fila quando um dispositivo que está sendo atualizado é colocado no estado **Modo de Manutenção de Firmware Pendente.**

Importante:

- Se o XClarity Administrator for reiniciado durante o trabalho de atualização, o trabalho de atualização será interrompido com erro.
- Se um servidor no estado **Modo de Manutenção de Firmware Pendente** for reiniciado enquanto o XClarity Administrator estiver desativado ou inacessível, o servidor será inicializado na BMU, mas como o XClarity Administrator não consegue se conectar à BMU e o tempo se esgota após 60 segundos, o status de energia do sistema será restaurado pelo Baseboard Management Controller (será desativado se ele estiver desligado, será reiniciado se estiver ligado).

- **Ativação priorizada**. As atualizações de firmware no Baseboard Management Controller são ativadas imediatamente. Todas as outras atualizações de firmware são ativadas na próxima vez em que o dispositivo é reiniciado. Em seguida, as reinicializações adicionais são executadas até o término do processo de atualização. Essa regra tem suporte apenas em servidores.

  Um evento é gerado quando o status muda para o Modo de Manutenção de Firmware Pendente para notificá-lo quando o servidor precisa ser reiniciado.

Nota: Quando ativada, a opção de inicialização Wake-on-LAN pode interferir nas operações do XClarity Administrator que desligam que o servidor, incluindo atualizações de firmware se houver um cliente Wake-on-LAN na rede que emite comandos "Wake on Magic Packet".

Etapa 7. **Opcional:** selecione **Forçar atualização** para atualizar o firmware em componentes selecionados mesmo se o nível de firmware estiver atualizado ou aplique uma atualização de firmware que seja anterior à atualmente instalada nos componentes selecionados.

Nota: É possível aplicar uma versão anterior do firmware em opções de dispositivo, adaptadores e unidades compatíveis com nivelamento inferior. Consulte a documentação do hardware para determinar se o nivelamento inferior é compatível.

Etapa 8. **Opcional:** desmarque **Instalar firmware pré-requisito** se você não quiser instalar um firmware pré-requisito. O firmware pré-requisito é instalado por padrão.

Nota: Ao usar a **Ativação atrasada** ou a **Ativação priorizada** atualizações de firmware de pré-requisito, talvez seja necessário reiniciar o servidor para ativar o firmware de pré-requisito. Após a reinicialização inicial, as atualizações de firmware restantes são instaladas usando **Ativação imediata**.

Etapa 9. **Opcional:** se você selecionou **Ativação Imediata**, selecione **Teste de Memória** para executar um teste de memória após a atualização de firmware ser concluída se o servidor for reinicializado durante a atualização.

Essa opção é suportada para servidores ThinkSystem v1 e v2 (excluindo servidores ThinkSystem SR635, SR645, SR655, SR665).

Etapa 10. Clique em **Realizar Atualização** para atualizar imediatamente ou clique em **Programação** para programar a execução dessa atualização para mais tarde.

Se necessário, você pode executar ações de energia nos dispositivos gerenciados. As ações de energia são úteis quando a opção **Ativação Atrasada** está selecionada e você quer que as atualizações continuem quando o dispositivo estiver em espera no estado "Manutenção Pendente". Para executar uma ação de energia em um dispositivo gerenciado desta página, clique em **Todas as Ações → Ações de Energia** e, em seguida, clique em uma das ações de energia a seguir.

- **Ligar**
- **Encerrar SO e desligar**
- **Desligar**
- **Encerrar SO e reiniciar**
- **Reiniciar**

Depois de concluir

Ao aplicar uma atualização de firmware, se o servidor não entrar no modo de manutenção, tente aplicar a atualização novamente.

Se as atualizações não forem concluídas com êxito, consulte Problemas de repositório e atualização de firmware na documentação online do XClarity Administrator para conhecer as ações de solução de problemas e correção.

Na página Atualizações de Firmware: Aplicar/Ativar, é possível realizar as seguintes:

- Exportar informações de firmware e de conformidade para cada dispositivo gerenciado clicando em **Todas as Ações → Exportar Exibição como CSV**.

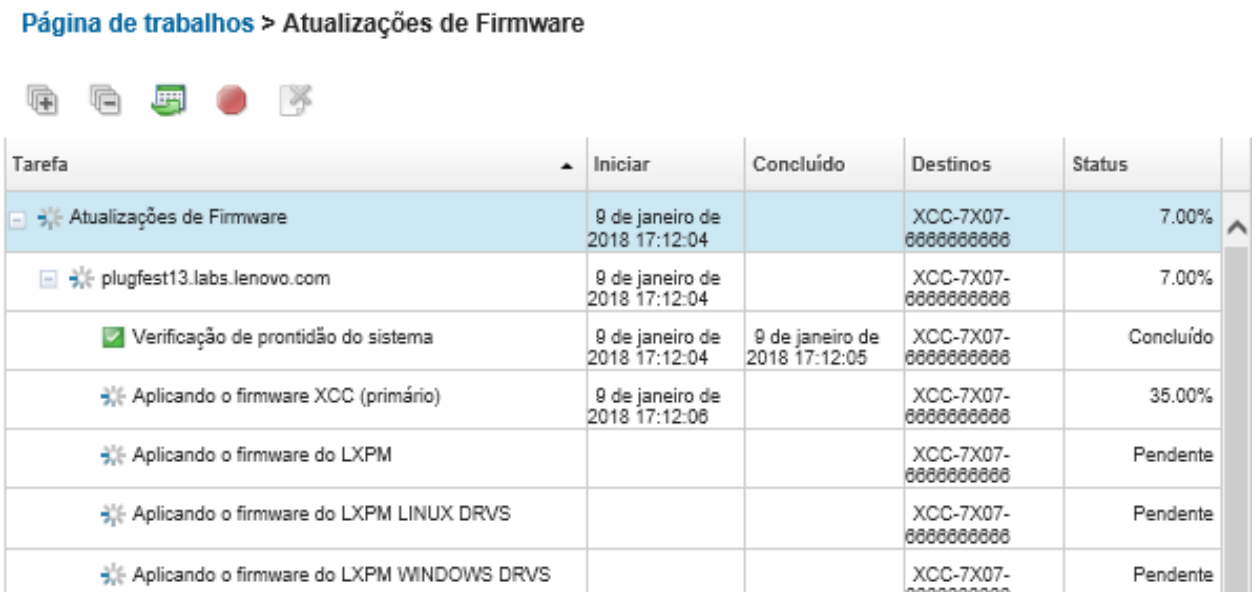
  Nota: O arquivo CSV contém apenas informações filtradas na exibição atual. Informações que são filtradas da exibição e informações em colunas ocultas não estão incluídas.

- Cancele uma atualização que está sendo aplicada a um dispositivo selecionando o dispositivo e clicando no ícone **Cancelar Atualização** ().

  Nota: Você pode cancelar atualizações de firmware que estão na fila para iniciar. Após o início do processo de atualização, a atualização de firmware pode ser cancelada somente quando o processo de atualização está executando uma tarefa diferente de aplicar a atualização, como alterar para modo de manutenção ou reiniciar o dispositivo.

- Exiba o status da atualização do firmware diretamente na página Aplicar/Ativar na coluna **Status**.
- Monitore o status do processo de atualização no log de trabalhos. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Trabalhos**.

  Para obter mais informações sobre o log de trabalhos, consulte Monitorando trabalhos.



Quando os trabalhos de atualização de firmware estiverem concluídos, você poderá verificar se os dispositivos estão em conformidade clicando em **Fornecimento → Atualizações de Firmware: Aplicar/Ativar** para voltar à página Atualizações de Firmware: Aplicar/Ativar e, em seguida, clica no ícone **Atualizar** ( ). A versão atual do firmware que está ativa em cada dispositivo é listada na coluna **Versão Instalada**.

Aplicando atualizações de firmware selecionadas sem usar políticas de conformidade

Você pode rapidamente aplicar e ativar um firmware mais recente do que o atualmente instalado em um único dispositivo gerenciado ou em um grupo de dispositivos sem usar políticas de conformidade.

Saiba mais:

- XClarity Administrator: aumentando a eficiência ao atualizar o firmware
- Melhores práticas nas atualizações de firmware e drivers do Lenovo ThinkSystem
- XClarity Administrator: bare metal para cluster
- XClarity Administrator: atualizações de firmware
- XClarity Administrator: fornecimento de atualizações de segurança de firmware

Antes de iniciar

- Leia as considerações sobre a atualização de firmware antes de tentar atualizar o firmware em seus dispositivos gerenciados (consulte Considerações de atualização de firmware).
- Inicialmente, os dispositivos sem suporte para atualizações são ocultos na exibição. Os dispositivos sem suporte não podem ser selecionados para atualizações.
- Por padrão, todos componentes detectados são listados como disponíveis para aplicação de atualizações; entretanto, o firmware de nível inferior pode impedir um componente de aparecer no inventário ou fazer o relatório de informações da versão completa. Para listar todos os pacotes baseados em política que estão disponíveis para você aplicar atualizações, clique em **Todas as Ações → Configurações Globais** e selecione **Suporte Aprimorado para Dispositivos de Nível Inferior**. Quando essa opção é selecionada, "Outro Software Disponível" é listado na coluna Versão Instalada para dispositivos não detectados. Para obter mais informações, consulte Definir configurações globais de atualização de firmware.

Notas:

- As configurações globais não podem ser alteradas quando há atualizações em andamento em dispositivos gerenciados.
- Leva alguns minutos para gerar as opções adicionais. Depois de alguns momentos, talvez você precise clicar no ícone **Atualizar** () para atualizar a tabela.

- Certifique-se de que nenhum trabalho esteja em execução atualmente no servidor de destino. Se houver trabalhos em execução, o trabalho de atualização será enfileirado até que todos os outros trabalhos sejam concluídos. Para ver uma lista de trabalhos ativos, clique em **Monitoramento → Trabalhos**.
- Verifique se o repositório das atualizações de firmware contém os pacotes de firmware que você pretende implantar. Se não contiver, atualize o catálogo de produtos e baixe as atualizações de firmware apropriadas (consulte Atualizando o catálogo de produtos e Baixando atualizações de firmware).

  Nota: Quando o XClarity Administrator é inicialmente instalado, o catálogo de produtos e o repositório estão vazios.

  Se você pretende instalar firmware de pré-requisito, certifique-se de que o firmware de pré-requisito também seja baixado no repositório.

  Em alguns casos, várias versões podem ser necessárias para atualizar o firmware, e todas as versões precisam ser baixadas para o repositório. Por exemplo, para atualizar o comutador escalável IBM FC5022 SAN de v7.4.0a para v8.2.0a, você deve primeiro instalar a v8.0.1-pha, em seguida, v8.1.1 e, em seguida, v8.2.0a. Todas as três versões devem estar no repositório para atualizar o comutador para v8.2.0a.
- Normalmente, os dispositivos devem ser reiniciados para ativar a atualização de firmware. Se você optar por reiniciar o dispositivo durante o processo de atualização (*ativação imediata*), certifique-se de que as cargas de trabalho em execução sejam interrompidas ou, se estiverem funcionando em um ambiente virtualizado, sejam movidas para um servidor diferente.

Sobre esta tarefa

- É possível atualizar o firmware selecionado em, no máximo, 50 dispositivos ao mesmo tempo. Se você optar por atualizar o firmware selecionado em mais de 50 dispositivos, os dispositivos restantes serão colocados na fila. Um dispositivo na fila é tirado da fila de "atualização de firmware selecionado" quando a ativação é concluída em um dispositivo atualizado ou um dispositivo atualizado é colocado no estado Modo de Manutenção Pendente (se uma reinicialização for necessária nesse dispositivo). Quando um dispositivo no estado Modo de Manutenção Pendente for reiniciado, o dispositivo será inicializado no Modo de Manutenção e continuará o processo de atualização, mesmo se o número máximo de atualizações de firmware já estiver em andamento.
- Você pode aplicar e ativar um firmware que seja mais recente do que o atualmente instalado.
- É possível optar por aplicar todas as atualizações para um dispositivo específico. Entretanto, também é possível optar por expandir um dispositivo para especificar atualizações para componentes específicos, como Baseboard Management Controller ou UEFI.
- Se você optar por instalar um pacote de atualização de firmware que contenha atualizações para vários componentes, todos os componentes aos quais o pacote de atualização se aplica serão atualizados.

Procedimento

Para aplicar e ativar atualizações em um dispositivo gerenciado, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Atualizações de Firmware: Aplicar/Ativar**. A página Atualizações de Firmware: Aplicar/Ativar é exibida.

Etapa 2. Clique na guia **Atualização sem Política**.

Etapa 3. Selecione o nível de firmware na coluna **Versões mais recentes baixadas** para cada dispositivo que você deseja atualizar.

Etapa 4. Selecione um ou mais dispositivos que você queira atualizar.

É possível classificar as colunas da tabela para facilitar a localização dos servidores específicos. Além disso, é possível filtrar a lista de dispositivos exibidos, selecionando uma opção no menu **Mostrar** para listar somente os dispositivos em um chassi, rack ou grupo específico, inserindo texto (como um nome ou endereço IP) no campo **Filtro** ou clicando nos ícones a seguir para listar somente os dispositivos com um status específico.

- Ícone **Ocultar componentes com versões mais recentes** ()
- Ícone **Ocultar componentes sem versões mais recentes** ()
- Ícone **Ocultar dispositivos não compatíveis com atualizações** ()
- Ícone **Ocultar dispositivos submetidos a atualizações de firmware** ()
- Ícone **Ocultar dispositivos com firmware não simulado** ()

A coluna **Grupos** indica os grupos dos quais cada dispositivo é membro. Você pode passar o mouse sobre a coluna **Grupos** para obter uma lista completa de grupos por tipo de grupos

A coluna **Versão Instalada** indica a versão do firmware instalada, o status de conformidade ou o status do dispositivo.

O status de conformidade pode ser um dos seguintes:

-  **Conforme**
-  **Erro de conformidade**
-  **Não Conforme**
-  **Sem Conjunto de Políticas de Conformidade**
-  **Não monitorado**

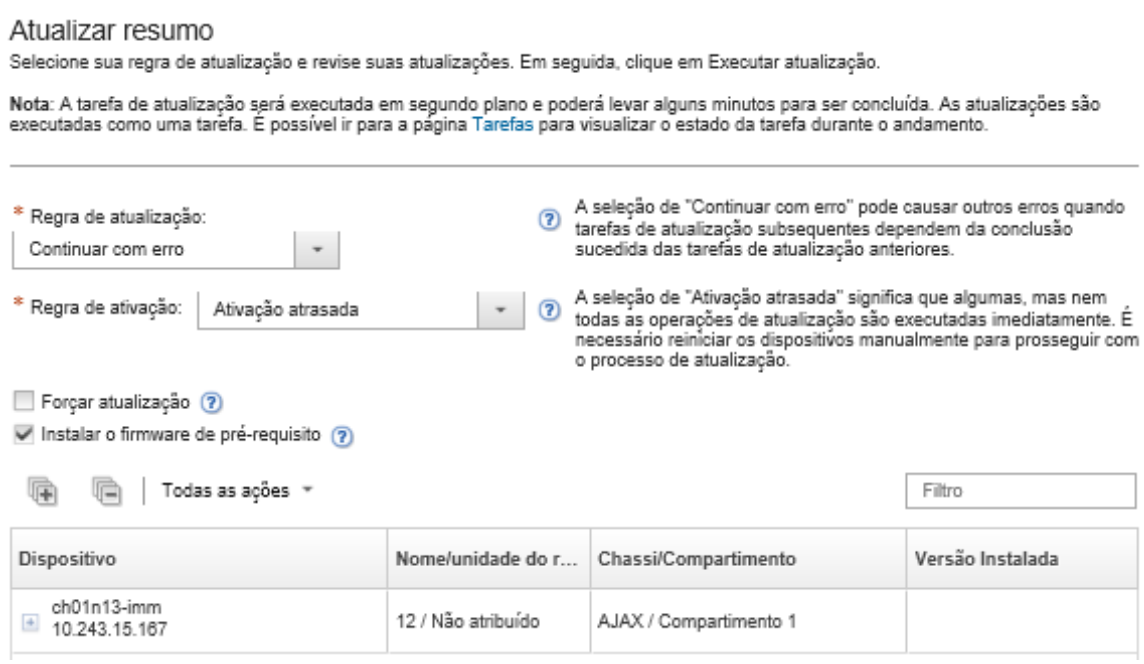
O status do dispositivo pode ser um dos seguintes:

-  **Sem Suporte para Atualizações**
-  **Atualização em Andamento**

Notas: Se a versão do firmware instalada for ativação pendente, "(Ativação pendente)" será anexada à versão do firmware instalada ou status de conformidade de cada dispositivo aplicável, por exemplo "2.20 / A9E12EUS (Ativação pendente)." Para ver o status de ativação pendente, a versão do firmware a seguir deve estar instalada no Baseboard Management Controller no servidor.

- **IMM2**: TCOO46F, TCOO46E ou posterior (dependendo da plataforma)
- **XCC**: CDI328M, PSI316N, TEI334I ou posterior (dependendo da plataforma)

Etapa 5. Clique no ícone **Realizar Atualizações** ( ). A caixa de diálogo Resumo de Atualização é exibida.



Etapa 6. Selecione uma das regras de atualização a seguir

- **Interromper todas as atualizações em caso de erro**. Se ocorrer um erro ao atualizar qualquer um dos componentes (como um adaptador ou controlador de gerenciamento) no dispositivo de destino, o processo de atualização de firmware será interrompido para todos os dispositivos selecionados no trabalho de atualização de firmware atual. Nesse caso, nenhuma das atualizações no pacote de atualização do dispositivo é aplicada. O firmware que estiver instalado em todos os sistemas selecionados permanecerá em vigor.
- **Continuar em caso de erro**. Se ocorrer um erro ao atualizar qualquer um dos dispositivos no dispositivo, o processo de atualização de firmware não atualizará o firmware desse dispositivo específico; entretanto, o processo de atualização de firmware continuará a atualizar os outros

dispositivos no dispositivo e todos os outros dispositivos no trabalho de atualização de firmware atual.

- **Continuar para o próximo sistema em caso de erro**. Se ocorrer um erro ao atualizar qualquer um dos dispositivos no dispositivo, o processo de atualização de firmware interromperá todas as tentativas de atualizar o firmware desse dispositivo específico; portanto, o firmware atual que estiver instalado nesse dispositivo permanecerá em vigor. O processo de atualização continuará a atualizar todos os outros dispositivos no trabalho de atualização de firmware atual.

Nota: Quando ativada, a opção de inicialização Wake-on-LAN pode interferir nas operações do XClarity Administrator que desligam que o servidor, incluindo atualizações de firmware se houver um cliente Wake-on-LAN na rede que emite comandos "Wake on Magic Packet".

Etapa 7. Selecione uma das regras de ativação a seguir:

- **Ativação imediata**. Durante o processo de atualização, o dispositivo poderá ser reiniciado automaticamente várias vezes até a conclusão de todo o processo de atualização. Certifique-se de fechar todos os aplicativos no dispositivo antes de continuar.
- **Ativação atrasada**. Algumas, mas nem todas as operações de atualização, são executadas. Os dispositivos devem ser reiniciados para continuar o processo de atualização. Em seguida, as reinicializações adicionais são executadas até o término do processo de atualização.

  Um evento é gerado quando o status muda para o **Modo de Manutenção de Firmware Pendente** para notificar você quando o servidor precisa ser reiniciado.

  Se um dispositivo reiniciar por algum motivo, o processo de atualização atrasado será concluído.

  Essa regra de ativação tem suporte apenas em servidores e comutadores de rack. Os CMMs e comutadores Flex são ativados de imediato, independentemente dessa configuração.

  Um evento é gerado quando o status muda para o **Modo de Manutenção de Firmware Pendente** para notificar você quando o servidor precisa ser reiniciado.

  O processo de atualização atrasada é concluído quando o dispositivo é reiniciado por qualquer motivo (inclusive uma reinicialização manual). Não há limite de tempo em que o servidor deve ser reiniciado.

  O XClarity Administrator pode aplicar atualizações com ativação atrasada para até 50 dispositivos ao mesmo tempo. Se você tentar aplicar atualizações com ativação atrasada para mais de 50 dispositivos, os dispositivos restantes serão colocados em fila. Um dispositivo sai da fila quando um dispositivo que está sendo atualizado é colocado no estado **Modo de Manutenção de Firmware Pendente.**

  Importante:

  – Se o XClarity Administrator for reiniciado durante o trabalho de atualização, o trabalho de atualização será interrompido com erro.

  – Se um servidor no estado **Modo de Manutenção de Firmware Pendente** for reiniciado enquanto o XClarity Administrator estiver desativado ou inacessível, o servidor será inicializado na BMU, mas como o XClarity Administrator não consegue se conectar à BMU e o tempo se esgota após 60 segundos, o status de energia do sistema será restaurado pelo Baseboard Management Controller (será desativado se ele estiver desligado, será reiniciado se estiver ligado).
- **Ativação priorizada**. As atualizações de firmware no Baseboard Management Controller são ativadas imediatamente. Todas as outras atualizações de firmware são ativadas na próxima vez em que o dispositivo é reiniciado. Em seguida, as reinicializações adicionais são executadas até o término do processo de atualização. Essa regra tem suporte apenas em servidores.

Um evento é gerado quando o status muda para o Modo de Manutenção de Firmware Pendente para notificá-lo quando o servidor precisa ser reiniciado.

Nota: Quando ativada, a opção de inicialização Wake-on-LAN pode interferir nas operações do XClarity Administrator que desligam que o servidor, incluindo atualizações de firmware se houver um cliente Wake-on-LAN na rede que emite comandos "Wake on Magic Packet".

Etapa 8. **Opcional:** selecione **Forçar atualização** para atualizar o firmware em componentes selecionados mesmo se o nível de firmware estiver atualizado ou aplique uma atualização de firmware que seja anterior à atualmente instalada nos componentes selecionados.

Nota: É possível aplicar uma versão anterior do firmware em opções de dispositivo, adaptadores e unidades compatíveis com nivelamento inferior. Consulte a documentação do hardware para determinar se o nivelamento inferior é compatível.

Etapa 9. **Opcional:** desmarque **Instalar firmware pré-requisito** se você não quiser instalar um firmware pré-requisito. O firmware pré-requisito é instalado por padrão.

Nota: Ao usar a **Ativação atrasada** ou a **Ativação priorizada** atualizações de firmware de pré-requisito, talvez seja necessário reiniciar o servidor para ativar o firmware de pré-requisito. Após a reinicialização inicial, as atualizações de firmware restantes são instaladas usando **Ativação imediata**.

Etapa 10. **Opcional:** se você selecionou **Ativação Imediata**, selecione **Teste de Memória** para executar um teste de memória após a atualização de firmware ser concluída se o servidor for reinicializado durante a atualização.

Essa opção é suportada para servidores ThinkSystem v1 e v2 (excluindo servidores ThinkSystem SR635, SR645, SR655, SR665).

Etapa 11. Clique em **Realizar Atualização** para atualizar imediatamente ou clique em **Programação** para programar a execução dessa atualização para mais tarde.

Se necessário, você pode executar ações de energia nos dispositivos gerenciados. As ações de energia são úteis quando a opção **Ativação Atrasada** está selecionada e você quer que as atualizações continuem quando o dispositivo estiver em espera no estado "Manutenção Pendente". Para executar uma ação de energia em um dispositivo gerenciado desta página, clique em **Todas as Ações → Ações de Energia** e, em seguida, clique em uma das ações de energia a seguir.

- **Ligar**
- **Encerrar SO e desligar**
- **Desligar**
- **Encerrar SO e reiniciar**
- **Reiniciar**

Depois de concluir

Ao aplicar uma atualização de firmware, se o servidor não entrar no modo de manutenção, tente aplicar a atualização novamente.

Se as atualizações não forem concluídas com êxito, consulte Problemas de repositório e atualização de firmware na documentação online do XClarity Administrator para conhecer as ações de solução de problemas e correção.

Na página Atualizações de Firmware: Aplicar/Ativar, é possível realizar as seguintes:

- Exportar informações de firmware e de conformidade para cada dispositivo gerenciado clicando em **Todas as Ações → Exportar Exibição como CSV**.

Nota: O arquivo CSV contém apenas informações filtradas na exibição atual. Informações que são filtradas da exibição e informações em colunas ocultas não estão incluídas.

- Cancele uma atualização que está sendo aplicada a um dispositivo selecionando o dispositivo e clicando no ícone **Cancelar Atualização** ( ).

  Nota: Você pode cancelar atualizações de firmware que estão na fila para iniciar. Após o início do processo de atualização, a atualização de firmware pode ser cancelada somente quando o processo de atualização está executando uma tarefa diferente de aplicar a atualização, como alterar para modo de manutenção ou reiniciar o dispositivo.
- Exiba o status da atualização do firmware diretamente na página Aplicar/Ativar na coluna **Status**.
- Monitore o status do processo de atualização no log de trabalhos. Na barra de menu do Lenovo XClarity Administrator, clique em **Monitoramento → Trabalhos**.

  Para obter mais informações sobre o log de trabalhos, consulte Monitorando trabalhos.

Quando os trabalhos de atualização de firmware estiverem concluídos, você poderá verificar se os dispositivos estão em conformidade clicando em **Fornecimento → Atualizações de Firmware: Aplicar/Ativar** para voltar à página Atualizações de Firmware: Aplicar/Ativar e, em seguida, clica no ícone **Atualizar** ( ). A versão atual do firmware que está ativa em cada dispositivo é listada na coluna **Versão Instalada**.

Capítulo 14. Atualizando drivers de dispositivo Windows em servidores gerenciados

Usando o Windows UpdateXpress System Packs (UXSPs), você pode atualizar drivers de dispositivos do SO nos sistemas operacionais Windows implantados.

Antes de iniciar

Você deve ter autoridade **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** ou **lxc-hw-admin** para gerenciar e implantar drivers de dispositivo do SO e executar ações de energia em servidores gerenciados nas páginas Atualizações de drivers Windows.

A atualização do firmware e a atualização dos drivers de dispositivo são processos separados no XClarity Administrator. Não há conexão entre esses processos. O XClarity Administrator não mantém a conformidade entre o firmware e os drivers de dispositivo em dispositivos gerenciados, mesmo que seja recomendado que você atualize os drivers de dispositivos ao mesmo tempo que o firmware.

Sobre esta tarefa

O Windows UpdateXpress System Packs (UXSPs) contém drivers de dispositivo Windows para versões do Windows com suporte e para servidores Lenovo que ofereçam suporte a Windows.

Apenas drivers de dispositivo para Windows Server 2012 R2 e posterior são compatíveis. o XClarity Administrator não é compatível com a atualização de drivers de dispositivos Linux nem VMware.

Para obter informações sobre como instalar drivers de dispositivo ao implantar sistemas operacionais, consulte Instalando sistemas operacionais em servidores bare-metal.

Procedimento

Etapa 1. **Configurando o Windows Server para atualizações de driver de dispositivo do SO**

Lenovo XClarity Administrator usa a escuta do Serviço de Gerenciamento Remoto do Windows (WinRM) sobre HTTPS ou HTTP para executar comandos de atualização de driver de dispositivo em sistemas Windows de destino. O serviço WinRM deve ser configurado corretamente nos servidores de destino antes de tentar atualizar drivers de dispositivo do SO (consulte Configurando o Windows Server para atualizações de driver de dispositivo do SO).

Etapa 2. **Gerenciar o repositório de drivers de dispositivo do SO**

O *repositório do driver de dispositivo do SO* contém um catálogo de drivers de dispositivo Windows disponíveis e os pacotes de drivers de dispositivo que podem ser aplicados aos dispositivos gerenciados.

O *catálogo* contém informações sobre todos os Windows UpdateXpress System Packs (UXSPs) e atualizações de drivers de dispositivo que estão disponíveis para todos os servidores Lenovo que dão suporte ao Windows. O catálogo organiza as atualizações de drivers de dispositivos por tipo de dispositivo. Quando você atualiza o catálogo, o XClarity Administrator recupera informações sobre os UXSPs disponíveis do Site de Suporte a data center da Lenovo (incluindo os arquivos metadata.xml e readme.txt) e armazena as informações no repositório. O arquivo de carga útil (. exe) não foi baixado. Para obter mais informações sobre como atualizar o catálogo, consulte Atualizando o catálogo de driver de dispositivo do SO.

É possível baixar ou importar Windows UXSPs no repositório. Os Windows UXSPs contêm drivers de dispositivo Windows para versões do Windows com suporte e para servidores Lenovo compatíveis com Windows. Os UXSPs devem estar disponíveis no repositório para que você possa atualizar drivers de dispositivos Windows em servidores gerenciados. Para obter mais informações sobre como baixar drivers de dispositivo, consulte Baixando drivers de dispositivo Windows .

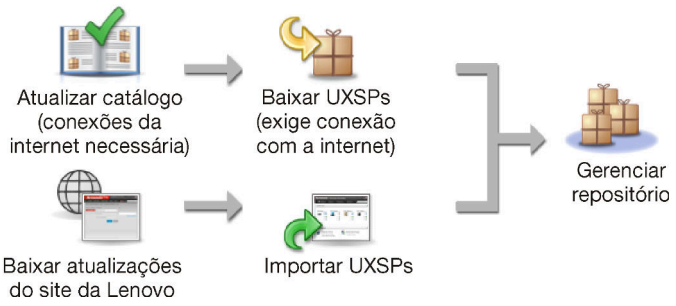
É possível determinar se os UXSPs estão armazenados no repositório de drivers de dispositivos de SO na coluna Status de download na guia Atualizações individuais da página Atualizações de drivers Windows: repositório. Essa coluna contém os seguintes valores.

- **Baixado**. O pacote inteiro ou a atualização individual é armazenada no repositório.
- ***x* de *y* baixado**. Algumas, mas nem as todas atualizações no pacote estão armazenadas no repositório. Os números entre parênteses indicam o número de atualizações disponíveis e o número de atualizações armazenadas, ou não há atualizações para o tipo de dispositivo específico.
- **Não baixado**. O pacote inteiro ou a atualização individual está disponível, mas não armazenado no repositório.

Nota: Quando você baixa ou importa os UXSPs da página Repositório de atualizações de drivers Windows, somente os drivers de dispositivo são baixados e armazenados no repositório. As atualizações de firmware são descartadas. Para obter informações sobre como baixar ou importar atualizações de firmware, consulte Gerenciando o repositório das atualizações de firmware.

O XClarity Administrator deve estar conectado à Internet para atualizar o catálogo e baixar os UXSPs. Se ele não estiver conectado à Internet, você poderá baixar manualmente o UXSPs para uma estação de trabalho que tenha acesso de rede ao host do XClarity Administrator usando um navegador da Web. Este download do UXSPs é um arquivo de formato zip e contém todos os arquivos de driver de dispositivo necessários para o UXSP, incluindo a carga útil (.exe), metadados (.xml) e o arquivo de histórico de alterações (.chg), além de arquivos leia-me (.txt).

Nota: Você pode ver mensagens de que os arquivos de firmware (fw) não são necessários e foram removidos. Isso é normal porque apenas os drivers de dispositivo Windows são atualizados usando esse processo.



Atenção:

- Não descompacte o UXSP antes de importá-lo.
- Os Windows UXSPs incluem drivers de dispositivo e atualizações de firmware. As atualizações de firmware no Windows UXSPs são descartadas quando os UXSPs são importados para o repositório e uma mensagem de aviso é exibida. Somente os drivers de dispositivo são importados.

Etapa 3. **Aplicando drivers de dispositivo do SO**

O XClarity Administrator não atualiza os drivers de dispositivo em servidores gerenciados automaticamente. Para atualizar os drivers de dispositivo, você deverá aplicar manualmente os drivers de dispositivo em servidores selecionados.

Atenção: Antes de tentar atualizar os drivers de dispositivo em servidores gerenciados, verifique as seguintes considerações e conclua as ações de pré-requisito aplicáveis.

- Os dispositivos sem suporte não podem ser selecionados para atualizações.
- Leia as considerações sobre a atualização de drivers de dispositivo antes de tentar atualizar os drivers em seus servidores gerenciados (consulte Considerações sobre atualização de drivers de dispositivo do SO).
- Verifique se o repositório contém o UXSPs e os drivers de dispositivo que você pretende implantar (consulte Baixando drivers de dispositivo Windows).

  Nota: Quando o XClarity Administrator for instalado, o catálogo de produtos e o repositório estarão vazios.
- O XClarity Administrator pode usar a escuta do Serviço de Gerenciamento Remoto do Windows (WinRM) sobre HTTPS ou HTTP para executar comandos de atualização de driver de dispositivo em sistemas Windows de destino. HTTPS é o padrão. Para usar HTTP, clique em **Todas as Ações → Configurações Globais** na página Atualizações de driver do Windows: Aplicar e, em seguida, desmarque **Usar HTTPS para atualizações de driver do Windows**.

  Atenção: Ao usar HTTP, as credenciais do usuário Windows são enviadas pela rede *sem* criptografia e podem ser facilmente exibidos usando ferramentas de solução de problemas de rede disponíveis com frequência.

  Importante:

  – Certifique-se de que o Gerenciamento Remoto do Windows (WinRM) no servidor de destino esteja configurado para usar a mesma configuração (HTTPS ou HTTP) que está definida no XClarity Administrator (consulte Configurando o Windows Server para atualizações de driver de dispositivo do SO).

  – Garanta que o WinRM no servidor de destino esteja configurado com autenticação básica.

  – Ao usar HTTPS, certifique-se de que o WinRM no servidor de destino esteja configurado com **allowUnencrypted=false**.
- Verifique se o PowerShell tem suporte no servidor de destino.
- Certifique-se de que o servidor de destino esteja ligado antes de tentar atualizar drivers de dispositivo. Se o servidor não estiver ligado, selecione o servidor de destino e clique em **Todas as Ações → Ações de Energia → Ligar**.
- Certifique-se de que o XClarity Administrator tenha informações necessárias para acessar o sistema operacional do host (consulte Gerenciando o acesso a sistemas operacionais em servidores gerenciados.
- Se você deseja usar uma conta de domínio ao atualizar drivers de dispositivo do SO, certifique-se de ter criado o arquivo de configuração necessário (consulte Configurando uma conta de domínio para atualizações de drivers de dispositivo do SO).
- Certifique-se de que nenhum trabalho esteja em execução atualmente no servidor de destino. Você não pode atualizar drivers de dispositivo em um servidor gerenciado bloqueado por um trabalho em execução. Se houver outro trabalho de atualização em execução no servidor de destino, esse trabalho de atualização será colocado na fila até o término do trabalho de atualização atual. Para ver uma lista de trabalhos ativos, clique em **Monitoramento → Trabalhos**.

Para obter mais informações sobre como atualizar os drivers de dispositivo, consulte Aplicando drivers de dispositivo Windows.

Considerações sobre atualização de drivers de dispositivo do SO

Antes de começar a atualizar os drivers de dispositivo do SO para dispositivos gerenciados usando o Lenovo XClarity Administrator, revise as considerações importantes a seguir.

Nota: Você deve ter autoridade **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** ou **lxc-hw-admin** para gerenciar e implantar drivers de dispositivo e executar ações de energia em servidores gerenciados nas páginas Atualizações de drivers Windows.

Considerações de rede

- As portas e os endereços de Internet necessários devem estar disponíveis antes de tentar baixar o UpdateXpress System Packs (UXSPs). Para obter mais informações, consulte Disponibilidade de porta e Firewalls e servidores proxy na documentação online do XClarity Administrator.
- O XClarity Administrator deve ter acesso à rede de gerenciamento e dados para acessar o sistema operacional.
- O XClarity Administrator deve poder se comunicar com o servidor de destino (o Baseboard Management Controller e a rede de dados do servidor) sobre a interface de rede (Eth0 ou Eth1) que foi selecionada quando você configurou o acesso de rede do XClarity Administrator e que a interface esteja configurada com um endereço IPv4 ou um endereço IPv6 auto ULA.

  Para especificar uma interface a ser usada para implantação do sistema operacional, consulte Configurando o acesso à rede.

  Para obter mais informações sobre a rede de implantação do sistema operacional e interfaces, consulte Considerações de rede na documentação online do XClarity Administrator.
- Endereços IP devem ser exclusivos para o sistema operacional do host.
- O XClarity Administrator pode usar a escuta do Serviço de Gerenciamento Remoto do Windows (WinRM) sobre HTTPS ou HTTP para executar comandos de atualização de driver de dispositivo em sistemas Windows de destino. HTTPS é o padrão. Para usar HTTP, clique em **Todas as Ações → Configurações Globais** na página Atualizações de driver do Windows: Aplicar e, em seguida, desmarque **Usar HTTPS para atualizações de driver do Windows**.

  Atenção: Ao usar HTTP, as credenciais do usuário Windows são enviadas pela rede *sem* criptografia e podem ser facilmente exibidos usando ferramentas de solução de problemas de rede disponíveis com frequência.

Considerações sobre dispositivo gerenciado

- Drivers de dispositivo do Windows não tem suporte para servidores ThinkAgile, ThinkSystem SR635 e ThinkSystemSR655.
- Somente servidores ThinkSystem, Lenovo System x e Lenovo Flex System são aceitos.
- XClarity Administrator não valida o relacionamento entre o controlador de gerenciamento e o sistema operacional. O Baseboard Management Controller é usado para ligar ou desligar o servidor.
- Verifique se a interface LAN sobre USB está ativada. LAN sobre USB é usada ao atualizar drivers de dispositivo do SO.

Considerações sobre o driver de dispositivo e o sistema operacional

- É possível atualizar os drivers de dispositivos para os seguintes sistemas operacionais.
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019

Nota: O XClarity Administrator é testado com apenas versões do Windows que são suportadas pela Microsoft no lançamento da versão XClarity Administrator.

- O Gerenciamento Remoto do Windows (WinRM) deve ser configurado para HTTPS no servidor de destino (consulte Configurando o Windows Server para atualizações de driver de dispositivo do SO).
- O PowerShell deve ter suporte no servidor de destino.
- Você deve fornecer informações necessárias para acessar o sistema operacional do host no servidor de destino, incluindo o endereço IP do SO e as credenciais (consulte Gerenciando o acesso a sistemas operacionais em servidores gerenciados). Você deve fornecer as credenciais para uma conta de usuário com autoridade de administrador.
- O XClarity Administrator atualiza apenas os drivers de dispositivo que estão fora de conformidade. Os drivers de dispositivo estarão fora de conformidade quando a versão no servidor for anterior à versão no UXSP selecionado. Os drivers de dispositivo que são iguais ou posterior à versão no UXSP selecionado são ignorados.
- A conformidade com driver de dispositivo só é precisa quando o hardware está presente. Se o hardware não estiver presente, os drivers de dispositivo continuarão sendo aplicados ao servidor. Quando o hardware ausente for adicionado ao servidor, o Windows carregará a versão mais recente.
- Os servidores System x não oferecem suporte a alguns drivers de dispositivo predefinidos fornecidos com o XClarity Administrator. Para implantar drivers de dispositivo nesses servidores, crie um perfil personalizado que inclua apenas os drivers de dispositivo necessários.

Gerenciando o repositório de drivers de dispositivo do SO

O *repositório de driver de dispositivo do SO* inclui o catálogo e os drivers de dispositivo Windows baixados.

Sobre esta tarefa

O *catálogo* contém informações sobre todos os Windows UpdateXpress System Packs (UXSPs) e atualizações de drivers de dispositivo que estão disponíveis para todos os servidores Lenovo que dão suporte ao Windows. O catálogo organiza as atualizações de drivers de dispositivos por tipo de dispositivo. Quando você atualiza o catálogo, o XClarity Administrator recupera informações sobre os UXSPs disponíveis do Site de Suporte a data center da Lenovo (incluindo os arquivos metadata.xml e readme.txt) e armazena as informações no repositório. O arquivo de carga útil (.exe) não foi baixado. Para obter mais informações sobre como atualizar o catálogo, consulte Atualizando o catálogo de driver de dispositivo do SO.

O Windows UpdateXpress System Packs (UXSPs) contém drivers de dispositivo Windows para versões do Windows com suporte e para servidores Lenovo que ofereçam suporte a Windows. É possível baixar ou importar Windows UXSPs no repositório. Os Windows UXSPs contêm drivers de dispositivo Windows para versões do Windows com suporte e para servidores Lenovo compatíveis com Windows. Os UXSPs devem estar disponíveis no repositório para que você possa atualizar drivers de dispositivos Windows em servidores gerenciados.Para obter mais informações sobre download de drivers de dispositivo, consulte Baixando drivers de dispositivo Windows .

O XClarity Administrator deve estar conectado à Internet para atualizar o catálogo e baixar os UXSPs. Se ele não estiver conectado à Internet, você poderá baixar manualmente o UXSPs para uma estação de trabalho que tenha acesso de rede ao host do XClarity Administrator usando um navegador da Web. Este download do UXSPs é um arquivo de formato zip e contém todos os arquivos de driver de dispositivo necessários para o UXSP, incluindo a carga útil (.exe), metadados (.xml) e o arquivo de histórico de alterações (.chg), além de arquivos leia-me (.txt).

Depois que um UXSPé baixado no repositório, informações sobre cada driver de dispositivo no pacote são adicionadas à página Repositório de atualizações de drivers Windows. Isso inclui a data de lançamento, o

tamanho e a gravidade. A severidade indica o impacto e a necessidade de aplicar a atualização para ajudar a avaliar como seu ambiente pode ser afetado.

- **Versão Inicial**. Essa é a primeira versão do driver de dispositivo.
- **Crítico**. O driver de dispositivo contém correções urgentes para problemas de dados corrompidos, segurança ou estabilidade.
- **Sugerido**. O driver de dispositivo contém correções significativas para problemas que você poderá encontrar.
- **Não Crítico**. O driver de dispositivo contém pequenas correções, melhorias de desempenho e alterações textuais.

Notas:

- A gravidade está relacionada à versão anteriormente liberada do driver de dispositivo. Por exemplo, se o driver de dispositivo instalado é v1.01, e a atualização v1.02 é Crítica e a atualização v1.03 é Recomendada, isso significa que a atualização de 1.02 para 1.03 é recomendada, mas a atualização de v1.01 para v1.03 é crítica porque é cumulativa (a v1.03 inclui problemas críticos da v1.02).
- Podem surgir casos especiais em que uma atualização seja crítica ou recomendada apenas para um tipo de máquina específico. Consulte as Notas de Versão para obter as informações adicionais.

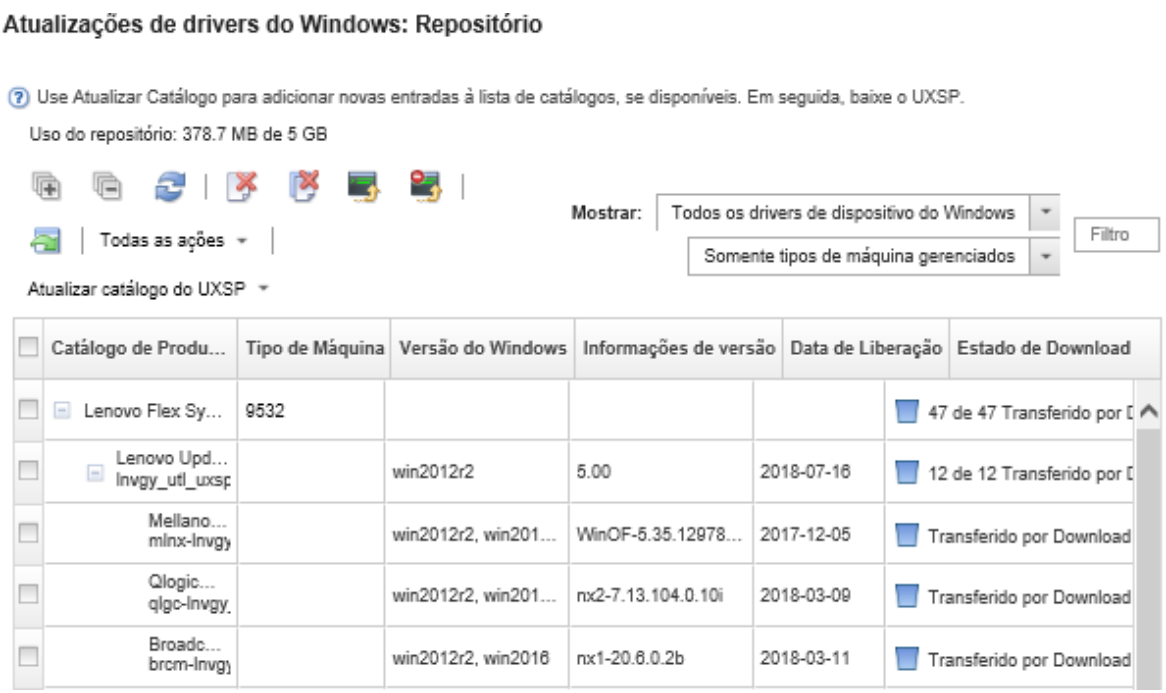
Procedimento

Para ver UXSPs e os drivers de dispositivo disponíveis no repositório, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Administrator, clique em **Fornecimento → Atualizações de driver do Windows: repositório**. A página Repositório das atualizações de driver de dispositivo é exibida com uma lista de pacotes de UXSPs disponíveis, organizados por tipo de dispositivo.

Etapa 2. Expanda um tipo de servidor e, em seguida, expanda os UXSPs que estão disponíveis para esse tipo de servidor para listar os drivers de dispositivo que estão disponíveis para esse tipo de servidor.

Você pode classificar as colunas da tabela e clicar no ícone **Expandir** tudo ( ) e no ícone **Reduzir** tudo ( ) para facilitar a localização de drivers de dispositivo específicos. Além disso, é possível filtrar a lista de tipos de servidor e drivers de dispositivo exibidos selecionando uma opção no menu **Mostrar** para listar somente os drivers de dispositivo de uma idade específica, os drivers de dispositivo de todos os tipos de servidor ou somente de tipos de servidor gerenciado ou inserindo texto no campo **Filtro**.



Nesta página, é possível executar as ações a seguir:

- Recuperar as informações os UXSPs mais recentes disponíveis clicando em **Atualizar Catálogo**.

  A recuperação dessas informações pode levar vários minutos para ser concluída. Para obter mais informações, consulte Atualizando o catálogo de driver de dispositivo do SO.
- Baixe UXSPs e os drivers de dispositivo usando o XClarity Administrator atualizando o catálogo e, em seguida, clicando no ícone **Baixar** ( ). Quando os UXSPs e os drivers de dispositivo são baixados e adicionados ao repositório, o status muda para "Baixado".

  Para obter mais informações sobre download UXSPs e drivers de dispositivo, consulte Baixando drivers de dispositivo Windows .
- Importe UXSPs que você baixou manualmente para uma estação de trabalho da Web ou os drivers de dispositivo que você exportou do XClarity Administrator (consulte Baixando drivers de dispositivo Windows).
- Interrompa os downloads selecionados em andamento no momento clicando no ícone **Cancelar Downloads** ( ).
- Exclua os UXSPs ou drivers de dispositivo individuais do repositório clicando no ícone **Excluir** ( ).

Atualizando o catálogo de driver de dispositivo do SO

O catálogo de driver de dispositivo do SO contém informações sobre todos os Windows UpdateXpress System Packs (UXSPs) e drivers de dispositivo que estão disponíveis para todos os servidores Lenovo que dão suporte a atualizações de driver de dispositivo Windows.

Antes de iniciar

Verifique se o Lenovo XClarity Administrator está conectado à Internet.

Sobre esta tarefa

Quando você atualiza o catálogo, o XClarity Administrator recupera informações sobre os UXSPs disponíveis do Site de Suporte a data center da Lenovo (incluindo os arquivos metadata.xml e readme.txt) e armazena as informações no repositório. O arquivo de carga útil (.exe) não foi baixado.Você deve baixar os UXSP desejados e as cargas de driver de dispositivo do SO antes de atualizar os drivers de dispositivo nos servidores gerenciados. Para obter mais informações sobre como baixar drivers de dispositivo, consulte Baixando drivers de dispositivo Windows .

Nota: A atualização do catálogo pode levar vários minutos para ser concluída.

Procedimento

Para atualizar o catálogo, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Atualizações de drivers do Windows: repositório** para exibir a página Atualizações de drivers de dispositivos: repositório.

Etapa 2. Clique em **Atualizar Catálogo** e clique em uma das opções a seguir para obter informações sobre os UXSPs mais recentes disponíveis.

- **Atualizar Selecionado - Somente Mais Recente**. Recupera informações sobre as versões mais atuais do UXSP disponíveis apenas para os servidores selecionados.
- **Atualizar Tudo - Somente Mais Recente**. Recupera informações sobre as versões mais recentes do UXSP para todos os servidores com suporte.
- **Atualizar Selecionado**. Recupera informações sobre todas as versões do UXSP disponíveis apenas para os servidores selecionados.
- **Atualizar Tudo**. Recupera informações sobre todas as versões do UXSP disponíveis para todos os servidores com suporte.

Etapa 3. Clique em **Atualizar Catálogo** para atualizar imediatamente ou clique em **Programação** para programar a execução dessa atualização para mais tarde.

Baixando drivers de dispositivo Windows

O Windows UpdateXpress System Packs (UXSPs) contém drivers de dispositivo Windows para versões do Windows com suporte e para servidores Lenovo que ofereçam suporte a Windows. É possível baixar ou importar Windows UXSPs no repositório. Os Windows UXSPs contêm drivers de dispositivo Windows para versões do Windows com suporte e para servidores Lenovo compatíveis com Windows. Os UXSPs devem estar disponíveis no repositório para que você possa atualizar drivers de dispositivos Windows em servidores gerenciados.

Antes de iniciar

Verifique se todas as portas e os endereços de Internet necessários estão disponíveis antes de tentar baixar o UpdateXpress System Packs (UXSPs). Para obter mais informações, consulte Disponibilidade de porta e Firewalls e servidores proxy na documentação online do XClarity Administrator.

Para baixar UXSPs usando o XClarity Administrator, certifique-se de que o XClarity Administrator esteja conectado à Internet.

Os navegadores da Web Internet Explorer e Microsoft Edge têm um limite de upload de 4 GB. Se o arquivo que você está importando for maior que 4 GB, considere usar outro navegador da Web (como o Chrome ou o Firefox).

Sobre esta tarefa

O XClarity Administrator deve estar conectado à Internet para atualizar o catálogo e baixar os UXSPs. Se o XClarity Administrator não estiver conectado à Internet, você poderá baixar manualmente os arquivos para

uma estação de trabalho que tenha acesso à rede no host do XClarity Administrator usando um navegador da Web e, em seguida, importar as atualizações para o repositório das atualizações de firmware.

É possível determinar se UXSPs estão armazenados no repositório na coluna **Status de Download** na página Atualizações de firmware: repositório. Essa coluna contém os seguintes valores:

- **Baixado**. Todos os drivers de dispositivo no UXSPou o driver de dispositivo individual é baixado no repositório.
- *x* **de** *y* **Baixado**. Alguns, mas nem todos os drivers de dispositivo no UXSP são baixados no repositório. Os números entre parênteses indicam o número de drivers de dispositivo disponíveis e o número de drivers de dispositivo baixados.
- **Não Baixado**. O UXSP ou o driver de dispositivo individual está disponível no site de suporte da Lenovo, mas não é baixado no repositório.

Uma mensagem é exibida na página Repositório de atualizações de driver Windows quando o espaço disponível para UXSPs está mais de 50% ocupado. Uma outra mensagem é exibida na página quando o repositório está mais de 85% completo. Para reduzir o espaço utilizado no repositório, você pode remover os arquivos não usados selecionando os arquivos de destino e, em seguida, clicando no ícone **Excluir** ( ). Para obter mais informações, consulte Gerenciando espaço em disco.

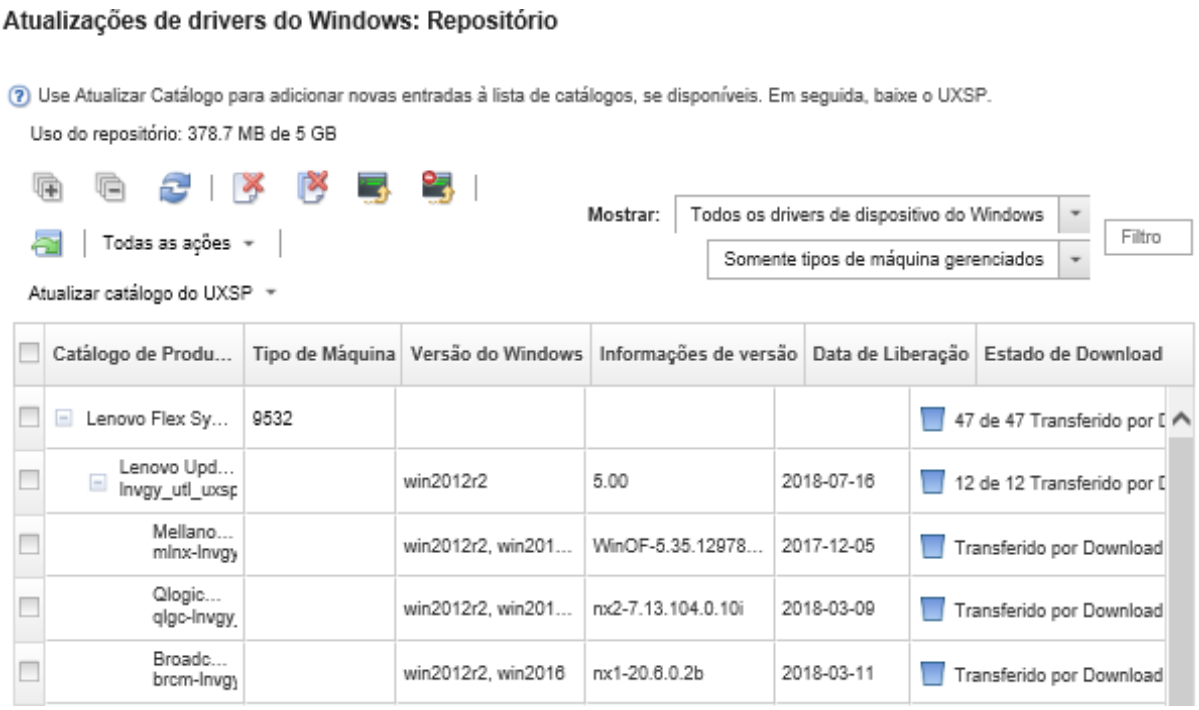
Atenção: Os Windows UXSPs incluem drivers de dispositivo e atualizações de firmware. As atualizações de firmware no Windows UXSPs são descartadas quando os UXSPs são importados para o repositório e uma mensagem de aviso é exibida. Somente os drivers de dispositivo são importados.

Procedimento

Para baixar o UXSPs e drivers de dispositivo específicos, execute um dos procedimentos a seguir.

- Quando o XClarity Administrator estiver conectado à Internet:
  1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Atualizações de drivers do Windows: repositório** para exibir a página Atualizações de drivers de dispositivos: repositório.
  2. Clique em **Atualizar Catálogo** e clique em uma das opções a seguir para obter informações sobre os UXSPs mais recentes disponíveis.
     - **Atualizar Selecionado - Somente Mais Recente**. Recupera informações sobre as versões mais atuais do UXSP disponíveis apenas para os servidores selecionados.
     - **Atualizar Tudo - Somente Mais Recente**. Recupera informações sobre as versões mais recentes do UXSP para todos os servidores com suporte.
     - **Atualizar Selecionado**. Recupera informações sobre todas as versões do UXSP disponíveis apenas para os servidores selecionados.
     - **Atualizar Tudo**. Recupera informações sobre todas as versões do UXSP disponíveis para todos os servidores com suporte.

     Nota: A atualização do catálogo pode levar vários minutos para ser concluída.
  3. Expanda o tipo de servidor para exibir a lista de UXSPs disponíveis. Expanda o UXSP para ver uma lista de drivers de dispositivo disponíveis.



4. Selecione um ou mais UXSPs e drivers de dispositivo de destino para download.
5. Clique no ícone **Baixar Selecionado** ( ).
6. Clique em **Baixar** para baixar imediatamente ou clique em **Programação** para programar a execução do download para mais tarde.

   O download dos UXSPs pode levar alguns minutos. Quando os UXSPs e os drivers de dispositivo tiverem sido baixados e armazenados no repositório, a linha será destacada no catálogo de produtos, e a coluna **Status de Download** será alterada para "Baixado".

   É possível monitorar o status do processo de download no log de trabalhos. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Trabalhos**. Para obter mais informações sobre o log de trabalhos, consulte Monitorando trabalhos.

- Se o XClarity Administrator *não estiver* conectado à Internet:
  1. Baixe os UXSPs para uma estação de trabalho que tenha uma conexão de rede com o host do XClarity Administrator do Site de Suporte a data center da Lenovo.
  2. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Atualizações de drivers do Windows: repositório** para exibir a página Atualizações de drivers de dispositivos: repositório.
  3. Clique no ícone **Importar** ( ).
  4. Clique em **Selecionar Arquivos** e navegue até o local do UXSP na estação de trabalho.
  5. Selecione o arquivo .zip do UXSP (não descompacte o arquivo zip antes de importar) e, em seguida, clique em **Abrir**.

     O arquivo .zip do UXSP contém o arquivo de metadados (.xml), a carga útil (.exe), o arquivo de histórico de alterações (.chg) e o arquivo leiame (.txt).
  6. Clique em **Importar**.

     É possível monitorar o status do processo de importação no log de trabalhos. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Trabalhos**. Para obter mais informações sobre o log de trabalhos, consulte Monitorando trabalhos.

Depois de concluir

Nesta página, é possível executar as ações a seguir nos UXSPs selecionados.

- Cancele um download em andamento clicando no ícone **Cancelar download** ().
- Exclua todos os arquivos associados com o UXSP clicando no ícone **Excluir** ().

Configurando o Windows Server para atualizações de driver de dispositivo do SO

O Lenovo XClarity Administrator usa a escuta do Serviço de Gerenciamento Remoto do Windows (WinRM) sobre HTTPS ou HTTP para executar comandos de atualização de driver de dispositivo em sistemas Windows de destino. O serviço WinRM deve ser configurado corretamente nos servidores de destino antes de tentar atualizar drivers de dispositivo do SO.

Antes de iniciar

As portas necessárias devem estar disponíveis. Para obter mais informações, consulte Disponibilidade de porta na documentação online do XClarity Administrator.

Para obter mais informações sobre como configurar o Windows Server antes de atualizar o driver de dispositivo do SO, consulte o XClarity Administrator: Preparação para atualizações de driver de dispositivo do SO (whitepaper).

Procedimento

Para configurar o Windows Server para oferecer suporte à atualização drivers de dispositivo do SO, conclua as seguintes etapas.

- **Para HTTPS**
  1. Assine e instale um certificado de servidor em cada um dos sistemas Windows de destino.

     Importante: O certificado deve conter as informações a seguir.

     – No Assunto, certifique-se de que o componente de domínio seja definido (por exemplo, DC=labs, DC=com, DC=company).

     – No Nome do assunto alternativo, certifique-se de que o nome DNS e o endereço IP do host sejam definidos (por exemplo, o nome DNS = node1325C554A6F.labs.company.com e o endereço IP = 10.245.43.149).
  2. Configure os comandos de gerenciamento remoto e os dados sobre uma conexão HTTPS executando um dos seguintes comandos de um prompt de comandos administrativo e, em seguida, confirme as alterações de configuração sugeridas.

     –
     ```
     winrm quickconfig -transport:https
     ```

     –
     ```
     winrm create winrm/config/Listener?Address=*+Transport=HTTPS
     @{Hostname="host_name";CertificateThumbprint="certificate_thumbprint"}
     ```

     Para configurar manualmente um ouvinte WinRM HTTPS de acordo com a documentação do WinRM, consulte a Como configurar WinRM para página da Web HTTPS.
  3. Ative a autenticação básica de usuários locais do Windows executando o seguinte comando de um prompt de comandos administrativo.
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```

4. Para evitar um possível tempo limite e enviar erros de solicitação do WinRM na verificação de conformidade e executar atualizações de driver, aumente o valor padrão para o tempo limite de resposta do WinRM executando o comando a seguir de um prompt de comando administrativo. Um valor de 280000 é recomendado. Para obter mais informações, consulte o Site de Instalação e Configuração para Gerenciamento Remoto do Windows.
   ```
   winrm set winrm/config @{MaxTimeoutms="280000"}
   ```
5. Abra a porta no firewall que é configurado para o ouvinte HTTPS do WinRM. A porta HTTPS padrão é 5986. Por exemplo
   ```
   netsh advfirewall firewall add rule name="Windows Remote Management (HTTPS-In)" dir=in action=allow
   protocol=TCP localport=5986
   ```
6. Se você estiver usando ouvintes HTTPS, adiciona o certificado para o armazenamento confiável do XClarity Administrator concluindo as etapas a seguir. Adicionar o certificado ao armazenamento confiável permite que o XClarity Administrator confie nos ouvintes HTTPS do WinRM para que ele se conecte. Repita as etapas a seguir para todos os caminhos de certificação adicionais que precisam ser confiáveis para o serviço Gerenciamento Remoto do Windows.
   a. Identifique e colete o certificado raiz da Autoridade de Certificação que é usada para assinar os certificados do servidor para os sistemas Windows de destino. Se você não tiver acesso ao Certificado raiz da CA, colete o certificado do servidor ou outro certificado no caminho de certificação.
   b. Na barra de menus do XClarity Administrator, clique em **Administração → Segurança** para exibir a página Segurança.
   c. Clique em **Certificados confiáveis** na seção Gerenciamento de Certificados.
   d. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Adicionar certificado.
   e. Navegue até o arquivo de certificado coletado na etapa 1 ou copie/cole o conteúdo do arquivo de certificado na caixa de texto.
   f. Clique em **Criar**.
7. Depois que o ouvinte do WinRM estiver em execução em sistemas Windows de destino, o XClarity Administrator poderá se conectar a esses sistemas e executar as atualizações do driver de dispositivo.

- **Para HTTP**
  1. Configure os comandos de gerenciamento remoto e os dados sobre uma conexão HTTP executando o seguinte comando de um prompt de comandos administrativo e, em seguida, confirme as alterações de configuração sugeridas.
     ```
     winrm quickconfig
     ```
  2. Ative a autenticação básica de usuários locais do Windows executando o seguinte comando de um prompt de comandos administrativo.
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```
  3. Aloque memória suficiente para os comandos de atualização no sistema executando o seguinte comando de um prompt de comandos administrativo.
     ```
     winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
     ```
  4. Permita dados não criptografados executando o seguinte comando de um prompt de comandos administrativo.
     ```
     winrm set winrm/config/service @{AllowUnencrypted="true"}
     ```
  5. Abra a porta no firewall que é configurado para o ouvinte HTTP do WinRM. A porta HTTPS padrão é 5985. Por exemplo
     ```
     netsh advfirewall firewall add rule name="Windows Remote Management (HTTP-In)" dir=in action=allow
     protocol=TCP localport=5985
     ```

  Depois que o ouvinte do WinRM estiver em execução em sistemas Windows de destino, o XClarity Administrator poderá se conectar a esses sistemas e executar as atualizações do driver de dispositivo.

Configurando uma conta de domínio para atualizações de drivers de dispositivo do SO

É possível optar por usar contas de domínio para gerenciar com facilidade os privilégios com um controlador de domínio. Para usar uma conta de domínio ao atualizar drivers de dispositivo do SO, é necessário configurar uma conta de domínio.

Antes de iniciar

Verifique se os servidores Windows gerenciados estão em uma rede de domínio antes de configurar contas de domínio.

Ao adicionar a conta do usuário do Windows no Lenovo XClarity Administrator, use o formato `USER@DOMAIN`. O formato `DOMAIN/USER` não é suportado.

Procedimento

Para configurar uma conta de domínio, conclua as etapas a seguir.

Etapa 1. Na barra de menus do Lenovo XClarity Administrator, clique em **Fornecimento → Atualizações de drivers do Windows: Aplicar**. A página Atualizações do driver do Windows: aplicar é exibida.

Etapa 2. Clique em **Todas as Ações → Gerenciar Conta de Domínio**. A página Contas de domínio é exibida.

Etapa 3. Clique no ícone **Criar** ( ) para adicionar um domínio para a conta de domínio. A caixa de diálogo Criar domínio é exibida.

Etapa 4. Especifique um nome e um ou mais nomes de hosts do centro de distribuição de chaves para o domínio. Use o ícone **Adicionar** ( ) para adicionar outro nome do host e use o ícone **Remover** ( ) para remover um nome do host.

Etapa 5. Clique em **OK** para salvar o domínio.

Etapa 6. Na página Contas de domínio, selecione opcionalmente o domínio a ser usado por padrão.

Etapa 7. Clique em **Salvar** para salvar a configuração.

Depois de concluir

É possível realizar as ações a seguir na página Configurar conta de domínio.

- Modifique um domínio selecionado clicando no ícone **Editar** ( ).
- Exclua um domínio selecionado clicando no ícone **Excluir** ( ).

Definindo as configurações globais de atualização do driver de dispositivo do Windows

Configurações globais servem como as configurações padrão quando as atualizações do driver de dispositivo Windows forem aplicadas.

Sobre esta tarefa

Na página Configurações Globais, é possível definir as seguintes configurações:
- Usar HTTPS para atualizações de drivers do Windows
- Mostrar drivers de dispositivo para o hardware instalado

Procedimento

Para definir as configurações globais a serem usadas para todos os servidores, conclua as etapas a seguir.

Etapa 1. Na barra de menus do Lenovo XClarity Administrator, clique em **Fornecimento → Atualizações de drivers do Windows: Aplicar**. A página Atualizações do driver do Windows: aplicar é exibida.

Etapa 2. Clique em **Todas as Ações → Configurações globais** para exibir a caixa de diálogo Configurações globais: aplicar atualizações do driver do Windows.

Etapa 3. Selecione, opcionalmente, uma das opções a seguir.

- Selecione **Usar HTTPS para atualizações do driver do Windows** para usar a escuta do Serviço de Gerenciamento Remoto do Windows (WinRM) sobre HTTPS para executar comandos de atualização de driver de dispositivo em sistemas Windows de destino. HTTPS é o padrão.

  Limpe esta configuração para usar HTTP.

  Atenção: Ao usar HTTP, as credenciais do usuário Windows são enviadas pela rede *sem* criptografia e podem ser facilmente exibidos usando ferramentas de solução de problemas de rede disponíveis com frequência.

- Selecione **Mostrar drivers de dispositivo para hardware instalado** para listar apenas drivers de dispositivo para hardware gerenciado.

  Desmarque essa configuração para listar todos os drivers de dispositivo em cada UpdateXpress System Packs (UXSPs) importado listado.

  Importante: Depois de selecionar essa opção, você deve executar uma verificação de conformidade clicando no ícone **Verificar Conformidade** ( ) na página Atualizações de drivers do Windows: Aplicar.

Etapa 4. Clique em **OK** para fechar a caixa de diálogo.

Aplicando drivers de dispositivo Windows

É possível aplicar drivers de dispositivo a servidores gerenciados que estejam executando o Windows.

Antes de iniciar

- Lenovo XClarity Administrator usa a escuta do Serviço de Gerenciamento Remoto do Windows (WinRM) sobre HTTPS ou HTTP para executar comandos de atualização de driver de dispositivo em sistemas Windows de destino. O serviço WinRM deve ser configurado corretamente nos servidores de destino antes de tentar atualizar drivers de dispositivo do SO (consulte Configurando o Windows Server para atualizações de driver de dispositivo do SO).
- Os dispositivos sem suporte não podem ser selecionados para atualizações.

- Leia as considerações sobre a atualização de drivers de dispositivo antes de tentar atualizar os drivers em seus servidores gerenciados (consulte Considerações sobre atualização de drivers de dispositivo do SO).
- Verifique se o repositório contém o UXSPs e os drivers de dispositivo que você pretende implantar (consulte Baixando drivers de dispositivo Windows).

  Nota: Quando o XClarity Administrator for instalado, o catálogo de produtos e o repositório estarão vazios.
- O XClarity Administrator pode usar a escuta do Serviço de Gerenciamento Remoto do Windows (WinRM) sobre HTTPS ou HTTP para executar comandos de atualização de driver de dispositivo em sistemas Windows de destino. HTTPS é o padrão. Para usar HTTP, clique em **Todas as Ações → Configurações Globais** na página Atualizações de driver do Windows: Aplicar e, em seguida, desmarque **Usar HTTPS para atualizações de driver do Windows**.

  Atenção: Ao usar HTTP, as credenciais do usuário Windows são enviadas pela rede *sem* criptografia e podem ser facilmente exibidos usando ferramentas de solução de problemas de rede disponíveis com frequência.

  Importante:

  – Certifique-se de que o Gerenciamento Remoto do Windows (WinRM) no servidor de destino esteja configurado para usar a mesma configuração (HTTPS ou HTTP) que está definida no XClarity Administrator (consulte Configurando o Windows Server para atualizações de driver de dispositivo do SO).

  – Garanta que o WinRM no servidor de destino esteja configurado com autenticação básica.

  – Ao usar HTTPS, certifique-se de que o WinRM no servidor de destino esteja configurado com **allowUnencrypted=false**.
- Verifique se o PowerShell tem suporte no servidor de destino.
- Certifique-se de que o servidor de destino esteja ligado antes de tentar atualizar drivers de dispositivo. Se o servidor não estiver ligado, selecione o servidor de destino e clique em **Todas as Ações → Ações de Energia → Ligar**.
- Certifique-se de que o XClarity Administrator tenha informações necessárias para acessar o sistema operacional do host (consulte Gerenciando o acesso a sistemas operacionais em servidores gerenciados.
- Se você deseja usar uma conta de domínio ao atualizar drivers de dispositivo do SO, certifique-se de ter criado o arquivo de configuração necessário (consulte Configurando uma conta de domínio para atualizações de drivers de dispositivo do SO).
- Certifique-se de que nenhum trabalho esteja em execução atualmente no servidor de destino. Você não pode atualizar drivers de dispositivo em um servidor gerenciado bloqueado por um trabalho em execução. Se houver outro trabalho de atualização em execução no servidor de destino, esse trabalho de atualização será colocado na fila até o término do trabalho de atualização atual. Para ver uma lista de trabalhos ativos, clique em **Monitoramento → Trabalhos**.

Sobre esta tarefa

O XClarity Administrator atualiza apenas os drivers de dispositivo que estão fora de conformidade. Os drivers de dispositivo estarão fora de conformidade quando a versão no servidor for anterior à versão no UXSP selecionado. Os drivers de dispositivo que são iguais ou posterior à versão no UXSP selecionado são ignorados.

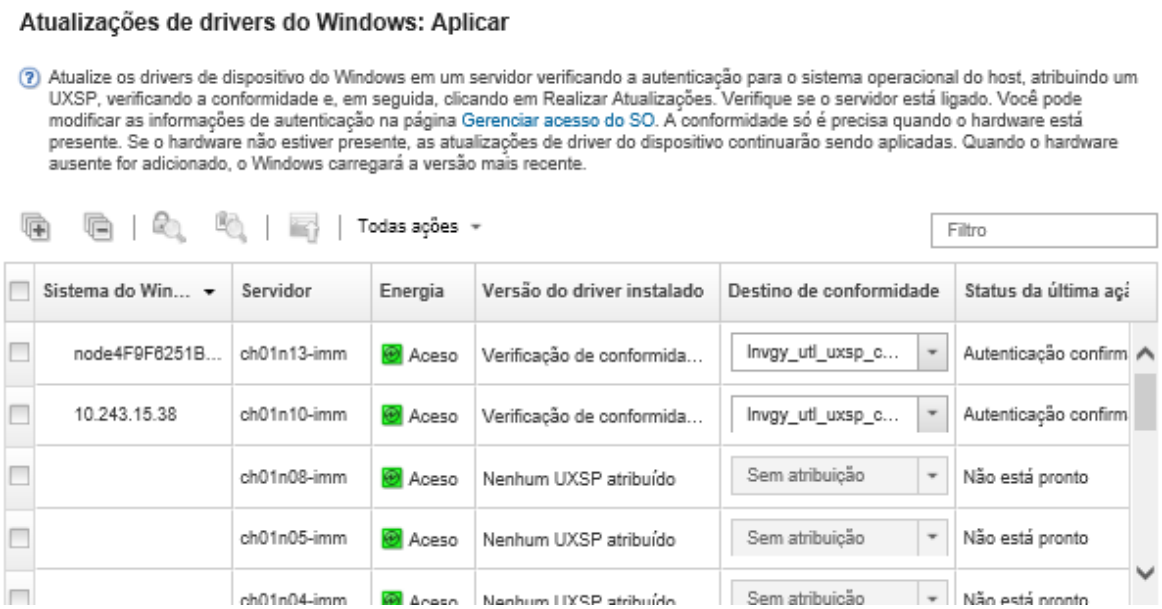
Procedimento

Para aplicar drivers de dispositivo Windows a servidores gerenciados, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Atualizações de drivers do Windows: Aplicar** para exibir a página Atualizações de drivers de dispositivo: Aplicar.

Importante:

- Para descobrir os drivers de dispositivo no servidor de destino e determinar a conformidade, você deve selecionar o servidor de destino e executar a verificação de conformidade. Depois que a verificação de conformidade for executada pela primeira vez, você poderá expandir a linha para ver uma lista de drivers de dispositivo no servidor de destino.
- A coluna **Sistema Windows** identifica o nome do host ou o endereço IP do sistema operacional do host.
- A coluna **Servidor** identifica o nome e o endereço IP do servidor gerenciado.



Etapa 2. Selecione um ou mais servidores de destino e drivers de dispositivo.

É possível classificar as colunas da tabela para facilitar a localização dos servidores específicos. Além disso, é possível filtrar a lista de servidores exibidos digitando texto (como um nome ou endereço IP) no campo **Filtro**.

Dica:

- É possível optar por atualizar todos os drivers de dispositivo para um sistema operacional específico ou expandir um sistema operacional e optar por atualizar apenas dispositivos específicos
- A coluna **Status da atualização** mostra o status de autenticação para cada servidor e o status de atualização para cada driver de dispositivo.
- A coluna **Credencial do SO** mostra a credencial armazenada que é usada para autenticar o sistema operacional (por exemplo, "901 – company\USER1."

  Se as credenciais do SO não estiverem definidas para o sistema operacional do host no servidor de destino, a caixa de diálogo Editar Credenciais do SO será exibida. Para um único servidor de destino, especifique o nome do usuário e a senha que você deseja usar para essa operação. Para vários servidores de destino, selecione a credencial armazenada a ser usada para cada servidor. Em seguida, clique em **Salvar**.

Nota: As credenciais do SO selecionadas na caixa de diálogo Editar Credenciais do SO não são salvas para o sistema operacional do host. Para salvar as credenciais do SO, consulte Gerenciando o acesso a sistemas operacionais em servidores gerenciados.

Etapa 3. Clique no ícone **Verificar autenticação** () para executar verificações de autenticação e pré-requisitos.

O XClarity Administrator se conecta ao sistema operacional do host usando as credenciais armazenadas listadas na coluna **Credencial do SO**, determina a versão do SO, verifica se o WinRM está ativado, executa verificações de pré-requisitos adicionais e desconecta-se do sistema operacional do host.

Para obter informações sobre como alterar a credencial armazenada do sistema operacional do host, consulte Gerenciando o acesso a sistemas operacionais em servidores gerenciados.

Etapa 4. Para cada servidor de destino, selecione o UXSP de destino que você deseja usar para atualizar drivers de dispositivo da coluna **Destino de Conformidade**.

Etapa 5. Selecione os servidores de destino novamente e clique no ícone **Verificar Conformidade** () para verificar a conformidade de cada driver de dispositivo.

A verificação de conformidade atualiza o status de conformidade na coluna **Versão do driver instalada**. Essa coluna exibe o status de conformidade geral do servidor e o status da versão instalada e de conformidade para cada driver de dispositivo conforme medido em relação ao UXSP atribuído.

- **Conforme**. O driver de dispositivo instalado é igual ou posterior à versão no UXSP atribuído.
- **Não conforme**. O driver de dispositivo instalado é anterior à versão no UXSP atribuído. É possível clicar no link para obter mais informações sobre a não conformidade.

Nota: A conformidade com driver de dispositivo só é precisa quando o hardware está presente. Se o hardware não estiver presente, os drivers de dispositivo continuarão sendo aplicados ao servidor. Quando o hardware ausente for adicionado ao servidor, o Windows carregará a versão mais recente.

Etapa 6. Clique no ícone **Realizar Atualizações** ().

Etapa 7. Selecione uma das regras de atualização a seguir.

- **Interromper todas as atualizações em caso de erro**. Se ocorrer um erro ao atualizar qualquer um dos drivers de dispositivo em um dispositivo de destino, o processo de atualização será interrompido para todos os dispositivos de destino no trabalho de atualização de driver de dispositivo atual. Nesse caso, nenhuma das atualizações de driver de dispositivo no UXSP do dispositivo de destino é aplicada. O driver de dispositivo atual que estiver instalado em todos os dispositivos de destino permanecerá em vigor.
- **Continuar em caso de erro**. Se ocorrer um erro ao atualizar qualquer um dos drivers de dispositivo no dispositivo de destino, o processo de atualização não atualizará o driver desse dispositivo específico. Entretanto, o processo de atualização continuará a atualizar os outros drivers no dispositivo e todos os outros dispositivos de destino no trabalho de atualização de driver de dispositivo atual.
- **Continuar para o próximo sistema em caso de erro**. Se ocorrer um erro ao atualizar qualquer um dos drivers no dispositivo, o processo de atualização de interromperá todas as tentativas de atualizar os drivers desse dispositivo específico, portanto, os drivers de dispositivo atuais que estiverem instalados nesse dispositivo permanecerão em vigor. O processo de atualização

continuará a atualizar todos os outros dispositivos no trabalho de atualização de driver de dispositivo atual.

Etapa 8. Clique em **Realizar Atualizações** para atualizar imediatamente ou clique em **Programação** para programar a execução dessa atualização para mais tarde.

Depois de concluir

Ao aplicar uma atualização, se o servidor de destino não entrar no modo de manutenção, tente aplicar a atualização novamente.

Se as atualizações não tiverem sido concluídas com êxito, consulte Considerações sobre atualização de drivers de dispositivo do SO para obter soluções de problemas e ações corretivas.

Na página Atualizações de drivers do Windows: Aplicar, é possível realizar as seguintes ações.

- Exibir o status da atualização do driver de dispositivo diretamente na página Aplicar na coluna **Atualizar status**.
- Monitorar o status da atualização do driver de dispositivo no log de trabalhos. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Trabalhos**.

  Para obter mais informações sobre o log de trabalhos, consulte Monitorando trabalhos.

  Quando o trabalho de atualização for concluído, você poderá verificar se os dispositivos estão em conformidade na página Atualizações de drivers do Windows: Aplicar. A versão atual do driver que está ativa em cada dispositivo é listada na coluna **Versão do driver instalada**.

Capítulo 15. Instalando sistemas operacionais em servidores bare-metal

É possível usar o Lenovo XClarity Administrator para gerenciar o Repositório de imagens do SO e implantar imagens do sistema operacional em até 28 servidores bare-metal ao mesmo tempo.

Saiba mais:
- XClarity Administrator: bare metal para cluster
- XClarity Administrator: implantação do sistema operacional

Antes de iniciar

Após o teste gratuito de 90 dias, é possível continuar a usar o XClarity Administrator para gerenciar e monitorar seu hardware gratuitamente; entretanto, você deve comprar licenças de habilitação com funcionalidade completa para cada servidor que ofereça suporte a funções avançadas do XClarity Administrator para continuar a usar a função de implantação do SO. O Lenovo XClarity Pro fornece direito ao serviço e suporte e a licença de habilitação com funcionalidade completa. Para obter mais informações sobre a aquisição do Lenovo XClarity Pro, entre em contato com seu representante Lenovo ou o parceiro de negócios autorizado. Para obter mais informações, consulte Instalando a licença de habilitação com funcionalidade completa na documentação online do XClarity Administrator.

Sobre esta tarefa

O XClarity Administrator fornece uma maneira simples de implantar imagens de sistema operacional em servidores *bare-metal*, que normalmente não têm um sistema operacional instalado.

Atenção: Se você implantar um sistema operacional em um servidor que possui um sistema operacional, o XClarity Administrator executará uma instalação nova que substitui as partições nos discos de destino

Vários fatores determinam a quantidade de tempo necessária para implantar um sistema operacional em um servidor:

- A quantia de RAM instalada no servidor, o que afeta quanto tempo o servidor leva para iniciar.
- O número e os tipos de adaptadores de E/S instalados no servidor, o que afeta o tempo gasto para o XClarity Administrator executar um inventário do servidor. Isso também afeta o tempo gasto para o firmware UEFI ser iniciado quando o servidor é iniciado. Durante a implantação do sistema operacional, o servidor é reiniciado várias vezes.
- Tráfego de rede. O XClarity Administrator baixa a imagem do sistema operacional na rede de dados ou na rede de implantação do sistema operacional.
- A configuração de hardware no host em que o dispositivo virtual do Lenovo XClarity Administrator está instalado. A quantia de RAM, processadores e armazenamento de disco rígido pode afetar os tempos de download.

Importante: Para implantar uma imagem do sistema operacional do XClarity Administrator, pelo menos uma das interfaces do XClarity Administrator (Eth0 ou Eth1) deve ter conectividade de rede IP com a interface de rede do servidor que é usada para acessar o sistema operacional do host. A implantação do sistema operacional usa a interface que é definida na página Acesso à Rede. Para obter mais informações sobre configurações de rede, consulte Configurando o acesso à rede.

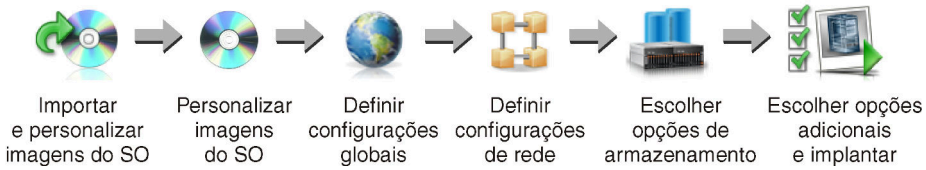
Antes de executar uma implantação do sistema operacional bare-metal em um servidor, prepare o servidor atualizando o firmware para os níveis mais recentes e configurando o servidor usando Padrões de

Configuração. Para obter mais informações, consulte Atualizando firmware em dispositivos gerenciados e Configurando servidores com padrões de configuração.

Atenção: É recomendado *não* usar o XClarity Administrator para executar uma implantação do sistema operacional bare-metal em dispositivos Converged e ThinkAgile.

Procedimento

A figura a seguir ilustra o fluxo de trabalho para implantar uma imagem do SO em um servidor.



Etapa 1. **Importe imagens do SO.**

Antes de implantar uma imagem do SO em um servidor, primeiro você deve importar o sistema operacional para o repositório. Quando você importa uma imagem do SO, o XClarity Administrator:

- Verifica se há espaço suficiente no Repositório de imagens do SO antes de importar o sistema operacional. Se você não tiver espaço suficiente para importar uma imagem, exclua uma imagem existente do repositório e tente importar novamente a nova imagem.
- Cria um ou mais perfis dessa imagem e armazena o perfil no Repositório de imagens do SO. Cada *perfil* inclui a imagem do SO e opções de instalação. Para obter informações adicionais sobre perfis predefinidos de imagem do SO, consulte Perfis de imagem do sistema operacional.

Um *sistema operacional de base* é a imagem do SO completa que foi importada para o repositório de imagens do SO. A imagem de base importada contém perfis predefinidos que descrevem as configurações de instalação para essa imagem. Você pode criar perfis personalizados na imagem de base do SO que podem ser implantados para configurações específicas.

Você também pode importar *sistemas operacionais personalizados* compatíveis. Essa imagem personalizada contém um perfil de marcador predefinido, que não pode ser implantado. Você deve importar um perfil personalizado que pode ser implantado ou criar seu próprio perfil personalizado com base no perfil de marcador. Depois que o perfil personalizado é adicionado, o perfil de marcador é removido automaticamente.

Para o Microsoft Windows Server 2016 e 2019, é possível importar uma imagem do sistema operacional personalizada para cada versão. A imagem de base importada contém perfis predefinidos que descrevem as configurações de instalação para essa imagem. Não é possível criar perfis personalizados na imagem do SO personalizada.

Para obter uma lista de sistemas operacionais de base e personalizados suportados, consulte Sistemas operacionais com suporteSistemas operacionais suportados na documentação online do Lenovo XClarity Administrator.

Etapa 2. **(Opcional) Personalize a imagem do SO.**

Você pode personalizar uma imagem do SO adicionando drivers de dispositivo, arquivos de inicialização (somente para Windows), definições de configuração, arquivos autônomos, scripts pós-instalação e software. Quando você personaliza uma imagem do SO de base, o XClarity

Administrator cria um perfil de imagem do SO personalizada que inclui os arquivos personalizados e opções de instalação.

O repositório de imagens do SO poderá armazenar um número ilimitado de arquivos personalizados e predefinidos, se houver espaço disponível para armazenar os arquivos.

Etapa 3. **Defina configurações globais.**

As configurações globais são opções de configuração que servem como padrões para implantação do sistema operacional. É possível definir as seguintes configurações globais.

- A senha da conta de usuário administrador a ser usada para implantar os sistemas operacionais
- O método a ser usado para atribuir endereços IP a servidores
- Chaves de licença para usar ao ativar sistemas operacionais instalados
- A opção de ingressar em um domínio do Active Directory como parte da implantação do sistema operacional Windows

Etapa 4. **Defina configurações de rede.**

É possível especificar as configurações de rede para cada servidor no qual os sistemas operacionais serão implantados.

Se estiver usando DHCP para atribuir endereços IP dinamicamente, você deverá configurar o endereço MAC.

Se estiver usando endereços IP estáticos, você deverá definir as configurações de rede a seguir para um servidor específico antes de implantar um sistema operacional nesse servidor. Após a definição dessas configurações, o status de implantação das alterações do servidor muda para "Pronto". (Observe que alguns campos não ficarão disponíveis para endereços IPv6 estáticos.)

- Nome do Host

  O nome do host deve obedecer as seguintes regras:
  - O nome do host de cada servidor gerenciado deve ser exclusivo.
  - O nome do host pode conter cadeias de caracteres (rótulos) separadas por um ponto (.).
  - Cada rótulo pode conter letras ASCII, dígitos e traços (-). No entanto, a string não pode começar ou terminar com um traço e não pode conter apenas dígitos.
  - O primeiro rótulo pode ter de 2 a 15 caracteres. Os rótulos subsequentes podem ter de 2 a 63 caracteres.
  - O comprimento total do nome do host deve ter no máximo 255 caracteres.
- Endereço MAC da porta no host em que o sistema operacional será instalado.

  O endereço MAC é definido como AUTO por padrão. Essa definição automaticamente detecta as portas Ethernet que podem ser configuradas e usadas para implantação. O primeiro endereço MAC (porta) detectado é usado por padrão. Se a conectividade for detectada em um endereço MAC diferente, o host do XClarity Administrator será reiniciado automaticamente para usar o endereço MAC recém-detectado para a implantação.

  É possível determinar o status da porta de endereço MAC usada para a implantação do SO no menu da lista suspensa **Endereço MAC** na caixa de diálogo Configurações de Rede. Se várias portas estiverem ativas ou se todas as portas estiverem desativadas, AUTO será usado por padrão.

  Notas:

  - Não há suporte para portas de rede virtual. Não use uma porta de rede física para simular várias portas de rede virtual.

  - Quando a configuração de rede do servidor é definida como AUTOMÁTICO, o XClarity Administrator pode detectar automaticamente as portas de rede nos slots 1 – 16. Pelo menos uma porta nos slots 1 – 16 deve ter uma conexão com XClarity Administrator.
  - Se você quiser usar uma porta de rede no slot 17 ou superior para o endereço MAC, não poderá usar AUTOMÁTICO. Em vez disso, você deve definir a configuração de rede do servidor como o endereço MAC da porta específica que você deseja usar.
  - Para os servidores ThinkServer, nem todos os endereços MAC de host são exibidos. Na maioria dos casos, os endereços MAC para adaptadores Ethernet AnyFabric são listados na caixa de diálogo Editar Configurações de Rede. Os endereços MAC para outros adaptadores Ethernet (como Lan-On-Motherboard) não são listados. Quando o endereço MAC de um adaptador não estiver disponível, use o método AUTO para implantações não VLAN.
- Endereço IP e máscara de sub-rede
- Gateway de IP
- Até dois servidores de Sistema de Nomes de Domínio (DNS)
- Velocidade da Unidade de Transmissão Máxima (MTU)
- ID da VLAN, se o modo IP da VLAN estiver habilitado

Se você optar por usar VLANs, poderá atribuir um ID de VLAN ao adaptador de rede do host que está sendo configurado.

Etapa 5. **Escolha as opções de armazenamento**

Para cada implantação, você pode escolher o local de armazenamento preferencial onde o sistema operacional deve ser implantado. Dependendo do sistema operacional, você pode optar pode implantar uma unidade de disco local, chave do hipervisor integrado ou SAN.

Etapa 6. **Escolha opções adicionais ce configurações personalizadas e implante a imagem do SO.**

É possível configurar opções de implantação adicionais, como chave de licença para a implantação do SO, e configurações personalizadas. Se você estiver instalando o Microsoft Windows, também poderá configurar o domínio do Active Directory a ser incluído.

Notas:

- Se você tiver definido configurações personalizadas para um perfil personalizado específico do SO, deverá definir valores para as configurações personalizadas necessárias antes de implantar o perfil em um servidor.
- Ao implantar um perfil do SO personalizado que inclui as configurações personalizadas, todos os servidores de destino devem usar o mesmo perfil personalizado do SO, e os valores das configurações personalizadas se aplicam a todos os servidores de destino.

Em seguida, escolha os servidores de destino da implantação e as imagens do SO a serem implantadas. Lembre-se de que para implantar um sistema operacional, o servidor deve ter um status de implantação de "Pronto".

É possível implantar imagens do sistema operacional em até 28 servidores ao mesmo tempo.

Antes de tentar implantar uma imagem do sistema operacional, revise Considerações sobre implantação do sistema operacional.

Considerações sobre implantação do sistema operacional

Antes de tentar implantar uma imagem do sistema operacional, revise as seguintes considerações.

Considerações sobre o Lenovo XClarity Administrator

- Certifique-se de que nenhum trabalho esteja em execução atualmente no servidor de destino. Para ver uma lista de trabalhos ativos, clique em **Monitoramento → Trabalhos**.
- Certifique-se de que o servidor de destino não tenha um padrão de servidor adiado ou ativado parcialmente. Se um padrão de servidor foi adiado ou ativado parcialmente no servidor gerenciado, você deve reiniciar o servidor para aplicar todas as definições de configuração. Não tente implantar um sistema operacional em um servidor com um padrão de servidor ativado parcialmente. Para determinar o status de configuração do servidor, consulte o campo **Status de Configuração** na página Resumo do servidor gerenciado (consulte Visualizando os detalhes de um servidor gerenciado).
- Certifique-se de que a senha para a conta de administrador que deve ser usada para implantar o sistema operacional esteja especificada na caixa de diálogo Configurações Globais: Implantar Sistemas Operacionais. Para obter mais informações sobre como configurar a senha, consulte Definindo configurações de implantação de SO globais.
- Certifique-se de que as configurações globais padrão estejam corretas para esta implantação do sistema operacional (consulte Definindo configurações de implantação de SO globais).

Considerações sobre o sistema operacional

- Certifique-se de ter todas as licenças do sistema operacional aplicáveis para ativar os sistemas operacionais instalados. Você é responsável por obter licenças diretamente do fabricante do sistema operacional.
- Assegure-se de que a imagem do sistema operacional que você pretende implantar já esteja carregada no Repositório de imagens do SO. Para obter informações sobre como importar imagens, consulte Importando imagens do sistema operacional.
- Imagens do sistema operacional no repositório XClarity Administrator podem não ter suporte apenas certas plataformas de hardware. Apenas os perfis de imagem do SO que são aceitos pelo servidor selecionado são listados na página Implantar Imagens de SO. É possível determinar se um sistema operacional é compatível com um servidor específico no Site do guia de interoperabilidade do SO da Lenovo.
- No Windows, você deve importar um arquivo de inicialização para o repositório de imagens do SO para que você possa implantar um perfil do Windows. A Lenovo reúne o arquivo de inicialização WinPE_64.wim predefinido junto com um conjunto de drivers de dispositivo em um único pacote que pode ser baixado no Página da Web dos drivers do Lenovo Windows e do repositório de imagens do WinPE e, em seguida, importado para o repositório de imagens do SO. Como o arquivo do pacote contém drivers de dispositivo e arquivos de inicialização, é possível importar o arquivo do pacote da guia **Driver de Dispositivo** ou **Arquivos de Inicialização**.
- No SLES 15 e 15 SP1, você deve importar a imagem do instalador e a imagem do pacote associado do Página da Web Centro de suporte do sistema operacional do servidor. Para o SLES 15 SP2 ou posterior, é necessário importar apenas a imagem de mídia de instalação completa porque os DVDs do Instalador Unificado e pacotes do SUSE Linux Enterprise Server 15 e 15 SP1 foram substituídos.
- Para servidores ThinkSystem, XClarity Administrator inclui os drivers de dispositivo para permitir a instalação do sistema operacional, bem como configuração básica de rede e de armazenamento para o sistema operacional final. Para outros servidores, certifique-se de que a imagem do sistema operacional que você pretende implantar inclua os drivers de dispositivo Ethernet, Fibre Channel e adaptador de armazenamento apropriados para seu hardware. Se o driver de dispositivo do adaptador de E/S não está incluído no sistema operacional, o adaptador não é suportado para implantação do SO. Sempre instale o sistema operacional mais recente para garantir que tenha os drivers de dispositivo do adaptador de E/S de caixa de entrada mais recentes e os arquivos de inicialização necessários. É possível também incluir os drivers de dispositivo predefinidos e arquivos de inicialização para os sistemas operacionais que foram importados para o XClarity Administrator (consulte Personalizando perfis de imagem do SO na documentação online do XClarity Administrator).

Para o VMware, use a última Imagem Personalizada da Lenovo para ESXi, que inclui suporte para os adaptadores mais recentes. Para informações sobre como obter essa imagem, consulte Suporte VMware – Página da Web de downloads.

- Para servidores ThinkSystem, se desejar implantar o SLES 12 SP2, use um perfil kISO. Para obter os perfis de kISO, você deve importar a imagem kISO SLES apropriada depois de importar o sistema operacional SLES de base. Você pode baixar a imagem kISO do SLES do Suporte Linux – Página da Web de downloads.

  Notas:

  – A imagem de SLES kISO conta para o número máximo de imagens de sistema operacional importadas.

    Para obter uma lista de sistemas operacionais de base e personalizados suportados, consulte Sistemas operacionais com suporteSistemas operacionais suportados na documentação online do Lenovo XClarity Administrator.

  – Se você excluir todos os perfis kISO, exclua o sistema operacional SLES de base e, em seguida, importe a imagem kISO e do sistema operacional de base novamente para implantar o SLES 12 SP2 em um servidor ThinkSystem.

  – Se você criar um perfil de SO personalizado com base em um perfil kISO, os drivers de dispositivo predefinidos no sistema operacional de base não serão incluídos. Os drivers de dispositivo que estão incluídos no kISO serão usados. É possível também incluir os drivers de dispositivo para o perfil de SO personalizado (consulte Criando um perfil da imagem do SO personalizada).

Para obter mais informações sobre limitações para sistemas operacionais específicos, consulte Sistemas operacionais suportados.

Considerações de rede

- Certifique-se de que todas as portas necessárias estejam abertas (consulte Disponibilidade da porta para sistemas operacionais implantados).
- Certifique-se de que o XClarity Administrator possa se comunicar com o servidor de destino (o Baseboard Management Controller e a rede de dados do servidor) pela interface (Eth0 ou Eth1) que foi selecionada quando você configurou o acesso de rede do XClarity Administrator.

  Para especificar uma interface a ser usada para implantação do sistema operacional, consulte Configurando o acesso à rede.

  Para obter mais informações sobre a rede de implantação do sistema operacional e interfaces, consulte Considerações de rede na documentação online do XClarity Administrator.
- Verifique se os endereços IP são exclusivos para o sistema operacional do host. O XClarity Administrator verifica se há endereços IP duplicados especificados para o endereço de rede durante o processo de implantação.
- Se a rede estiver lenta ou instável, você poderá ter resultados imprevisíveis ao implantar sistemas operacionais.
- A interface de rede do XClarity Administrator usada para gerenciamento deve ser configurada para conectar-se a baseboard management controller usando o mesmo método de endereço IP escolhido na caixa de diálogo Configurações Globais: Implantar Sistemas Operacionais. Por exemplo, se o XClarity Administrator é configurado para usar eth0 para o gerenciamento, e você optar por usar endereços IPv6 estáticos atribuídos manualmente ao configurar o SO implantado, o eth0 deve ser configurado com um endereço IPv6 que tenha conectividade com o baseboard controlador de gerenciamento.
- Se você optar por usar endereços IPv6 para as configurações globais de implantação de SO, o endereço IPv6 para XClarity Administrator deverá ser roteado para o baseboard management controller e rede de dados nos servidores.

- O modo IPv6 não é compatível com o ThinkServer (consulte Limitações de configuração IPv6 na documentação online do XClarity Administrator).
- Se estiver usando DHCP para atribuir endereços IP dinamicamente, você deverá configurar o endereço MAC.
- Se estiver usando endereços IP estáticos, você deverá definir as configurações de rede a seguir para um servidor específico antes de implantar um sistema operacional nesse servidor. Após a definição dessas configurações, o status de implantação das alterações do servidor muda para "Pronto". (Observe que alguns campos não ficarão disponíveis para endereços IPv6 estáticos.)
  - Nome do Host

    O nome do host deve obedecer as seguintes regras:
    - O nome do host de cada servidor gerenciado deve ser exclusivo.
    - O nome do host pode conter cadeias de caracteres (rótulos) separadas por um ponto (.).
    - Cada rótulo pode conter letras ASCII, dígitos e traços (-). No entanto, a string não pode começar ou terminar com um traço e não pode conter apenas dígitos.
    - O primeiro rótulo pode ter de 2 a 15 caracteres. Os rótulos subsequentes podem ter de 2 a 63 caracteres.
    - O comprimento total do nome do host deve ter no máximo 255 caracteres.
  - Endereço MAC da porta no host em que o sistema operacional será instalado.

    O endereço MAC é definido como AUTO por padrão. Essa definição automaticamente detecta as portas Ethernet que podem ser configuradas e usadas para implantação. O primeiro endereço MAC (porta) detectado é usado por padrão. Se a conectividade for detectada em um endereço MAC diferente, o host do XClarity Administrator será reiniciado automaticamente para usar o endereço MAC recém-detectado para a implantação.

    É possível determinar o status da porta de endereço MAC usada para a implantação do SO no menu da lista suspensa **Endereço MAC** na caixa de diálogo Configurações de Rede. Se várias portas estiverem ativas ou se todas as portas estiverem desativadas, AUTO será usado por padrão.

    Notas:

    - Não há suporte para portas de rede virtual. Não use uma porta de rede física para simular várias portas de rede virtual.
    - Quando a configuração de rede do servidor é definida como AUTOMÁTICO, o XClarity Administrator pode detectar automaticamente as portas de rede nos slots 1 – 16. Pelo menos uma porta nos slots 1 – 16 deve ter uma conexão com XClarity Administrator.
    - Se você quiser usar uma porta de rede no slot 17 ou superior para o endereço MAC, não poderá usar AUTOMÁTICO. Em vez disso, você deve definir a configuração de rede do servidor como o endereço MAC da porta específica que você deseja usar.
    - Para os servidores ThinkServer, nem todos os endereços MAC de host são exibidos. Na maioria dos casos, os endereços MAC para adaptadores Ethernet AnyFabric são listados na caixa de diálogo Editar Configurações de Rede. Os endereços MAC para outros adaptadores Ethernet (como Lan-On-Motherboard) não são listados. Quando o endereço MAC de um adaptador não estiver disponível, use o método AUTO para implantações não VLAN.
  - Endereço IP e máscara de sub-rede
  - Gateway de IP
  - Até dois servidores de Sistema de Nomes de Domínio (DNS)
  - Velocidade da Unidade de Transmissão Máxima (MTU)
  - ID da VLAN, se o modo IP da VLAN estiver habilitado
- Se você optar por usar VLANs, poderá atribuir um ID de VLAN ao adaptador de rede do host que está sendo configurado.

Para obter mais informações sobre a rede de implantação do sistema operacional e interfaces, consulte Definindo as configurações de rede para servidores gerenciados e Definindo as configurações de rede para servidores gerenciados e Considerações de rede na documentação online do XClarity Administrator.

Considerações de armazenamento e opções de inicialização

- Certifique-se de que a opção de inicialização UEFI no servidor de destino esteja configurada como "Apenas inicialização UEFI" antes de implantar um sistema operacional. As opções de inicialização "Apenas legado" e "UEFI primeiro, depois legado" não são suportadas para implantação do sistema operacional.
- Cada servidor deve ter um adaptador RAID de hardware instalado e configurado.

  Atenção:

  – Somente o armazenamento configurado com RAID de hardware é suportado.

  – O RAID do software que geralmente está presente no adaptador de armazenamento Intel SATA integrado ou que é configurado como JBOD não é suportado. No entanto, se um adaptador RAID de hardware não estiver presente, configurar o adaptador SATA no **Modo AHCI SATA** habilitado para implantação do sistema operacional ou configurar discos bons não configurados como JBOD poderá funcionar em alguns casos. Para obter mais informações, consulte O instalador do SO não pode localizar o disco no qual você deseja instalar o XClarity Administrator na documentação online do XClarity Administrator.

    Essa exceção não se aplica a unidades M.2.

  – Se um dispositivo gerenciado tiver ambas as unidades locais (SATA, SAS ou SSD) que não são configuradas para RAID de hardware e unidades M.2, você deverá desabilitar as unidades locais se desejar usar unidades M.2 ou deverá desabilitar as unidades M.2 se desejar usar unidades locais. É possível desativar dispositivos do controlador de armazenamento integrado e ROMs de opção de armazenamento legada e UEFI usando Padrões de Configuração, selecionando Desabilitar disco local na guia Armazenamento Local do assistente ou criando um Padrão de Configuração de um servidor existente e, em seguida, desativando dispositivos M.2 no padrão de UEFI estendida.

  – Se um adaptador SATA estiver ativado, o modo SATA *não deverá* ser configurado como "IDE."
- O armazenamento NVMe que é conectado à placa-mãe do servidor ou controlador HBA não tem suporte e não deve ser instalado no dispositivo; caso contrário, a implantação do SO em armazenamento não NVMe falhará.
- Ao implantar o RHEL, várias portas conectadas ao mesmo LUN no armazenamento de destino não são suportadas.
- Certifique-se que o modo de inicialização seguro esteja desabilitado para o servidor. Se estiver implantando um sistema operacional habilitado para o modo de inicialização seguro (como o Windows), desabilite o modo de inicialização seguro, implante o sistema operacional e então habilite novamente o modo de inicialização seguro.
- Ao implementar o Microsoft Windows em um servidor, as unidades conectadas não devem ter partições do sistema existentes (consulte A implantação do SO falha devido a partições do sistema existentes em uma unidade de disco conectada na documentação online do XClarity Administrator).
- Para servidores ThinkServer, assegure que os seguintes requisitos sejam atendidos:

  – As configurações de inicialização no servidor devem incluir uma Política de OpROM de Armazenamento que é configurada para `UEFI Only`. Para obter mais informações, consulte O instalador do SO não pode ser inicializado em um servidor ThinkServer – XClarity Administrator na documentação online do XClarity Administrator.

  – Se estiver implantando o ESXi e houver adaptadores de rede inicializáveis em PXE, desabilite o suporte para PXE nesses adaptadores de rede antes de implantar o sistema operacional. A implantação será concluída, e você poderá reabilitar o suporte para PXE se desejar.

– Se estiver implantando o ESXi e houver dispositivos inicializáveis na lista de ordem de inicialização além da unidade na qual o sistema operacional deve ser instalado, remova-os dessa lista antes de implantar o sistema operacional. Após a conclusão da implantação, você poderá voltar a adicionar o dispositivo inicializável à lista. Certifique-se de que a unidade instalada esteja no topo da lista.

Para obter mais informações sobre as configurações de local de armazenamento, consulte Escolhendo o local de armazenamento para servidores gerenciados.

Considerações sobre dispositivo gerenciado

- Para obter informações sobre as limitações de implantação do sistema operacional para dispositivos específicos, consulte Página da Web Suporte do XClarity Administrator – Compatibilidade, clique na guia **Compatibilidade** e, em seguida, clique no link para os tipos de dispositivo apropriados.
- Certifique-se de que não há nenhuma mídia montada (como ISOs) no servidor de destino. Além disso, certifique-se de que não haja nenhuma sessão de mídia remota ativa abertas para o controlador de gerenciamento.
- Certifique-se de que o carimbo de data/hora no BIOS esteja definido para a data e a hora atuais.
- Para servidores com XCC2 que tenham o protetor do sistema habilitado e a ação definida para **Impedir a inicialização do SO**, o protetor do sistema deve ser compatível com o dispositivo. Se o protetor do sistema não for compatível, os dispositivos serão impedidos de concluir o processo de inicialização, o que faz com que a implantação do SO falhe. Para provisionar esses dispositivos, responda manualmente ao prompt de inicialização do protetor do sistema para permitir que os dispositivos seja inicializados normalmente.
- Para servidores ThinkSystem e System x, certifique-se de que a opção do BIOS legado esteja desativada. No utilitário de configuração BIOS/UEFI (F1), clique em **Configuração UEFI → Configurações do Sistema** e verifique se BIOS legado é definido como Desabilitado.
- Para servidores Flex System, certifique-se de que o chassi esteja ligado.
- Para servidores Converged, NeXtScale e System x, verifique se uma chave FoD (Feature on Demand) para presença remota está instalada. Você pode determinar se a presença remota está ativada, desativada ou não está instalada em um servidor na página Servidores (consulte Visualizando o status de um servidor gerenciado). Para obter mais informações sobre chaves FoD instaladas nos seus servidores, consulte Exibindo chaves do Features on Demand.
- Para servidores ThinkSystem e dispositivos ThinkAgile, o recurso XClarity Controller Enterprise é necessário para a implantação do sistema operacional. Para obter mais informações, consulte Exibindo chaves do Features on Demand.
- Para dispositivos Converged e ThinkAgile, é recomendado *não* usar o XClarity Administrator para executar uma implantação do sistema operacional bare-metal.

Sistemas operacionais suportados

O Lenovo XClarity Administrator permite a implantação de diversos sistemas operacionais. Somente as versões compatíveis dos sistemas operacionais podem ser carregadas no XClarity Administrator Repositório de imagens do SO.

Importante:

- Para obter informações sobre as limitações de implantação do sistema operacional para dispositivos específicos, consulte Página da Web Suporte do XClarity Administrator – Compatibilidade, clique na guia **Compatibilidade** e, em seguida, clique no link para os tipos de dispositivo apropriados.
- O recurso de gerenciamento criptográfico do XClarity Administrator permite limitar a comunicação com determinados modos SSL/TLS mínimos. Por exemplo, se o TLS 1.2 for selecionado, apenas os sistemas operacionais com um processo de instalação compatível com o TLS 1.2 e algoritmos criptográficos fortes poderão ser implantados por meio do XClarity Administrator.

- Imagens do sistema operacional no repositório XClarity Administrator podem não ter suporte apenas certas plataformas de hardware. Apenas os perfis de imagem do SO que são aceitos pelo servidor selecionado são listados na página Implantar Imagens de SO. É possível determinar se um sistema operacional é compatível com um servidor específico no Site do guia de interoperabilidade do SO da Lenovo.
- Para obter informações de suporte e compatibilidade relacionadas ao sistema operacional e hipervisor, bem como recursos para servidores e soluções Lenovo, consulte o Página da Web Centro de suporte do sistema operacional do servidor.

A seguinte tabela lista os sistemas operacionais de 64 bits em que o XClarity Administrator pode ser implantado.

Sistema Operacional	Versões	Notas
CentOS Linux	7.2 and later 8.0 8.1 8.2	**Notas:** • Todas as versões secundárias existentes e futuras são compatíveis, a menos que seja indicado o contrário. • Os endereços DHCP, IPv4 estático e o IPv6 estático são suportados. • A marcação de VLAN não é compatível. • Não há suporte para os drivers não incluídos. • Não há suporte para personalização do perfil do SO. • Não há suporte para o CentOS 8.3.
Microsoft® Windows® Azure Stack HCI	20H2 21H2	Não há suporte para personalização do perfil do SO.
Microsoft Windows Client	10 21H2 10 22H2 11 22H2	
Microsoft Windows Server	2012 R2 2012 R2U1 2016 2019 2022	Cópias de licença de varejo e volume têm suporte. **Nota:** O XClarity Administrator é testado com apenas versões do Windows que são suportadas pela Microsoft no lançamento da versão XClarity Administrator. Os itens a seguir *não têm suporte*: • Windows Reseller Option Kit (ROK) • Canal semestral do Windows Server (SAC) v1709, v1803 e v1809 • Windows Server 2019 Essentials • Windows Server 2016 Nanoserver • Cópia de avaliação Windows Server 2012 • Imagens do Windows Server em servidores gerenciados com chaves de hipervisor integrado Windows Server 2012 R2 nos servidores que contêm processadores Intel CLX Você deve remover fisicamente a chave de Embedded Hypervisor dos servidores de destino antes de implantar uma imagem Windows. Isso inclui Hyper-V por meio de um dos perfis de virtualização. – Datacenter – Núcleo de datacenter – Virtualização de datacenter (Hyper-V) – Núcleo de virtualização de datacenter (Hyper-V com núcleo) – Padrão – Núcleo padrão – Virtualização padrão (Hyper-V) – Núcleo de virtualização padrão (Hyper-V com núcleo)

Sistema Operacional	Versões	Notas
Red Hat® Enterprise Linux (RHEL) Server	6.8 and later 7.2 and later 8.x 9.x	Inclui o KVM **Notas:** • Todas as versões secundárias existentes e futuras são compatíveis, a menos que seja indicado o contrário. • Ao importar a versão de DVD da imagem do SO, apenas o DVD1 é suportado. • Ao instalar o RHEL em servidores ThinkSystem, o RHEL v7.4 ou posterior é recomendado. • Para implantar o RHEL 7.2, a atribuição de IP global deve ser definida para usar endereços IPv4. Para obter informações sobre as configurações globais, consulte Definindo configurações de implantação de SO globais. • Falhas de implementação do SO foram observadas em redes IPv6 com larguras de banda inferior devido a tempos limites no instalador do SO. • A marcação de VLAN não é compatível.
Rocky Linux	8.x 9.x	**Notas:** • Todas as versões secundárias existentes e futuras são compatíveis, a menos que seja indicado o contrário. • Os endereços DHCP, IPv4 estático e o IPv6 estático são suportados. • A marcação de VLAN não é compatível. • Não há suporte para os drivers não incluídos.
SUSE® Linux Enterprise Server (SLES)	12.x 15.x	Inclui hipervisores KVM e Xen **Notas:** • Todos os service packs existentes e futuros são compatíveis, a menos que seja indicado o contrário. • Ao importar a versão de DVD da imagem do SO, apenas o DVD1 é suportado. • Falhas de implementação do SO foram observadas em redes IPv6 com larguras de banda inferiores devido a tempos limites no instalador do SO. • Se desejar implantar o SLES 12 SP2 em um servidor ThinkSystem, use um perfil kISO. Para obter os perfis kISO, você deve importar a imagem kISO SLES apropriada. Para obter mais informações, consulte Considerações sobre implantação do sistema operacional. • No SLES 15 e 15 SP1, você deve importar a imagem do instalador e a imagem do pacote associado do Página da Web Centro de suporte do sistema operacional do servidor. Para o SLES 15 SP2 ou posterior, é necessário importar apenas a imagem de mídia de instalação completa porque os DVDs do Instalador Unificado e pacotes do SUSE Linux Enterprise Server 15 e 15 SP1 foram substituídos. • A marcação de VLAN não é compatível.

Sistema Operacional	Versões	Notas
Servidor Ubuntu	20.04.x 22.04.x	**Notas:** • A imagem pode ser instalada na opção de armazenamento selecionada (unidade de disco local, unidade M.2 ou volume FC SAN). • Todas as versões secundárias existentes e futuras são compatíveis, a menos que seja indicado o contrário. • Apenas DHCP é suportado. Os endereços IPv4 e IPv6 estáticos *não são* suportados. • A marcação de VLAN *não é* suportada. • *Não* há suporte para os drivers não incluídos. • *Não* há suporte para personalização do perfil do SO.
VMware vSphere® Hypervisor (ESXi)	5.5 5.5u1 5.5u2 5.5u3 6.0.x 6.5.x 6.7.x 7.0.x 8.0.x	Imagens do Base VMware vSphere Hypervisor (ESXi) e imagens personalizadas do Lenovo VMware ESXi são compatíveis. Imagens personalizadas do Lenovo VMware ESXi são personalizadas para um hardware selecionado para fornecer gerenciamento de plataformas online, incluindo atualização e configuração de firmware, diagnósticos de plataformas e alertas de hardware aprimorados. Ferramentas de gerenciamento Lenovo também oferecem suporte ao gerenciamento simplificado do ESXi com servidores System x selecionados. Essa imagem está disponível para download no Suporte VMware – Página da Web de downloads. A licença fornecida com a imagem é uma versão de avaliação gratuita de 60 dias. Você é responsável por cumprir todos os requisitos de licenciamento do VMware. **Importante:** • Todos os pacotes de atualização existentes e futuros são compatíveis para 6.0, 6.5, 6.7, 7.0 e 8.0, a menos que seja indicado o contrário. • Imagens de base do ESXi (sem personalização da Lenovo) incluem apenas os drivers de dispositivo básicos predefinidos para armazenamento e rede. A imagem de base não inclui os drivers de dispositivo predefinidos (que são incluídos em imagens personalizadas do Lenovo VMware ESXi). É possível incluir drivers de dispositivo predefinidos criando seus próprios perfis de imagem do sistema operacional personalizados (consulte Personalizando perfis de imagem do SO). • Para algumas versões de imagens personalizadas do Lenovo VMware ESXi, imagens separadas podem estar disponíveis para System x, ThinkSystem e ThinkServer. Somente uma imagem para uma versão específica pode existir no repositório de imagens do SO por vez. • Não há suporte para a implantação do ESXi para determinados servidores mais antigos. Para obter informações sobre quais servidores têm suporte, consulte o Site do guia de interoperabilidade do SO da Lenovo. • Há suporte para as seguintes versões dos dispositivos ThinkServer: ESXi 6.0u3, 6.5 e posterior. • Durante a instalação do ESXi 5.5 (qualquer atualização) ou 6.0 em um servidor no chassi do Flex System, o servidor poderá deixar de responder ou ser reiniciado imediatamente depois da exibição da seguinte mensagem: `Carregando image.pld` • O ESXi 5.5 requer espaço E/S de memória mapeada (MMIO) para ser configurado com os 4 GB iniciais do sistema. Dependendo da configuração, determinados sistemas tentam usar uma memória maior que 4 GB, o que pode causar uma falha. Para resolver o problema, consulte A implantação do VMware trava ou reinicia o sistema na documentação online do XClarity Administrator.

Sistema Operacional	Versões	Notas
		• Ao implantar o ESXi usando um modo IPv6 estático, o nome do host definido na página Configurações de Rede do XClarity Administrator não é configurado na instância ESXi do implantada. Em vez disso, o nome padrão `localhost` é usado. Você precisa definir manualmente o nome do host no ESXi implantado para que ele corresponda ao nome do host que está definido no XClarity Administrator. • Ao implantar o ESXi em um servidor gerenciado, o sistema operacional não move explicitamente a unidade na qual o sistema operacional está instalado para a parte superior da lista de ordem de inicialização. Se um dispositivo de inicialização que contém um SO inicializável ou um servidor PXE for especificado antes do dispositivo de inicialização que contém o ESXi, o ESXi não será inicializado. Para a implantação do ESXi, o XClarity Administrator atualiza a lista de ordem de inicialização para a maioria dos servidores, para garantir que o dispositivo de inicialização ESXi esteja na parte superior dessa lista. No entanto, os servidores ThinkServer não fornecem uma maneira para o XClarity Administrator atualizar a lista de ordem de inicialização. Você deve desabilitar o suporte para inicialização PXE ou remover dispositivos inicializáveis que não sejam a unidade de instalação antes de implantar o sistema operacional. Para obter mais informações, consulte O sistema operacional não é inicializado após ter implementado o ESXi em um servidor ThinkServer na documentação online do XClarity Administrator. **Dica:** Em vez de definir **MM Config** usando o Setup Utility de cada servidor, avalie a possibilidade de usar um dos padrões de UEFI estendida predefinidos que estão relacionados à virtualização, o que configura a opção MM Config para 3 GB e desabilita a alocação do PCI 64-Bit Resource. Para obter mais informações sobre esses padrões, consulte Definindo configurações UEFI estendidas.

Perfis de imagem do sistema operacional

Ao importar uma imagem do sistema operacional para o Repositório de imagens do SO, o Lenovo XClarity Administrator cria um ou mais perfis para essa imagem e armazena os perfis no Repositório de imagens do SO. Cada *perfil* predefinido inclui opções de imagem de SO e opções de instalação para essa imagem.

Atributos de perfil da imagem do SO

Atributos de perfil da imagem do SO fornecem informações adicionais sobre um perfil da imagem do SO. Os seguintes atributos podem ser mostrados.

- **kISO**. Use um perfil kISO para implantar o SLES 12 SP2 em um servidor ThinkSystem. Você pode baixar a imagem kISO do SLES do Suporte Linux – Página da Web de downloads.

Perfis de imagem do SO predefinida

A tabela a seguir lista os perfis predefinidos pelo XClarity Administrator quando você importa uma imagem do sistema operacional. Esta tabela lista também os pacotes que estão incluídos em cada perfil.

Você pode criar um perfil da imagem do SO personalizada para um sistema operacional de base. Para obter mais informações, consulte Personalizando perfis de imagem do SO.

Sistema Operacional	Perfil	Pacotes incluídos no perfil	
CentOS Linux	Básico	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Mínima	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Virtualização	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
Microsoft® Windows® Azure Stack HCI	Azure	<selection name="Microsoft-Hyper-V" state="true" /> <selection name="MultipathIo" state="true" /> <selection name="FailoverCluster-PowerShell" state="true" /> <selection name="FailoverCluster-FullServer" state="true" /> <selection name="FailoverCluster-CmdInterface" state="true" /> <selection name="FailoverCluster-AutomationServer" state="true" /> <selection name="FailoverCluster-AdminPak" state="true" /> <selection name="Containers" state="true" /> <selection name="MicrosoftWindowsPowerShellRoot" state="true" /> <selection name="MicrosoftWindowsPowerShell" state="true" /> <selection name="ServerManager-Core-RSAT" state="true" /> <selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />	
Microsoft Windows Client	Enterprise		
	Enterprise N		
	Workstations Pro		
	Workstations_Pro N		

Sistema Operacional	Perfil	Pacotes incluídos no perfil
Microsoft Windows Hyper-V Server 2016	Hyper_V	<selection name="Microsoft-Hyper-V" state="true" /> <selection name="MultipathIo" state="true" /> <selection name="FailoverCluster-PowerShell" state="true" /> <selection name="FailoverCluster-FullServer" state="true" /> <selection name="FailoverCluster-CmdInterface" state="true" /> <selection name="FailoverCluster-AutomationServer" state="true" /> <selection name="FailoverCluster-AdminPak" state="true" /> <selection name="MicrosoftWindowsPowerShellRoot" state="true" /> <selection name="MicrosoftWindowsPowerShell" state="true" /> <selection name="ServerManager-Core-RSAT" state="true" /> <selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />
Microsoft Windows Server **Nota:** Inclui Hyper-V com *Perfil de virtualização.*	Datacenter	GUI
	Datacenter de virtualização	GUI Hyper-V role
	Núcleo de datacenter de virtualização	Hyper-V role
	Núcleo de datacenter	
	Padrão	GUI
	Virtualização padrão	GUI Hyper-V role
	Núcleo de virtualização padrão	Hyper-V role
	Núcleo padrão	
Microsoft Windows Server Personalizado	Datacenter_ customized	
	Standard_ customized	
Red Hat Enterprise Linux (RHEL) **Nota:** Inclui o KVM	Básico	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686
	Mínima	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686

Sistema Operacional	Perfil	Pacotes incluídos no perfil	
	Virtualização	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
Rocky Linux	Básico	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Mínima	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Virtualização	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms

Sistema Operacional	Perfil	Pacotes incluídos no perfil
SUSE Linux Enterprise Server (SLES) 15	Básico e básico	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	Mínimo e mínimo	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	Virtualização KVM e Virtualização KVM	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
	Virtualização Xen e Virtualização Xen	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
Ubuntu	Mínima	Openssh-server

Sistema Operacional	Perfil	Pacotes incluídos no perfil
	Virtualização	qemu qemu-kvm libvirt-daemon libvirt-clients bridge-utils virt-manager
VMware vSphere® Hypervisor (ESXi)	Virtualização	Imagens do Base VMware vSphere Hypervisor (ESXi) e imagens personalizadas do Lenovo VMware ESXi são compatíveis.

Disponibilidade da porta para sistemas operacionais implantados

Algumas portas são bloqueadas por determinados perfis de sistema operacional. As tabelas a seguir listam as portas que devem ser abertas (desbloqueadas).

Comunicação	Perfil de virtualização RHEL, Centos e Rocky[1]	Perfis Básico e Mínimo de RHEL, Centos e Rocky[1]	SLES, virtualização, perfis Básico e Mínimo[2]	Perfis de virtualização e mínimo Ubuntu[3]	Perfil de Virtualização de VMware ESXi[4]	Perfis do Windows
Saída (portas abertas em sistemas externos)	• Comunicação com dispositivos de rede RHEL KVM – TCP e UDP nas portas **53** e **67** • Comunicação com agentes SNMP – UDP na porta **161** • Comunicação com o agente de serviço SLP, agente de diretório SLP – TCP e UDP na porta **427** • Comunicação CIM-XML sobre HTTP – TCP nas portas **15988** e **15989** • Comunicação do Servidor Virtual KVM – TCP nas portas **49152 – 49215**					• Comunicação SMB – TCP na porta **445**
Entrada (portas abertas no dispositivo XClarity Administrator)	• SSH – TCP na porta **22** • Dispositivos de rede RHEL KVM – TCP e UDP nas portas **53** e **67** • Agentes SNMP –	• SSH – TCP na porta **22** • Implantação do SO – TCP e UDP nas portas **445, 3900** e **8443**	• Implantação do SO – TCP e UDP nas portas **445, 3900** e **8443**	• Implantação do SO – TCP e UDP nas portas **445, 3900** e **8443**	• Implantação do SO – TCP e UDP nas portas **445, 3900** e **8443**	• Implantação do SO – TCP e UDP nas portas **445, 3900** e **8443**

Co-muni-cação	Perfil de virtualização RHEL, Centos e Rocky[1]	Perfis Básico e Mínimo de RHEL, Centos e Rocky[1]	SLES, virtualização, perfis Básico e Mínimo[2]	Perfis de virtualização e mínimo Ubuntu[3]	Perfil de Virtualização de VMware ESXi[4]	Perfis do Windows
	UDP na porta **162** • Implantação do SO – TCP e UDP nas portas **445, 3900** e **8443** • Agente de serviço SLP, agente de diretório SLP – TCP e UDP na porta **427** • Servidor Virtual KVM – TCP nas portas **49152 – 49215**					

1. Por padrão, os perfis de Red Hat Enterprise Linux (RHEL) bloqueiam todas as portas, exceto aquelas que estão listadas na tabela a seguir.
2. Para o SUSE Linux Enterprise Server (SLES), algumas portas abertas são designadas dinamicamente com base na versão e nos perfis de sistema operacional. Para obter uma lista completa das portas abertas, consulte a documentação do SUSE Linux Enterprise Server.
3. Para o Ubuntu Linux Server, algumas portas abertas são designadas dinamicamente com base na versão e nos perfis de sistema operacional. Para obter uma lista completa das portas abertas, consulte a documentação do Ubuntu Server.
4. Para obter uma lista completa de portas abertas para o VMware vSphere Hypervisor (ESXi) com personalização de Lenovo, consulte a documentação da VMware para ESXi no Site da Base de conhecimento do VMware.

Configurando um servidor de arquivos remoto

É possível importar imagens do SO, drivers de dispositivos e arquivos de inicialização para o repositório de imagens do SO do sistema local ou de um servidor de arquivos remoto. Para importar arquivos de um servidor de arquivos remoto, primeiro é necessário criar um perfil que seja usado para autenticar a conexão no servidor de arquivos remoto.

Sobre esta tarefa

Os seguintes algoritmos de criptografia são suportados:
- RSA–2048 bits
- RSA–4096 bits
- ECDSA–521 bits (curva secp521r1)

Os seguintes protocolos são suportados:
- HTTP sem autenticação.
- HTTP com autenticação básica.
- HTTPS (validação de certificados) com autenticação básica.
- HTTPS (validação de certificados) sem autenticação.

- FTP com autenticação de senha.
- SFTP (validação de cliente) com autenticação de senha.
- SFTP (validação de cliente) com autenticação de chaves públicas.

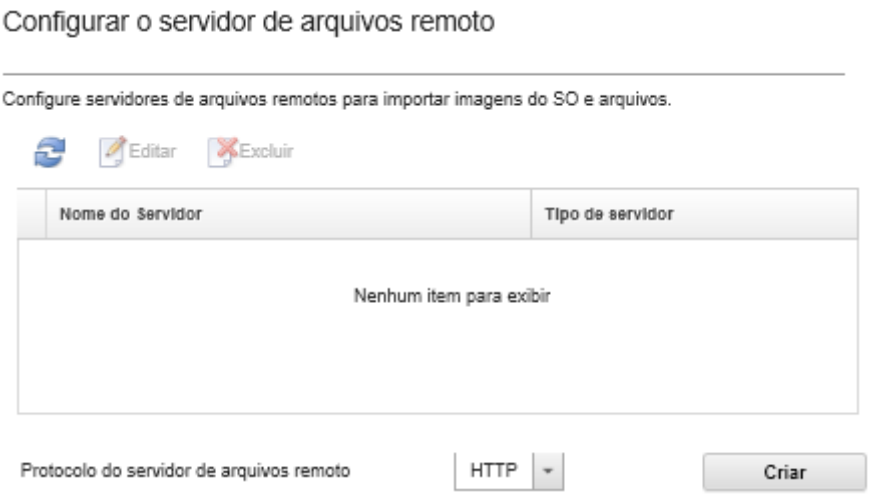
Para autenticação de chaves públicas SFTP e validação de certificados HTTPS, o Lenovo XClarity Administrator valida o certificado do servidor de arquivos remoto. Se o certificado do servidor não estiver no armazenamento confiável, você será solicitado a aceitar o certificado do servidor e incluí-lo no armazenamento confiável. Para obter informações sobre solução de problemas de validação, consulte Falha na validação de certificação do servidor a documentação online do XClarity Administrator.

Procedimento

Para configurar um servidor de arquivos remoto, conclua as etapas a seguir:

Etapa 1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.

Etapa 2. Clique no ícone **Configurar Servidor de Arquivos** ( ) para exibir a caixa de diálogo Configurar Servidor de Arquivos Remoto.



Etapa 3. Selecione o protocolo para o servidor de arquivos remoto na lista **Protocolo do Servidor de Arquivos Remoto**.

Etapa 4. Clique em **Criar**. A caixa de diálogo Configurar Servidor de Arquivos Remoto é exibida.

Nota: Essa caixa de diálogo difere dependendo do protocolo selecionado.

Etapa 5. Insira o nome do servidor, o endereço e a porta.

Etapa 6. Para HTTP, HTTPS, FTP e SFTP com autenticação básica, insira um nome de usuário e senha se a autenticação for necessária para acessar o servidor.

Etapa 7. Para SFTP com autenticação básica, clique em **Validar Certificado do Servidor** para obter a assinatura de chave pública.

Nota: Uma caixa de diálogo pode ser exibida informando que o processo de implantação do SO não confia na chave pública do servidor de arquivos SFTP. Clique em **OK** para armazenar e confiar na chave pública SFTP no armazenamento de chave confiável da implantação do SO. Se bem-sucedida, a assinatura de chave pública é mostrada no campo **Assinatura de chave pública servidor SFTP**.

Etapa 8. Para SFTP com autenticação de chave pública:

a. Insira uma passphrase de chave e uma senha e selecione o tipo de chave se a autenticação for necessária para acessar o servidor.
b. Clicar em **Gerar Chave do Servidor de Gerenciamento** para obter a assinatura de chave pública.
c. Copie a chave gerada para o arquivo authorized_keys no servidor de arquivos remoto SFTP.
d. Marque a caixa de seleção **A chave de gerenciamento foi copiada para o servidor** em XClarity Administrator.
e. Clique em **Validar Certificado do Servidor** para validar a assinatura de chave pública.

   Nota: Uma caixa de diálogo pode ser exibida informando que o processo de implantação do SO não confia na chave pública do servidor de arquivos SFTP. Clique em **OK** para armazenar e confiar na chave pública SFTP no armazenamento de chave confiável da implantação do SO. Se bem-sucedida, a assinatura de chave pública é mostrada no campo **Assinatura de chave pública servidor SFTP**.
f. Clique em **Salvar**.

Etapa 9. Clique em **Salvar Servidor**.

Depois de concluir

Na caixa de diálogo Configurar Servidor de Arquivos Remoto, você pode executar as seguintes ações:

- Atualize a lista de servidor de arquivos remoto clicando no ícone **Atualizar** ( ).
- Modifique um servidor de arquivos remoto selecionado clicando no ícone **Editar** ( ).
- Remova um servidor de arquivos remoto selecionado clicando no ícone **Excluir** ( ).

Importando imagens do sistema operacional

Antes de poder implantar um sistema operacional licenciado para servidores gerenciados, importe a imagem para o XClarity Administrator Repositório de imagens do SO.

Sobre esta tarefa

Para obter informações sobre imagens de sistemas operacionais que você pode importar e implantar, consulte Sistemas operacionais suportados.

Para obter uma lista de sistemas operacionais de base e personalizados suportados, consulte Sistemas operacionais com suporteSistemas operacionais suportados na documentação online do Lenovo XClarity Administrator.

Você só pode importar uma imagem por vez. Aguarde até a imagem ser exibida no Repositório de imagens do SO antes de tentar importar outra imagem. A importação do sistema operacional pode demorar um pouco.

Somente para ESXi, é possível importar várias imagens ESXi com a mesma versão principal/secundária para o repositório de imagens do SO.

Somente para ESXi, é possível importar várias imagens ESXi personalizadas com a mesma versão principal/secundária e o número de build para o repositório de imagens do SO.

Ao importar uma imagem do sistema operacional, XClarity Administrator:

- Verifica se há espaço suficiente no Repositório de imagens do SO antes de importar o sistema operacional. Se você não tiver espaço suficiente para importar uma imagem, exclua uma imagem existente do repositório e tente importar novamente a nova imagem.
- Cria um ou mais perfis dessa imagem e armazena o perfil no Repositório de imagens do SO. Cada *perfil* inclui a imagem do SO e opções de instalação. Para obter informações adicionais sobre perfis predefinidos de imagem do SO, consulte Perfis de imagem do sistema operacional.

Nota: Os navegadores da Web Internet Explorer e Microsoft Edge têm um limite de upload de 4 GB. Se o arquivo que você está importando for maior que 4 GB, considere usar outro navegador da Web (como o Chrome ou o Firefox) ou copie o arquivo para um servidor de arquivos remoto e importe usando a opção **Importação remota**.

Procedimento

Para importar uma imagem do sistema operacional para o Repositório de imagens do SO, execute as etapas a seguir.

Etapa 1. Obtenha uma imagem ISO licenciada do sistema operacional.

Nota: Você é responsável por obter as licenças aplicáveis para o sistema operacional.

Etapa 2. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistemas Operacionais: Gerenciar Imagens de SO.

Etapa 3. Clique no ícone **Importar Arquivos** () para exibir a caixa de diálogo Importar Arquivos e Imagens do SO.

Etapa 4. Clique na guia **Local** para fazer upload de arquivos do sistema local ou clique na guia **Remoto** para fazer upload de arquivos de um servidor de arquivos remoto.

Nota: Para fazer upload de um servidor de arquivos remoto, você deve primeiro criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** (). Para obter mais informações, consulte Configurando um servidor de arquivos remoto .

Etapa 5. Se você escolheu usar um servidor de arquivos remoto, selecione o servidor que você deseja usar na lista **Servidor de Arquivos Remoto**.

Etapa 6. Digite o caminho e o nome do arquivo da imagem ISO ou clique em **Procurar** para encontrar a imagem ISO que você deseja importar.

Se você escolheu usar o *servidor de arquivos local*, você deverá inserir o caminho absoluto para o arquivo de imagem ISO. Se você escolheu usar um *servidor de arquivos remoto*, você deve inserir o caminho absoluto (por exemplo, `/home/user/isos. osimage.iso`) ou caminho relativo (por exemplo, `/ ISOs.OSImage.ISO`) para o arquivo de imagem ISO (dependendo da configuração do servidor de arquivos remoto). Se o arquivo não for localizado, verifique se o caminho para o arquivo está correto e tente novamente.

Etapa 7. **Opcional:** forneça uma descrição da imagem do SO.

Etapa 8. **Opcional:** selecione um tipo de soma de verificação para verificar se a imagem ISO que está sendo importada para o XClarity Administrator não está danificada e copie e cole o valor de soma de verificação no campo de texto fornecido.

Se você selecionar um tipo de soma de verificação, especifique um valor de soma de verificação para verificar a integridade e a segurança da imagem de SO transferida por upload. O valor deve se originar de uma fonte segura de uma organização em que você confie. Se a imagem transferida por upload corresponde ao valor de soma de verificação, é seguro continuar com a implantação. Caso contrário, você deverá fazer upload da imagem novamente ou verificar o valor de soma de verificação.

Três tipos de soma de verificação têm suporte:

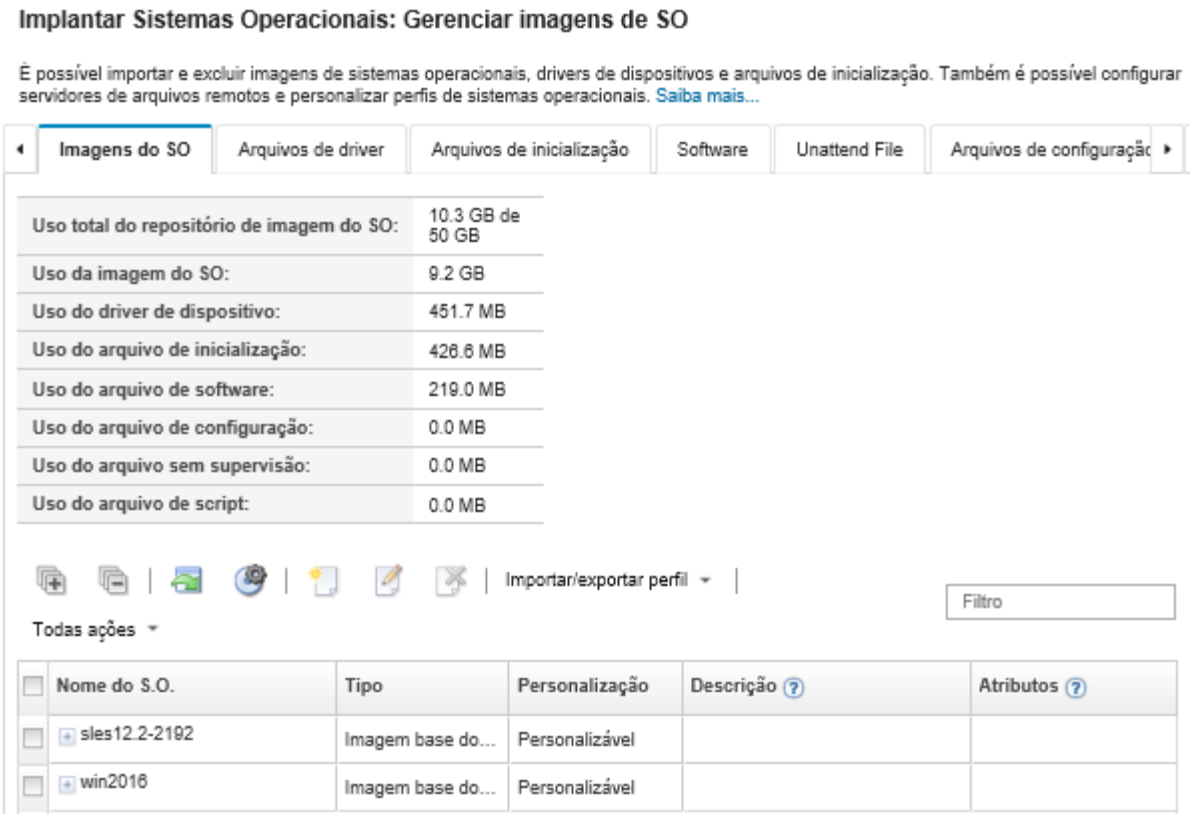
- **MD5**
- **SHA1**
- **SHA256**

Etapa 9. Clique em **Importar**.

Dica: a imagem ISO é transferida por upload por uma conexão de rede segura. Dessa forma, a confiabilidade e o desempenho da rede afetam o tempo necessário para importar a imagem. Se você fechar a guia ou a janela do navegador da Web na qual a imagem do sistema operacional está sendo transferida por upload antes do término do processo, ocorrerá falha na importação.

Resultados

O XClarity Administrator faz upload da imagem do SO e cria um perfil de imagem no Repositório de imagens do SO.



Nesta página, é possível executar as ações a seguir:

- Criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** ( ).
- Personalizar uma imagem do SO clicando no ícone **Criar Perfil Personalizado** ( ).
- Modificar uma imagem do SO clicando no ícone **Editar** ( ).
- Importe um perfil da imagem do SO personalizada e aplique a uma imagem do SO básica clicando em **Importar/Exportar Perfil → Importar Imagem do Perfil Personalizado** (consulte Importando um perfil de imagem do SO personalizada).
- Exclua uma imagem do SO selecionada ou um perfil da imagem do SO personalizada clicando no ícone **Excluir** ( ).

- Exporte um perfil da imagem do SO personalizada selecionado clicando em **Importar/Exportar Perfil → Exportar Imagem do Perfil Personalizado**.

Nota: Ao importar imagens do Windows Server, você também deve importar o arquivo de pacote associado. A Lenovo reúne o arquivo de inicialização WinPE_64.wim predefinido junto com um conjunto de drivers de dispositivo em um único pacote que pode ser baixado no Página da Web dos drivers do Lenovo Windows e do repositório de imagens do WinPE e, em seguida, importado para o repositório de imagens do SO. Como o arquivo do pacote contém drivers de dispositivo e arquivos de inicialização, é possível importar o arquivo do pacote da guia **Driver de Dispositivo** ou **Arquivos de Inicialização**..Para obter informações adicionais, consulte Importar arquivos de inicialização e Importando drivers de dispositivo.

Personalizando perfis de imagem do SO

Um *sistema operacional de base* é a imagem do SO completa que foi importada para o repositório de imagens do SO. A imagem de base importada contém perfis predefinidos que descrevem as configurações de instalação para essa imagem. Você também pode criar perfis personalizados na imagem do SO que pode ser implantada para configurações específicas. O perfil personalizado contém os arquivos personalizados e opções de instalação.

Nota: Não é possível criar um perfil de imagem do SO personalizado para uma imagem do Microsoft Windows Server personalizado.

Diversos cenários de exemplo para personalizar e Implantar imagens de SO, incluindo Windows e SLES, estão disponíveis somente em inglês. Para obter mais informações, consulte Cenários completos para configurar novos dispositivos.

Você pode adicionar que os seguintes tipos de arquivos a um perfil da imagem do SO personalizada.

- **Arquivos de inicialização**

  Um arquivo de inicialização age como o ambiente de instalação de autoinicialização. Para Windows, isso é um arquivo de Pré-instalação do Windows (WinPE). Um arquivo de inicialização WinPE é necessário para implantar o Windows

  O Lenovo XClarity Administrator dá suporte a arquivos de inicialização predefinidos e personalizados.

  – **Arquivos de inicialização predefinidos**. A Lenovo fornece um arquivo de inicialização WinPE_64.wim que pode ser usado para implantar perfis predefinidos de imagem do SO.

    A Lenovo reúne o arquivo de inicialização WinPE_64.wim predefinido junto com um conjunto de drivers de dispositivo em um único pacote que pode ser baixado no Página da Web dos drivers do Lenovo Windows e do repositório de imagens do WinPE e, em seguida, importado para o repositório de imagens do SO. Como o arquivo do pacote contém drivers de dispositivo e arquivos de inicialização, é possível importar o arquivo do pacote da guia **Driver de Dispositivo** ou **Arquivos de Inicialização**.

    Notas:

    – Um arquivo de inicialização predefinido não é pré-carregado com o XClarity Administrator. Você deve importar um arquivo de inicialização para o repositório de imagens do SO para que você possa implantar um perfil do Windows.

    – Não é possível excluir arquivos de inicialização predefinidos que foram carregados quando você instalou o XClarity Administrator. No entanto, você pode excluir arquivos de inicialização predefinidos importados de um pacote da Lenovo.

    – O XClarity Administrator requer que os arquivos do pacote importados sejam assinados pela Lenovo. Ao importar um arquivo do pacote, um arquivo de assinatura .asc também deve ser importado.

– **Arquivos de inicialização personalizados**. É possível criar um arquivo de inicialização do WinPE para personalizar as opções de inicialização para uma implantação do Windows. Em seguida, é possível incluir o arquivo de inicialização para perfis personalizados do Windows.

  O XClarity Administrator fornece scripts para criar arquivos de inicialização no formato correto. Para obter informações sobre como criar arquivos de inicialização personalizados, consulte Criando um arquivo de inicialização (WinPE) e Site de introdução ao Windows PE (WinPE).

  Os seguintes tipos de arquivo são suportados para importação dearquivos de inicialização personalizados.

Sistema Operacional	Tipos de arquivo de Inicialização compatíveis	Tipos de arquivo do pacote compatíveis
CentOS Linux	Não aceita	Não aceita
Microsoft® Windows® Azure Stack HCI	Não aceita	Não aceita
Microsoft Windows Hyper-V Server	Um arquivo .zip que contenha um arquivo WinPE que é criado usando o script **genimage.cmd**	Um arquivo .zip que contenha drivers de dispositivo e arquivos de inicialização
Microsoft Windows Server	Um arquivo .zip que contenha um arquivo WinPE que é criado usando o script **genimage.cmd**	Um arquivo .zip que contenha drivers de dispositivo e arquivos de inicialização
Red Hat® Enterprise Linux (RHEL) Server	Não aceita	Não aceita
Rocky Linux	Não aceita	Não aceita
SUSE® Linux Enterprise Server (SLES)	Não aceita	Não aceita
Ubuntu	Não aceita	Não aceita
VMware vSphere® Hypervisor (ESXi) com Lenovo Customization	Não aceita	Não aceita

- **Drivers de diapositivo**

  Você deve se certificar de que a imagem do sistema operacional que você pretende implantar inclua os drivers de dispositivo Ethernet, Fibre Channel e adaptador de armazenamento apropriados para seu hardware. Se o driver de dispositivo do adaptador de E/S não está incluído no sistema operacional, imagem ou perfil, o adaptador não é suportado para implantação do SO. Você pode criar perfis de imagem do SO personalizados que incluem os drivers de dispositivo necessários.

  O Lenovo XClarity Administrator dá suporte a drivers de dispositivo predefinidos, bem como aos personalizados.

  – **Drivers de dispositivo predefinidos**. O XClarity Administrator não gerencia drivers de dispositivo predefinidos. Sempre instale o sistema operacional mais recente para garantir que possui os drivers de dispositivo predefinidos mais recentes necessários.

    Nota: É possível adicionar drivers de dispositivo predefinidos a um perfil personalizado do Windows, criando um arquivo de inicialização do WinPE personalizado e copiando os arquivos de driver de dispositivo para o sistema host no diretório `C:\drivers`. Quando você cria um perfil de imagens do SO personalizadas que usa o arquivo de inicialização personalizado, os drivers de dispositivo que estão no diretório C:\drivers são incluídos no WinPE e no SO final. Eles são tratados como se fossem predefinidos. Portanto, não é necessário importar esses drivers de dispositivo predefinidos para o XClarity Administrator quando você especifica os drivers de dispositivo a serem usados na criação do perfil de imagens do SO personalizadas.

– **Drivers de dispositivo predefinidos**. Para servidores ThinkSystem, XClarity Administrator é pré-carregado com um conjunto de drivers de dispositivo para Linux para permitir a instalação do sistema operacional, bem como configuração básica de rede e de armazenamento para o sistema operacional final. Você pode adicionar esses drivers de dispositivo predefinidos para os perfis de imagem do SO personalizados e, em seguida, implantar os perfis em servidores gerenciados

  A Lenovo também reúne conjuntos de drivers de dispositivo predefinidos em um único pacote que pode ser baixado do Página da Web dos drivers do Lenovo Windows e do repositório de imagens do WinPE e, em seguida, importado para o repositório de imagens do SO. No momento, os arquivos do pacote estão disponíveis apenas para Windows. Se o arquivo contém drivers de dispositivo e arquivos de inicialização, é possível importar o arquivo do pacote do **Driver de Dispositivo** ou da guia **Imagem de Inicialização**.

  Notas:

  – Por padrão, os perfis de imagem do SO predefinidos incluem os drivers de dispositivo predefinidos.
  – Não é possível excluir drivers de dispositivo predefinidos que foram carregados quando você instalou o XClarity Administrator. No entanto, você pode excluir drivers de dispositivo predefinidos importados de um pacote da Lenovo.
  – O XClarity Administrator requer que os arquivos do pacote importados sejam assinados pela Lenovo. Ao importar um arquivo do pacote, um arquivo de assinatura .asc também deve ser importado.

– **Drivers de dispositivo personalizados**. É possível importar drivers de dispositivo predefinidos para o repositório de imagens do SO e, em seguida, adicioná-los em um perfil de imagem do SO personalizado.

  É possível obter drivers de dispositivos do Página da Web do repositório Lenovo YUM, do fornecedor (como Red Hat) ou com um driver de dispositivo personalizado que você mesmo criou. Para alguns drivers de dispositivo Windows, é possível gerar um driver de dispositivo personalizado extraindo o driver de dispositivo a partir do arquivo .exe de instalação para seu sistema local e criando um arquivo .zip.

  Os seguintes tipos de arquivo são suportados para serem importador para drivers de dispositivo personalizados.

Sistema Operacional	Tipos de arquivo do Driver de Dispositivo suportados
CentOS Linux	Não aceita
Microsoft® Windows® Azure Stack HCI	Não aceita
Microsoft Windows Hyper-V Server	Um arquivo .zip que contém os arquivos de driver de dispositivo brutos, que são normalmente agrupamentos de arquivos .inf, .cat e .dll.
Microsoft Windows Server	Um arquivo .zip que contém os arquivos de driver de dispositivo brutos, que são normalmente agrupamentos de arquivos .inf, .cat e .dll.
Red Hat® Enterprise Linux (RHEL) Server	Disco de atualização de driver (DUD) no formato de imagem .rpm ou .iso **Nota:** Se você aplicar um DUD .rpm ao perfil personalizado, o .rpm será instalado apenas no sistema operacional final. Ele não será instalado no ambiente de instalação (initrd). Para instalar um driver de dispositivo personalizado no initrd, importe um DUD .iso e aplique o .iso ao perfil personalizado.
Rocky Linux	Não aceita

Sistema Operacional	Tipos de arquivo do Driver de Dispositivo suportados
SUSE® Linux Enterprise Server (SLES)	Disco de atualização de driver (DUD) no formato de imagem .rpm ou .iso **Nota:** Se você aplicar um DUD .rpm ao perfil personalizado, o .rpm será instalado apenas no sistema operacional final. Ele não será instalado no ambiente de instalação (initrd). Para instalar um driver de dispositivo personalizado no initrd, importe um DUD .iso e aplique o .iso ao perfil personalizado.
Ubuntu	Não aceita
VMware vSphere® Hypervisor (ESXi) com Lenovo Customization	Drivers de dispositivo no formato de imagem .vib

Nota: O repositório de imagens do SO poderá armazenar um número ilimitado de arquivos personalizados e predefinidos, se houver espaço disponível para armazenar os arquivos.

- **Definições de configuração personalizadas**

  As definições de configuração descrevem dados que precisam ser coletados dinamicamente durante a implantação do SO. O Lenovo XClarity Administrator usa um conjunto de configurações predefinidas, incluindo configurações globais, de rede e de local de armazenamento. Você pode usar essas configurações predefinidas e adicionar configurações personalizadas que não estão disponíveis por meio do XClarity Administrator.

  As configurações personalizadas são definidas na forma de um esquema JSON. O esquema deve estar em conformidade com a especificação JSON.

  Quando você importa as configurações personalizadas para XClarity Administrator, o XClarity Administrator valida o esquema JSON. Se a validação for aprovada, o XClarity Administrator gerará macros personalizadas para cada configuração.

  É possível usar as macros personalizadas no arquivo sem supervisão e no script pós-instalação.

  Em arquivos sem supervisão

  Você pode associar o arquivo de configuração personalizado a um arquivo sem supervisão e incluir esses macros personalizadas (e macros predefinidas) no arquivo sem supervisão.

  É possível incluir um ou mais arquivos de configurações personalizadas em um perfil personalizado. Quando você implanta o perfil do SO em um conjunto de servidores de destino, é possível escolher qual arquivo de configuração deve ser usado. O XClarity Administrator processa a guia **Configurações personalizadas** na caixa de diálogo Implantar imagens de SO com base no esquema JSON no arquivo de configuração e permite que você especifique valores para cada configuração (objeto JSON) que está definida no arquivo.

  Nota: A implantação do SO não continuará se a entrada não for especificada para alguma configuração personalizada.

  Em scripts pós-instalação

  Depois que os dados são coletados durante a implantação do SO, o XClarity Administrator cria uma instância do arquivo de configuração (que inclui as configurações personalizadas no arquivo selecionado e um subconjunto de configurações predefinidas) no sistema host que pode ser usada pelo script pós-instalação.

  Notas:

  – O arquivo de configuração é exclusivo de um perfil de imagem do SO personalizado.
  – Você não pode modificar definições de configuração para perfis predefinidos de imagem do SO.

  - Definições de configuração são suportadas somente para os seguintes sistemas operacionais:
    - Microsoft® Windows® Server
    - Red Hat® Enterprise Linux (RHEL) Server
    - Rocky Linux
    - SUSE® Linux Enterprise Server (SLES)
    - VMware vSphere® Hypervisor (ESXi) com Lenovo Customization 6.0u3 e atualizações posteriores e 6.5 e atualizações posteriores.

  O repositório de imagens do SO poderá armazenar um número ilimitado de arquivos personalizados e predefinidos, se houver espaço disponível para armazenar os arquivos.

- **Arquivos sem supervisão personalizados**

  Você pode personalizar perfis de imagem do SO para usar arquivos sem supervisão para automatizar a implantação do sistema operacional.

  Os seguintes tipos de arquivo são suportados para arquivos sem supervisão personalizados.

Sistema Operacional	**Tipos de arquivo compatíveis**	**Mais informações**
CentOS Linux	Não aceita	
Microsoft® Windows® Azure Stack HCI	Não aceita	
Microsoft Windows Hyper-V Server	Não aceita	
Microsoft Windows Server	Sem supervisão (.xml)	Para obter mais informações sobre arquivos sem supervisão, consulte Página da Web de referência do Windows Setup sem supervisão.
Red Hat® Enterprise Linux (RHEL) Server	Kickstart (.cfg)	Para obter mais informações sobre arquivos sem supervisão, consulte Red Hat: página Automatizar a instalação com o Kickstart. Considere o seguinte ao incluir seções %pre, %post, % firstboot no arquivo. – Você pode incluir várias seções %pre, %post, %firstboot no arquivo sem supervisão. No entanto, preste atenção à ordem das seções. – Quando a macro **#predefined.unattendSettings. preinstallConfig#** recomendada estiver presente no arquivo sem supervisão, XClarity Administrator incluirá uma seção %pre antes de todas as outras seções %pre no arquivo. – Quando a macro **#predefined.unattendSettings. postinstallConfig#** recomendada estiver presente no arquivo sem supervisão, o XClarity Administrator incluirá seções %post e %firstboot antes de todas as outras seções %post e %firstboot no arquivo.

Sistema Operacional	Tipos de arquivo compatíveis	Mais informações
Rocky Linux	Kickstart (.cfg)	Para obter mais informações sobre arquivos sem supervisão, consulte o Red Hat: página Automatizar a instalação com o Kickstart. Considere o seguinte ao incluir seções %pre, %post, % firstboot no arquivo. – Você pode incluir várias seções %pre, %post, %firstboot no arquivo sem supervisão. No entanto, preste atenção à ordem das seções. – Quando a macro **#predefined.unattendSettings. preinstallConfig#** recomendada estiver presente no arquivo sem supervisão, XClarity Administrator incluirá uma seção %pre antes de todas as outras seções %pre no arquivo. – Quando a macro **#predefined.unattendSettings. postinstallConfig#** recomendada estiver presente no arquivo sem supervisão, o XClarity Administrator incluirá seções %post e %firstboot antes de todas as outras seções %post e %firstboot no arquivo.
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	Para obter mais informações sobre arquivos sem supervisão, consulte SUSE: Página da Web do AutoYaST.
Ubuntu	Não aceita	
VMware vSphere® Hypervisor (ESXi) com Lenovo Customization	Kickstart (.cfg)	Suportados somente para ESXi 6.0u3 e atualizações mais recentes e 6.5 e posterior. Para obter mais informações sobre arquivos sem supervisão, consulte VMware: Instalando ou atualizando hosts usando uma página da Web de script. Considere o seguinte ao incluir seções %pre, %post, % firstboot no arquivo. – Você pode incluir várias seções %pre, %post, %firstboot no arquivo sem supervisão. No entanto, preste atenção à ordem das seções. – Quando a macro **#predefined.unattendSettings. preinstallConfig#** recomendada estiver presente no arquivo sem supervisão, XClarity Administrator incluirá uma seção %pre antes de todas as outras seções %pre no arquivo. – Quando a macro **#predefined.unattendSettings. postinstallConfig#** recomendada estiver presente no arquivo sem supervisão, o XClarity Administrator incluirá seções %post e %firstboot antes de todas as outras seções %post e %firstboot no arquivo.

Atenção:

– É possível inserir macros predefinidas e personalizadas (definições de configuração) no arquivo sem supervisão usando o nome exclusivo do objeto. Valores predefinidos são dinâmicos com base nas instâncias XClarity Administrator. Macros personalizadas são dinâmicas com base na entrada do usuário que é especificada durante a implantação do SO.

Notas:

– Coloque uma cerquilha (#) ao redor do nome da macro.

  - Para objetos aninhados, separe cada nome de objeto usando um ponto (por exemplo, **#server_settings.server0.locale#**).
  - Para macros personalizadas, não inclua o nome de objeto mais alto. Para as macros predefinidas, inclua no nome da macro o prefixo "predefinido".
  - Quando um objeto é criado de um modelo, o nome é anexado com um número exclusivo, começando com 0 (por exemplo, **server0** e **server1**).
  - Você pode ver o nome de cada macro da caixa de diálogo Implantar imagens de SO nas guias de Configurações personalizadas passando o mouse sobre o ícone Ajuda () próximo de cada configuração personalizada.
  - Para obter uma lista de macros predefinidas, consulte Macros predefinidas. Para obter informações sobre as configurações e macros personalizadas, consulte Macros personalizadas.
- O XClarity Administrator fornece as macros predefinidas a seguir que são usadas para comunicar o status do instalador do SO, além de várias outras etapas de instalação críticas. É altamente recomendável incluir essas macros no arquivo sem supervisão (consulte Inserindo macros predefinidas e personalizadas para um arquivo sem supervisão).
  - #predefined.unattendSettings.preinstallConfig#
  - #predefined.unattendSettings postinstallConfig#

- **Scripts de instalação personalizados**

  Você pode personalizar perfis de imagem do SO para executar um script de instalação após a implantação do SO.

  Atualmente, apenas os scripts pós-instalação são suportados.

  A tabela a seguir lista os tipos de arquivo para scripts de instalação para os quais Lenovo XClarity Administrator oferece suporte para cada sistema operacional. Observe que determinadas versões de sistema operacional não oferecem suporte a todos os tipos de arquivo a que o XClarity Administrator oferece suporte (por exemplo, alguns versões RHEL podem não incluir Perl no mínimo perfil e, portanto, não serão executado scripts Perl). Certifique-se de usar o tipo de arquivo correto para as versões de sistema operacional que você deseja implantar.

Sistema Operacional	Tipos de arquivo compatíveis	Mais informações
CentOS Linux	Não aceita	
Microsoft® Windows® Azure Stack HCI	Não aceita	
Microsoft Windows Hyper-V Server	Não aceita	
Microsoft® Windows® Server	Arquivo de comando (. cmd), PowerShell (. ps1)	O caminho de arquivos e dados personalizado padrão é `C:\lxca`. Para obter mais informações sobre scripts de instalação, consulte o Página da Web Adicionar um script personalizado ao Windows Setup
Red Hat® Enterprise Linux (RHEL) Server	Bash (.sh), Perl (.pm ou. pl), Python (. py)	O caminho arquivos e dados personalizados padrão é `/home/lxca`. Para obter mais informações sobre scripts de instalação, consulte o RHEL: Página da Web de script pós-instalação.

Sistema Operacional	Tipos de arquivo compatíveis	Mais informações
Rocky Linux	Bash (.sh), Perl (.pm ou. pl), Python (.py)	O caminho arquivos e dados personalizados padrão é `/home/lxca`. Para obter mais informações sobre scripts de instalação, consulte o RHEL: Página da Web de script pós-instalação
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm ou. pl), Python (.py)	O caminho arquivos e dados personalizados padrão é `/home/lxca`. Para obter mais informações sobre scripts de instalação, consulte o SUSE: Página da Web de script de usuário personalizado
Ubuntu	Não aceita	
VMware vSphere® Hypervisor (ESXi) com Lenovo Customization	Bash (.sh), Python (.py)	O caminho arquivos e dados personalizados padrão é `/home/lxca`. Para obter mais informações sobre scripts de instalação, consulte o VMware: Página da Web de instalação e scripts de atualização

- **Software personalizado**

  Você pode personalizar perfis de imagem do sistema operacional para instalar cargas de software personalizado depois de concluir os scripts de implantação e pós-instalação do sistema operacional.

  Os seguintes tipos de arquivo são suportados para software personalizado.

Sistema Operacional	Tipos de arquivo compatíveis	Mais informações
CentOS Linux	Não aceita	
Microsoft® Windows® Azure Stack HCI	Não aceita	
Microsoft Windows Hyper-V Server	Não aceita	
Microsoft Windows® Server	Um arquivo .zip que contém a carga de software.	O caminho de arquivos e dados personalizado padrão é `C:\lxca`.
Red Hat® Enterprise Linux (RHEL) Server	Um arquivo .tar.gz que contém a carga de software	O caminho arquivos e dados personalizados padrão é `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	Um arquivo .tar.gz que contém a carga de software	O caminho arquivos e dados personalizados padrão é `/home/lxca`.
Rocky Linux	Um arquivo .tar.gz que contém a carga de software	O caminho arquivos e dados personalizados padrão é `/home/lxca`.
Ubuntu	Não aceita	
VMware vSphere® Hypervisor (ESXi) com Lenovo Customization	Um arquivo .tar.gz que contém a carga de software	O caminho arquivos e dados personalizados padrão é `/home/lxca`.

Importando um perfil de imagem do SO personalizada

É possível importar um perfil de imagem do SO personalizada e incluí-lo em uma imagem do SO de base compatível existente.

Sobre esta tarefa

A imagem do SO de base deve ser importada antes de você importar um perfil personalizado.

Um perfil da imagem do SO personalizada só pode ser adicionado a uma imagem do SO de base do mesmo tipo. Por exemplo, se o perfil exportado for para uma imagem do Windows 2016, o perfil só poderá ser importado e incluído em uma imagem do Windows 2016 existente no repositório de imagens de SO.

O repositório de imagens do SO poderá armazenar um número ilimitado de perfis personalizados, se houver espaço disponível para armazenar os arquivos.

Procedimento

Para importar um perfil da imagem do SO personalizada, conclua as etapas a seguir.

Etapa 1. Na barra de menus Lenovo XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.

Etapa 2. Na guia **Imagens do SO**, selecione a imagem do SO de base na qual você deseja incluir o perfil de imagem do SO personalizada.

Etapa 3. Clique em **Importar/Exportar Perfil → Importar Imagem do Perfil Personalizada**. A caixa de diálogo Importar Perfil de Imagem do SO Personalizada é exibida

Etapa 4. Clique na guia **Importação Local** para fazer upload de arquivos do sistema local ou clique na guia **Importação Remota** para fazer upload de arquivos de um servidor de arquivos remoto.

Nota: Para fazer upload de um arquivo de um servidor de arquivos remoto, você deve primeiro criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** (). Para obter mais informações, consulte Configurando um servidor de arquivos remoto

Etapa 5. Se você escolheu usar um servidor de arquivos remoto, selecione o servidor que você deseja usar na lista **Servidor de Arquivos Remoto**.

Etapa 6. Digite o nome do perfil ou clique em **Procurar** para encontrar o perfil que você deseja importar.

Etapa 7. **Opcional:** Para importações locais, selecione um tipo de soma de verificação para verificar se o arquivo que está transferido por upload não está danificado e copie e cole o valor de soma de verificação no campo de texto fornecido.

Se você selecionar um tipo de soma de verificação, especifique um valor de soma de verificação para verificar a integridade e a segurança do arquivo transferido por upload. O valor deve se originar de uma fonte segura de uma organização em que você confie. Se o arquivo transferido por upload corresponde ao valor de soma de verificação, será seguro continuar com a implantação. Caso contrário, você deverá fazer upload novamente do arquivo ou verificar o valor de soma de verificação.

Três tipos de soma de verificação têm suporte:
- **MD5**
- **SHA1**
- **SHA256**

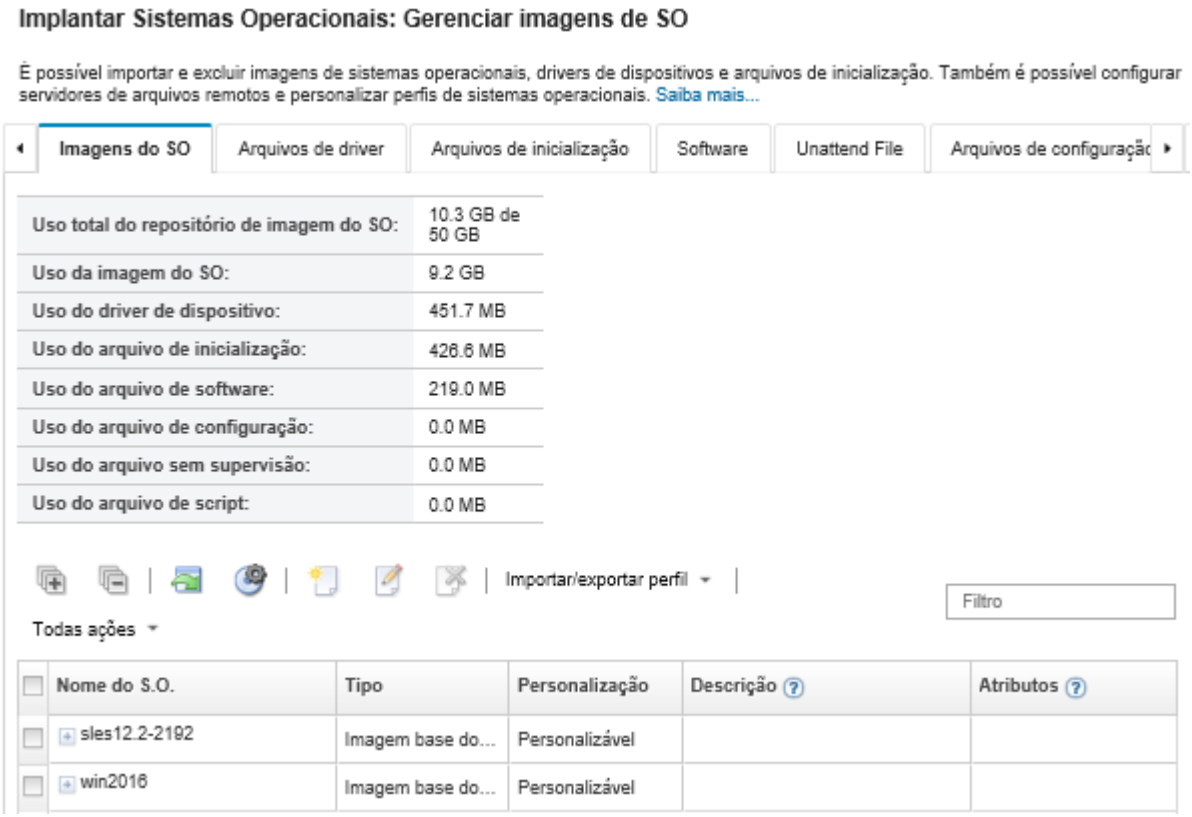
Etapa 8. Clique em **Importar**.

Dica: o arquivo é transferido por upload por uma conexão de rede segura. Dessa forma, a confiabilidade e o desempenho da rede afetam o tempo que demora para importar o arquivo.

Se você fechar a guia ou a janela do navegador da Web na qual o arquivo está sendo transferido por upload localmente antes do término do processo, ocorrerá falha na importação.

Depois de concluir

O perfil de imagem do SO personalizada está listado abaixo do sistema operacional de base na página Gerenciar Imagens do SO.



Nesta página, é possível executar as ações a seguir:

- Crie um perfil da imagem do SO personalizada (consulte Criando um perfil da imagem do SO personalizada).
- Exporte um perfil da imagem do SO personalizada selecionado clicando em **Importar/Exportar Perfil → Exportar Imagem do Perfil Personalizado**.

  Importante: É possível exportar perfis de imagem do SO personalizada para um servidor de arquivos remoto configurado para usar protocolos FTP ou SFTP. Não é possível exportar para um servidor de arquivos remoto que seja configurado para usar HTTPS ou HTTP.
- Modifique um perfil da imagem do SO personalizada selecionado no ícone **Editar** ( ).
- Remova um perfil da imagem do SO personalizada selecionado no ícone **Excluir** ( ).

Importar arquivos de inicialização

É possível importar arquivos de inicialização para o repositório de imagens do SO. Esses arquivos podem ser usados para personalizar e implantar as imagens do Windows.

Sobre esta tarefa

Um arquivo de inicialização age como o ambiente de instalação de autoinicialização. Para Windows, isso é um arquivo de Pré-instalação do Windows (WinPE). Um arquivo de inicialização WinPE é necessário para implantar o Windows

O Lenovo XClarity Administrator dá suporte a arquivos de inicialização predefinidos e personalizados.

- **Arquivos de inicialização predefinidos**. A Lenovo fornece um arquivo de inicialização WinPE_64.wim que pode ser usado para implantar perfis predefinidos de imagem do SO.

  A Lenovo reúne o arquivo de inicialização WinPE_64.wim predefinido junto com um conjunto de drivers de dispositivo em um único pacote que pode ser baixado no Página da Web dos drivers do Lenovo Windows e do repositório de imagens do WinPE e, em seguida, importado para o repositório de imagens do SO. Como o arquivo do pacote contém drivers de dispositivo e arquivos de inicialização, é possível importar o arquivo do pacote da guia **Driver de Dispositivo** ou **Arquivos de Inicialização**.

  Notas:

  – Um arquivo de inicialização predefinido não é pré-carregado com o XClarity Administrator. Você deve importar um arquivo de inicialização para o repositório de imagens do SO para que você possa implantar um perfil do Windows.

  – Não é possível excluir arquivos de inicialização predefinidos que foram carregados quando você instalou o XClarity Administrator. No entanto, você pode excluir arquivos de inicialização predefinidos importados de um pacote da Lenovo.

  – O XClarity Administrator requer que os arquivos do pacote importados sejam assinados pela Lenovo. Ao importar um arquivo do pacote, um arquivo de assinatura .asc também deve ser importado.

- **Arquivos de inicialização personalizados**. É possível criar um arquivo de inicialização do WinPE para personalizar as opções de inicialização para uma implantação do Windows. Em seguida, é possível incluir o arquivo de inicialização para perfis personalizados do Windows.

  O XClarity Administrator fornece scripts para criar arquivos de inicialização no formato correto. Para obter informações sobre como criar arquivos de inicialização personalizados, consulte Criando um arquivo de inicialização (WinPE) e Site de introdução ao Windows PE (WinPE).

  Os seguintes tipos de arquivo são suportados para importação dearquivos de inicialização personalizados.

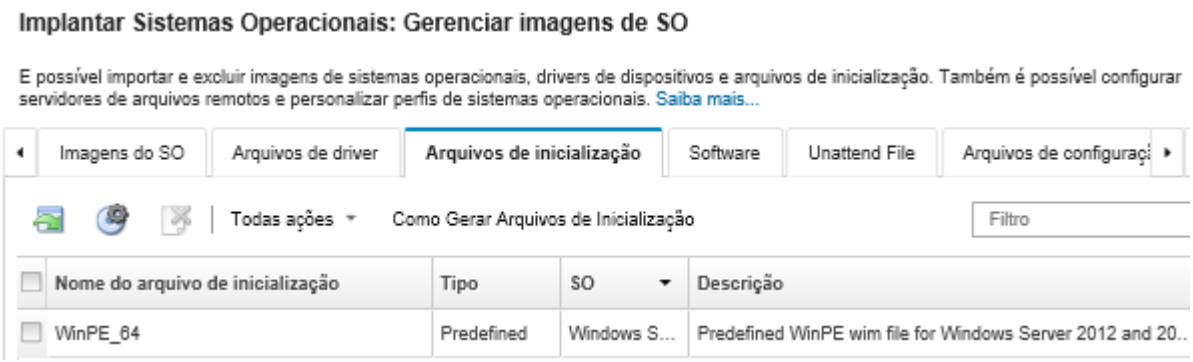
Sistema Operacional	Tipos de arquivo de Inicialização compatíveis	Tipos de arquivo do pacote compatíveis
CentOS Linux	Não aceita	Não aceita
Microsoft® Windows® Azure Stack HCI	Não aceita	Não aceita
Microsoft Windows Hyper-V Server	Um arquivo .zip que contenha um arquivo WinPE que é criado usando o script **genimage.cmd**	Um arquivo .zip que contenha drivers de dispositivo e arquivos de inicialização
Microsoft Windows Server	Um arquivo .zip que contenha um arquivo WinPE que é criado usando o script **genimage.cmd**	Um arquivo .zip que contenha drivers de dispositivo e arquivos de inicialização

Sistema Operacional	Tipos de arquivo de Inicialização compatíveis	Tipos de arquivo do pacote compatíveis
Red Hat® Enterprise Linux (RHEL) Server	Não aceita	Não aceita
Rocky Linux	Não aceita	Não aceita
SUSE® Linux Enterprise Server (SLES)	Não aceita	Não aceita
Ubuntu	Não aceita	Não aceita
VMware vSphere® Hypervisor (ESXi) com Lenovo Customization	Não aceita	Não aceita

Nota: O repositório de imagens do SO poderá armazenar um número ilimitado de arquivos personalizados e predefinidos, se houver espaço disponível para armazenar os arquivos.

Procedimento

- Para importar um arquivo do pacote do Windows que contém arquivos de inicialização para o repositório de imagens do SO, conclua as etapas a seguir.
  1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
  2. Clique na guia **Arquivos de Inicialização**.



  3. Clique em **Downloads → Arquivos do Pacote do Windows** para ir para a página de Suporte Lenovo e baixe o arquivo do pacote apropriado e o arquivo de assinatura associado para a imagem d SO para o sistema local.
  4. Clique no ícone **Importar Arquivo do Pacote** ( ). A caixa de diálogo Importar Arquivo do Pacote é exibida.
  5. Clique na guia **Importação Local** para fazer upload de arquivos do sistema local ou clique na guia **Importação Remota** para fazer upload de arquivos de um servidor de arquivos remoto.

     Nota: Para fazer upload de um arquivo de um servidor de arquivos remoto, você deve primeiro criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** ( ). Para obter mais informações, consulte Configurando um servidor de arquivos remoto
  6. Se você escolheu usar um servidor de arquivos remoto, selecione o servidor que você deseja usar na lista **Servidor de Arquivos Remoto**.
  7. Selecione o tipo de sistema operacional e a versão.
  8. Digite o nome do arquivo para o arquivo do pacote e para o arquivo de assinatura associado ou clique em **Procurar** para encontrar os arquivos que deseja importar.

9. **Opcional:** digite uma descrição para o arquivo do pacote.
10. Clique em **Importar**.

    Dica: o arquivo é transferido por upload por uma conexão de rede segura. Dessa forma, a confiabilidade e o desempenho da rede afetam o tempo que demora para importar o arquivo.

    Se você fechar a guia ou a janela do navegador da Web na qual o arquivo está sendo transferido por upload localmente antes do término do processo, ocorrerá falha na importação.

- Para importar um arquivo do pacote individual para o repositório de imagens do SO, conclua as seguintes etapas.
  1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
  2. Clique na guia **Arquivos de Inicialização**.
  3. Clique no ícone **Importar Arquivo** (). A caixa de diálogo Importar Arquivo é exibida.
  4. Clique na guia **Importação Local** para fazer upload de arquivos do sistema local ou clique na guia **Importação Remota** para fazer upload de arquivos de um servidor de arquivos remoto.

     Nota: Para fazer upload de um arquivo de um servidor de arquivos remoto, você deve primeiro criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** (). Para obter mais informações, consulte Configurando um servidor de arquivos remoto
  5. Se você escolheu usar um servidor de arquivos remoto, selecione o servidor que você deseja usar na lista **Servidor de Arquivos Remoto**.
  6. Selecione o tipo de sistema operacional e a versão.
  7. Digite o nome do arquivo ou clique em **Procurar** para encontrar o arquivo de inicialização que você deseja importar.
  8. **Opcional:** Digite uma descrição para o arquivo de inicialização.
  9. **Opcional:** Selecione um tipo de soma de verificação para verificar se o arquivo que está sendo transferido por upload não está danificado e copie e cole o valor de soma de verificação no campo de texto fornecido.

     Se você selecionar um tipo de soma de verificação, especifique um valor de soma de verificação para verificar a integridade e a segurança do arquivo transferido por upload. O valor deve se originar de uma fonte segura de uma organização em que você confie. Se o arquivo transferido por upload corresponde ao valor de soma de verificação, será seguro continuar com a implantação. Caso contrário, você deverá fazer upload novamente do arquivo ou verificar o valor de soma de verificação.

     Três tipos de soma de verificação têm suporte:
     - **MD5**
     - **SHA1**
     - **SHA256**
  10. Clique em **Importar**.

      Dica: o arquivo é transferido por upload por uma conexão de rede segura. Dessa forma, a confiabilidade e o desempenho da rede afetam o tempo que demora para importar o arquivo.

      Se você fechar a guia ou a janela do navegador da Web na qual o arquivo está sendo transferido por upload localmente antes do término do processo, ocorrerá falha na importação.

Depois de concluir

O arquivo de inicialização é listado na guia **Arquivos de Inicialização** na página Gerenciar Imagens do SO.

Nesta página, é possível executar as ações a seguir:

- Criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** ().
- Remova um arquivo de inicialização selecionado clicando no ícone **Excluir** ().
- Adicione um arquivo de inicialização a um perfil de imagem do SO personalizada (consulte Criando um perfil da imagem do SO personalizada).

Criando um arquivo de inicialização (WinPE)

É possível criar arquivos de inicialização que podem ser usados para personalizar imagens Windows.

Antes de iniciar

- Certifique-se de que o sistema operacional que você pretende fornecer esteja instalado no host. Por exemplo, se você planeja fornecer o Windows 2016 usando os arquivos WinPE, instale o Windows 2016 no host.
- Certifique-se de que o Microsoft ADK que é compatível com o sistema operacional instalado também esteja instalado no host. Por exemplo, o Windows 2012R2 requer o ADK versão 8.1 Atualizado.
- Obtenha os drivers de dispositivo no formato .inf, que você deseja incluir no arquivo de inicialização.

  É possível obter drivers de dispositivos do Página da Web do repositório Lenovo YUM, do fornecedor (como Red Hat) ou com um driver de dispositivo personalizado que você mesmo criou. Para alguns drivers de dispositivo Windows, é possível gerar um driver de dispositivo personalizado extraindo o driver de dispositivo a partir do arquivo .exe de instalação para seu sistema local e criando um arquivo .zip.

  A Lenovo também reúne conjuntos de drivers de dispositivo predefinidos em um único pacote que pode ser baixado do Página da Web dos drivers do Lenovo Windows e do repositório de imagens do WinPE e, em seguida, importado para o repositório de imagens do SO. No momento, os arquivos do pacote estão disponíveis apenas para Windows. Se o arquivo contém drivers de dispositivo e arquivos de inicialização, é possível importar o arquivo do pacote do **Driver de Dispositivo** ou da guia **Imagem de Inicialização**.
- Baixe os arquivos `genimage.cmd` e `startnet.cmd` no host em um diretório temporário, como `C:\customwim`.

  O comando `genimage.cmd` é usado para gerar os arquivos de inicialização WinPE, incluindo o arquivo .wim. O comando `startnet.cmd` é usado XClarity Administrator para inicializar automaticamente o instalador Windows.
- Decida como deseja inserir drivers de dispositivo no arquivo de inicialização. É possível fazer isso de uma das seguintes maneiras:
  - Inclua drivers de dispositivo predefinidos em um perfil personalizado do Windows copiando os arquivos dos drivers de dispositivo no sistema host no diretório C:\drivers. Eles serão incluídos no arquivo de inicialização quando genimage.cmd for executado posteriormente.

    Nota: Quando você cria um perfil de imagens do SO personalizadas que usa o arquivo de inicialização personalizado, os drivers de dispositivo que estão no diretório C:\drivers são incluídos no WinPE e no SO final. Eles são tratados como se fossem predefinidos. Portanto, não é necessário importar esses drivers de dispositivo predefinidos para o XClarity Administrator quando você especifica os drivers de dispositivo a serem usados na criação do perfil de imagens do SO personalizadas.
  - Inclua drivers de dispositivo predefinidos diretamente no arquivo de inicialização.

    Nota: Se você usar esse método, os drivers de dispositivo serão aplicados somente ao arquivo de inicialização e, portanto, ao ambiente de instalação do WinPE. Os drivers de dispositivo não são aplicados ao SO instalado final. Você precisará importar os drivers de dispositivo manualmente para o repositório de driver de dispositivo de imagens do SO e selecioná-los para serem usados como parte da personalização do perfil de imagem do SO.

- Para obter mais informações arquivos de inicialização, consulte Site de introdução ap Window PE (WinPE).

Procedimento

Para criar um arquivo de inicialização, execute as etapas a seguir.

Etapa 1. Usando um ID de usuário com autoridade de administrador, execute o comando do ADK "Deployment and Imaging Tools Environment." Uma sessão de comando é exibida.

Etapa 2. Na sessão do comando, altere para o diretório onde os arquivos `genimage.cmd` e `starnet.cmd` foram baixados (por exemplo, `C:\customwim`).

Etapa 3. Garanta que nenhuma imagem montada anteriormente esteja no host executando o seguinte comando:
```
dism /get-mountedwiminfo
```

Se houver imagens montadas, rejeite-as executando o seguinte comando:

```
dism /unmount-wim /MountDir:C:\<mount_path> /Discard
```

Etapa 4. Se estiver adicionando drivers de dispositivo predefinidos a um perfil personalizado do Windows copie os arquivos dos drivers de dispositivo brutos no formato .inf no sistema host no diretório `C:\drivers`.

Etapa 5. Execute o seguinte comando ao gerar o arquivo de inicialização, no formato .wim, e espere alguns minutos pela conclusão.
```
genimage.cmd amd64 <ADK_Version>
```

Em que *<ADK_Version>* é um dos valores a seguir.

- **8.1**. Para Windows 2012 R2
- **10**. Para Windows 2016

Esse comando cria o arquivo de inicialização: `C:\WinPE_64\media\Boot\WinPE_64.wim`.

Etapa 6. Monte o arquivo de inicialização executando o seguinte comando:
```
DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount
```

Etapa 7. Se você estiver incluindo drivers de dispositivo predefinidos diretamente no arquivo de inicialização, conclua as seguintes etapas.

1. Crie a estrutura de diretório a seguir, em que *<os_release>* é `2012`, `2012R2` ou `2016`
   ```
   drivers\<os_release>\
   ```
2. Copie os drivers de dispositivo, no formato .inf, em um diretório dentro desse caminho, por exemplo:
   ```
   drivers\<os_release>\<driver1>\<driver1_files>
   ```
3. Copie o diretório `drivers` no diretório montado, por exemplo:
   ```
   C:\WinPE_64\mount\drivers
   ```

Etapa 8. Faça personalizações adicionais no arquivo de inicialização, como adicionar pastas, arquivos, scripts de inicialização, pacotes de idioma e aplicativos. Para obter mais informações sobre personalização de arquivos de inicialização, consulte Site WinPE: Montar e personalizar.

Etapa 9. Desmonte a imagem executando o seguinte comando.
```
DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit
```

Etapa 10. Compacte o conteúdo do diretório `C:\WinPE_64\media` em um arquivo zip chamado `WinPE_64.zip`.

Etapa 11. Importe o arquivo .zip no XClarity Administrator (consulte Importar arquivos de inicialização).

Importando drivers de dispositivo

É possível importar drivers de dispositivo individuais e arquivos de pacote para o repositório de imagens do SO. Esses arquivos podem ser usados para personalizar as imagens do Linux e do Windows.

Sobre esta tarefa

Você deve se certificar de que a imagem do sistema operacional que você pretende implantar inclua os drivers de dispositivo Ethernet, Fibre Channel e adaptador de armazenamento apropriados para seu hardware. Se o driver de dispositivo do adaptador de E/S não está incluído no sistema operacional, imagem ou perfil, o adaptador não é suportado para implantação do SO. Você pode criar perfis de imagem do SO personalizados que incluem os drivers de dispositivo necessários.

O Lenovo XClarity Administrator dá suporte a drivers de dispositivo predefinidos, bem como aos personalizados.

- **Drivers de dispositivo predefinidos**. O XClarity Administrator não gerencia drivers de dispositivo predefinidos. Sempre instale o sistema operacional mais recente para garantir que possui os drivers de dispositivo predefinidos mais recentes necessários.

  Nota: É possível adicionar drivers de dispositivo predefinidos a um perfil personalizado do Windows, criando um arquivo de inicialização do WinPE personalizado e copiando os arquivos de driver de dispositivo para o sistema host no diretório `C:\drivers`. Quando você cria um perfil de imagens do SO personalizadas que usa o arquivo de inicialização personalizado, os drivers de dispositivo que estão no diretório C:\drivers são incluídos no WinPE e no SO final. Eles são tratados como se fossem predefinidos. Portanto, não é necessário importar esses drivers de dispositivo predefinidos para o XClarity Administrator quando você especifica os drivers de dispositivo a serem usados na criação do perfil de imagens do SO personalizadas.

- **Drivers de dispositivo predefinidos**. Para servidores ThinkSystem, XClarity Administrator é pré-carregado com um conjunto de drivers de dispositivo para Linux para permitir a instalação do sistema operacional, bem como configuração básica de rede e de armazenamento para o sistema operacional final. Você pode adicionar esses drivers de dispositivo predefinidos para os perfis de imagem do SO personalizados e, em seguida, implantar os perfis em servidores gerenciados

  A Lenovo também reúne conjuntos de drivers de dispositivo predefinidos em um único pacote que pode ser baixado do Página da Web dos drivers do Lenovo Windows e do repositório de imagens do WinPE e, em seguida, importado para o repositório de imagens do SO. No momento, os arquivos do pacote estão disponíveis apenas para Windows. Se o arquivo contém drivers de dispositivo e arquivos de inicialização, é possível importar o arquivo do pacote do **Driver de Dispositivo** ou da guia **Imagem de Inicialização**.

  Notas:

  – Por padrão, os perfis de imagem do SO predefinidos incluem os drivers de dispositivo predefinidos.

  – Não é possível excluir drivers de dispositivo predefinidos que foram carregados quando você instalou o XClarity Administrator. No entanto, você pode excluir drivers de dispositivo predefinidos importados de um pacote da Lenovo.

  – O XClarity Administrator requer que os arquivos do pacote importados sejam assinados pela Lenovo. Ao importar um arquivo do pacote, um arquivo de assinatura .asc também deve ser importado.

- **Drivers de dispositivo personalizados**. É possível importar drivers de dispositivo predefinidos para o repositório de imagens do SO e, em seguida, adicioná-los em um perfil de imagem do SO personalizado.

  É possível obter drivers de dispositivos do Página da Web do repositório Lenovo YUM, do fornecedor (como Red Hat) ou com um driver de dispositivo personalizado que você mesmo criou. Para alguns drivers de dispositivo Windows, é possível gerar um driver de dispositivo personalizado extraindo o driver de dispositivo a partir do arquivo .exe de instalação para seu sistema local e criando um arquivo .zip.

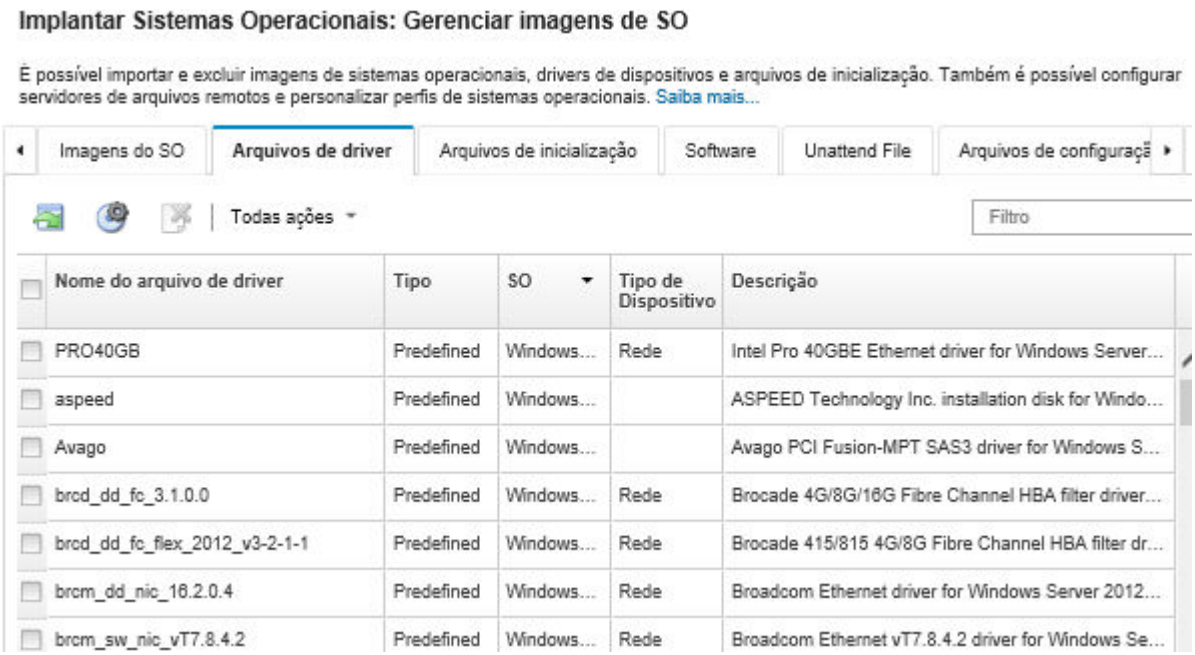
Os seguintes tipos de arquivo são suportados para serem importador para drivers de dispositivo personalizados.

Sistema Operacional	Tipos de arquivo do Driver de Dispositivo suportados
CentOS Linux	Não aceita
Microsoft® Windows® Azure Stack HCI	Não aceita
Microsoft Windows Hyper-V Server	Um arquivo .zip que contém os arquivos de driver de dispositivo brutos, que são normalmente agrupamentos de arquivos .inf, .cat e .dll.
Microsoft Windows Server	Um arquivo .zip que contém os arquivos de driver de dispositivo brutos, que são normalmente agrupamentos de arquivos .inf, .cat e .dll.
Red Hat® Enterprise Linux (RHEL) Server	Disco de atualização de driver (DUD) no formato de imagem .rpm ou .iso **Nota:** Se você aplicar um DUD .rpm ao perfil personalizado, o .rpm será instalado apenas no sistema operacional final. Ele não será instalado no ambiente de instalação (initrd). Para instalar um driver de dispositivo personalizado no initrd, importe um DUD .iso e aplique o .iso ao perfil personalizado.
Rocky Linux	Não aceita
SUSE® Linux Enterprise Server (SLES)	Disco de atualização de driver (DUD) no formato de imagem .rpm ou .iso **Nota:** Se você aplicar um DUD .rpm ao perfil personalizado, o .rpm será instalado apenas no sistema operacional final. Ele não será instalado no ambiente de instalação (initrd). Para instalar um driver de dispositivo personalizado no initrd, importe um DUD .iso e aplique o .iso ao perfil personalizado.
Ubuntu	Não aceita
VMware vSphere® Hypervisor (ESXi) com Lenovo Customization	Drivers de dispositivo no formato de imagem .vib

Nota: O repositório de imagens do SO poderá armazenar um número ilimitado de arquivos personalizados e predefinidos, se houver espaço disponível para armazenar os arquivos.

Procedimento

- Para importar um arquivo do pacote do Windows que contém drivers de dispositivo para o repositório de imagens do SO, conclua as etapas a seguir.
  1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
  2. Clique na guia **Arquivo de Driver**.



3. Clique em **Downloads → Arquivos do Pacote do Windows** para ir para a página de Suporte Lenovo e baixe o arquivo do pacote apropriado e o arquivo de assinatura associado para a imagem d SO para o sistema local.
4. Clique no ícone **Importar Arquivo do Pacote** ( ). A caixa de diálogo Importar Arquivo do Pacote é exibida.
5. Clique na guia **Importação Local** para fazer upload de arquivos do sistema local ou clique na guia **Importação Remota** para fazer upload de arquivos de um servidor de arquivos remoto.

   Nota: Para fazer upload de um arquivo de um servidor de arquivos remoto, você deve primeiro criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** ( ). Para obter mais informações, consulte Configurando um servidor de arquivos remoto
6. Se você escolheu usar um servidor de arquivos remoto, selecione o servidor que você deseja usar na lista **Servidor de Arquivos Remoto**.
7. Selecione o tipo de sistema operacional e a versão.
8. Digite o nome do arquivo para o arquivo do pacote e para o arquivo de assinatura associado ou clique em **Procurar** para encontrar os arquivos que deseja importar.
9. **Opcional:** digite uma descrição para o arquivo do pacote.
10. Clique em **Importar**.

    Dica: o arquivo é transferido por upload por uma conexão de rede segura. Dessa forma, a confiabilidade e o desempenho da rede afetam o tempo que demora para importar o arquivo.

    Se você fechar a guia ou a janela do navegador da Web na qual o arquivo está sendo transferido por upload localmente antes do término do processo, ocorrerá falha na importação.

- Para importar um driver de dispositivo individual para o repositório de imagens do SO, conclua as seguintes etapas.
  1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
  2. Clique na guia **Arquivos de Driver**.
  3. Clique no ícone **Importar Arquivo** ( ). A caixa de diálogo Importar Arquivo é exibida.

4. Clique na guia **Importação Local** para fazer upload de arquivos do sistema local ou clique na guia **Importação Remota** para fazer upload de arquivos de um servidor de arquivos remoto.

   Nota: Para fazer upload de um arquivo de um servidor de arquivos remoto, você deve primeiro criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** (). Para obter mais informações, consulte Configurando um servidor de arquivos remoto
5. Se você escolheu usar um servidor de arquivos remoto, selecione o servidor que você deseja usar na lista **Servidor de Arquivos Remoto**.
6. Selecione o tipo de sistema operacional e a versão.
7. Digite o nome do arquivo ou clique em **Procurar** para encontrar o driver de dispositivo que você deseja importar.
8. **Opcional:** digite uma descrição para o driver de dispositivo.
9. **Opcional:** selecione um tipo de soma de verificação para verificar se o arquivo que está sendo transferido por upload não está danificado e copie e cole o valor de soma de verificação no campo de texto fornecido.

   Se você selecionar um tipo de soma de verificação, especifique um valor de soma de verificação para verificar a integridade e a segurança do arquivo transferido por upload. O valor deve se originar de uma fonte segura de uma organização em que você confie. Se o arquivo transferido por upload corresponde ao valor de soma de verificação, será seguro continuar com a implantação. Caso contrário, você deverá fazer upload novamente do arquivo ou verificar o valor de soma de verificação.

   Três tipos de soma de verificação têm suporte:
   - **MD5**
   - **SHA1**
   - **SHA256**
10. Clique em **Importar**.

    Dica: o arquivo é transferido por upload por uma conexão de rede segura. Dessa forma, a confiabilidade e o desempenho da rede afetam o tempo que demora para importar o arquivo.

    Se você fechar a guia ou a janela do navegador da Web na qual o arquivo está sendo transferido por upload localmente antes do término do processo, ocorrerá falha na importação.

Depois de concluir

A imagem do driver de dispositivo é listada na guia **Arquivos de Driver** na página Gerenciar Imagens do SO.

Nesta página, é possível executar as ações a seguir:

- Criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** ().
- Remova um driver de dispositivo selecionado clicando no ícone **Excluir** ().
- Adicione um driver de dispositivo a um perfil da imagem do SO personalizada (consulte Criando um perfil da imagem do SO personalizada).

Importando definições de configuração personalizadas

As definições de configuração descrevem dados que precisam ser coletados dinamicamente durante a implantação do SO. O Lenovo XClarity Administrator usa um conjunto de configurações predefinidas, incluindo configurações globais, de rede e de local de armazenamento. Você pode usar essas configurações predefinidas e adicionar configurações personalizadas que não estão disponíveis por meio do XClarity Administrator.

Sobre esta tarefa

As configurações personalizadas são definidas na forma de um esquema JSON. O esquema deve estar em conformidade com a especificação JSON.

Quando você importa as configurações personalizadas para XClarity Administrator, o XClarity Administrator valida o esquema JSON. Se a validação for aprovada, o XClarity Administrator gerará macros personalizadas para cada configuração.

É possível usar as macros personalizadas no arquivo sem supervisão e no script pós-instalação.

Em arquivos sem supervisão

Você pode associar o arquivo de configuração personalizado a um arquivo sem supervisão e incluir esses macros personalizadas (e macros predefinidas) no arquivo sem supervisão.

É possível incluir um ou mais arquivos de configurações personalizadas em um perfil personalizado. Quando você implanta o perfil do SO em um conjunto de servidores de destino, é possível escolher qual arquivo de configuração deve ser usado. O XClarity Administrator processa a guia **Configurações personalizadas** na caixa de diálogo Implantar imagens de SO com base no esquema JSON no arquivo de configuração e permite que você especifique valores para cada configuração (objeto JSON) que está definida no arquivo.

Nota: A implantação do SO não continuará se a entrada não for especificada para alguma configuração personalizada.

Em scripts pós-instalação

Depois que os dados são coletados durante a implantação do SO, o XClarity Administrator cria uma instância do arquivo de configuração (que inclui as configurações personalizadas no arquivo selecionado e um subconjunto de configurações predefinidas) no sistema host que pode ser usada pelo script pós-instalação.

Notas:

- O arquivo de configuração é exclusivo de um perfil de imagem do SO personalizado.
- Você não pode modificar definições de configuração para perfis predefinidos de imagem do SO.
- Definições de configuração são suportadas somente para os seguintes sistemas operacionais:
  - Microsoft® Windows® Server
  - Red Hat® Enterprise Linux (RHEL) Server
  - Rocky Linux
  - SUSE® Linux Enterprise Server (SLES)
  - VMware vSphere® Hypervisor (ESXi) com Lenovo Customization 6.0u3 e atualizações posteriores e 6.5 e atualizações posteriores.

O repositório de imagens do SO poderá armazenar um número ilimitado de arquivos personalizados e predefinidos, se houver espaço disponível para armazenar os arquivos.

Procedimento

Para importar arquivos de configuração para o repositório de imagens do SO, conclua as seguintes etapas.

Etapa 1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.

Etapa 2. Clique na guia **Opções de configuração**.

Etapa 3. Clique no ícone **Importar Arquivo** ( ). A caixa de diálogo Importar Configurações é exibida.

Etapa 4. Clique na guia **Importação Local** para fazer upload de arquivos do sistema local ou clique na guia **Importação Remota** para fazer upload de arquivos de um servidor de arquivos remoto.

Nota: Para fazer upload de um arquivo de um servidor de arquivos remoto, você deve primeiro criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** ( ). Para obter mais informações, consulte Configurando um servidor de arquivos remoto

Etapa 5. Se você escolheu usar um servidor de arquivos remoto, selecione o servidor que você deseja usar na lista **Servidor de Arquivos Remoto**.

Etapa 6. Selecione o tipo de sistema operacional.

Etapa 7. Digite o nome do arquivo de configuração ou clique em **Procurar** para encontrar o arquivo que você deseja importar.

Etapa 8. **Opcional:** digite uma descrição das configurações.

Dica: use o campo **Descrição** para distinguir entre arquivos personalizados com o mesmo nome.

Etapa 9. **Opcional:** selecione um tipo de soma de verificação para verificar se o arquivo que está sendo transferido por upload não está danificado e copie e cole o valor de soma de verificação no campo de texto fornecido.

Se você selecionar um tipo de soma de verificação, especifique um valor de soma de verificação para verificar a integridade e a segurança do arquivo transferido por upload. O valor deve se originar de uma fonte segura de uma organização em que você confie. Se o arquivo transferido por upload corresponde ao valor de soma de verificação, será seguro continuar com a implantação. Caso contrário, você deverá fazer upload novamente do arquivo ou verificar o valor de soma de verificação.

Três tipos de soma de verificação têm suporte:
- **MD5**
- **SHA1**
- **SHA256**

Etapa 10. Clique em **Importar**. O formato JSON é validado quando você importa o arquivo. Se forem encontrados erros, uma caixa de diálogo será exibida com a mensagem de erro e o local.

Dica: o arquivo é transferido por upload por uma conexão de rede segura. Dessa forma, a confiabilidade e o desempenho da rede afetam o tempo que demora para importar o arquivo.

Atenção: Se você fechar a guia ou a janela do navegador da Web na qual o arquivo está sendo transferido por upload localmente antes do término do processo, ocorrerá falha na importação.

Depois de concluir

Os arquivos de configuração são listados na guia **Opções de configuração** na página Gerenciar imagens de SO.

Nessa página, também é possível executar as seguintes ações.

- Crie um arquivo de configuração clicando no ícone **Criar** () e especificando o nome do arquivo, descrição, tipo de SO e definições e valores de configuração. Clique em **Validar** para validar o esquema antes de salvar o arquivo.

  O editor identifica o local dos erros encontrados no arquivo. Observe que algumas mensagens estão somente em inglês.

- Visualize e modifique o arquivo de configuração clicando no ícone **Editar** ().

  Não é possível editar um arquivo de configuração que esteja associado a um arquivo sem supervisão.

  O editor identifica o local dos erros encontrados no arquivo. Observe que algumas mensagens estão somente em inglês.

- Copie o arquivo de configuração clicando no ícone **Copiar** ().

  Se você copiar um arquivo de configuração associado a um arquivo sem supervisão, o arquivo sem supervisão associado também será copiado e a associação será criada automaticamente entre os dois arquivos copiados.

- Remova o arquivo de configuração selecionado clicando no ícone **Excluir** ().

- Criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** ().

Para obter informações sobre como adicionar uma configuração a um perfil da imagem do SO personalizada, consulte Criando um perfil da imagem do SO personalizada.

Macros personalizadas

As *macros* fornecem a capacidade de adicionar dados variáveis (definições de configuração) a um arquivo sem supervisão ou script de pós-instalação. O Lenovo XClarity Administrator permite definir suas próprias configurações personalizadas, criando um arquivo de definições de configuração personalizada, usando o formato JSON.

O valor para cada definição de configuração personalizada varia de acordo com a entrada do usuário especificada durante a implantação do SO.

Quando você importa as configurações personalizadas no XClarity Administrator, o XClarity Administrator valida o esquema JSON. Se a validação for aprovada, o XClarity Administrator gerará macros personalizadas para cada configuração.

Para inserir macros personalizadas em um arquivo sem supervisão ou script pós-instalação, use o nome exclusivo do objeto, separe objetos aninhados usando um ponto e, em seguida, coloque uma cerquilha (#) ao redor do nome da macro, por exemplo, **#server_settings.server0.locale#**.

Notas:

- Não inclua o nome do objeto mais alto.
- Quando um objeto é criado de um modelo, o nome é anexado com um número exclusivo, começando com 0 (por exemplo, server0 e server1).

- Você pode ver o nome de cada macro da caixa de diálogo Implantar imagens de SO nas guias de Configurações personalizadas passando o mouse sobre o ícone **Ajuda** () próximo de cada configuração personalizada.

Definições de configuração

Você pode definir configurações personalizadas que:

- São comuns para todos os servidores de destino ou exclusivas de um servidor de destino específico.
- Tenham valores estáticos (não configurável) ou valores dinâmicos (configuráveis) que são inseridos ao implantar o perfil da imagem do SO.
- Tenham um número variável de elementos com base em um modelo. Por exemplo, é possível definir uma configuração que permite que você especifique 0 – 3 servidores NTP durante a implantação.

Configurações comuns

Durante a implantação do SO, os elementos da interface do usuário nas guias **Configurações comuns** na caixa de diálogo Implantar imagens de SO são processados com base nos objetos representados no objeto **content**. Os objetos descrevem as configurações e valores de que todos os servidores de destino precisam para a implantação do SO.

Para representar as configurações que são comuns para todos os servidores, o arquivo JSON deve conter um objeto pai com um objeto aninhado que contém o par nome/valor `"common":true`.

O exemplo a seguir usa os mesmos servidores NTP configuráveis (dinâmicos) para todos os servidores.

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": true,
      "description": "NTP Servers",
      "label": "NTP Servers",
      "maxElements": 3,
      "minElements": 0,
      "name": "common-ntpservers",
      "optional": true,
      "template": [{
         "autoCreateInstance": true,
         "category": "dynamic",
         "common": true,
         "description": "A NTP Server",
         "label": "NTP Server",
         "name": "ntpserver",
         "optional": true,
         "regex": "[\\w\\.]{1,64}$",
         "type": "string"
      }],
      "type": "array"
   },
   ...,
}
```

O exemplo a seguir usa o mesmo log de script pós-instalação não configurável (estático).

```
{
   "category": "dynamic",
   "content": [{
      "category": "static",
      "common": true,
```

```
      "description": "Directory location for post-installation script logging.",
      "name": "logpath",
      "optional": false,
      "type": "string",
      "value": "/tmp/mylogger.log"
   },
   ...,
}
```

Configurações específicas de servidor

Durante a implantação do SO, os elementos da interface do usuário na guia **Configurações específicas do servidor** na caixa de diálogo Implantar imagens de SO são processados com base nos objetos representados nos objetos **content** do modelo. Os objetos descrevem as configurações e valores de que um servidor de destino específico precisa para a implantação do SO.

Depois que os valores específicos de servidor são coletados na interface do usuário, um objeto **content** é criado em JSON para cada servidor de destino com base no objeto **template**. Cada objeto **content** contém um campo **name** e **targetServer** exclusivo, e os valores que foram inseridos para o servidor.

Para representar as configurações específicas do servidor, o arquivo JSON deve conter um objeto pai com o conteúdo a seguir:

- O par nome/valor `"category":"dynamic"`.
- Um objeto aninhado que contém o par nome/valor `"common":false`. Há suporte para apenas um objeto `"common": false` no conteúdo do objeto pai.
- Um objeto de modelo com um objeto de conteúdo integrado. Esta matriz do modelo pode conter apenas um objeto.

Por exemplo, se você deseja definir um local de SO exclusivo para cada servidor de destino

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": false,
      "name": "server-settings",
      "optional": false,
      "template": [{
         "category": "dynamic",
         "common": false,
         "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
         }],
         "name": "server",
         "optional": false,
         "type": "assoc_array"
      }],
      "type": "assoc_array"
   },
   ...,
}
```

Especificação JSON

A tabela a seguir descreve os campos que são permitidos na especificação JSON.

Parâmetro	Obrigatório / opcional	Tipo	Descrição
autoCreateInstance	opcional	Booleano	Indica se uma instância do objeto de modelo é criada automaticamente no arquivo JSON durante a implantação. Este pode ser um dos valores a seguir. • **true**. Uma instância do objeto de modelo é criada automaticamente no arquivo JSON durante a implantação. • **false**. (padrão) Uma instância do objeto de modelo *não é* criada automaticamente no arquivo JSON durante a implantação **Nota:** Esse campo pode ser colocado apenas no objeto de modelo.
categoria	Obrigatório	Sequência	Indica como o valor de cada configuração é preenchido. Este pode ser um dos valores a seguir: • **dynamic**. O valor é inserido pelo usuário em tempo de execução. O Lenovo XClarity Administrator solicita esse valor durante a implantação do SO. • **predefined**. O valor é predefinido pelo Lenovo XClarity Administrator. • **static**. O valor é especificado no esquema e não é alterado no tempo de execução. Os objetos aninhados herdam o valor desse campo de seu objeto pai. Se **category** estiver definido como `static` no objeto pai, deverá ser definido como `static` em todos os objetos aninhados também. Se **category** estiver definido como `dynamic` no objeto pai, poderá ser `static` ou `dynamic` nos objetos aninhados.
choices	opcional	Matriz de valores que correspondem à propriedade **type**	Matriz de valores estáticos (como strings ou números inteiros) para a configuração na qual o usuário pode selecionar durante a implantação do SO (por exemplo, `["enabled","disabled"]`).
comum	opcional	Booleano	Indica se este esquema de configuração se aplica a todos os servidores de destino. • **true**. O objeto se aplica a todos os servidores de destino. • **false**. (padrão) O objeto se aplica a um servidor de destino específico. Os objetos aninhados herdam o valor desse campo de seu objeto pai. Se **common** estiver definido como `true` no objeto pai, deverá ser definido como `true` em todos os objetos aninhados também. Se **common** estiver definido como `false` no objeto pai, deverá ser definido como `false` em todos os objetos aninhados.

Parâmetro	Obrigatório / opcional	Tipo	Descrição
content	opcional	Matriz de objetos	Padrão que representa objetos aninhados no esquema. Depois que os dados inseridos pelo usuário são coletados durante a implantação do SO, esse campo é usado para representar os valores finais para um determinado modelo na instância do arquivo de definições de configuração que é criado para a implantação.
padrão	opcional	Varia dependendo do **type**	O valor padrão.
descrição	opcional	Sequência	Descrição do objeto
label	opcional	Sequência	Rótulo para a configuração na interface do usuário que é exibida durante a implantação do SO
max	opcional	Número inteiro	Valor máximo, quando **type** estiver configurado como inteiro. O valor padrão é unlimited.
maxElements	opcional	Número inteiro	Número máximo de entradas na matriz para este objeto.
min	opcional	Número inteiro	Valor mínimo, quando **type** estiver configurado como inteiro. O valor padrão é 0.
minElements	opcional	Número inteiro	Número mínimo de entradas na matriz para este objeto.
nome	Obrigatório	Sequência	Nome exclusivo do objeto. Esse nome só pode conter os seguintes caracteres: alfanuméricos (a-z, A-Z e 0-9), sublinhado (_) e traço (-). Você pode fazer referência a **name** como uma macro personalizada no arquivo sem supervisão. Ao fazer referência a um objeto aninhado **name**, separe cada objeto usando um ponto (por exemplo, `mydeploy.node.locale`).
opcional	Obrigatório	Booleano	Indica se o objeto é opcional. Este pode ser um dos valores a seguir. • **true**. O campo é opcional. • **false**. O campo é obrigatório.
regex	opcional	Sequência	Expressão regular para validar o valor (por exemplo, `"[\\w\\.]{1,64}$"`)
script	opcional	Matriz de cadeias de caracteres	Lista de scripts, separados por vírgula, que têm dependências nos dados de objeto (por exemplo, `["/opt/lenovo/saphana/bin/saphana-create-saphana.sh", "create_hana.sh"]`). **Nota:** Os scripts devem estar disponíveis para o perfil de imagem do SO como um script de instalação ou software personalizado.

Parâmetro	Obrigatório / opcional	Tipo	Descrição
targetServer	opcional	Sequência	UUID de servidor de destino para a implantação do sistema operacional. Se common for verdadeiro, esse campo poderá ser vazio ou nulo e o servidor de destino será especificado durante a implantação do SO.

modelo	opcional	Matriz de objetos	Padrão que representa objetos reutilizáveis.
			Durante a implantação do SO, este modelo pode representar várias instâncias do objeto. Os campos **minElements** e **maxElements** podem ser usados para limitar o número de instâncias.
			
			O exemplo a seguir usa um modelo para representar uma matriz de servidores NTP de 1 a 3.
			`{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "NTP Servers",`
			`"label": "NTP Servers",`
			`"maxElements": 3,`
			`"minElements": 0,`
			`"name": "common-ntpservers",`
			`"optional": true,`
			`"template": [{`
			`"autoCreateInstance": true,`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "A NTP Server",`
			`"label": "NTP Server",`
			`"name": "ntpserver",`
			`"optional": true,`
			`"regex": "[\\w\\.]{1,64}$",`
			`"type": "string"`
			`}],`
			`"type": "array"`
			`},`
			
			Depois que os valores inseridos pelo usuário são coletados durante a implantação do SO, uma instância do arquivo de definições de configuração é criada com conteúdo específico para cada dispositivo no qual o sistema operacional deve ser implantado.
			`{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "NTP Servers",`
			`"label": "NTP Servers",`
			`"maxElements": 3,`
			`"minElements": 0,`
			`"name": "common-ntpservers",`
			`"optional": true,`
			`"content": [{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "A NTP Server",`
			`"label": "NTP Server",`
			`"name": "ntpserver0",`

Parâmetro	Obrigatório / opcional	Tipo	Descrição

			<pre>"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string",
			"value": "192.0.2.1"
			}],
			"template": [{
			"category": "dynamic",
			"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string"
			}],
			"type": "array"
			}</pre> **Notas:**
			• Um modelo é *necessário* no nível superior de objetos específicos do servidor (comum = falso).
			• Se **category** for `static`, o campo de modelo será ignorado.

tipo	Obrigatório	Sequência	Tipo de dados para o objeto. Este pode ser um dos valores a seguir. • **array** • **assoc_array** • **booleano** • **inteiro** • **senha** • **string** • **user_data**
value	opcional	Sequência	Um valor estático único para a configuração. **Notas:** • Se **default** estiver definido, esse campo poderá ser vazio ou nulo. Caso contrário, especifique um valor que corresponda a **type**. • Se **type** for `password`, especifique uma string não criptografada. • Se **type** for `assoc_array`ou `array`, você também deverá especificar um campo **content** vazio. • Se **type** for `user_data`, especifique um **value** com formato JSON válido. • Se **regex** estiver definido, esse valor será validado usando a expressão regular especificada.

As definições de configuração de exemplo a seguir definem as configurações de idioma em implementações SLES que podem ser adicionadas a um perfil personalizado.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
```

```
    "common": false,
    "name": "server-settings",
    "optional": false,
    "template": [{
        "autoCreateInstance": true,
        "category": "dynamic",
        "common": false,
        "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server",
        "optional": false,
        "type": "assoc_array"
    }],
    "type": "assoc_array"
},
{
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "template": [{
        "category": "dynamic",
        "common": true,
        "description": "A NTP Server",
        "label": "NTP Server",
        "name": "ntpserver",
        "optional": true,
        "regex": "[\\w\\.]{1,64}$",
        "type": "string"
    }],
    "type": "array"
},
{
    "category": "static",
    "common": true,
```

```
        "description": "Directory for post-installation script logging.",
        "name": "logpath",
        "optional": false,
        "type": "string",
        "value": "/tmp/mylogger.log"
    }],
    "description": "Custom configuration file for deployment of custom locale, NTP server,
                    and directory for post-installation script logs.",
    "label": "My Custom Deployment",
    "name": "myCustomDeploy",
    "optional": false,
    "type": "array"
}
```

O exemplo a seguir é a instância do arquivo de configuração que é criado no sistema de host depois que os valores inseridos pelo usuário são definidos durante a implantação.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
        "common": false,
        "name": "server-settings",
        "optional": false,
        "content": [{
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the OS language locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "OS Locale",
                "name": "locale",
                "optional": false,
                "type": "string",
                "value": "en_US"
            },
            {
                "category": "dynamic",
                "choices": ["english-us", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the keyboard locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "Keyboard Locale",
                "name": "keyboardLocale",
                "optional": false,
                "type": "string",
                "value": "english-us"
            }],
            "name": "server0",
            "optional": false,
            "type": "assoc_array",
            "targetServer": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
        },
        {
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
```

```
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server1",
        "optional": false,
        "type": "assoc_array",
        "targetServer": "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
    }],
    "template": [{
        "category": "dynamic",
        "common": false,
        "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server",
        "optional": false,
        "type": "assoc_array"
    }],
    "type": "assoc_array"
},
{
    "category": "dynamic",
```

```
        "common": true,
        "description": "NTP Servers",
        "label": "NTP Servers",
        "maxElements": 3,
        "minElements": 0,
        "name": "common-ntpservers",
        "optional": true,
        "content": [{
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver0,
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.1"
        },
        {
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver1",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.2"
        }],
        "template": [{
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string"
        }],
        "type": "array"
    },
    {
        "category": "static",
        "common": true,
        "description": "Directory for post-installation script logs.",
        "name": "logpath",
        "optional": false,
        "type": "string",
        "value": "/tmp/mylogger.log"
    }],
    "description": "Custom configuration file for deployment of custom locale, NTP server,
                    and directory for post-installation script logs.",
    "label": "My Custom Deployment",
    "name": "myCustomDeploy",
    "optional": false,
    "type": "array"
}
```

Macros predefinidas

As *macros* fornecem a capacidade de adicionar dados variáveis (definições de configuração) a um arquivo sem supervisão ou script de pós-instalação. O Lenovo XClarity Administrator fornece um conjunto de configurações predefinidas que você pode usar.

Para inserir macros predefinidas a um arquivo sem supervisão ou de script pós-instalação, prefixe a macro com "predefinida" para macros predefinidas, separe objetos aninhados usando um ponto e, em seguida, coloque uma cerquilha (#) ao redor do nome da macro, por exemplo **#predefined.globalSettings.ipAssignment#**.

O valor para cada macro predefinida varia com base na instância do XClarity Administrator. Por exemplo, o campo **Implantar imagens de SO → Configurações globais → Atribuição de IP** permite que você especifique o modo de IP. Depois que o valor inserido pelo usuário é coletado durante a implantação do SO, o valor é representado nas configurações predefinidas pela macro predefinida **#predefined.globalSettings.ipAssignment#** e na instância do arquivo JSON de configuração sob o nome do objeto ipAssignment.

A tabela a seguir lista as macros predefinidas (definições de configuração) que estão disponíveis em XClarity Administrator.

Nome da macro	Tipo	Descrição
predefinido	Objeto	Informações sobre todas as configurações de implantação do SO predefinidas
globalSettings	Objeto	Informações sobre configurações de implantação do SO
credenciais	Matriz de objetos	Informações sobre as credenciais do usuário
nome	Sequência	
tipo	Sequência	Tipo de sistema operacional. Este pode ser um dos valores a seguir. • **ESXi** • **LINUX** • **WINDOWS**
ipAssignment	Sequência	Opção de configuração de rede de host para implantação de sistema operacional. Este pode ser um dos valores a seguir. • **dhcpv4** • **staticv4** • **staticv6**
isVLANMode	Sequência	Indica se o modo VLAN é usado. Este pode ser um dos valores a seguir. • **true**. O modo VLAN é usado. • **false**. O modo VLAN não é usado.
hostPlatforms	Objeto	Configurações de implantação das plataformas de host
licenseKey	Sequência	Chave de licença a ser usada para Microsoft Windows ou VMware ESXi. Se você não tiver uma chave de licença, poderá definir esse campo como nulo.
networkSettings	Matriz	Informações sobre configurações de rede
dns1	Sequência	Servidor DNS preferencial para o host a ser usado após a implantação do sistema operacional
dns2	Sequência	Servidor DNS para o host a ser usado após a implantação do sistema operacional

Nome da macro	Tipo	Descrição
gateway	Sequência	Gateway do servidor de host a ser usado após a implantação do sistema operacional. Isso é usado quando a configuração de rede é definida como estática nas configurações globais de implantação do SO. **Dica:** para determinar o modo de IP, use GET /osdeployment/globalSettings.
nome do host	Sequência	Nome do host para o servidor de host. Se um nome do host não for especificado, um nome do host padrão será atribuído.
ipAddress	Sequência	Endereço IP do servidor de host a ser usado após a implantação do sistema operacional. Isso é usado quando a configuração de rede é definida como estática nas configurações globais de implantação do SO.
mtu	Longo	Unidade máxima de transmissão para o host a ser usada após a implantação do sistema operacional.
prefixLength	Sequência	Comprimento de prefixo do endereço IP do host a ser usado após a implantação do sistema operacional. Isso é usado quando a configuração de rede é definida como IPv6 estático nas configurações globais de implantação do SO.
selectedMAC	Sequência	Endereço MAC do servidor de host ao qual o endereço IP deve estar associado. O endereço MAC é definido como AUTO por padrão. Essa definição automaticamente detecta as portas Ethernet que podem ser configuradas e usadas para implantação. O primeiro endereço MAC (porta) detectado é usado por padrão. Se a conectividade for detectada em um endereço MAC diferente, o host do XClarity Administrator será reiniciado automaticamente para usar o endereço MAC recém-detectado para a implantação e selectedMAC é definido como o endereço MAC recentemente detectado. O modo VLAN é compatível somente para servidores que têm endereços MAC no inventário. Se AUTO for o único endereço MAC disponível para um servidor, VLANs não poderão ser usadas para implantar sistemas operacionais neste servidor. **Dica:** para obter o endereço MAC, use a propriedade de resposta **macaddress** em GET /hostPlatforms.
subnetCIDRNumber	Número inteiro	Máscara de sub-rede do servidor host a ser usada após a implantação do sistema operacional, no formato Classless Inter-Domain Routing (CIDR). Isso é usado quando a configuração de rede é definida como estática nas configurações globais de implantação do SO. O número CIDR é normalmente precedido por uma barra "/" e segue o endereço IP. Por exemplo, um endereço IP de 131.10.55.70 com uma máscara de sub-rede 255.0.0.0 (que tem 8 bits de rede) seria representado como 131.10.55.70/8. Para obter mais informações, consulte o Página da Web Tutorial da notação CIDR. **Dica:** para determinar o modo de IP, use GET /osdeployment/globalSettings.
subnetMask	Sequência	Máscara de sub-rede do servidor host a ser usada após a implantação do sistema operacional, em notação decimal pontilhada (por exemplo, 255.0.0.0.). Isso é usado quando a configuração de rede é definida como estática nas configurações globais de implantação do SO. **Dica:** para determinar o modo de IP, use GET /osdeployment/globalSettings.

Nome da macro	Tipo	Descrição
vlanId	Sequência	ID da VLAN para a marcação de VLAN do sistema operacional. Esse parâmetro será válido somente se estiver habilitado no modo VLAN. Para determinar se o modo VLAN está ativado, use GET /osdeployment/globalSettings na documentação online do XClarity Administrator. **Importante:** Especifique um ID de VLAN somente quando uma marca VLAN for necessária para funcionar na rede. O uso de tags de VLAN pode afetar a roteabilidade da rede entre o sistema operacional do host e o XClarity Administrator.
selectedImage	Sequência	ID do perfil da imagem do sistema operacional a ser implantada. **Dica:** para obter os IDs de perfil da imagem do sistema operacional, use a propriedade de resposta **availableImages** em GET /hostPlatforms.
storageSettings	Matriz	Local de armazenamento preferencial onde você quer implantar imagens do sistema operacional
targetDevice	Sequência	Dispositivo de destino. Este pode ser um dos valores a seguir. • **localdisk**. Unidade de disco local. A primeira unidade de disco local enumerada no servidor gerenciado é usada. • **M.2drive**. Unidade M.2. A primeira unidade M.2 enumerada no servidor gerenciado é usada. • **usbdisk**. Hipervisor USB Integrado. Esse local é aplicável apenas quando uma imagem do VMware ESXi está sendo implantada nos servidores gerenciados. Se há duas chaves do hipervisor instaladas no servidor gerenciado, o instalador do VMware seleciona a primeira chave enumerada para implantação. • **lunpluswwn=***LUN@WWN*. Armazenamento FC SAN (por exemplo, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. Armazenamento iSCSI SAN (por exemplo, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). A especificação de *IQN* será opcional se apenas um destino iSCSI for configurado. Se o *IQN* não for especificado, o primeiro destino iSCSI detectado será selecionado para OSDN. Se especificado, uma correspondência exata será feita. **Nota:** Para servidores ThinkServer, esse valor é sempre "localdisk."
unattendFileId	Sequência	ID do arquivo sem supervisão a ser usado com essa implantação
uuid do	Sequência	UUID do servidor de host no qual o sistema operacional deve ser implantado
imageSettings	Objeto	Informações sobre cada imagem do SO e o perfil de imagem
nome	Sequência	Nome da imagem do sistema operacional
perfil	Sequência	Nome do perfil da imagem
otherSettings	Objeto	Configurações adicionais que estão relacionadas aos trabalhos de implantação do SO em execução no momento
deployDataAndSoftwareLocation	Sequência	Caminho até a carga de software extraído, arquivos personalizados e dados de implantação (como certificados e logs)

Nome da macro	Tipo	Descrição

installRepoUrl	Sequência	(SLES 15 e posterior somente) URL da imagem do pacote importado
		Você pode usar essa macro predefinida em arquivos sem supervisão personalizados para a media_url na seção complementar, por exemplo:
		`<add-on>`
		`<add_on_products config:type="list">`
		`<listentry>`
		`<media_url>`**#predefined.otherSettings.installRepoUrl#**
		`</media_url>`
		`<product>sle-module-basesystem</product>`
		`<product_dir>/Module-Basesystem</product_dir>`
		`</listentry>`
		`</add_on_products>`
		`</add-on>`

lxcaIp	Sequência	O endereço IP da instância do XClarity Administrator
lxcaRelease	Sequência	Versão do XClarity Administrator (por exemplo, 2.0.0)
jobId	Sequência	ID do trabalho de implantação do SO em execução no momento
ntpServer	Sequência	Servidor NTP que está associado com o XClarity Administrator
statusSettings	Objeto	Configurações de status de implantação do SO
urlStatus	Sequência	URL HTTPS (incluindo a porta) que o XClarity Administrator usa para registro de status
certLocation	Sequência	Pasta que contém os certificados necessários para acessar o serviço da Web **urlStatus** no SO do host na primeira inicialização
sdkLocation	Sequência	Local dos scripts auxiliares e interfaces fornecidos pelo XClarity Administrator para acessar o XClarity Administrator
timezone	Sequência	Fuso horário configurado para XClarity Administrator (por exemplo, América/Nova_York)
unattendSettings	Objeto	Configurações que são usadas para preencher o arquivo sem supervisão. Esses valores são específicos da versão do XClarity Administrator
networkConfig	Sequência	(Somente para ESXi e RHEL) Conteúdo predefinido do XClarity Administrator para uso durante a instalação sem supervisão. Isso define as configurações de rede para o sistema operacional
preinstallConfig	Sequência	Conteúdo predefinido do XClarity Administrator para uso durante a pré-instalação sem supervisão. Isso inclui o status pré-instalação. • Para ESXi e RHEL, isso usa o gancho de scripts pré-instalação %pre. • Para SLES, isso usa o gancho de scripts pré-instalação <scripts>. **Atenção:** É altamente recomendado incluir essa macro no arquivo sem supervisão personalizado. Você pode colocar a macro no arquivo sem supervisão em qualquer lugar após a linha 1 (após a tag <xml>).

Nome da macro	Tipo	Descrição
postinstallConfig	Sequência	Conteúdo predefinido do XClarity Administrator para uso após o servidor ser configurado e inicializado pela primeira vez. Isso inclui o status pós-instalação. • Para ESXi e RHEL, isso usa o gancho de scripts pós-instalação %post • Para SLES, isso usa o gancho de scripts pós-instalação <scripts>. • Para Windows, isso usa a seção "specialize configurações". **Atenção:** É altamente recomendado que essa macro seja incluída no arquivo sem supervisão personalizado. Você pode colocar a macro no arquivo sem supervisão em qualquer lugar após a linha 1 (após a tag <xml>).
reportWorkloadNotComplete	Sequência	Quando essa macro estiver presente, a macro postinstallConfig não relatará o status Instalação do SO concluída (17). O perfil personalizado deve relatar a conclusão.
storageConfig	Sequência	(Somente para ESXi e RHEL) Conteúdo predefinido do XClarity Administrator para uso durante a instalação sem supervisão. Isso define as configurações de armazenamento para o sistema operacional.

Importando arquivos sem supervisão personalizados

É possível importar arquivos sem supervisão personalizados para o repositório de imagens do SO. Esses arquivos podem ser usados para personalizar perfis de imagens do Linux e do Windows.

Sobre esta tarefa

Os seguintes tipos de arquivo são suportados para arquivos sem supervisão personalizados.

Sistema Operacional	Tipos de arquivo compatíveis	Mais informações
CentOS Linux	Não aceita	
Microsoft® Windows® Azure Stack HCI	Não aceita	
Microsoft Windows Hyper-V Server	Não aceita	
Microsoft Windows Server	Sem supervisão (.xml)	Para obter mais informações sobre arquivos sem supervisão, consulte Página da Web de referência do Windows Setup sem supervisão.

Sistema Operacional	Tipos de arquivo compatíveis	Mais informações
Red Hat® Enterprise Linux (RHEL) Server	Kickstart (.cfg)	Para obter mais informações sobre arquivos sem supervisão, consulte Red Hat: página Automatizar a instalação com o Kickstart. Considere o seguinte ao incluir seções %pre, %post, % firstboot no arquivo. • Você pode incluir várias seções %pre, %post, %firstboot no arquivo sem supervisão. No entanto, preste atenção à ordem das seções. • Quando a macro **#predefined.unattendSettings. preinstallConfig#** recomendada estiver presente no arquivo sem supervisão, XClarity Administrator incluirá uma seção %pre antes de todas as outras seções %pre no arquivo. • Quando a macro **#predefined.unattendSettings. postinstallConfig#** recomendada estiver presente no arquivo sem supervisão, o XClarity Administrator incluirá seções %post e %firstboot antes de todas as outras seções %post e %firstboot no arquivo.
Rocky Linux	Kickstart (.cfg)	Para obter mais informações sobre arquivos sem supervisão, consulte o Red Hat: página Automatizar a instalação com o Kickstart. Considere o seguinte ao incluir seções %pre, %post, % firstboot no arquivo. • Você pode incluir várias seções %pre, %post, %firstboot no arquivo sem supervisão. No entanto, preste atenção à ordem das seções. • Quando a macro **#predefined.unattendSettings. preinstallConfig#** recomendada estiver presente no arquivo sem supervisão, XClarity Administrator incluirá uma seção %pre antes de todas as outras seções %pre no arquivo. • Quando a macro **#predefined.unattendSettings. postinstallConfig#** recomendada estiver presente no arquivo sem supervisão, o XClarity Administrator incluirá seções %post e %firstboot antes de todas as outras seções %post e %firstboot no arquivo.
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	Para obter mais informações sobre arquivos sem supervisão, consulte SUSE: Página da Web do AutoYaST.

Sistema Operacional	Tipos de arquivo compatíveis	Mais informações
Ubuntu	Não aceita	
VMware vSphere® Hypervisor (ESXi) com Lenovo Customization	Kickstart (.cfg)	Suportados somente para ESXi 6.0u3 e atualizações mais recentes e 6.5 e posterior. Para obter mais informações sobre arquivos sem supervisão, consulte VMware: Instalando ou atualizando hosts usando uma página da Web de script. Considere o seguinte ao incluir seções %pre, %post, % firstboot no arquivo. • Você pode incluir várias seções %pre, %post, %firstboot no arquivo sem supervisão. No entanto, preste atenção à ordem das seções. • Quando a macro **#predefined.unattendSettings. preinstallConfig#** recomendada estiver presente no arquivo sem supervisão, XClarity Administrator incluirá uma seção %pre antes de todas as outras seções %pre no arquivo. • Quando a macro **#predefined.unattendSettings. postinstallConfig#** recomendada estiver presente no arquivo sem supervisão, o XClarity Administrator incluirá seções %post e %firstboot antes de todas as outras seções %post e %firstboot no arquivo.

Atenção:

- É possível inserir macros predefinidas e personalizadas (definições de configuração) no arquivo sem supervisão usando o nome exclusivo do objeto. Valores predefinidos são dinâmicos com base nas instâncias XClarity Administrator. Macros personalizadas são dinâmicas com base na entrada do usuário que é especificada durante a implantação do SO.

  Notas:

  - Coloque uma cerquilha (#) ao redor do nome da macro.
  - Para objetos aninhados, separe cada nome de objeto usando um ponto (por exemplo, **#server_ settings.server0.locale#**).
  - Para macros personalizadas, não inclua o nome de objeto mais alto. Para as macros predefinidas, inclua no nome da macro o prefixo "predefinido".
  - Quando um objeto é criado de um modelo, o nome é anexado com um número exclusivo, começando com 0 (por exemplo, **server0** e **server1**).
  - Você pode ver o nome de cada macro da caixa de diálogo Implantar imagens de SO nas guias de Configurações personalizadas passando o mouse sobre o ícone Ajuda () próximo de cada configuração personalizada.
  - Para obter uma lista de macros predefinidas, consulte Macros predefinidas. Para obter informações sobre as configurações e macros personalizadas, consulte Macros personalizadas.
- O XClarity Administrator fornece as macros predefinidas a seguir que são usadas para comunicar o status do instalador do SO, além de várias outras etapas de instalação críticas. É altamente recomendável incluir essas macros no arquivo sem supervisão (consulte Inserindo macros predefinidas e personalizadas para um arquivo sem supervisão).
  - #predefined.unattendSettings.preinstallConfig#
  - #predefined.unattendSettings postinstallConfig#

O repositório de imagens do SO poderá armazenar um número ilimitado de arquivos personalizados e predefinidos, se houver espaço disponível para armazenar os arquivos.

Procedimento

Para importar arquivos sem supervisão para o repositório de imagens do SO, conclua as seguintes etapas.

Etapa 1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.

Etapa 2. Clique na guia **Arquivos sem supervisão**.

Etapa 3. Clique no ícone **Importar Arquivo** ( ). A caixa de diálogo Importar Arquivo é exibida.

Etapa 4. Clique na guia **Importação Local** para fazer upload de arquivos do sistema local ou clique na guia **Importação Remota** para fazer upload de arquivos de um servidor de arquivos remoto.

Nota: Para fazer upload de um arquivo de um servidor de arquivos remoto, você deve primeiro criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** ( ). Para obter mais informações, consulte Configurando um servidor de arquivos remoto .

Etapa 5. Se você escolheu usar um servidor de arquivos remoto, selecione o servidor que você deseja usar na lista **Servidor de Arquivos Remoto**.

Etapa 6. Selecione o tipo de sistema operacional.

Etapa 7. Digite o nome do arquivo sem supervisão ou clique em **Procurar** para encontrar o arquivo que você deseja importar.

Etapa 8. **Opcional:** digite uma descrição para o arquivo sem supervisão.

Dica: use o campo **Descrição** para distinguir entre arquivos personalizados com o mesmo nome.

Etapa 9. **Opcional:** selecione um tipo de soma de verificação para verificar se o arquivo que está sendo transferido por upload não está danificado e copie e cole o valor de soma de verificação no campo de texto fornecido.

Se você selecionar um tipo de soma de verificação, especifique um valor de soma de verificação para verificar a integridade e a segurança do arquivo transferido por upload. O valor deve se originar de uma fonte segura de uma organização em que você confie. Se o arquivo transferido por upload corresponde ao valor de soma de verificação, será seguro continuar com a implantação. Caso contrário, você deverá fazer upload novamente do arquivo ou verificar o valor de soma de verificação.

Três tipos de soma de verificação têm suporte:
- **MD5**

- **SHA1**
- **SHA256**

Etapa 10. Clique em **Importar**.

Dica: o arquivo é transferido por upload por uma conexão de rede segura. Dessa forma, a confiabilidade e o desempenho da rede afetam o tempo que demora para importar o arquivo.

Se você fechar a guia ou a janela do navegador da Web na qual o arquivo está sendo transferido por upload localmente antes do término do processo, ocorrerá falha na importação.

Depois de concluir

A imagem do arquivo sem supervisão é listada na guia **Arquivos sem supervisão** na página Gerenciar imagens de SO.

Nesta página, é possível executar as ações a seguir:

- Crie um arquivo sem supervisão clicando no ícone **Criar** ( ).

  O editor identifica o local dos erros encontrados no arquivo. Observe que algumas mensagens estão somente em inglês.
- Associe um arquivo sem supervisão a um arquivo de configuração (consulte Associando um arquivo sem supervisão a um arquivo de configuração).
- Visualize e modifique um arquivo sem supervisão clicando no ícone **Editar** ( ).

  O editor identifica o local dos erros encontrados no arquivo. Observe que algumas mensagens estão somente em inglês.
- Copiar um arquivo sem supervisão clicando no ícone **Copiar** ( ).

  Se você copiar um arquivo sem supervisão associado a um arquivo de configuração, o arquivo de configuração associado também será copiado e a associação será criada automaticamente entre os dois arquivos copiados.
- Remova os arquivos sem supervisão selecionados clicando no ícone **Excluir** ( ).
- Criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** ( ).

Para obter informações sobre como adicionar um arquivo sem supervisão a um perfil da imagem do SO personalizada, consulte Criando um perfil da imagem do SO personalizada.

Inserindo macros predefinidas e personalizadas para um arquivo sem supervisão

Você pode adicionar macros predefinidas e personalizadas a um arquivo sem supervisão.

Sobre esta tarefa

Macros fornecem a capacidade de adicionar dados dinâmicos (definições de configuração) a um arquivo sem supervisão. Você fornece os valores de dados quando o perfil de imagem do SO é implantado.

O Lenovo XClarity Administrator fornece um conjunto de macros *predefinidas* que você pode adicionar a um arquivo sem supervisão sem a associação de um arquivo de configuração personalizado. Para obter uma lista de macros predefinidas, consulte Macros predefinidas.

É altamente recomendado incluir as seguintes macros predefinidas nos arquivos sem supervisão personalizados.

- **#predefined.unattendSettings.preinstallConfig#** e **#predefined.unattendSettings postinstallConfig#**. Usadas para comunicar o status do instalador do SO, além de várias outras etapas de instalação críticas.

  Consulte os seguintes cenários de implantação do SO de exemplo para obter mais informações sobre como incluir macros de configuração da instalação.
  - Implantando o RHEL e um aplicativo Hello World PHP com o uso de um arquivo sem supervisão personalizado
  - Implantando o SLES 12 SP3 com um código do idioma configurável e servidores NTP
  - Implantando o VMware ESXi v6.7 com Lenovo Customization em um disco local usando um endereço IP estático
  - Implantação do Windows 2016 com recursos personalizados
- **#predefined.unattendSettings.networkConfig#**. (Somente para ESXi e RHEL) Permite que o XClarity Administrator configure a rede. Essa macro usa as configurações de rede especificadas na página Implantar imagens de SO. Se você não incluir esta macro no arquivo sem supervisão ou se as configurações de rede não estiverem definidas no XClarity Administrator, configure a interface IP como parte do arquivo sem supervisão para que o host roteie uma rede de volta para o XClarity Administrator.

  Consulte os seguintes cenários de implantação do SO de exemplo para obter mais informações sobre como incluir a macro de configuração da rede.
  - Implantando o RHEL e um aplicativo Hello World PHP com o uso de um arquivo sem supervisão personalizado
  - Implantando o VMware ESXi v6.7 com Lenovo Customization em um disco local usando um endereço IP estático
- **#predefined.unattendSettings.storageConfig#**. (Somente para ESXi e RHEL) Permite que o XClarity Administrator configure armazenamento no host. Essa macro usa as configurações de armazenamento especificadas na página Implantar imagens de SO. Se você não incluir esta macro no arquivo sem supervisão ou se as configurações de armazenamento não estiverem definidas no XClarity Administrator, especifique a configuração de armazenamento no arquivo sem supervisão.

  Consulte os seguintes cenários de implantação do SO de exemplo para obter mais informações sobre como incluir a macro de configuração de armazenamento.
  - Implantando o RHEL e um aplicativo Hello World PHP com o uso de um arquivo sem supervisão personalizado
  - Implantando o VMware ESXi v6.7 com Lenovo Customization em um disco local usando um endereço IP estático

Você pode criar macros *personalizadas* criando um arquivo de definições de configuração e associando o arquivo sem supervisão a um arquivo de definições de configuração personalizado. Quando você importa o arquivo de definições de configuração personalizado, XClarity Administrator cria uma macro para cada configuração no arquivo.

Procedimento

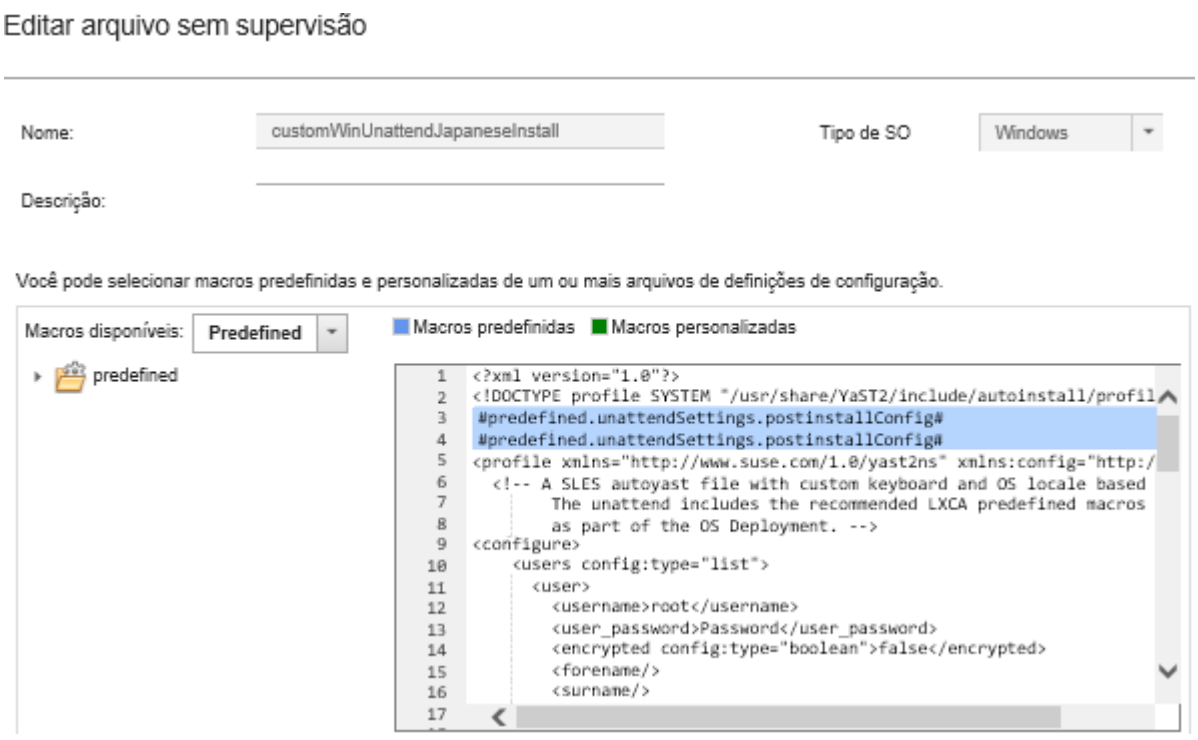
Conclua as seguintes etapas para adicionar macros a um arquivo sem supervisão.

Etapa 1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.

Etapa 2. Clique na guia **Arquivos sem supervisão**.

Etapa 3. Selecione o arquivo sem supervisão que você deseja editar.

Etapa 4. Clique no ícone **Editar** ( ) para exibir a caixa de diálogo Editar arquivo sem supervisão.



Etapa 5. Adicione as macros predefinidas recomendadas, por exemplo:

1. Coloque o cursor no arquivo sem supervisão em qualquer lugar após a linha 1 (após a tag <xml>).
2. Expanda a lista **predefinir → unattendSettings** na lista de macros disponíveis.
3. Clique no **preinstallConfig** e **postinstallConfig** para adicionar as macros predefinidas ao arquivo sem supervisão.

   O seguinte código é adicionado ao arquivo:

   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#

Etapa 6. Adicione adicionais macros predefinidas ou personalizadas, colocando o cursor no local correto no arquivo sem supervisão e, em seguida, clicando a macro na lista.

Etapa 7. Clique em **Salvar**.

Associando um arquivo sem supervisão a um arquivo de configuração

É possível associar (vincular) definições de configuração a um arquivo sem supervisão e, em seguida, adicionar as macros personalizadas associadas ao arquivo sem supervisão.

Sobre esta tarefa

É possível incluir macros predefinidas em um arquivo sem supervisão sem a associação de um arquivo de configuração personalizado.

Não é possível editar arquivos de configuração que estão associados a arquivos sem supervisão. No entanto, é possível copiar um arquivo associado e, em seguida, editar a cópia.

Procedimento

Conclua os seguintes passos para associar arquivos sem supervisão a um arquivo de configuração.

Etapa 1. Na barra de menus Lenovo XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.

Etapa 2. Clique na guia **Arquivos sem supervisão**.

Etapa 3. Selecione o arquivo sem supervisão personalizado.

Etapa 4. Clique no ícone **Associar um arquivo de configuração** () para exibir a caixa de diálogo Associar um arquivo sem supervisão.

Etapa 5. Selecione um ou arquivo de configuração para associar ao arquivo sem supervisão.

Etapa 6. Adicione macros predefinidas e personalizadas ao arquivo sem supervisão colocando o cursor no local no editor onde você quer adicionar a macro e, em seguida, selecionando a macro na lista disponível (consulte Inserindo macros predefinidas e personalizadas para um arquivo sem supervisão).

É possível inserir macros no arquivo sem supervisão usando o nome exclusivo do objeto. Para objetos de nome aninhados, separe cada objeto usando um ponto (por exemplo, `server_specific_settings.server.locale`). Observe que você não inclui o nome mais alto.

Etapa 7. Clique em **Associar** para associar os arquivos juntos.

Importando scripts de instalação personalizados

É possível importar scripts de instalação para o repositório de imagens do SO. Esses arquivos podem ser usados para personalizar as imagens do Linux e do Windows.

Sobre esta tarefa

Atualmente, apenas os scripts pós-instalação são suportados.

A tabela a seguir lista os tipos de arquivo para scripts de instalação para os quais Lenovo XClarity Administrator oferece suporte para cada sistema operacional. Observe que determinadas versões de sistema operacional não oferecem suporte a todos os tipos de arquivo a que o XClarity Administrator oferece suporte (por exemplo, alguns versões RHEL podem não incluir Perl no mínimo perfil e, portanto, não serão executado scripts Perl). Certifique-se de usar o tipo de arquivo correto para as versões de sistema operacional que você deseja implantar.

Sistema Operacional	Tipos de arquivo compatíveis	Mais informações
CentOS Linux	Não aceita	
Microsoft® Windows® Azure Stack HCI	Não aceita	
Microsoft Windows Hyper-V Server	Não aceita	
Microsoft® Windows® Server	Arquivo de comando (. cmd), PowerShell (. ps1)	O caminho de arquivos e dados personalizado padrão é `C:\lxca`. Para obter mais informações sobre scripts de instalação, consulte o Página da Web Adicionar um script personalizado ao Windows Setup
Red Hat® Enterprise Linux (RHEL) Server	Bash (.sh), Perl (.pm ou. pl), Python (. py)	O caminho arquivos e dados personalizados padrão é `/home/lxca`. Para obter mais informações sobre scripts de instalação, consulte o RHEL: Página da Web de script pós-instalação.

Sistema Operacional	Tipos de arquivo compatíveis	Mais informações
Rocky Linux	Bash (.sh), Perl (.pm ou. pl), Python (. py)	O caminho arquivos e dados personalizados padrão é `/home/lxca`. Para obter mais informações sobre scripts de instalação, consulte o RHEL: Página da Web de script pós-instalação
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm ou. pl), Python (. py)	O caminho arquivos e dados personalizados padrão é `/home/lxca`. Para obter mais informações sobre scripts de instalação, consulte o SUSE: Página da Web de script de usuário personalizado
Ubuntu	Não aceita	
VMware vSphere® Hypervisor (ESXi) com Lenovo Customization	Bash (.sh), Python (.py)	O caminho arquivos e dados personalizados padrão é `/home/lxca`. Para obter mais informações sobre scripts de instalação, consulte o VMware: Página da Web de instalação e scripts de atualização

Nota: O repositório de imagens do SO poderá armazenar um número ilimitado de arquivos personalizados e predefinidos, se houver espaço disponível para armazenar os arquivos.

Depois que os dados são coletados durante a implantação do SO, o XClarity Administrator cria uma instância do arquivo de configuração (que inclui as configurações personalizadas no arquivo selecionado e um subconjunto de configurações predefinidas) no sistema host que pode ser usada pelo script pós-instalação.

É possível inserir macros predefinidas e personalizadas (definições de configuração) no script de pós-instalação usando o nome exclusivo do objeto. Valores predefinidos são dinâmicos com base nas instâncias XClarity Administrator. Macros personalizadas são dinâmicas com base na entrada do usuário que é especificada durante a implantação do SO.

Notas:

- Coloque uma cerquilha (#) ao redor do nome da macro.
- Para objetos aninhados, separe cada nome de objeto usando um ponto (por exemplo, **#server_settings.server0.locale#**).
- Para macros personalizadas, não inclua o nome de objeto mais alto. Para as macros predefinidas, inclua no nome da macro o prefixo "predefinido".
- Quando um objeto é criado de um modelo, o nome é anexado com um número exclusivo, começando com 0 (por exemplo, **server0** e **server1**).
- Você pode ver o nome de cada macro da caixa de diálogo Implantar imagens de SO nas guias de Configurações personalizadas passando o mouse sobre o ícone Ajuda ( ) próximo de cada configuração personalizada.
- Para obter uma lista de macros predefinidas, consulte Macros predefinidas. Para obter informações sobre as configurações e macros personalizadas, consulte Macros personalizadas.

As macros predefinidas recomendadas no arquivo sem supervisão reportam o status de implantação do sistema operacional final e o status ao baixar e executar scripts pós-instalação. Você pode modificar o script pós-instalação para incluir o registro do status personalizado, dependendo do sistema operacional de

destino. Para obter mais informações, consulte Adicionando relatório de status personalizado aos scripts de instalação.

Procedimento

Para importar scripts de instalação para o repositório de imagens do SO, conclua as seguintes etapas.

Etapa 1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.

Etapa 2. Clique na guia **Scripts de instalação**.

Etapa 3. Clique no ícone **Importar Arquivo** ( ). A caixa de diálogo Importar script de instalação é exibida.

Etapa 4. Clique na guia **Importação Local** para fazer upload de arquivos do sistema local ou clique na guia **Importação Remota** para fazer upload de arquivos de um servidor de arquivos remoto.

Nota: Para fazer upload de um arquivo de um servidor de arquivos remoto, você deve primeiro criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** ( ). Para obter mais informações, consulte Configurando um servidor de arquivos remoto

Etapa 5. Se você escolheu usar um servidor de arquivos remoto, selecione o servidor que você deseja usar na lista **Servidor de Arquivos Remoto**.

Etapa 6. Selecione o tipo de sistema operacional.

Etapa 7. Digite o nome do arquivo do script de instalação ou clique em **Procurar** para encontrar o arquivo que você deseja importar.

Etapa 8. **Opcional:** digite uma descrição para o script de instalação.

Dica: use o campo **Descrição** para distinguir entre arquivos personalizados com o mesmo nome.

Etapa 9. **Opcional:** selecione um tipo de soma de verificação para verificar se o arquivo que está sendo transferido por upload não está danificado e copie e cole o valor de soma de verificação no campo de texto fornecido.

Se você selecionar um tipo de soma de verificação, especifique um valor de soma de verificação para verificar a integridade e a segurança do arquivo transferido por upload. O valor deve se originar de uma fonte segura de uma organização em que você confie. Se o arquivo transferido por upload corresponde ao valor de soma de verificação, será seguro continuar com a implantação. Caso contrário, você deverá fazer upload novamente do arquivo ou verificar o valor de soma de verificação.

Três tipos de soma de verificação têm suporte:

- **MD5**

- **SHA1**
- **SHA256**

Etapa 10. Clique em **Importar**.

Dica: o arquivo é transferido por upload por uma conexão de rede segura. Dessa forma, a confiabilidade e o desempenho da rede afetam o tempo que demora para importar o arquivo.

Se você fechar a guia ou a janela do navegador da Web na qual o arquivo está sendo transferido por upload localmente antes do término do processo, ocorrerá falha na importação.

Depois de concluir

Os scripts de instalação estão listados na guia **Scripts de instalação** na página Gerenciar imagens de SO.

Nesta página, é possível executar as ações a seguir:

- Criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** ().
- Remova os scripts de instalação selecionados clicando no ícone **Excluir** ().

Para obter informações sobre como adicionar um script de instalação a um perfil da imagem do SO personalizada, consulte Criando um perfil da imagem do SO personalizada.

Adicionando relatório de status personalizado aos scripts de instalação

As macros predefinidas recomendadas no arquivo sem supervisão reportam o status de implantação do sistema operacional final e o status ao baixar e executar scripts pós-instalação. Você pode incluir relatórios de status adicionais nos scripts pós-instalação.

Linux

No Linux, é possível usar o comando `curl` a seguir para relatar status.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"<status_ID>"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Em que <*status_ID*> pode ser um dos valores a seguir.

- **44**. Implantação de carga de trabalho bem-sucedida
- **45**. Implantação de carga de trabalho em execução com aviso
- **46**. Falha na implantação da carga de trabalho
- **47**. Mensagem de implantação da carga de trabalho
- **48**. Erro de script pós-instalação personalizado

Observe que o comando `curl` usa macros predefinidas para a URL HTTPS URL que o Lenovo XClarity Administrator usa para relatório de status (**predefined.otherSettings.statusSettings.urlStatus**) e para a pasta que contém os certificados necessários para acessar o serviço Web urlStatus do SO do host na primeira inicialização (**predefined.otherSettings.statusSettings.certLocation**). O exemplo a seguir relata um erro no script pós-instalação.

O exemplo a seguir relata que ocorreu um erro no script pós-instalação.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"48"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Windows

No Windows, é possível importar o script `LXCA.psm1` e chamar os seguintes comandos para relatar status.

- **initializeRestClient**

  Inicializa o cliente REST. Use a seguinte sintaxe para executar este comando. Esse comando é necessário antes de executar os comandos de geração de relatórios.

  ```
  initializeRestClient
  ```

- **testLXCAConnection**

  Verifica se o XClarity Administrator pode se conectar ao servidor host. Use a seguinte sintaxe para executar este comando. Esse comando é opcional, mas recomendado no script de instalação antes de executar os comandos de geração de relatórios.

  ```
  testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"
  ```

- **reportWorkloadDeploymentSucceeded**

  Relata uma mensagem de conclusão bem-sucedida para ser registrada no log de tarefas doXClarity Administrator. Use a seguinte sintaxe para executar este comando.

  Dica: se a macro **#predefined.unattendSettings.reportWorkloadNotComplete#** for incluída em um arquivo sem supervisão personalizado ou em um script pós-instalação, inclua o comando **reportWorkloadDeploymentSucceeded** no script pós-instalação para indicar a conclusão bem-sucedida. Caso contrário, XClarity Administrator reportará automaticamente um status concluído depois que todos os scripts pós-instalação forem executados.

  ```
  reportWorkloadDeploymentSucceeded -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#"
  ```

- **reportWorkloadDeploymentRunningWithWarning**

  Relata uma mensagem de aviso para ser registrada no log de tarefas doXClarity Administrator. Use a seguinte sintaxe para executar este comando.

  ```
  reportWorkloadDeploymentRunningWithWarning -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" –WarningMessage "<message_text>"
  ```

- **reportWorkloadDeploymentFailed**

  Relata uma mensagem de falha para ser registrada no log de tarefas doXClarity Administrator. Use a seguinte sintaxe para executar este comando.

  ```
  reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "<message_text>"
  ```

- **reportCustomPostInstallScriptError**

  Relata uma mensagem de scrip pós-instalação para ser registrada no log de tarefas doXClarity Administrator. Use a seguinte sintaxe para executar este comando.

  ```
  reportCustomPostInstallScriptError -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

- **reportWorkloadDeploymentMessage**

  Relata uma mensagem geral para ser registrada no log de tarefas do XClarity Administrator sem afetar o estado da implantação. Use a seguinte sintaxe para executar este comando.

  ```
  reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

Em que <*message_text*> é a mensagem para a qual você deseja retornar XClarity Administrator para cada condição de status.

Observe que esses comandos usam macros predefinidas para o endereço IP da instância do XClarity Administrator (**#predefined.otherSettings.lxcaIp#**) e para o UUID do servidor de host ao qual o sistema operacional deve ser implantado (**#predefined.hostPlatforms.uuid#**).

O exemplo a seguir é um script de instalação do PowerShell que instala Java e relata um erro se a instalação falhar

```
import-module C:\windows\system32\WindowsPowerShell\v1.0\Modules\LXCA\LXCA.psm1

initializeRestClient

testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"

Write-Output "Reporting status to Lenovo XClarity Administator..."
   reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
   -UUID "#predefined.hostPlatforms.uuid#" -Message "Installing Java"

Write-Output "Install Java...."
   Invoke-Command -ScriptBlock {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
   [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg] /s}

if ($LastExitCode -ne 0) {
   reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
      -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "Java could not be installed"
}

Write-Output "Completed install of Java for Administrator user."
```

Importando software personalizado

É possível importar software para o repositório de imagens do SO. Esses arquivos podem ser usados para personalizar as imagens do Linux e do Windows.

Sobre esta tarefa

Os arquivos de software personalizado são instalados após a implantação do sistema operacional e os scripts pós-instalação serem concluídos.

Os seguintes tipos de arquivo são suportados para software personalizado.

Sistema Operacional	Tipos de arquivo compatíveis	Mais informações
CentOS Linux	Não aceita	
Microsoft® Windows® Azure Stack HCI	Não aceita	
Microsoft Windows Hyper-V Server	Não aceita	
Microsoft Windows® Server	Um arquivo .zip que contém a carga de software.	O caminho de arquivos e dados personalizado padrão é `C:\lxca`.
Red Hat® Enterprise Linux (RHEL) Server	Um arquivo .tar.gz que contém a carga de software	O caminho arquivos e dados personalizados padrão é `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	Um arquivo .tar.gz que contém a carga de software	O caminho arquivos e dados personalizados padrão é `/home/lxca`.
Rocky Linux	Um arquivo .tar.gz que contém a carga de software	O caminho arquivos e dados personalizados padrão é `/home/lxca`.

Sistema Operacional	Tipos de arquivo compatíveis	Mais informações
Ubuntu	Não aceita	
VMware vSphere® Hypervisor (ESXi) com Lenovo Customization	Um arquivo .tar.gz que contém a carga de software	O caminho arquivos e dados personalizados padrão é `/home/lxca`.

Nota: O repositório de imagens do SO poderá armazenar um número ilimitado de arquivos personalizados e predefinidos, se houver espaço disponível para armazenar os arquivos.

Procedimento

Para importar software para o repositório de imagens do SO, conclua as seguintes etapas.

Etapa 1. Na barra de menus Lenovo XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.

Etapa 2. Clique na guia **Software**.

Etapa 3. Clique no ícone **Importar Arquivo** ( ). A caixa de diálogo Importar script de instalação é exibida.

Etapa 4. Clique na guia **Importação Local** para fazer upload de arquivos do sistema local ou clique na guia **Importação Remota** para fazer upload de arquivos de um servidor de arquivos remoto.

Nota: Para fazer upload de um arquivo de um servidor de arquivos remoto, você deve primeiro criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** ( ). Para obter mais informações, consulte Configurando um servidor de arquivos remoto .

Etapa 5. Se você escolheu usar um servidor de arquivos remoto, selecione o servidor que você deseja usar na lista **Servidor de Arquivos Remoto**.

Etapa 6. Selecione o tipo de sistema operacional.

Etapa 7. Digite o nome do arquivo de software ou clique em **Procurar** para encontrar o arquivo que você deseja importar.

Etapa 8. **Opcional:** insira uma descrição do arquivo de software.

Dica: use o campo **Descrição** para distinguir entre arquivos personalizados com o mesmo nome.

Etapa 9. **Opcional:** selecione um tipo de soma de verificação para verificar se o arquivo que está sendo transferido por upload não está danificado e copie e cole o valor de soma de verificação no campo de texto fornecido.

Se você selecionar um tipo de soma de verificação, especifique um valor de soma de verificação para verificar a integridade e a segurança do arquivo transferido por upload. O valor deve se originar de uma fonte segura de uma organização em que você confie. Se o arquivo transferido

por upload corresponde ao valor de soma de verificação, será seguro continuar com a implantação. Caso contrário, você deverá fazer upload novamente do arquivo ou verificar o valor de soma de verificação.

Três tipos de soma de verificação têm suporte:
- **MD5**
- **SHA1**
- **SHA256**

Etapa 10. Clique em **Importar**.

Dica: o arquivo é transferido por upload por uma conexão de rede segura. Dessa forma, a confiabilidade e o desempenho da rede afetam o tempo que demora para importar o arquivo.

Se você fechar a guia ou a janela do navegador da Web na qual o arquivo está sendo transferido por upload localmente antes do término do processo, ocorrerá falha na importação.

Depois de concluir

Os scripts de instalação estão listados na guia **Software** na página Gerenciar imagens de SO.

Nesta página, é possível executar as ações a seguir:

- Criar um perfil de servidor de arquivos remoto clicando no ícone **Configurar Servidor de Arquivos** ( ).
- Remova os arquivos de software selecionados clicando no ícone **Excluir** ( ).

Para obter informações sobre como adicionar um arquivo de software a um perfil da imagem do SO personalizada, consulte Criando um perfil da imagem do SO personalizada.

Criando um perfil da imagem do SO personalizada

É possível adicionar drivers de dispositivo personalizados, arquivos de inicialização (Windows apenas), arquivos sem supervisão, scripts de instalação e software a um perfil de imagem de SO predefinido que exista no repositório de imagens de SO. Ao adicionar arquivos a uma imagem de SO, o Lenovo XClarity Administrator cria um perfil de imagem do SO personalizada. O perfil personalizado inclui os arquivos personalizados e opções de instalação.

Antes de iniciar

Os arquivos personalizados que você deseja adicionar devem existir no repositório de imagens do SO (consulte Importar arquivos de inicialização, Importando drivers de dispositivo, Importando definições de configuração personalizadas, Importando arquivos sem supervisão personalizados, Importando scripts de instalação personalizados e Importando software personalizado).

Procedimento

Para personalizar uma imagem do SO, conclua as seguintes etapas.

Etapa 1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.

Etapa 2. Clique na guia **Imagens do SO**.

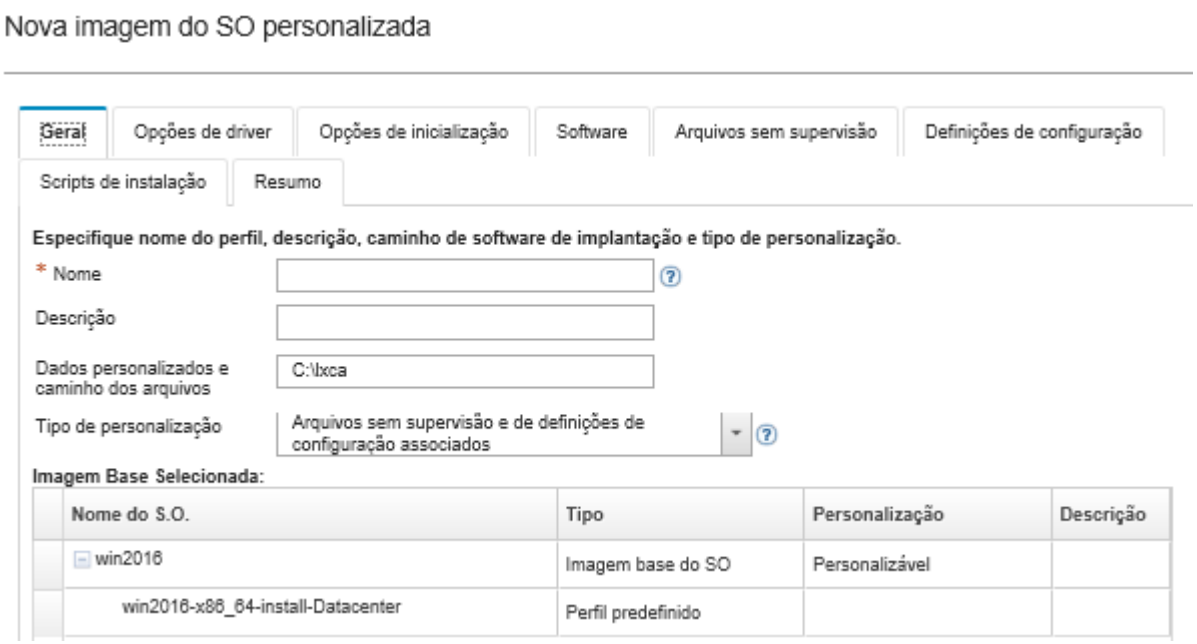
Etapa 3. Selecione o perfil de imagem do SO predefinido que deseja personalizar.

A coluna **Personalização** identifica as imagens do SO que podem ser personalizadas. Clique no ícone **Ajuda** ( ) para obter mais informações sobre a personalização para uma imagem do SO específica.

- **Personalizável**. A personalização do suporte de imagem do SO, mas não está personalizada.
- **Não Personalizável**. A imagem do SO não oferece suporte à personalização.

Nota: É possível importar imagens de SO de base adicionais (no formato .iso) de um sistema local ou remoto clicando no ícone **Importar Arquivo** ( ).

Etapa 4. Clique no ícone **Criar Perfil Personalizado** ( ). A caixa de diálogo Nova Imagem do SO Personalizada é exibida.



Etapa 5. Na guia **Geral**, especifique um nome, a descrição, o caminho para os arquivos personalizados e dados de implantação no host de implantação e o tipo de personalização para o novo perfil de imagem do SO personalizada.

O tipo de personalização pode ser um dos valores a seguir:

- **Somente arquivos sem supervisão**
- **Somente arquivos de configuração**
- **Arquivos sem supervisão e de configuração não associados**
- **Arquivos de configuração e sem supervisão associados**
- **Nenhum**

Etapa 6. Clique em **Avançar**.

Etapa 7. Na guia **Drivers de dispositivo**, selecione a unidade de dispositivo que você deseja incluir no perfil de imagem do SO do Linux.

Para obter uma lista de formatos suportados, consulte Importando drivers de dispositivo.

O arquivo selecionado é aplicado depois que você conclui o assistente de configuração.

Nota: É possível importar drivers de dispositivo adicionais de um sistema local ou remoto clicando no ícone **Importar Arquivo** ( ).

Etapa 8. Clique em **Avançar**.

Etapa 9. (Windows apenas) Na guia **Opções de Inicialização**, selecione os arquivos de inicialização que você deseja incluir no perfil de imagem do SO do Windows.

Para obter uma lista de formatos suportados, consulte Importar arquivos de inicialização.

O arquivo selecionado é aplicado depois que você conclui o assistente de configuração.

Etapa 10. Clique em **Avançar**.

Etapa 11. Na guia **Opções de configuração** (se aplicável), selecione um ou mais arquivos de configuração personalizados que você deseja incluir no perfil de imagem do SO. É possível selecionar no máximo um arquivo

Etapa 12. Clique em **Avançar**.

Etapa 13. Na guia **Arquivos sem supervisão**:

a. Selecione o arquivo sem supervisão que deseja adicionar ao perfil da imagem do SO.

Para obter uma lista de formatos suportados, consulte Importando arquivos sem supervisão personalizados.

O arquivo selecionado é aplicado depois que você conclui o assistente de configuração.

b. Selecione um arquivo de configuração para associar o arquivo sem supervisão na coluna **Arquivo de configuração associado**

c. Opcionalmente, selecione macros personalizadas que estão disponíveis no arquivo de configuração selecionado ou adicionar macros personalizadas no formato .xml.

Etapa 14. Clique em **Avançar**.

Etapa 15. Na guia **Scripts de instalação** (se aplicável), selecione os scripts de instalação que você deseja incluir no perfil de imagem do SO do Windows. É possível selecionar no máximo um script pós-instalação.

Para obter uma lista de formatos suportados, consulte Importando scripts de instalação personalizados.

O arquivo selecionado é aplicado depois que você conclui o assistente de configuração.

Nota: É possível importar scripts de instalação adicionais de um sistema local ou remoto clicando no ícone **Importar arquivo** ( ).

Etapa 16. Clique em **Avançar**.

Etapa 17. Na guia **Software**, selecione o software que você deseja incluir no perfil de imagem do SO do Linux.

Para obter uma lista de formatos suportados, consulte Importando software personalizado.

O arquivo selecionado é aplicado depois que você conclui o assistente de configuração.

Nota: É possível importar software adicional de um sistema local ou remoto clicando no ícone **Importar arquivo** ( ).

Etapa 18. Clique em **Avançar**.

Etapa 19. Revise as configurações na guia **Resumo** e clique em **Personalizar** para criar o perfil de imagem do SO personalizada.

Depois de concluir

O perfil de imagem do SO personalizada está listado abaixo do sistema operacional de base na guia **Imagens do SO** na página Gerenciar Imagens do SO.

Nesta página, é possível executar as ações a seguir:

- Importe um perfil da imagem do SO personalizada e aplique a uma imagem do SO básica clicando em **Importar/Exportar Perfil → Exportar Imagem do Perfil Personalizado** (consulte Importando um perfil de imagem do SO personalizada).
- Exporte um perfil da imagem do SO personalizada selecionado clicando em **Importar/Exportar Perfil → Exportar Imagem do Perfil Personalizado**.
- Modifique um perfil da imagem do SO personalizada selecionado no ícone **Editar** ().
- Remova um perfil da imagem do SO personalizada selecionado no ícone **Excluir** ().

Definindo configurações de implantação de SO globais

As configurações globais servem como as configurações padrão quando os sistemas operacionais são implantados.

Sobre esta tarefa

Na página Configurações Globais, é possível definir as seguintes configurações:

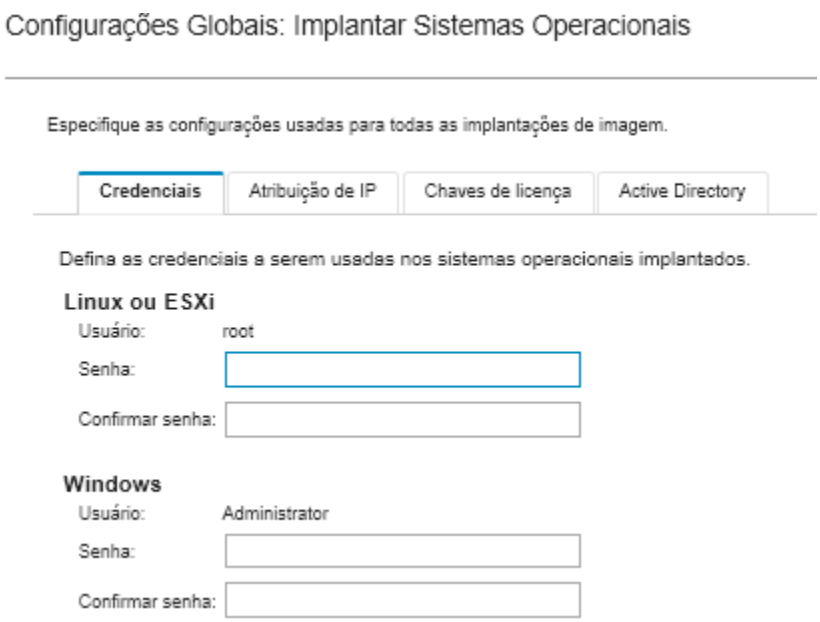
- A senha da conta de usuário administrador a ser usada para implantar os sistemas operacionais
- O método a ser usado para atribuir endereços IP a servidores
- Chaves de licença para usar ao ativar sistemas operacionais instalados
- A opção de ingressar em um domínio do Active Directory como parte da implantação do sistema operacional Windows

Procedimento

Para definir as configurações globais a serem usadas para todos os servidores, conclua as etapas a seguir.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Implantar Imagens de SO** para exibir a página Implantar Imagens de SO.

Etapa 2. Clique no ícone **Configurações Globais** () para exibir a caixa de diálogo Configurações Globais: Implantar Sistemas Operacionais.



Etapa 3. Na guia **Credenciais**, insira a senha da conta de administrador a ser usada para fazer login no sistema operacional.

Etapa 4. Na guia **Atribuição de IP**, selecione as opções a seguir.

a. **Opcional:** Selecione **Use VLANs** para permitir a configuração de definições VLAN na caixa de diálogo Configurações de rede (consulte Definindo as configurações de rede para servidores gerenciados).

Notas: Notas:

- Não há suporte para a marcação de VLAN para implantações de sistema operacional Linux.
- Não há suporte para a marcação de VLAN para implantações de sistema operacional nos dispositivos ThinkServer.
- O modo VLAN é compatível somente para servidores que têm endereços MAC no inventário. Se AUTO for o único endereço MAC disponível para um servidor, VLANs não poderão ser usadas para implantar sistemas operacionais nesse servidor.

b. Selecione o método para atribuir endereços IP ao configurar o sistema operacional implantado:

Nota: A interface de rede do XClarity Administrator usada para gerenciamento deve ser configurada para conectar-se a baseboard management controller usando o mesmo método de endereço IP escolhido na caixa de diálogo Configurações Globais: Implantar Sistemas Operacionais. Por exemplo, se o XClarity Administrator é configurado para usar eth0 para o gerenciamento, e você optar por usar endereços IPv6 estáticos atribuídos manualmente ao configurar o SO implantado, o eth0 deve ser configurado com um endereço IPv6 que tenha conectividade com o baseboard controlador de gerenciamento.

- **Atribuir um endereço IPv4 estático manualmente**. Se você optar por atribuir endereços IPv4 estáticos, certifique-se de configurar o endereço IPv4 estático, o endereço do gateway e a máscara de sub-rede para o servidor antes de implantar o sistema operacional (consulte Definindo as configurações de rede para servidores gerenciados).
- **Usar Protocolo de Configuração Dinâmica de Host (DHCP) para atribuir os endereços**. Se você já tiver uma infraestrutura DHCPv4 existente na rede, poderá usar essa infraestrutura para atribuir endereços IP a servidores.

Nota: Não há suporte para DHCP IPv6 na implantação de sistemas operacionais.

- **Atribuir um endereço IPv6 estático manualmente**. Se você optar por atribuir endereços IPv6 estáticos, certifique-se de configurar o endereço IPv6 estático, o endereço do gateway e a máscara de sub-rede para o servidor antes de implantar o sistema operacional (consulte Definindo as configurações de rede para servidores gerenciados).

Etapa 5. **Opcional:** Na guia **Chaves de Licença**, especifique as chaves de licença de volume globais para usar ao ativar sistemas operacionais Windows instalados.

Ao especificar chaves globais de licença por volume nessa guia, você pode selecionar as chaves de licença especificadas para qualquer perfil de sistema operacional Windows na página Implantar Imagens de SO.

Dica: O XClarity Administrator oferece suporte a chaves de licença de volume padrão para instalações do Windows e chaves de licença de varejo individuais para Windows e VMware ESXi. É possível especificar chaves de licença de varejo individuais como parte do procedimento de implantação (consulte Implantando uma imagem do sistema operacional).

Etapa 6. **Opcional:** Na guia **Active Directory**, defina as configurações do Active Directory para implantações do sistema operacional Windows. Para obter informações sobre a integração com o Active Directory, consulte Integração com Windows Active Directory.

Etapa 7. Clique em **OK** para fechar a caixa de diálogo.

Definindo as configurações de rede para servidores gerenciados

Configurações de rede são opções de configuração específicas a cada servidor. Você deve definir as configurações de rede para um servidor gerenciado para poder implantar um sistema operacional nesse servidor.

Sobre esta tarefa

Se estiver usando DHCP para atribuir endereços IP dinamicamente, você deverá configurar o endereço MAC.

Se estiver usando endereços IP estáticos, você deverá definir as configurações de rede a seguir para um servidor específico antes de implantar um sistema operacional nesse servidor. Após a definição dessas configurações, o status de implantação das alterações do servidor muda para "Pronto". (Observe que alguns campos não ficarão disponíveis para endereços IPv6 estáticos.)

- Nome do Host

  O nome do host deve obedecer as seguintes regras:
  - O nome do host de cada servidor gerenciado deve ser exclusivo.
  - O nome do host pode conter cadeias de caracteres (rótulos) separadas por um ponto (.).
  - Cada rótulo pode conter letras ASCII, dígitos e traços (-). No entanto, a string não pode começar ou terminar com um traço e não pode conter apenas dígitos.
  - O primeiro rótulo pode ter de 2 a 15 caracteres. Os rótulos subsequentes podem ter de 2 a 63 caracteres.
  - O comprimento total do nome do host deve ter no máximo 255 caracteres.
- Endereço MAC da porta no host em que o sistema operacional será instalado.

  O endereço MAC é definido como AUTO por padrão. Essa definição automaticamente detecta as portas Ethernet que podem ser configuradas e usadas para implantação. O primeiro endereço MAC (porta) detectado é usado por padrão. Se a conectividade for detectada em um endereço MAC diferente, o host do XClarity Administrator será reiniciado automaticamente para usar o endereço MAC recém-detectado para a implantação.

É possível determinar o status da porta de endereço MAC usada para a implantação do SO no menu da lista suspensa **Endereço MAC** na caixa de diálogo Configurações de Rede. Se várias portas estiverem ativas ou se todas as portas estiverem desativadas, AUTO será usado por padrão.

Notas:

- Não há suporte para portas de rede virtual. Não use uma porta de rede física para simular várias portas de rede virtual.
- Quando a configuração de rede do servidor é definida como AUTOMÁTICO, o XClarity Administrator pode detectar automaticamente as portas de rede nos slots 1 – 16. Pelo menos uma porta nos slots 1 – 16 deve ter uma conexão com XClarity Administrator.
- Se você quiser usar uma porta de rede no slot 17 ou superior para o endereço MAC, não poderá usar AUTOMÁTICO. Em vez disso, você deve definir a configuração de rede do servidor como o endereço MAC da porta específica que você deseja usar.
- Para os servidores ThinkServer, nem todos os endereços MAC de host são exibidos. Na maioria dos casos, os endereços MAC para adaptadores Ethernet AnyFabric são listados na caixa de diálogo Editar Configurações de Rede. Os endereços MAC para outros adaptadores Ethernet (como Lan-On-Motherboard) não são listados. Quando o endereço MAC de um adaptador não estiver disponível, use o método AUTO para implantações não VLAN.

- Endereço IP e máscara de sub-rede
- Gateway de IP
- Até dois servidores de Sistema de Nomes de Domínio (DNS)
- Velocidade da Unidade de Transmissão Máxima (MTU)
- ID da VLAN, se o modo IP da VLAN estiver habilitado

Se você optar por usar VLANs, poderá atribuir um ID de VLAN ao adaptador de rede do host que está sendo configurado.

Procedimento

Para definir configurações de rede para um ou mais servidores, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar Sistema Operacional: Implantar Imagens do SO.

Etapa 2. Selecione um ou mais servidores para configurar. É possível selecionar até 28 servidores para configurar ao mesmo tempo.

Etapa 3. Clique em **Selecionado Alterado → Configurações de Rede** para exibir a página Editar Configurações de Rede.

Etapa 4. Preencha os campos da tabela para cada servidor.

Dica: Como uma alternativa ao preenchimento de cada linha, você poderá atualizar todas as linhas na tabela para alguns dos campos:

a. Clique em **Alterar Todas as Linhas → Nome do host** para definir os nomes de host para todos os servidores, usando um esquema de nomenclatura personalizado ou predefinido.

b. Clique em **Alterar Todas as Linhas → Endereço IP** para atribuir um intervalo de endereços IP, máscara de sub-rede e gateway. O endereço IP é atribuído a cada servidor, começando com o primeiro endereço IP e terminando com o último endereço IP exibido. A máscara de sub-rede e o endereço IP de gateway são aplicados a cada servidor.

c. Clique em **Alterar Todas as Linhas → Sistema de Nomes de Domínio (DNS)** para configurar os servidores DNS a serem usados pelo sistema operacional para consulta do DNS. Se a rede definir servidores DNS automaticamente, ou se você não quiser definir servidores DNS, selecione **Nenhum**.

d. Clique em **Alterar Todas as Linhas → Unidade de Transmissão Máxima (MTU)** para definir a MTU a ser usada no adaptador Ethernet configurado no sistema operacional implantado.

e. Clique em **Alterar Todas as Linhas → ID de VLAN** para definir um ID de VLAN específico para a marcação de VLAN do sistema operacional.

   É possível especificar um valor de 1 a 4095. O valor padrão é 1, o que significa que o modo VLAN não é usado.

   Essa opção está disponível somente quando a opção Usar VLANs está habilitada na caixa de diálogo Configurações Globais (consulte Definindo configurações de implantação de SO globais).

   Importante:

   - Especifique um ID de VLAN somente quando uma marca VLAN for necessária para funcionar na rede. O uso de **marcas VLAN** pode afetar a roteabilidade da rede entre o sistema operacional do host e o XClarity Administrator.
   - Os chassis ou comutadores top-of-rack devem ser configurados de forma independente para manipular pacotes com marcação VLAN. Certifique-se de que o XClarity Administrator e a rede de dados estejam configurados para manipular esses pacotes corretamente.
   - O modo VLAN é compatível somente para servidores que têm endereços MAC no inventário. Se AUTO for o único endereço MAC disponível para um servidor, VLANs não poderão ser usadas para implantar sistemas operacionais nesse servidor.
   - A marcação de VLAN não é compatível com implantações do sistema operacional Linux; Entretanto, se você deseja implantar com VLAN em alguns servidores e também implantar em outros servidores sem VLAN ao mesmo tempo, poderá forçar a implantação no modo VLAN configurando o ID da VLAN como 1.

Etapa 5. Clique em **OK** para salvar as configurações. As configurações são salvas e persistentes apenas no cache de armazenamento local do navegador da Web.

Resultados

Cada servidor configurado agora mostra **Pronto** como o status de implantação na página Implantar Sistema Operacional: Implantar Imagens do SO.

Escolhendo o local de armazenamento para servidores gerenciados

Escolha o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional em um ou mais servidores.

Antes de iniciar

Revise as considerações de armazenamento e opções de inicialização antes de escolher o local de armazenamento (consulte Considerações sobre implantação do sistema operacional).

É possível implantar um sistema operacional nos seguintes tipos de armazenamento:

- **Unidade de disco local**

  Somente os discos conectados a um controlador RAID ou SAS/SATA HBA são suportados.

  O Lenovo XClarity Administrator instala a imagem do sistema operacional no primeiro disco RAID local enumerado no servidor gerenciado.

Se a configuração do RAID no servidor não estiver configurada corretamente, ou se estiver inativo, talvez o disco local não esteja visível para Lenovo XClarity Administrator. Para resolver o problema, ative a configuração do RAID por meio de padrões de configuração (consulte Definindo o armazenamento local) ou pelo software de gerenciamento do RAID no servidor.

Notas:

- Se uma unidade M.2 também estiver presente, a unidade de disco local deverá ser configurada para RAID de hardware.
- Se um adaptador SATA estiver ativado, o modo SATA *não deverá* ser definido como "IDE".
- Para servidores ThinkServer, os sistemas operacionais podem ser implantados apenas no disco local. O armazenamento SAN e os hipervisores integrados não são suportados.
- Para servidores ThinkServer, a configuração só está disponível por meio do software de gerenciamento do RAID no servidor.

Para ver um cenário de exemplo para implantar o VMware ESXi 5.5 em uma unidade de disco instalada localmente, consulte Implantando o ESXi em um disco rígido local.

- **Hipervisor integrado (apenas ESXi) (adaptador de mídia USB ou SD)**

  Esse local é aplicável apenas quando uma imagem do VMware ESXi está sendo implantada nos servidores gerenciados.

  O hipervisor integrado pode ser um dos seguintes dispositivos:

  - Chave USB de licença da IBM (PN 41Y8298) ou chave USB Licenciado da Lenovo que é montada em uma porta específica de um dos seguintes servidores:
    - Flex System x222
    - Flex System x240
    - Flex System x440
    - Flex System x480
    - Flex System x880
    - System x3850 X6
    - System x3950 X6
  - Adaptador de mídia SD instalado nos seguintes servidores:
    - Flex System x240 M5
    - System x3500 M5
    - System x3550 M5
    - System x3650 M5

    Além disso, a unidade deve ser configurada como mostrado a seguir:
    - As unidades adequadas no adaptador de mídia devem ser definidas.
    - O modo do adaptador de mídia SD deve ser configurado como **Operacional**.
    - O proprietário deve ser configurado como Sistema ou Apenas sistema.
    - O acesso deve ser configurado como Leitura/Gravação.
    - Deve ser atribuído um número LUN 0 à unidade.

    Importante: Se o Adaptador de mídia SD não estiver configurado corretamente, a implantação do sistema operacional no Adaptador de mídia SD do Lenovo XClarity Administrator não será bem-sucedida.

    Você pode alterar o modo do Adaptador de mídia SD em **Configuração** e configurar o adaptador de mídia pelo controlador de gerenciamento CLI usando o comando `sdraid`. Para obter informações adicionais sobre como configurar o modo do Adaptador de mídia SD e como configurar o adaptador do CLI, consulte Documentação online do Integrated Management Module II.

Se há duas chaves do hipervisor instaladas no servidor gerenciado, o instalador do VMware seleciona a primeira chave enumerada para implantação.

Nota: Tentar implantar o Microsoft Windows em um servidor gerenciado que possui uma chave de hipervisor instalada pode causar problemas mesmo se você não selecionar a chave do hipervisor integrado. Se ocorrerem erros de implantação do Windows, remova a chave do hipervisor integrado do servidor gerenciado e tente implantar novamente o Microsoft Windows nesse servidor.

- **Unidade M.2**

  O Lenovo XClarity Administrator instala a imagem do sistema operacional na primeira unidade M.2 que é configurada no servidor gerenciado.

  O armazenamento M.2 é suportado somente em servidores de ThinkSystem.

  Atenção: Se um dispositivo gerenciado tiver ambas as unidades locais (SATA, SAS ou SSD) que não são configuradas para RAID de hardware e unidades M.2, você deverá desabilitar as unidades locais se desejar usar unidades M.2 ou deverá desabilitar as unidades M.2 se desejar usar unidades locais. É possível desativar dispositivos do controlador de armazenamento integrado e ROMs de opção de armazenamento legada e UEFI usando Padrões de Configuração, selecionando Desabilitar disco local na guia Armazenamento Local do assistente ou criando um Padrão de Configuração de um servidor existente e, em seguida, desativando dispositivos M.2 no padrão de UEFI estendida.

- **Armazenamento SAN**

  O Lenovo XClarity Administrator instala a imagem do sistema operacional no destino de inicialização de SAN que é configurado no servidor gerenciado.

  Os seguintes protocolos são suportados.
  - Fibre Channel
  - Fibre Channel sobre Ethernet
  - SAN iSCSI (usando somente adaptadores VFA5.2 2x10 GbE SFP+ e FCoE/iSCSI SW ou Emulex VFA5.2 ML2 2x10 GbE SFP+ e adaptadores FCoE/iSCSI SW)

  Em servidores de rack gerenciados, é possível implantar apenas Windows ou RHEL em armazenamento SAN. Assegure-se de que o destino de inicialização de SAN esteja configurado nos servidores gerenciados. Você também pode configurar o destino de inicialização de FC SAN usando um padrão de servidor (consulte Definindo opções de inicialização)

  Ao implantar o VMware ESXi:

  - Os discos rígidos locais devem ser desativados ou removidos do servidor. É possível desativar os discos rígidos locais usando padrões de servidor (consulte Definindo o armazenamento local).
  - Se vários volumes SAN estiverem disponíveis, apenas o primeiro volume será usado para implantação.

  Certifique-se que o volume do SO que você está instalando é o único volume visível para o sistema operacional.

  Em um cenário de exemplo sobre como implantar o VMware ESXi 5.5 aos volumes SAN conectados aos servidores, consulte Implantando o ESXi ao armazenamento SAN.

Nota: Cada servidor deve ter um adaptador RAID de hardware ou SAS/SATA HBA instalado e configurado. O RAID do software que geralmente está presente no adaptador de armazenamento Intel SATA integrado ou que é configurado como JBOD não é suportado. No entanto, se um adaptador RAID de hardware não estiver presente, configurar o adaptador SATA no **Modo AHCI SATA** habilitado para implantação do sistema operacional ou configurar discos bons não configurados como JBOD poderá funcionar em alguns casos. Para obter mais informações, consulte O instalador do SO não pode localizar o disco no qual você deseja instalar o XClarity Administrator na documentação online do XClarity Administrator.

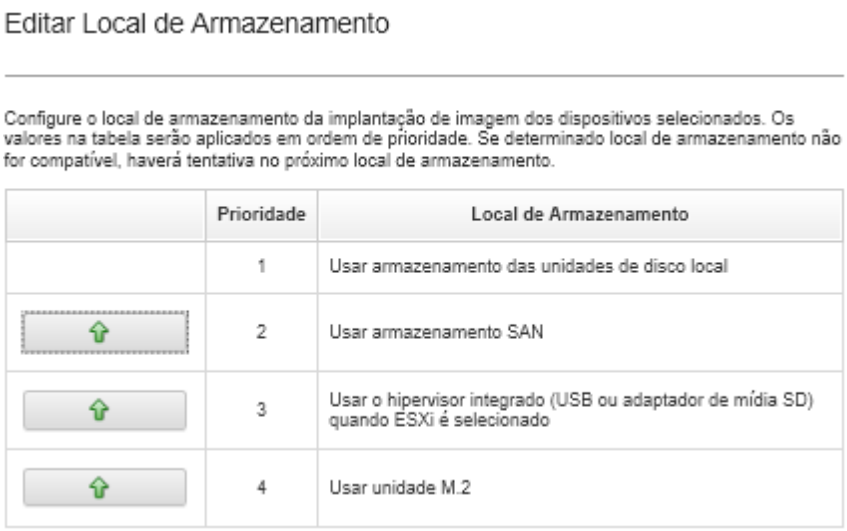
Procedimento

Para escolher o local de armazenamento para um ou mais servidores gerenciados, conclua as seguintes etapas.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar imagens de SO.

Etapa 2. Selecione os servidores para os quais você deseja alterar configurações de armazenamento.

Etapa 3. Clique em **Alterar Selecionado → Local de Armazenamento** para alterar a ordem de prioridade dos locais de armazenamento para todos os servidores selecionados. Se o primeiro local de armazenamento não for compatível, haverá tentativa no próximo local de armazenamento.



É possível configurar a prioridade para os seguintes locais de armazenamento:
- **Usar armazenamento de unidade de disco local**
- **Usar o hipervisor integrado (USB ou adaptador de mídia SD) quando ESXi é selecionado**
- **Usar unidade M.2**
- **Usar armazenamento SAN**

Etapa 4. Para cada servidor, selecione o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional na coluna **Armazenamento**. É possível escolher os valores a seguir, que correspondem aos valores da etapa anterior.
- **Unidade de disco local**
- **Hipervisor Integrado**
- **Unidade M.2**
- **Armazenamento SAN**

Se você selecionar **Armazenamento SAN**, uma caixa de diálogo será exibida para configurar o volume SAN. Certifique-se de que o volume SAN de destino esteja acessível durante a implantação.

Se o local de armazenamento selecionado não for compatível com o servidor, o Lenovo XClarity Administrator tenta implantar o sistema operacional no próximo local de armazenamento de acordo com a prioridade definida na etapa anterior.

Implantando uma imagem do sistema operacional

É possível usar o Lenovo XClarity Administrator para implantar simultaneamente uma imagem do sistema operacional em até 28 servidores.

Antes de iniciar

Leia as considerações de implantação do sistema operacional antes de tentar implantar sistemas operacionais em servidores gerenciados (consulte Considerações sobre implantação do sistema operacional).

Na guia **Imagens do SO**, certifique-se de que o **Status de Implantação** do sistema operacional que você deseja implantar esteja definido como "Pronto." Para implantar o sistema operacional Windows é necessário um arquivo de inicialização do WinPE. Se um arquivo WinPE correspondente não estiver disponível, o **Status de implantação** estará definido como "Não Está Pronto" e o sistema operacional não poderá ser implantado. Você deve baixar e importar um arquivo WinPE manualmente (consulte Importar arquivos de inicialização).

Na guia **Gerenciar imagens de SO**, é possível filtrar a lista de imagens do SO, clicando em **Mostrar Tudo → Status de implantação**. É possível filtrar a lista para mostrar somente os servidores que tenham um status de "Pronto," "Não Pronto," e "Aviso". Se o status de implantação de uma imagem do sistema operacional é "Não Está Pronto," o sistema operacional não será incluído na lista de sistemas operacionais implantáveis.

O código do idioma inglês é suportado por padrão. Para especificar um determinado código do idioma, você deve usar um arquivo de configuração personalizado e um arquivo sem supervisão. Para obter mais informações, consulte Implantando o SLES 12 SP3 com um código do idioma configurável e servidores NTP e Implantação do Windows 2016 para japonês.

A implantação do sistema operacional para armazenamento conectado não RAID não é suportada.

Atenção: Se o servidor possui, atualmente, um sistema operacional, a implantação de um perfil de imagem do SO substituirá o sistema operacional atual.

Para servidores com XCC2 que tenham o protetor do sistema habilitado e a ação definida para **Impedir a inicialização do SO**, o protetor do sistema deve ser compatível com o dispositivo. Se o protetor do sistema não for compatível, os dispositivos serão impedidos de concluir o processo de inicialização, o que faz com que a implantação do SO falhe. Para provisionar esses dispositivos, responda manualmente ao prompt de inicialização do protetor do sistema para permitir que os dispositivos seja inicializados normalmente.

Procedimento

Para implantar uma imagem do sistema operacional em um ou mais servidores gerenciados, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar Sistema Operacional: Implantar Imagens do SO.

Dica: para complexos escaláveis, o sistema operacional é implantado na partição primária; portanto, apenas a partição primária será incluída na lista do servidor.

Etapa 2. Selecione um ou mais servidores no(s) qual(is) o sistema operacional deve ser implantado. É possível implantar um sistema operacional em até 28 servidores ao mesmo tempo.

É possível classificar as colunas da tabela para facilitar a localização dos servidores específicos. Além disso, é possível filtrar a lista de dispositivos exibidos selecionando uma opção no menu **Mostrar** para listar apenas os dispositivos em um chassi, rack ou grupo específico ou inserindo texto (como um nome ou endereço IP) no campo **Filtro**.

Dica: é possível escolher mais nós de cálculo de diversos chassis se você pretende implantar o mesmo sistema operacional em todos os nós.

Etapa 3. Clique em **Alterar Selecionado → Configurações de Rede** para definir as configurações de rede.

Para obter mais informações, consulte Definindo as configurações de rede para servidores gerenciados.

Etapa 4. Para cada servidor, selecione o perfil da imagem do SO a ser implantado na lista suspensa na coluna **Imagem para implantação**.

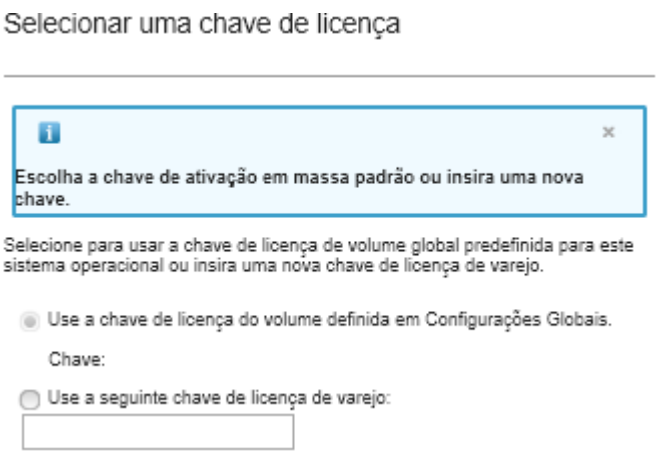
Certifique-se de selecionar um perfil de imagem do SO compatível com o servidor selecionado. É possível determinar compatibilidade de atributos de perfil que estão listados na coluna **Atributo**, na página Gerenciar imagens de SO. Para obter informações sobre atributos de perfil, consulte Perfis de imagem do sistema operacional.

Etapa 5. Para cada servidor, clique no ícone **Chave de Licença** ( ) e especifique a chave de licença a ser usada para ativar o sistema operacional após ser instalado.

O XClarity Administrator dá suporte a chaves de licença de volume padrão para instalações do Windows e chaves de varejo individuais para Windows e VMware ESXi.

Para usar a chave de licença de volume global especificada na caixa de diálogo Configurações Globais, selecione **Usar a chave de licença de volume definida nas Configurações Globais**. Para obter informações sobre as chaves de licença de volume global, consulte Definindo configurações de implantação de SO globais.

Para usar uma chave licença de varejo individual, selecione **Usar a seguinte chave de licença de varejo** e insira a chave no campo a seguir.



Etapa 6. **Opcional:** se você selecionou um sistema operacional Windows para o servidor, é possível incluir o sistema operacional Windows em um domínio do Active Directory como parte da implantação do sistema operacional clicando no ícone **Pasta** ( ) exibido ao lado da imagem do sistema operacional e, em seguida, selecionando o nome do Active Directory.

Para usar o Active Directory padrão especificado na caixa de diálogo Configurações Globais, selecione **Usar o Active Directory definido nas Configurações Globais**. Para obter informações sobre como ingressar em um domínio do Active Directory, consulte Integração com Windows Active Directory.

Para usar um Active Directory específico, selecione **Usar o seguinte Active Directory** e selecione o domínio do Active Directory.

Etapa 7. Para cada servidor, selecione o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional na coluna **Armazenamento**.
- **Unidade de disco local**
- **Hipervisor Integrado**
- **Unidade M.2**
- **Armazenamento SAN**

Se o local de armazenamento selecionado não for compatível com o servidor, o XClarity Administrator tentará implantar o sistema operacional no próximo local de armazenamento de acordo com a prioridade.

Nota: Para servidores ThinkServer, apenas **Disco local** está disponível

Para obter mais informações sobre como configurar local de armazenamento, consulte Escolhendo o local de armazenamento para servidores gerenciados.

Nota: Para garantir que as implantações do sistema operacional foram feitas com êxito, remova qualquer armazenamento do servidor gerenciado, exceto o armazenamento que será escolhido para a implantação do sistema operacional.

Etapa 8. Verifique se o status da implantação para todos os servidores selecionados é Pronto.

Importante: Certifique-se de que o status da implantação de todos os servidores selecionados seja Pronto. Se o status do servidor for Não Pronto, não será possível implantar uma imagem do sistema operacional nesse servidor. Clique no link **Não Pronto** para obter informações para ajudar a resolver o problema. Se as configurações de rede forem inválidas, clique em **Alterar Selecionado → Configurações de Rede** para definir as configurações de rede.

Etapa 9. Clique no ícone **Implantar imagens** ( ) para iniciar a implantação do sistema operacional.

Se as configurações personalizadas tiverem sido incluídas no perfil de imagem do SO, a guia **Configurações personalizadas** será exibida na caixa de diálogo Implantar imagem do SO. Especifique as configurações personalizadas, configurações comuns e específicas de servidor e, em seguida, clique em **Avançar** para continuar com a implantação do SO. Observe que a implantação do SO não continuará se a entrada não for especificada para alguma configuração personalizada.

Depois de concluir

É possível monitorar o status do processo de implantação no log de trabalhos. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Trabalhos**. Para obter mais informações sobre o log de trabalho, consulte Monitorando trabalhos.

Também é possível configurar uma sessão de controle remoto por meio do Baseboard Management Controller do servidor para observar o progresso da instalação. Para obter mais informações sobre controle remoto, consulte Usando o controle remoto para gerenciar servidores Converged, Flex System, NeXtScale e System x.

As informações de implantação são salvas para o sistema operacional. É possível exibir as informações de implantação clicando em **Fornecimento → Gerenciar acesso do SO** e, em seguida, passando o mouse sobre o nome do servidor.

Integração com Windows Active Directory

Quando você implanta uma imagem do Windows usando Lenovo XClarity Administrator, é possível incluir um domínio do Active Directory como parte da implantação do sistema operacional.

Antes de iniciar

Para incluir um domínio do Active Directory como parte de uma implantação de imagem do Windows, configure o servidor de gerenciamento e o Windows Server que está executando o controlador de domínio do Active Directory afetado. Para executar essa configuração, é necessário o seguinte acesso:

- Uma conta de administrador com autoridade para autenticar e incluir o domínio de servidores do Active Directory. Essa conta deve ter privilégios semelhantes àqueles do grupo de administradores de domínio padrão, e você pode usar uma conta nesse grupo para essa configuração.
- Acesso a um sistema de nomes de domínio (DNS) que seja resolvido para o servidor do Active Directory que está executando o controlador de domínio. Esse DNS deve ser especificado na opção **Configurações de Rede → DNS** para o servidor no qual você está implantando o sistema operacional.
- O administrador do servidor do Active Directory deve criar o nome do computador necessário no servidor de domínio antes de você implantar o sistema operacional. A tentativa de união não cria o nome do computador. Se nenhum nome for especificado, a união falhará.
- O administrador do servidor do Active Directory deve especificar o nome de host do servidor no qual a imagem está sendo implantada como um nome de computador na unidade organizacional de destino clicando no campo **Configurações de Rede → Nome do host**.

  O nome do host (nome do computado) especificado deve ser exclusivo. Especificar um nome que já esteja sendo usado por outra instalação do Windows causa falha no ingresso.

É possível incluir o domínio do Active Directory usando um destes métodos:

- **Usar um domínio do Active Directory**

É possível usar um domínio específico do Active Directory em uma lista de domínios predefinidos. Execute as seguintes etapas para definir um domínio do Active Directory no XClarity Administrator. Se você pretende utilizar vários domínios, repita estas etapas para cada nome de domínio.

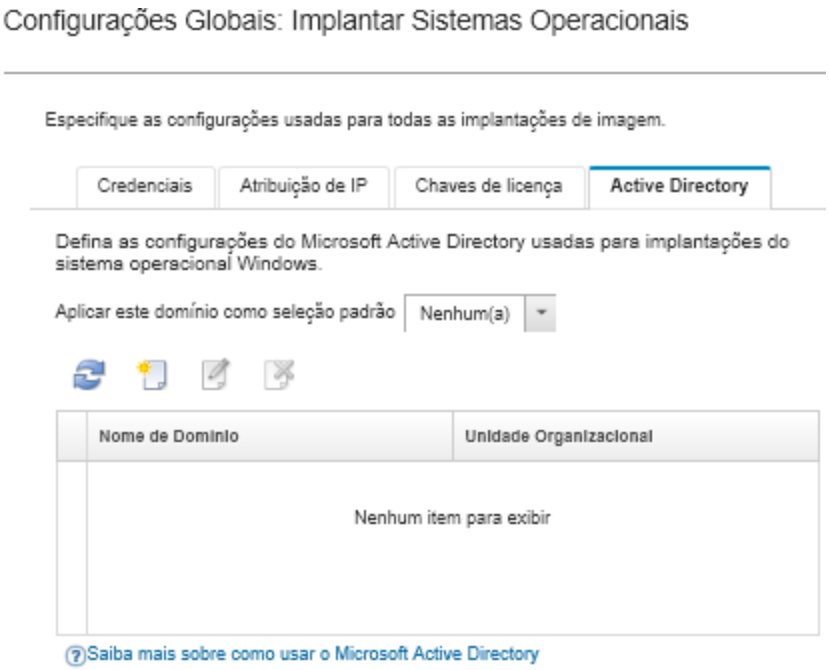
1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar imagens de SO.
2. Clique no ícone **Configurações Globais** ( ) para exibir a caixa de diálogo Configurações Globais: Implantar Sistemas Operacionais.
3. Clique na guia **Active Directory**.
4. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Adicionar Novo Domínio do Active Directory.
5. Especifique o nome do domínio e a unidade organizacional.

   A implantação do sistema operacional oferece suporte ao ingresso de um domínio e à criação de unidades organizacionais aninhadas em um domínio. Se você estiver especificando unidades organizacionais, não será necessário especificar explicitamente a UO como parte do ingresso. O Active Directory pode gerar a UO correta usando o nome do domínio e o nome do computador.
6. Clique em **OK**.

- **Usar o domínio padrão do Active Directory**

  É possível usar o domínio ativo padrão do Active Directory que está definido nas configurações globais. Execute as seguintes etapas para definir um domínio padrão do Active Directory no XClarity Administrator.

  1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar imagens de SO.
  2. Clique no ícone **Configurações Globais** ( ) para exibir a caixa de diálogo Configurações Globais: Implantar Sistemas Operacionais.
  3. Clique na guia **Active Directory**.



  4. No menu suspenso **Aplicar este domínio como seleção padrão**, selecione o domínio do Active Directory a ser usado por padrão para cada implantação do Windows.

5. Clique em **OK**.

- **Usar dados de blob de metadados**

  É possível usar os Metadados de Computador do Active Directory (no formato de blob codificado Base-64) para ingressar no domínio do Active Directory para qualquer servidor. Conclua as seguintes etapas para gerar dados de blob de metadados.

  1. Use uma conta de administrador para fazer login no computador. O computador deve fazer parte do domínio do Active Directory no qual você está ingressando.
  2. Clique em **Iniciar → Programas → Acessórios**. Clique com o botão direito do mouse em **Prompt de Comandos** e, em seguida, clique em **Executar como administrador**.
  3. Mude para o diretório C:\windows\system32 directory.
  4. Execute o comando `djoin` usando o seguinte formato para executar uma associação de offline:
     `djoin /provision /domain <AD_domain_name> /machine <hostname> /savefile blob`

     onde:

     – *<AD_domain_name>* é o nome do domínio do Active Directory.
     – O *<hostname>* é o nome de host do servidor no qual a imagem está sendo implantada como um nome de computador na unidade organizacional de destino clicando no campo **Configurações de Rede → Nome do host**.

     Esse comando cria um arquivo chamado `blob` que contém os dados do blob de metadados. O conteúdo desse arquivo é usado pelo processo de implantação do sistema operacional para especificar detalhes da associação ao Active Directory, portanto mantenha esses dados próximos.

     Os dados do blob de metadados são sigilosos.

Para obter informações detalhadas sobre como implantar uma imagem do sistema operacional, consulte Implantando uma imagem do sistema operacional.

Procedimento

Para incluir um domínio do Active Directory, conclua as seguintes etapas.

Etapa 1. Importe a imagem do sistema operacional Windows para o Repositório de imagens do SO (consulte Importando imagens do sistema operacional).

Etapa 2. Selecione um ou mais servidores no(s) qual(is) o sistema operacional deve ser implantado. É possível implantar um sistema operacional em até 28 servidores ao mesmo tempo.

Dica: é possível escolher mais nós de cálculo de diversos chassis se você pretende implantar o mesmo sistema operacional em todos os nós.

Etapa 3. Clique em **Alterar Selecionado → Configurações de Rede** para definir as configurações de rede.

a. Clique em **Alterar Todas as Linhas → Sistema de Nomes de Domínio (DNS)** e especifique, no mínimo, um DNS que seja resolvido para o domínio do Active Directory.

b. Para cada servidor, especifique um nome de host que corresponda a um nome de computador existente no domínio e unidade organizacional que você está incluindo.

Para obter mais informações sobre como definir as configurações de rede, consulte Definindo as configurações de rede para servidores gerenciados.

Etapa 4. Para cada servidor, selecione a imagem do sistema operacional Windows a ser implantada na coluna **Imagem para implantação**. Os ícones de pasta e chave de licença são exibidos ao lado do nome da imagem.

Etapa 5. Para cada servidor, clique no ícone **Chave de Licença** ( ) e especifique a chave de licença a ser usada para ativar o sistema operacional após ser instalado:

Etapa 6. Para cada servidor, clique no ícone **Pasta** ( ) e especifique o domínio do Active Directory. É possível escolher um dos valores a seguir:

- **Usar o Active Directory definido nas Configurações Globais** para usar o domínio padrão.
- **Usar o seguinte Active Directory** para selecionar um domínio específico.
- **Usar dados de bloco de metadados** para especificar o conteúdo do arquivo de blob.

  Os dados de blob de metadados contêm informações sigilosas e não são exibidos no campo. Essas informações ficam disponíveis somente quando a operação de implantação é concluída. Isso não é persistente.

Etapa 7. Para cada servidor, selecione o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional na coluna **Armazenamento**.

- **Unidade de disco local**
- **Hipervisor Integrado**
- **Unidade M.2**
- **Armazenamento SAN**

Se o local de armazenamento selecionado não for compatível com o servidor, o XClarity Administrator tentará implantar o sistema operacional no próximo local de armazenamento de acordo com a prioridade.

Para obter mais informações sobre como configurar local de armazenamento, consulte Escolhendo o local de armazenamento para servidores gerenciados.

Nota: Para garantir que as implantações do sistema operacional sejam feitas com êxito, remova todo o armazenamento do servidor gerenciado, exceto o armazenamento escolhido para a implantação do sistema operacional.

Etapa 8. Verifique se o status da implantação para todos os servidores selecionados é Pronto.

Se o status do servidor for Não Pronto, não será possível implantar uma imagem do sistema operacional nesse servidor. Clique no link **Não Pronto** para obter informações para ajudar a resolver o problema. Se as configurações de rede não forem inválidas, clique em **Selecionado Alterado → Configurações de Rede** para definir as configurações de rede.

Etapa 9. Clique no ícone **Implantar imagens** () para iniciar a implantação do sistema operacional.

A caixa de diálogo Confirmação de Implantação solicita as credenciais a serem usadas para autenticação do servidor do Active Directory e ingresso do domínio. Por questões de segurança, essas credenciais não são armazenadas no XClarity Administrator. Você deve fornecer as credenciais para cada implantação do Windows que ingressar no domínio.

É possível monitorar o status do processo de implantação no log de trabalhos. Na barra de menu do XClarity Administrator, clique em **Monitoramento → Trabalhos**. Para obter mais informações sobre o log de trabalho, consulte Monitorando trabalhos.

Resultados

Quando a implantação do sistema operacional for concluída, abra um navegador da Web para o endereço IP que você especificou na página Editar Configurações de Rede e faça logon para continuar com o processo de configuração.

Cenários de implantação do SO

Use estes cenários para ajudá-lo a personalizar e implantar sistemas operacionais em servidores gerenciados.

Implantação do RHEL com drivers de dispositivo personalizados

Este cenário instala o sistema operacional Red Hat Enterprise Linux (RHEL) e drivers de dispositivo adicionais que não estão disponíveis no sistema operacional de base. Um perfil personalizado que inclui os drivers de dispositivo adicionais é usado. O perfil personalizado pode ser selecionado na página Implantar imagens de SO.

Antes de iniciar

Ao implantar sistemas operacionais usando o Lenovo XClarity Administrator, o sistema operacional deve incluir os drivers de dispositivo Ethernet, Fibre Channel e adaptador de armazenamento apropriados para seu hardware. Se um driver de dispositivo não estiver incluído no sistema operacional, esse adaptador não será suportado para implantação do SO. No XClarity Administrator v 1.2.0 e posterior, você pode personalizar um sistema operacional adicionando drivers de dispositivo.

É possível obter drivers de dispositivos do Página da Web do repositório Lenovo YUM, do fornecedor (como Red Hat) ou com um driver de dispositivo personalizado que você mesmo criou. Para alguns drivers de dispositivo Windows, é possível gerar um driver de dispositivo personalizado extraindo o driver de dispositivo a partir do arquivo .exe de instalação para seu sistema local e criando um arquivo .zip.

Nota: Os drivers de dispositivo RHEL devem estar no .rpm ou .iso.

Procedimento

Para implantar o RHEL com drivers de dispositivo personalizados, conclua as etapas a seguir.

Etapa 1. Baixe o sistema operacional RHEL base do site Red Hat para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando imagens do sistema operacional.

1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
2. Clique na guia **Imagens do SO**.
3. Clique no ícone **Importar** ( ).
4. Clique em **Importação Local**.
5. Clique em **Procurar** para encontrar e selecionar a imagem RHEL a ser importada (por exemplo, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Clique em **Importar** para fazer o upload da imagem do SO no repositório de imagens do SO.
7. Aguarde a conclusão da importação. Isso pode levar alguns minutos.

Etapa 2. Baixe o drivers de dispositivo personalizados no sistema local e importe os arquivos para o repositório de imagens do SO. Para obter mais informações, consulte Importando drivers de dispositivo.

1. Clique na guia **Drivers de Dispositivo**.
2. Clique no ícone **Importar** ( ).
3. Clique em **Importação Local**.
4. Selecione `RHEL` do sistema operacional.
5. Selecione a versão do sistema operacional.
6. Selecione o tipo do dispositivo.
7. Clique em **Procurar** para localizar e selecionar o driver de dispositivo a ser importador (por exemplo, `kmod-i40e-2.0.12-1.el7.x86_64.rpm`).
8. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.

Etapa 3. Crie um perfil de imagem do SO personalizado que inclui os drivers de dipositivo personalizados. Para obter mais informações, consulte Criando um perfil da imagem do SO personalizada.

1. Clique na guia **Imagens do SO**.
2. Selecione o perfil de imagem de SO a ser personalizado (por exemplo, `Virtualization`).
3. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Criar Perfil Personalizado.
4. Na guia **Geral**:
   a. Insira um nome para o perfil (por exemplo, `RHEL personalizado com drivers de dispositivo`).
   b. Use o valor padrão para o campo **Caminho de dados e arquivo personalizado**.
   c. Selecione **Nenhum** para o tipo de personalização.
   d. Clique em **Avançar**.
5. Na guia **Opções de Driver**, selecione os drivers de dispositivo personalizados a serem incluídos no perfil e clique em **Próximo**. Os drivers de dispositivo de entrada são incluídos por padrão.
6. Na guia **Software**, clique em **Próximo**.
7. Clique em **Personalizar** para criar o perfil de imagem do SO personalizado.

Etapa 4. Implante o perfil de imagem do SO personalizado nos servidores de destino. Para obter mais informações, consulte Implantando uma imagem do sistema operacional.

1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar Sistema Operacional: Implantar Imagens do SO.
2. Para cada servidor de destino:
   a. Selecione o servidor.
   b. Clique em **Alterar Selecionado → Configurações de Rede** e especifique o nome do host, endereço IP, as configurações de DNS, MTU e VLAN para o servidor.

      Dica: As configurações de VLAN estão disponíveis apenas quando o modo VLAN é definido em **Configurações Globais → Atribuição de IP → Usar VLANs**.
   c. Selecione o perfil da imagem do SO personalizada (por exemplo, <*base_OS*>|<*timestamp*>_RHEL personalizado com drivers de dispositivo) na lista suspensa na coluna **Imagem para implantação**.

      Nota: Certifique-se de que todos os servidores de destino usem o mesmo perfil personalizado.
   d. (Opcional) Clique no ícone **Chave de Licença** () e especifique a chave de licença a ser usada para ativar o sistema operacional após a sua instalação.
   e. Selecione o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional na coluna **Armazenamento**.

      Nota: Para garantir que as implantações do sistema operacional foram feitas com êxito, remova qualquer armazenamento do servidor gerenciado, exceto o armazenamento que será escolhido para a implantação do sistema operacional.
   f. Verifique se o status da implantação para o servidor selecionado é **Pronto**.
3. Selecione todos os servidores de destino e clique no ícone **Implantar imagem** () para iniciar a implementação do sistema operacional.
4. Na guia **Resumo**, revise as configurações.
5. Clique em **Implantar** para implantar o sistema operacional.

Implantando o RHEL e um aplicativo Hello World PHP com o uso de um arquivo sem supervisão personalizado

Este cenário instala um sistema operacional RHEL junto com o software personalizado (Apache HTTP, PHP e um aplicativo hello-world PHP). Um perfil de imagem do SO personalizada é usado que inclui o arquivo sem supervisão personalizado que registra o sistema operacional com o serviço de assinatura Lenovo RHEL interno para que ele possa usar os repositórios yum, instala os pacotes Apache e PHP, configura o firewall para permitir conexões Apache, cria um aplicativo Hello World PHP e cópia para o diretório de servidor da Web Apache e configura os arquivos de configuração Apache para oferecer suporte a PHP.

Antes de iniciar

É possível implantar o RHEL com software personalizado de algumas maneiras diferentes. Este exemplo usa um arquivo com supervisão personalizado que você inclui no perfil da imagem de SO personalizada. Você também pode usar um script pós-instalação que instala software personalizado que você importa para o repositório e inclui no perfil da imagem do SO personalizada. Para instalar o software usando um script pós-instalação, consulte Implantando o RHEL e um aplicativo Hello World PHP com o uso de um software personalizado e um script pós-instalação.

Esse cenário usa o seguinte arquivo de exemplo.

- RHEL_installSoftware_customUnattend.cfg Este arquivo sem supervisão personalizado usa valores nas macros predefinidas e personalizadas e instala e configura o software personalizado.

Procedimento

Para implantar o RHEL com software personalizado usando um arquivo sem supervisão personalizado, conclua as etapas a seguir.

Etapa 1. Baixe o sistema operacional RHEL base do site Red Hat para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando imagens do sistema operacional.

1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
2. Clique na guia **Imagens do SO**.
3. Clique no ícone **Importar** ( ).
4. Clique em **Importação Local**.
5. Clique em **Procurar** para encontrar e selecionar a imagem RHEL a ser importada (por exemplo, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Clique em **Importar** para fazer o upload da imagem do SO no repositório de imagens do SO.
7. Aguarde a conclusão da importação. Isso pode levar alguns minutos.

Etapa 2. Modifique o arquivo sem supervisão (kickstart) RHEL para registrar o sistema operacional com o serviço de assinatura de satélite RHEL, instale pacotes HTTP (Apache) e PHP e crie um aplicativo Hello World PHP simples, adicione que as macros predefinidas necessárias e outras macros predefinidas onde aplicável, como o endereço IP, gateway, configurações DNS e nome do host e, em seguida, importe o arquivo personalizado para o repositório de imagens do SO. Para obter mais informações, consulte Importando arquivos sem supervisão personalizados.

Adicione comandos para registrar o host com o satélite RHEL, por exemplo:

```
rpm -Uvh http://<YOUR_SATELLITE_SERVER_IP>/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="<YOUR_ORGANIZATION>" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms
```

Importante: No arquivo de exemplo sem supervisão, especifique o endereço IP do seu servidor satélite e da sua organização com base na nossa configuração de serviço de assinatura.

Adicione comandos para atualizar o host e instalar e configurar pacotes Apache e PHP, por exemplo:

```
%packages
@base
@core
@fonts
@gnome-desktop
@internet-browser
@multimedia
@x11
@print-client
-gnome-initial-setup

#Add the Apache and PHP packages
httpd
mod_ssl
openssl
php
php-mysql
php-gd
```

```
%end

yum -y update

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload

echo "<?PHP
echo 'Hello World !! ';
?>" | tee /var/www/html/index.php

sudo cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original

sudo sed -i -e 's/^[ \t]*//' /etc/httpd/conf/httpd.conf
sudo sed -i "s|IncludeOptional|#IncludeOptional|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|#ServerName www.example.com:80|ServerName localhost|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|DirectoryIndex index.html|DirectoryIndex index.html index.php|" /etc/httpd/conf/httpd.conf

echo "AddType application/x-httpd-php .php" | tee -a /etc/httpd/conf/httpd.conf
```

Nota: O arquivo de exemplo sem supervisão modifica os pacotes padrão que estão sendo instalados com o arquivo kickstart. Ele especifica os pacotes Apache e PHP como parte da seção de pacotes.

Somente para ESXi e RHEL, o XClarity Administrator fornece a macro **#predefined.unattendSettings.networkConfig#**, que adiciona todas as configurações de rede definidas na interface do usuário para o arquivo sem supervisão e a macro **#predefined.unattendSettings.storageConfig#**, que adiciona todas as configurações de armazenamento definidas na interface do usuário para o arquivo sem supervisão. O arquivo de exemplo sem supervisão já contém essas macros.

O XClarity Administrator também fornece algumas macros básicas, como inserção de driver OOB, relatório de status, scripts pós-instalação e software personalizado. No entanto, para aproveitar essas macros predefinidas, especifique as seguintes macros no arquivo sem supervisão personalizado. O arquivo de exemplo já contém as macros necessárias.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

O arquivo de exemplo já contém as macros necessárias e as macros predefinidas adicionais para especificar dinamicamente configurações de rede para o servidor de destino e fuso horário. Para obter mais informações sobre como adicionar macros para arquivos sem supervisão, consulte Inserindo macros predefinidas e personalizadas para um arquivo sem supervisão.

É possível também incluir comandos para enviar mensagens personalizadas para o log de trabalhos no XClarity Administrator. Para obter mais informações, consulte Adicionando relatório de status personalizado aos scripts de instalação.

Para importar o script de instalação personalizado, conclua estas etapas. Para obter mais informações, consulte Importando scripts de instalação personalizados.

Para importar o arquivo sem supervisão personalizado, conclua estas etapas.

1. Clique na guia **Arquivos sem supervisão**.
2. Clique no ícone **Importar** ( ).

3. Clique em **Importação Local**.
4. Selecione `RHEL` do sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o arquivo de software a ser importado (por exemplo, `RHEL_installSoftware_customUnattend.cfg`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.

Etapa 3. Crie um perfil de imagem do SO personalizado que inclui o software personalizado e scripts pós-instalação. Para obter mais informações, consulte Criando um perfil da imagem do SO personalizada.

1. Clique na guia **Imagens do SO**.
2. Selecione o perfil de imagem de SO a ser personalizado (por exemplo, `Basic`).
3. Clique no ícone **Criar** () para exibir a caixa de diálogo Criar Perfil Personalizado.
4. Na guia **Geral**:
   a. Insira um nome para o perfil (por exemplo, `RHEL personalizado com software usando arquivo sem supervisão personalizado`).
   b. Use o valor padrão para o campo **Caminho de dados e arquivo personalizado**.
   c. Selecione **Apenas arquivos sem supervisão** para o tipo de personalização.
   d. Clique em **Avançar**.
5. Na guia **Opções de Driver**, clique em **Próximo**. Os drivers de dispositivo de entrada são incluídos por padrão.
6. Na guia **Software**, clique em **Próximo**.
7. Na guia **Não supervisionar arquivos**, selecione o arquivo sem supervisão personalizado (por exemplo, `RHEL_installSoftware_customUnattend.cfg`) e clique em **Avançar**.
8. Na guia **Scripts de instalação**, clique em **Próximo**.
9. Na guia **Resumo**, revise as configurações.
10. Clique em **Personalizar** para criar o perfil de imagem do SO personalizado.

Etapa 4. Implante o perfil de imagem do SO personalizado nos servidores de destino. Para obter mais informações, consulte Implantando uma imagem do sistema operacional.

1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar Sistema Operacional: Implantar Imagens do SO.
2. Para cada servidor de destino:
   a. Selecione o servidor.
   b. Clique em **Alterar Selecionado → Configurações de Rede** e especifique o nome do host, endereço IP, as configurações de DNS, MTU e VLAN para o servidor.

      Dica:

      - As configurações de VLAN estão disponíveis apenas quando o modo VLAN é definido em **Configurações Globais → Atribuição de IP → Usar VLANs**.
      - As configurações de rede que você especifica na caixa de diálogo Configurações de Rede são incluídas no arquivo sem supervisão em tempo de execução usando as macros **#predefined.hostPlatforms.networkSettings.<*setting*>#**.

   c. Selecione o perfil da imagem do SO personalizada (por exemplo, <*base_OS*>|<*timestamp*>`_RHEL personalizado com software usando sem supervisão personalizado`) na lista suspensa na coluna **Imagem para implantação**

      Nota: Certifique-se de que todos os servidores de destino usem o mesmo perfil personalizado.

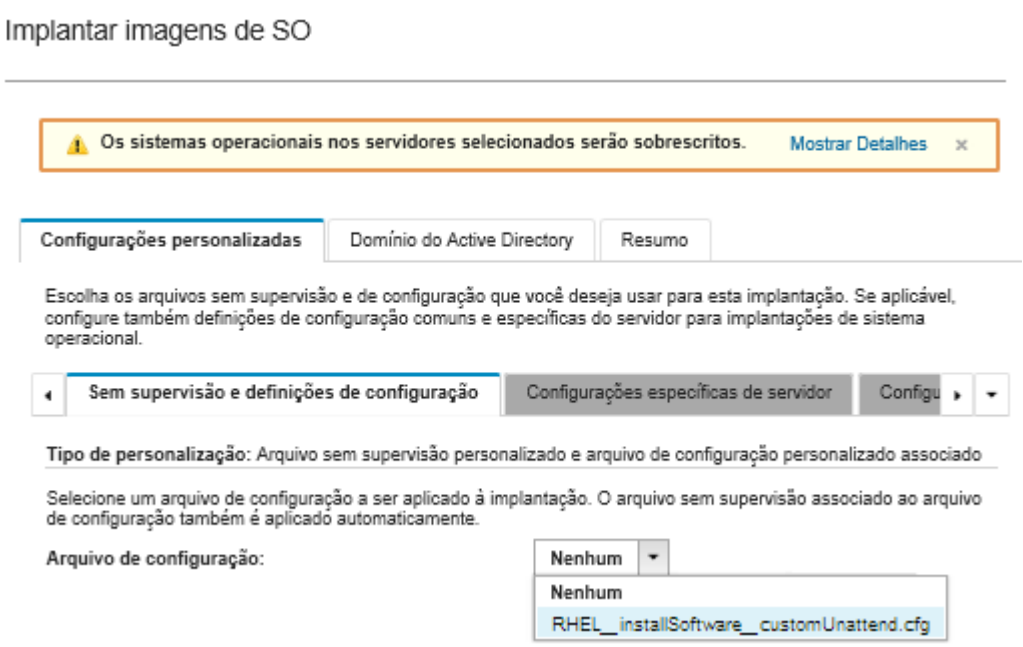
d. (Opcional) Clique no ícone **Chave de Licença** ( ) e especifique a chave de licença a ser usada para ativar o sistema operacional após a sua instalação.

e. Selecione o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional na coluna **Armazenamento**.

Nota: Para garantir que as implantações do sistema operacional foram feitas com êxito, remova qualquer armazenamento do servidor gerenciado, exceto o armazenamento que será escolhido para a implantação do sistema operacional.

f. Verifique se o status da implantação para o servidor selecionado é **Pronto**.

3. Selecione todos os servidores de destino e clique no ícone **Implantar imagem** ( ) para iniciar a implementação do sistema operacional.
4. Na guia Configurações personalizadas, clique na subguia **Sem supervisão e definições de configuração** e selecione o arquivo sem supervisão personalizado (por exemplo, `RHEL_installSoftware_customUnattend.cfg`).



5. Na guia **Resumo**, revise as configurações.
6. Clique em **Implantar** para implantar o sistema operacional.

Implantando o RHEL e um aplicativo Hello World PHP com o uso de um software personalizado e um script pós-instalação

Este cenário instala um sistema operacional RHEL junto com o software personalizado (Apache HTTP, PHP e um aplicativo hello-world PHP). Um perfil de imagem do SO personalizada é usado que inclui o software personalizado e um script pós-instalação que registra o sistema operacional com o serviço de assinatura Lenovo RHEL interno para que ele possa usar os repositórios yum, instala os pacotes Apache e PHP, configura o firewall para permitir conexões Apache, cria um aplicativo Hello World PHP e cópia para o diretório de servidor da Web Apache e configura os arquivos de configuração Apache para oferecer suporte a PHP. Os pacotes de software personalizados são exportados para o host durante a implantação e disponibilizados para o script pós-instalação personalizado a ser usado.

Antes de iniciar

É possível implantar o RHEL e um aplicativo Hello World PHP de algumas maneiras diferentes. Este exemplo usa um script pós-instalação que instala software personalizado que você importa para o repositório e inclui no perfil da imagem do SO personalizada. Você também pode usar um arquivo com supervisão personalizado que você inclui no perfil da imagem de SO personalizada. Para instalar o software usando um arquivo com supervisão personalizados, consulte Implantando o RHEL e um aplicativo Hello World PHP com o uso de um arquivo sem supervisão personalizado.

Esse cenário usa os seguintes arquivos de amostra.

- httpd.conf. Este é o arquivo de instalação para Apache HTTP.
- hello_world.php Este é o aplicativo Hello World PHP.
- RHEL_installSoftware_customScript.sh Este script pós-instalação instala e configura o software personalizado.

Notas:

- Os scripts de instalação do RHEL podem estar em um dos seguintes formatos: Bash (.sh), Perl (.pm ou. pl), Python (.py)
- Arquivos de software e scripts de instalação são instalados do caminho de dados e arquivos personalizado que você especificar durante a implantação. O caminho arquivos e dados personalizados padrão é `/home/lxca`.

Procedimento

Para implantar o RHEL com software personalizado usando um script pós-instalação, conclua as etapas a seguir.

Etapa 1. Baixe o sistema operacional RHEL base do site Red Hat para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando imagens do sistema operacional.

1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
2. Clique na guia **Imagens do SO**.
3. Clique no ícone **Importar** ().
4. Clique em **Importação Local**.
5. Clique em **Procurar** para encontrar e selecionar a imagem RHEL a ser importada (por exemplo, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Clique em **Importar** para fazer o upload da imagem do SO no repositório de imagens do SO.
7. Aguarde a conclusão da importação. Isso pode levar alguns minutos.

Etapa 2. Baixe o software personalizado no sistema local e importar os arquivos para o repositório de imagens do SO. Para obter mais informações, consulte Importando software personalizado.

Dica: para importar software personalizado no XClarity Administrator, os arquivos devem ser contidos em um arquivo tar.gz. Neste exemplo, compacte os arquivos de software de exemplo `httpd.conf` e `index.php` e em um arquivo tar.gz chamado `RHEL_installSoftware_customsw.tar.gz` antes de continuar

1. Clique na guia **Software**.
2. Clique no ícone **Importar** ().
3. Clique em **Importação Local**.
4. Selecione `RHEL` do sistema operacional.

5. Clique em **Procurar** para localizar e selecionar o arquivo de software a ser importado (por exemplo, `RHEL_installSoftware_customsw.tar.gz`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.

Etapa 3. Crie um script pós-instalação personalizado e importe o arquivo para o repositório de imagens do SO.

Adicione comandos para registrar o host com satélite RHEL, por exemplo:

```
rpm -Uvh http://satellite.labs.lenovo.com/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="Default_Organization" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms A
```

Adicione um comando para atualizar o host e instalar e configurar pacotes Apache e PHP, por exemplo:

```
yum -y update
yum -y install httpd mod_ssl openssl php php-mysql php-gd

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload
```

Adicione comandos para adicionar o aplicativo PHP ao satélite do servidor da Web, por exemplo:

```
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/lxca/index.php /var/www/html/index.php
```

Adicione comandos para configurar Apache HTTP, por exemplo:

```
cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/httpd.conf /etc/httpd/conf/httpd.conf
```

Observe que esses comandos usam macros predefinidas para o caminho para os dados extraídos e arquivos de software (**predefined.otherSettings.deployDataAndSoftwareLocation**).

É possível também incluir comandos para enviar mensagens personalizadas para o log de trabalhos no XClarity Administrator. Para obter mais informações, consulte Adicionando relatório de status personalizado aos scripts de instalação.

Para importar o script de instalação personalizado, conclua estas etapas. Para obter mais informações, consulte Importando scripts de instalação personalizados.

1. Clique na guia **Scripts de instalação**.
2. Clique no ícone **Importar** ().
3. Clique em **Importação Local**.
4. Selecione `RHEL` do sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o script de pós-instalação que você deseja importar, por exemplo, `RHEL_installSoftware_customScript.sh`.
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.

Etapa 4. Crie um perfil de imagem do SO personalizado que inclui o software personalizado e scripts pós-instalação. Para obter mais informações, consulte Criando um perfil da imagem do SO personalizada.

1. Clique na guia **Imagens do SO**.
2. Selecione o perfil de imagem de SO a ser personalizado (por exemplo, `Basic`).
3. Clique no ícone **Criar** () para exibir a caixa de diálogo Criar Perfil Personalizado.

4. Na guia **Geral**:
   a. Insira um nome para o perfil (por exemplo, `RHEL personalizado com software usando script pós-instalação`).
   b. Use o valor padrão para o campo **Caminho de dados e arquivo personalizado**.
   c. Selecione **Nenhum** para o tipo de personalização.
   d. Clique em **Avançar**.
5. Na guia **Opções de Driver**, clique em **Próximo**. Os drivers de dispositivo de entrada são incluídos por padrão.
6. Na guia **Software**, selecione os arquivos de instalação de software (por exemplo `httpd.conf` e `index.php`) e clique em **Avançar**.
7. Na guia **Scripts de instalação**, selecione os scripts de instalação (por exemplo, `RHEL_installSoftware_customScript.sh`) e clique em **Avançar**.
8. Na guia **Resumo**, revise as configurações.
9. Clique em **Personalizar** para criar o perfil de imagem do SO personalizado.

Etapa 5. Implante o perfil de imagem do SO personalizado nos servidores de destino. Para obter mais informações, consulte Implantando uma imagem do sistema operacional.

1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar Sistema Operacional: Implantar Imagens do SO.
2. Para cada servidor de destino:
   a. Selecione o servidor.
   b. Clique em **Alterar Selecionado → Configurações de Rede** e especifique o nome do host, endereço IP, as configurações de DNS, MTU e VLAN para o servidor.

      Dica: As configurações de VLAN estão disponíveis apenas quando o modo VLAN é definido em **Configurações Globais → Atribuição de IP → Usar VLANs**.
   c. Selecione o perfil da imagem do SO personalizada (por exemplo, <*base_OS*>|<*timestamp*>`_RHEL personalizado com software usando script pós-instalação`) na lista suspensa na coluna **Imagem para implantação**.

      Nota: Certifique-se de que todos os servidores de destino usem o mesmo perfil personalizado.
   d. Selecione o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional na coluna **Armazenamento**.

      Nota: Para garantir que as implantações do sistema operacional foram feitas com êxito, remova qualquer armazenamento do servidor gerenciado, exceto o armazenamento que será escolhido para a implantação do sistema operacional.
   e. Verifique se o status da implantação para o servidor selecionado é **Pronto**.
3. Selecione todos os servidores de destino e clique no ícone **Implantar imagem** () para iniciar a implementação do sistema operacional.
4. Na guia **Resumo**, revise as configurações.
5. Clique em **Implantar** para implantar o sistema operacional.

Implantação do SLES 12 SP3 com pacotes personalizados e fuso horário

Este cenário instala o sistema operacional SLES 12 SP3 (em inglês) e vários pacotes SLES opcionais. Ele também solicita o fuso horário. Um perfil de imagem de SO personalizado é usado que inclui um arquivo de configuração personalizado e um arquivo sem supervisão personalizado. Esse perfil personalizado pode ser selecionado na página Implantar imagens de SO. Em seguida, os pacotes SLE que você deseja implantar podem ser selecionados e fuso horário pode ser especificado na guia **Configurações personalizadas**. Os

valores selecionados são substituídos para macros personalizadas no arquivo sem supervisão, e o instalador do autoyast SLES usa esses valores no arquivo sem supervisão para configurar o sistema operacional.

Antes de iniciar

Esse cenário usa os seguintes arquivos de amostra.

- SLES_installPackages_customConfig.json. Esse arquivo de configuração solicita o fuso horário e pacotes SLES opcionais (Linux, Apache, MySQL, pacote do servidor de arquivos do pacote de software PHP, pacote do servidor de e-mail SLES e SLES) para instalar.
- SLES_installPackages_customUnattend.xml Esse arquivo sem supervisão usa os valores em macros predefinidas e macros personalizadas que são definidas no arquivo de configuração.

Procedimento

Para implantar o SLES 12 SP3 em servidores usando perfil de imagem de SO personalizado, conclua as seguintes etapas.

Etapa 1. Baixe o sistema operacional SLES base do site SUSE para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando imagens do sistema operacional.

1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
2. Clique na guia **Imagens do SO**.
3. Clique no ícone **Importar** ( ).
4. Clique em **Importação Local**.
5. Clique em **Procurar** para encontrar e selecionar a imagem SLES 12 SP3 a ser importada (por exemplo, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Clique em **Importar** para fazer o upload da imagem do SO no repositório de imagens do SO.
7. Aguarde a conclusão da importação. Isso pode levar alguns minutos.

Etapa 2. Crie um arquivo de configuração personalizado e importe o arquivo para o repositório de imagens do SO.

O arquivo de definições de configuração é um arquivo JSON que descreve os dados que precisam ser coletados dinamicamente durante o processo de implantação do SO. Neste cenário, deseja especificar os pacotes de SLES opcionais que podem ser instalados (incluindo SLES Linux, Apache, MySQL, software PHP pacote, pacote de SLES do servidor de e-mail e pacote do servidor de arquivos SLES) e um fuso horário a ser usada para cada implantação do SO. Para obter mais informações sobre criação de arquivo de configuração, consulte Macros personalizadas.

Para importar o arquivo de configuração, conclua estas etapas. Para obter mais informações, consulte Importando definições de configuração personalizadas.

1. Clique na guia **Arquivos de configuração**.
2. Clique no ícone **Importar** ( ).
3. Clique em **Importação Local**.
4. Selecione `SLES` do sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o arquivo de definições de configuração para importar (por exemplo, `SLES_installPackages_customConfig.json`).

6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.

   Nota: Quando você importar o arquivo de definições de configuração personalizada, XClarity Administrator cria uma macro personalizada para cada configuração no arquivo. Você pode adicioná-las para o arquivo sem supervisão. Durante a implantação do SO, as macros são substituídas por valores reais.

Etapa 3. Modifique o arquivo de assistido SLES para especificar os valores dinâmicos para os pacotes SLES opcionais e o fuso horário e, em seguida, importe o arquivo personalizado para o repositório de imagens do SO. Para obter mais informações, consulte Importando arquivos sem supervisão personalizados.

Na seção **<general>**, adicione as informações de fuso horário, por exemplo:

```
<timezone>
   <hwclock></hwclock>
   <timezone></timezone>
</timezone>
```

Na seção **<patterns>**, adicione três marcas padrão. Essas marcas são usadas para as macros personalizadas para as configurações de pacote SLES opcionais, por exemplo:

```
<patterns config:type="list">
   <pattern>32bit</pattern>
   <pattern>Basis-Devel</pattern>
   <pattern>Minimal</pattern>
   <pattern>WBEM</pattern>
   <pattern>apparmor</pattern>
   <pattern>base</pattern>
   <pattern>documentation</pattern>
   <pattern>fips</pattern>
   <pattern>gateway_server</pattern>
   <pattern>ofed</pattern>
   <pattern>printing</pattern>
   <pattern>sap_server</pattern>
   <pattern>x11</pattern>
   <pattern></pattern>
   <pattern></pattern>
   <pattern></pattern>
</patterns>
```

Notas:

- Essas marcas estão no arquivo sem supervisão de amostra.
- Ao usar um arquivo sem supervisão personalizado, o XClarity Administrator não fornece vários dos recursos normais disponíveis quando você usa um arquivo sem supervisão predefinido. Por exemplo, os destinos **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>** e **<UserAccounts>** para administrador, **<Interfaces>** para acesso à rede e **<package>** lista para recursos de instalação devem ser especificados no arquivo sem supervisão personalizado que está sendo transferido por upload.

Para importar o arquivo sem supervisão personalizado, conclua estas etapas.

1. Clique na guia **Arquivos sem supervisão**.
2. Clique no ícone **Importar** ().
3. Clique em **Importação Local**.
4. Selecione `SLES` do sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o arquivo sem supervisão a ser importado (por exemplo, `SLES_installPackages_customUnattend.xml`).

6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.

   Nota: Um aviso de que há macros predefinidas ausentes no arquivo sem supervisão é exibido. É possível ignorar o aviso por enquanto. Você adicionará as macros predefinidas na próxima etapa

7. Clique em **Fechar** na caixa de diálogo de aviso para abrir a caixa de diálogo Editar arquivo sem supervisão.

Etapa 4. Associar o arquivo sem supervisão personalizado com o arquivo de configurações personalizadas e inclua as predefinidas e personalizadas macros necessárias (configurações) do arquivo de definições de configuração no arquivo sem supervisão. Para obter mais informações, consulte Associando um arquivo sem supervisão a um arquivo de configuração e Inserindo macros predefinidas e personalizadas para um arquivo sem supervisão.

Dica: Como opção, você pode associar o arquivo sem supervisão personalizado com o arquivo de definições de configuração personalizado e adicionar macros ao importar o arquivo sem supervisão.

1. Na caixa de diálogo Editar arquivo sem supervisão, selecione o arquivo de definições de configuração para associar ao arquivo sem supervisão da lista suspensa **Associar um arquivo de configuração** (por exemplo, `SLES_installPackages_customConfig`).
2. Adicione as macros predefinidas necessárias para o arquivo sem supervisão.
   a. Selecione **Predefinido** da lista suspensa **Macros disponíveis**.
   b. Coloque o cursor no arquivo assistido em qualquer lugar após a linha 1 (após a marca **<xml>**).
   c. Expanda a lista **predefinida → unattendSettings** na lista de macros predefinidas disponíveis.
   d. Clique em macros **preinstallConfig** e **postinstallConfig** para adicionar as macros no arquivo sem supervisão.

   Exemplo:

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

3. Adicione a macro personalizada para especificar o fuso horário.
   a. Selecione **Personalizada** da lista suspensa **Macros disponíveis**.
   b. Coloque o cursor após a marca **<hwclock>**, e clique em **fuso horário** para adicionar a macro de fuso horário.
   c. Coloque o cursor após a marca **<timezone>**, e clique em **fuso horário** para adicionar a macro de fuso horário.

   Exemplo:

```
<timezone>
   <hwclock>#timezone#</hwclock>
   <timezone>#timezone#</timezone>
</timezone>
```

4. Adicione a macro personalizada para especificar os pacotes SLES opcionais.
   a. Expanda a lista **server-settings → node** na lista de macros personalizadas disponíveis.
   b. Coloque o cursor em uma das marcas vazias **<pattern>** e clique em **fileserver**.
   c. Coloque o cursor em uma das marcas vazias **<pattern>** e clique em **lampserver**.
   d. Coloque o cursor em uma das marcas vazias **<pattern>** e clique em **mailserver**.

Exemplo:

```
<patterns config:type="list">
   <pattern>32bit</pattern>
   <pattern>Basis-Devel</pattern>
   <pattern>Minimal</pattern>
   <pattern>WBEM</pattern>
   <pattern>apparmor</pattern>
   <pattern>base</pattern>
   <pattern>documentation</pattern>
   <pattern>fips</pattern>
   <pattern>gateway_server</pattern>
   <pattern>ofed</pattern>
   <pattern>printing</pattern>
   <pattern>sap_server</pattern>
   <pattern>x11</pattern>
   <pattern>#server-settings.node.fileserver#</pattern>
   <pattern>#server-settings.node.lampserver#</pattern>
   <pattern>#server-settings.node.mailserver#</pattern>
</patterns>
```

5. Clique em **Salvar** para associar os arquivos e salvar as alterações no arquivo sem supervisão.

Etapa 5. Crie um perfil de imagem do SO personalizado que inclui as definições de configuração personalizadas e arquivos não atendidos. Para obter mais informações, consulte Criando um perfil da imagem do SO personalizada.

1. Clique na guia **Imagens do SO**.
2. Selecione o perfil de imagem de SO a ser personalizado (por exemplo, `Basic`).
3. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Criar Perfil Personalizado.
4. Na guia **Geral**:
   a. Insira um nome para o perfil, por exemplo, `SLES personalizado com pacotes opcionais`.
   b. Use o valor padrão para o campo **Caminho de dados e arquivo personalizado**.
   c. Selecione **Arquivos de definições de configuração e sem supervisão associados** para o tipo de personalização.
   d. Clique em **Avançar**.
5. Na guia **Opções de Driver**, clique em **Próximo**. Os drivers de dispositivo de entrada são incluídos por padrão.
6. Na guia **Software**, clique em **Próximo**.
7. Na guia **Não supervisionar arquivos**, selecione o arquivo sem supervisão (por exemplo, `SLES_installPackages_customUnattend.xml`) e clique em **Avançar**.

   O arquivo de definições de configuração associados é selecionado automaticamente.
8. Na guia **Scripts de instalação**, clique em **Próximo**.
9. Na guia **Resumo**, revise as configurações.
10. Clique em **Personalizar** para criar o perfil de imagem do SO personalizado.

Etapa 6. Implante o perfil de imagem do SO personalizado nos servidores de destino. Para obter mais informações, consulte Implantando uma imagem do sistema operacional.

1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar Sistema Operacional: Implantar Imagens do SO.
2. Para cada servidor de destino:
   a. Selecione o servidor.
   b. Clique em **Alterar Selecionado → Configurações de Rede** e especifique o nome do host, endereço IP, as configurações de DNS, MTU e VLAN para o servidor.

Dica: As configurações de VLAN estão disponíveis apenas quando o modo VLAN é definido em **Configurações Globais → Atribuição de IP → Usar VLANs**.

c. Selecione o perfil da imagem do SO personalizada (por exemplo, *<base_OS>*|*<timestamp>*_SLES personalizado com pacotes opcionais) na lista suspensa na coluna **Imagem para implantação**.

Nota: Certifique-se de que todos os servidores de destino usem o mesmo perfil personalizado.

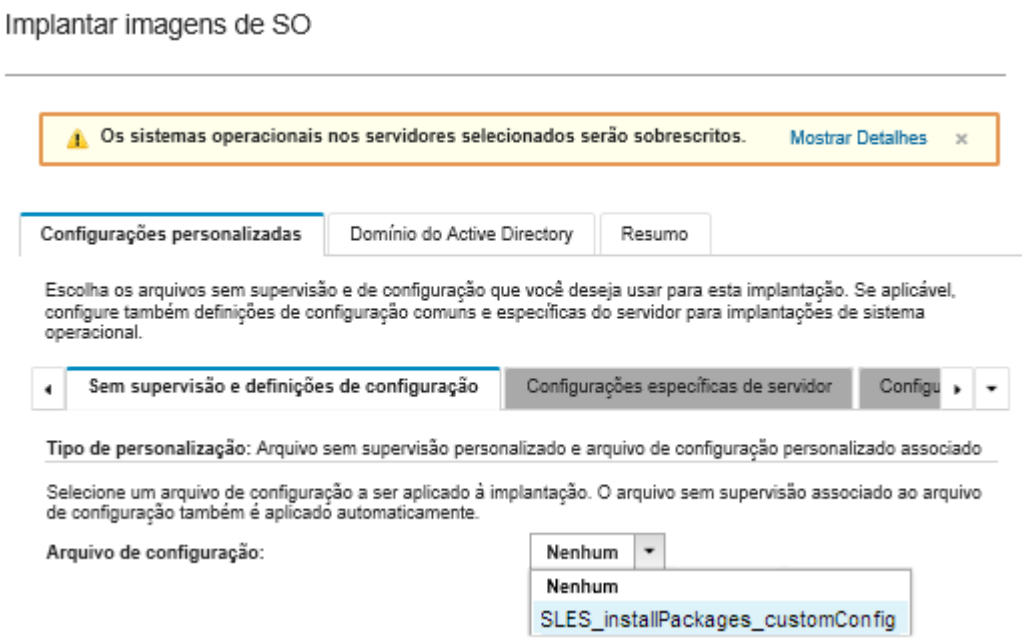
d. Selecione o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional na coluna **Armazenamento**.

Nota: Para garantir que as implantações do sistema operacional foram feitas com êxito, remova qualquer armazenamento do servidor gerenciado, exceto o armazenamento que será escolhido para a implantação do sistema operacional.

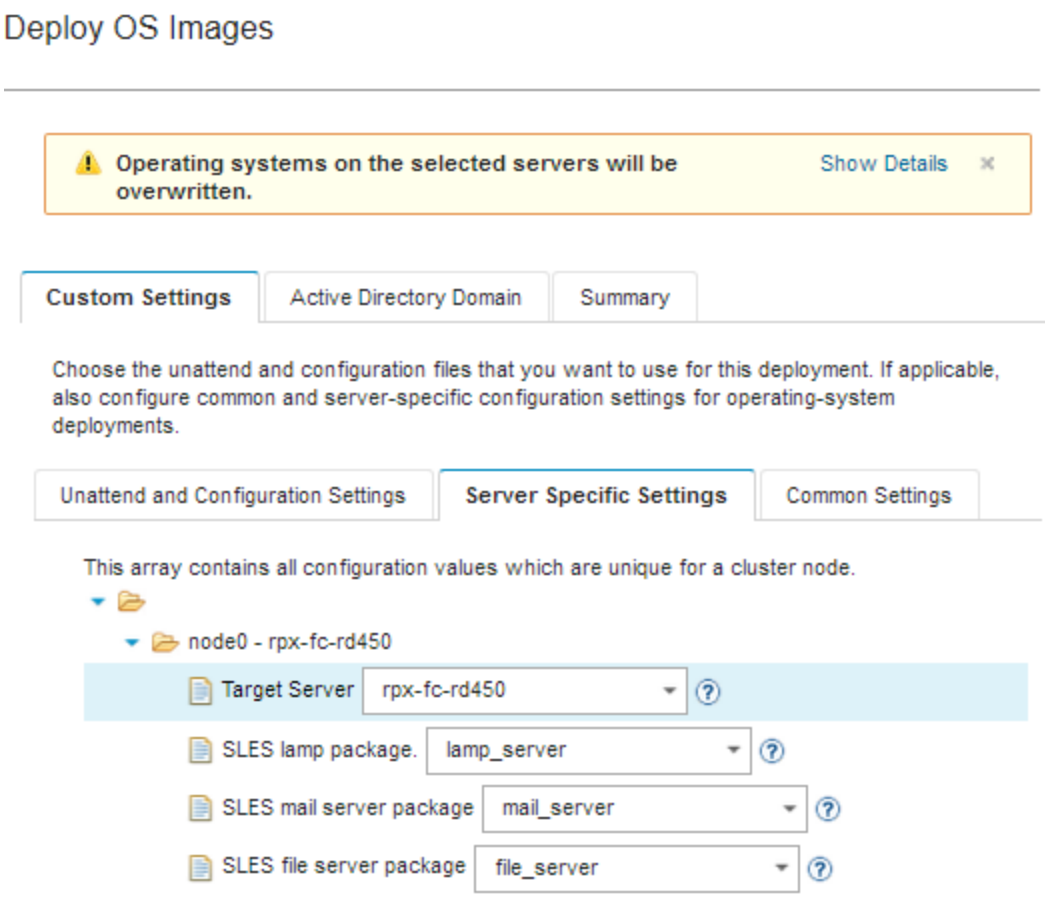
e. Verifique se o status da implantação para o servidor selecionado é **Pronto**.

3. Selecione todos os servidores de destino e clique no ícone **Implantar imagem** ( ) para iniciar a implementação do sistema operacional.
4. Na guia **Configurações personalizadas**, clique na subguia **Sem supervisão e definições de configuração** e selecione o arquivo de definições de configuração personalizado (por exemplo, SLES_installPackages_customConfig).

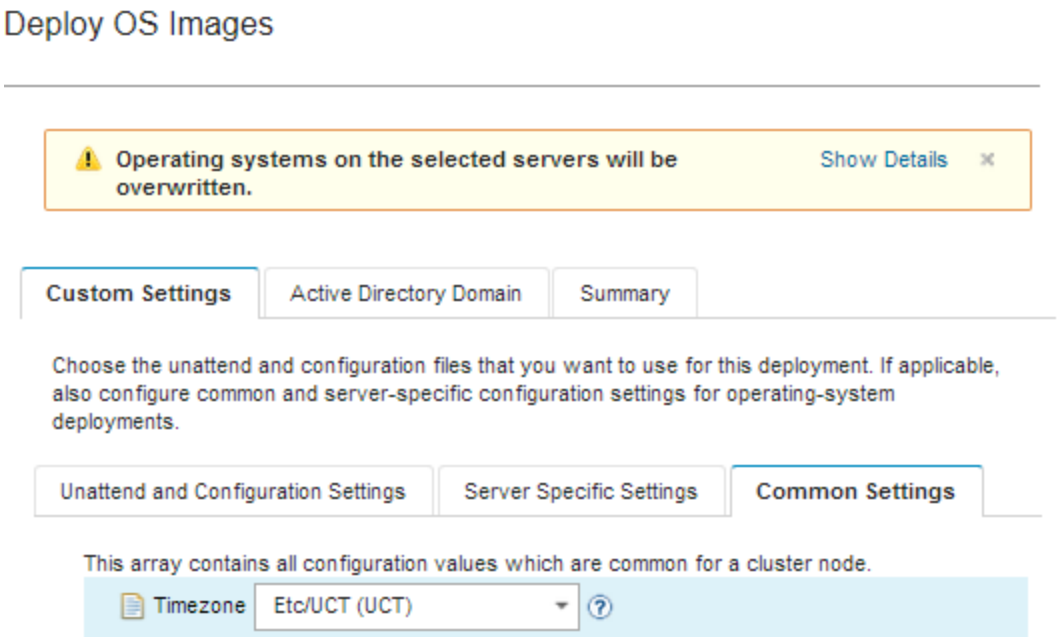
Nota: O arquivo sem supervisão personalizado associado é selecionado automaticamente.



5. Na subguia **Configurações específicas do servidor**, selecione o servidor de destino e os pacotes SLES opcionais que você deseja implantar.



6. Na subguia **Configurações comuns**, selecione o fuso horário para configurar todos os servidores de destino.



7. Na guia **Resumo**, revise as configurações.
8. Clique em **Implantar** para implantar o sistema operacional.

Implantação do SLES 12 SP3 com software personalizado

Este cenário instala o sistema operacional SLES 12 SP3 juntamente com o software personalizado (Java e Eclipse IDE). Um perfil personalizado que inclui o software personalizado e scripts pós-instalação é usado para instalar e configurar o software personalizado. Os pacotes de software personalizados são copiados para o host durante a implantação e disponibilizados para o script pós-instalação personalizado a ser usado.

Antes de iniciar

Esse cenário usa os seguintes arquivos de amostra.

- jre-8u151-linux-x64.tar.gz. Este é o arquivo de instalação para Java para o Eclipse.
- eclipse-4.6.3-3.1.x86_64.tar.gz Este é o arquivo de instalação para o Eclipse IDE.
- SLES_installSoftware_customScript.sh Este script pós-instalação cria um usuário para iniciar o Eclipse e instala o Eclipse IDE e o Java.

Notas:

- Os scripts de instalação do SLES podem estar em um dos seguintes formatos: Bash (.sh), Perl (.pm ou. pl), Python (.py)
- Arquivos de software e scripts de instalação são instalados do caminho de dados e arquivos personalizado que você especificar durante a implantação. O caminho arquivos e dados personalizados padrão é `/home/lxca`.
- Para SLES 12 SP3, o Eclipse IDE requer o compilador GCC, que está incluído no perfil básico predefinido. Este cenário cria um perfil de imagem do SO personalizado com o perfil básico predefinido como base. Se você optar por usar outro perfil, certifique-se de que o perfil inclua o compilador GCC.

Procedimento

Para implantar o SLES 12 SP3 com software personalizado, conclua as etapas a seguir.

Etapa 1. Baixe o sistema operacional SLES 12 SP3 do site SUSE para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando imagens do sistema operacional.

1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
2. Clique na guia **Imagens do SO**.
3. Clique no ícone **Importar** ( ).
4. Clique em **Importação Local**.
5. Clique em **Procurar** para encontrar e selecionar a imagem SLES 12 SP3 a ser importada (por exemplo, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Clique em **Importar** para fazer o upload da imagem do SO no repositório de imagens do SO.
7. Aguarde a conclusão da importação. Isso pode levar alguns minutos.

Etapa 2. Baixe o software personalizado no sistema local e importar os arquivos para o repositório de imagens do SO. Para obter mais informações, consulte Importando software personalizado.

1. Clique na guia **Software**.
2. Clique no ícone **Importar** ( ).
3. Clique em **Importação Local**.
4. Selecione `SLES` do sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o arquivo de software a ser importado (por exemplo, `jre-8u151-linux-x64.tar.gz`).

6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.
7. Clique no ícone **Importar** () novamente.
8. Clique em **Importação Local**.
9. Selecione `SLES` do sistema operacional.
10. Clique em **Procurar** para localizar e selecionar o arquivo de software a ser importado (por exemplo, `eclipse-4.6.3-3.1.x86_64.tar.gz`).
11. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.

Etapa 3. Crie um script pós-instalação personalizado e importe o arquivo para o repositório de imagens do SO.

Adicione comandos para criar um usuário para iniciar o eclipse para esse arquivo, por exemplo:

```
echo "Create a user called lenovo..."
egrep "lenovo" /etc/passwd >/dev/null
pass=$(perl -e 'print crypt($ARGV[0], "password")' "PasswOrd")
useradd -m -p $pass lenovo
[ $? -eq 0 ] &amp;amp;&amp;amp; echo "User has been created." || curl -X PUT
--globoff #predefined.otherSettings.statusSettings.urlStatus# -H "Content-Type: application/json"
-d '{"deployStatus":{"id":"46","parameters":["'"Could not create lenovo user"'"]}}'
--cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
--key #predefined.otherSettings.statusSettings.certLocation#/key.pem
--cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Adicione comandos para instalar o software, por exemplo:

```
#Install Java for eclipse
echo "Installing Java JRE 8...."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/jre-8u151-linux-x64.rpm

#Install eclipse
echo "Installing Eclipse IDE..."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/eclipse-4.6.3-3.1.x86_64.rpm
```

Observe que esses comandos usam macros predefinidas para a URL HTTPS que o XClarity Administrator usa para relatório de status (**predefined.otherSettings.statusSettings.urlStatus**), para a pasta que contém os certificados necessários para acessar o serviço Web urlStatus do sistema operacional do host na primeira inicialização (**predefined.otherSettings.statusSettings.certLocation**) e o caminho para os dados extraídos e arquivos de software (**predefined.otherSettings.deployDataAndSoftwareLocation**).

É possível também incluir os comandos para enviar mensagens personalizadas para as tarefas de login no XClarity Administrator, conforme mostrado no arquivo de exemplo. Para obter mais informações, consulte Adicionando relatório de status personalizado aos scripts de instalação.

Para importar o script de instalação personalizado, conclua estas etapas. Para obter mais informações, consulte Importando scripts de instalação personalizados.

1. Clique na guia **Scripts de instalação**.
2. Clique no ícone **Importar** ().
3. Clique em **Importação Local**.
4. Selecione `SLES` do sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o script de pós-instalação que você deseja importar, por exemplo, `SLES_installSoftware_customScript.sh`.
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.

Etapa 4. Crie um perfil de imagem do SO personalizado que inclui o software personalizado e scripts pós-instalação. Para obter mais informações, consulte Criando um perfil da imagem do SO personalizada.

1. Clique na guia **Imagens do SO**.
2. Selecione o perfil de imagem de SO a ser personalizado (por exemplo, `Basic`).
3. Clique no ícone **Criar** () para exibir a caixa de diálogo Criar Perfil Personalizado.
4. Na guia **Geral**:
   a. Insira um nome para o perfil, por exemplo, `SLES personalizado com software`.
   b. Use o valor padrão para o campo **Caminho de dados e arquivo personalizado**.
   c. Selecione **Nenhum** para o tipo de personalização.
   d. Clique em **Avançar**.
5. Na guia **Opções de Driver**, clique em **Próximo**. Os drivers de dispositivo de entrada são incluídos por padrão.
6. Na guia **Software**, selecione os arquivos de instalação de software (por exemplo, `jre-8u151-linux-x64.tar.gz` e `eclipse-4.6.3-3.1.x86_64.tar.gz`) e clique em **Avançar**.
7. Na guia **Scripts de instalação**, selecione os scripts de instalação (por exemplo, `SLES_installSoftware_customScript.sh`) e clique em **Avançar**.
8. Na guia **Resumo**, revise as configurações.
9. Clique em **Personalizar** para criar o perfil de imagem do SO personalizado.

Etapa 5. Implante o perfil de imagem do SO personalizado nos servidores de destino. Para obter mais informações, consulte Implantando uma imagem do sistema operacional.

1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar Sistema Operacional: Implantar Imagens do SO.
2. Para cada servidor de destino:
   a. Selecione o servidor.
   b. Clique em **Alterar Selecionado → Configurações de Rede** e especifique o nome do host, endereço IP, as configurações de DNS, MTU e VLAN para o servidor.

      Dica: As configurações de VLAN estão disponíveis apenas quando o modo VLAN é definido em **Configurações Globais → Atribuição de IP → Usar VLANs**.
   c. Selecione o perfil da imagem do SO personalizada (por exemplo, *<base_OS>*|*<timestamp>*`_SLES personalizado com software`) na lista suspensa na coluna **Imagem para implantação**

      Nota: Certifique-se de que todos os servidores de destino usem o mesmo perfil personalizado.
   d. Selecione o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional na coluna **Armazenamento**.

      Nota: Para garantir que as implantações do sistema operacional foram feitas com êxito, remova qualquer armazenamento do servidor gerenciado, exceto o armazenamento que será escolhido para a implantação do sistema operacional.
   e. Verifique se o status da implantação para o servidor selecionado é **Pronto**.
3. Selecione todos os servidores de destino e clique no ícone **Implantar imagem** () para iniciar a implementação do sistema operacional.
4. Na guia **Resumo**, revise as configurações.
5. Clique em **Implantar** para implantar o sistema operacional.

Implantando o SLES 12 SP3 com um código do idioma configurável e servidores NTP

Este cenário instala o sistema operacional SLES 12 SP3 com inglês, português (Brasil) ou japonês habilitado para o teclado e a localização do sistema operacional. Ele também configura o endereço IP para até três servidores NTP. Um perfil de imagem do SO personalizado é usado para incluir um arquivo sem supervisão (com macros predefinidas e personalizadas) e um arquivo de definições de configuração para selecionar a localização e configurações do servidor NTP. Esse perfil personalizado pode ser selecionado na página Implantar imagens de SO. Em seguida, os códigos de idioma e as configurações do servidor NTP podem ser selecionados na guia **Configurações personalizadas**. Os valores especificados são substituídos para as macros personalizadas contidas no arquivo sem supervisão personalizado, e o instalador do autoyast SLES usa esses valores no arquivo sem supervisão para configurar o sistema operacional.

Antes de iniciar

Esse cenário usa os seguintes arquivos de amostra.

- SLES_locale_customConfig.json. Esse arquivo de configuração personalizado solicita para o idioma para instalar, para o teclado e o SO local para SLES e para o servidor NTP.
- SLES_locale_customUnattend.xml. Esse arquivo assistido personalizado usa os valores no macros personalizadas que são definidas no arquivo de configuração.

Procedimento

Para implantar o SLES 12 SP3 usando perfil de imagem de SO personalizado, conclua as seguintes etapas.

Etapa 1. Baixe o sistema operacional SLES base do site SUSE para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando imagens do sistema operacional.

1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
2. Clique na guia **Imagens do SO**.
3. Clique no ícone **Importar** ( ).
4. Clique em **Importação Local**.
5. Clique em **Procurar** para encontrar e selecionar a imagem SLES 12 SP3 a ser importada (por exemplo, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Clique em **Importar** para fazer o upload da imagem do SO no repositório de imagens do SO.
7. Aguarde a conclusão da importação.

Etapa 2. Crie um arquivo de configuração personalizado e importe o arquivo para o repositório de imagens do SO.

O arquivo de definições de configuração é um arquivo JSON que descreve os dados que precisam ser coletados dinamicamente durante o processo de implantação do SO. Para esse cenário, desejamos especificar a localização do sistema operacional (en_US, ja_JP, pt_BR), o idioma do teclado (english-us, Japanese, ou portugese-br) e até três endereços IP de servidor NTP a ser usada para cada implantação do SO. Para obter mais informações sobre criação de arquivo de configuração, consulte Macros personalizadas.

Para importar o arquivo de configuração, conclua estas etapas. Para obter mais informações, consulte Importando definições de configuração personalizadas.

1. Clique na guia **Arquivos de configuração**.
2. Clique no ícone **Importar** ( ).

3. Clique em **Importação Local**.
4. Selecione `SLES` do sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o arquivo de definições de configuração para importar (por exemplo, `SLES_locale_customConfig.json`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO

   Nota: Quando você importar o arquivo de definições de configuração personalizada, XClarity Administrator cria uma macro personalizada para cada configuração no arquivo. Você pode adicioná-las para o arquivo sem supervisão. Durante a implantação do SO, as macros são substituídas por valores reais.

Etapa 3. Modifique o arquivo sem supervisão SLES para especificar os valores dinâmicos para localização do sistema operacional, localização do teclado e endereços IP do servidor NTP e, então, importe o arquivo personalizado para o repositório de imagens do SO. Para obter mais informações, consulte Importando arquivos sem supervisão personalizados.

Logo após a marca **<profile>**, adicione as informações de rede e do servidor NTP. O exemplo a seguir inclui marcas de dois servidores NTP. Os endereços IP serão adicionados como macros em uma etapa posterior.

```
<ntp-client>
   <configure_dhcp config:type="boolean">false</configure_dhcp>
   <peers config:type="list">
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
   </peers>
   <start_at_boot config:type="boolean">true</start_at_boot>
   <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

Na seção **<general>**, inclua as informações de localização do teclado e do SO, conforme mostrado na exemplo a seguir. As configurações de teclado e localidade do sistema operacional serão adicionadas como macros em uma etapa posterior.

```
<keyboard>
   <keymap></keymap>
</keyboard>
<language></language>
```

Nota: Ao usar um arquivo sem supervisão personalizado, o XClarity Administrator não fornece vários dos recursos normais disponíveis quando você usa um arquivo sem supervisão predefinido. Por exemplo, os destinos **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>** e **<UserAccounts>** para administrador, **<Interfaces>** para acesso à rede e **<package>** lista para recursos de instalação devem ser especificados no arquivo sem supervisão personalizado que está sendo transferido por upload.

Para importar o arquivo sem supervisão personalizado, conclua estas etapas.

1. Clique na guia **Arquivos sem supervisão**.

2. Clique no ícone **Importar** ().
3. Clique em **Importação Local**.
4. Selecione `SLES` do sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o arquivo sem supervisão a ser importado (por exemplo, `SLES_locale_customUnattend.xml`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO

Etapa 4. Associar o arquivo sem supervisão personalizado com o arquivo de configurações personalizadas e inclua as predefinidas e personalizadas macros necessárias (configurações) do arquivo de definições de configuração no arquivo sem supervisão. Para obter mais informações, consulte Associando um arquivo sem supervisão a um arquivo de configuração e Inserindo macros predefinidas e personalizadas para um arquivo sem supervisão.

Dica: Como opção, você pode associar o arquivo sem supervisão personalizado com o arquivo de definições de configuração personalizado e adicionar macros ao importar o arquivo sem supervisão.

1. Na guia **Não supervisionar arquivos**, selecione o arquivo com supervisão personalizado (por exemplo, `SLES_locale_customUnattend.xml`).
2. Clique no ícone **Associar um arquivo de configuração** () para exibir a caixa de diálogo Associar um arquivo sem supervisão.
3. Selecione o arquivo de configuração para associar ao arquivo sem supervisão (por exemplo, `SLES_locale_customConfig`).
4. Adicione as macros predefinidas necessárias para o arquivo sem supervisão.
   a. Selecione **Predefinido** da lista suspensa **Macros disponíveis**.
   b. Coloque o cursor no arquivo assistido em qualquer lugar após a linha 1 (após a marca **<xml>**).
   c. Expanda a lista **predefinida → unattendSettings** na lista de macros predefinidas disponíveis.
   d. Clique em macros **preinstallConfig** e **postinstallConfig** para adicionar as macros.

   Exemplo:

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/YaST2/include/autoinstall/profile.dtd">
   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

5. Adicione a macro personalizada para especificar a localização do sistema operacional.
   a. Selecione **Personalizada** da lista suspensa **Macros disponíveis**
   b. Coloque o cursor após a marca **<language>**.
   c. Expanda **configurações do servidor → nó** na lista de macros personalizadas disponíveis e, em seguida, clique em **localização** para adicionar a macro de localização do SO.

   Exemplo:

```
<language>#server-settings.node.locale#</language>
```

6. Adicione a macro personalizada para especificar a localização do teclado.
   a. Coloque o cursor após a marca **<keymap>**.
   b. Expanda **configurações do servidor → nó** na lista de macros personalizadas disponíveis e, em seguida, clique em **keyboardLocale** para adicionar a macro localização do teclado.

Exemplo:

```
<keyboard>
   <keymap>#server-settings.node.keyboardLocale#</keymap>
</keyboard>
```

7. Adicione a macro personalizada para especificar os endereços IP do servidor NTP.

   Neste cenário, o arquivo de definições de configuração personalizado usa um modelo para especificar zero a três servidores NTP. Ao usar modelos no arquivo de definições de configuração, macros que estão associadas com modelo não são exibidas na caixa de diálogo Associar arquivo sem supervisão. Em vez disso, você deve editar manualmente o arquivo sem supervisão e adicionar as macros e marcas apropriadas.

   Por exemplo, para incluir três servidores NTP, você deve adicionar as seguintes marcas e macros ao arquivo sem supervisão. Essas marcas e macros já existem no arquivo sem supervisão de exemplo para esse cenário.

```
<ntp-client>
   <configure_dhcp config:type="boolean">false</configure_dhcp>
   <peers config:type="list">
      <peer>
         <address>#server-settings.ntpserver1#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address>#server-settings.ntpserver2#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address>#server-settings.ntpserver3#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
   </peers>
   <start_at_boot config:type="boolean">true</start_at_boot>
    <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

8. Clique em **Associar** para associar os arquivos e salvar as alterações no arquivo sem supervisão.

Etapa 5. Crie um perfil de imagem do SO personalizado que inclui as definições de configuração personalizadas e arquivos não atendidos. Para obter mais informações, consulte Criando um perfil da imagem do SO personalizada.

1. Clique na guia **Imagens do SO**.
2. Selecione o perfil de imagem de SO a ser personalizado (por exemplo, `Basic`).
3. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Criar Perfil Personalizado.
4. Na guia **Geral**:
   a. Insira um nome para o perfil (por exemplo, `SLES personalizada de idioma do SO e teclado e servidor NTP`).
   b. Use o valor padrão para o campo **Caminho de dados e arquivo personalizado**.
   c. Selecione **Arquivos de definições de configuração e sem supervisão associados** para o tipo de personalização.
   d. Clique em **Avançar**.

5. Na guia **Opções de Driver**, clique em **Próximo**. Os drivers de dispositivo de entrada são incluídos por padrão.
6. Na guia **Software**, clique em **Próximo**.
7. Na guia **Não supervisionar arquivos**, selecione o arquivo sem supervisão (por exemplo, `SLES_locale_customUnattend.xml`) e clique em **Avançar**.

   O arquivo de definições de configuração associados é selecionado automaticamente.
8. Na guia **Scripts de instalação**, clique em **Próximo**.
9. Na guia **Resumo**, revise as configurações.
10. Clique em **Personalizar** para criar o perfil de imagem do SO personalizado.

Etapa 6. Implante o perfil de imagem do SO personalizado no servidor de destino. Para obter mais informações, consulte Implantando uma imagem do sistema operacional.

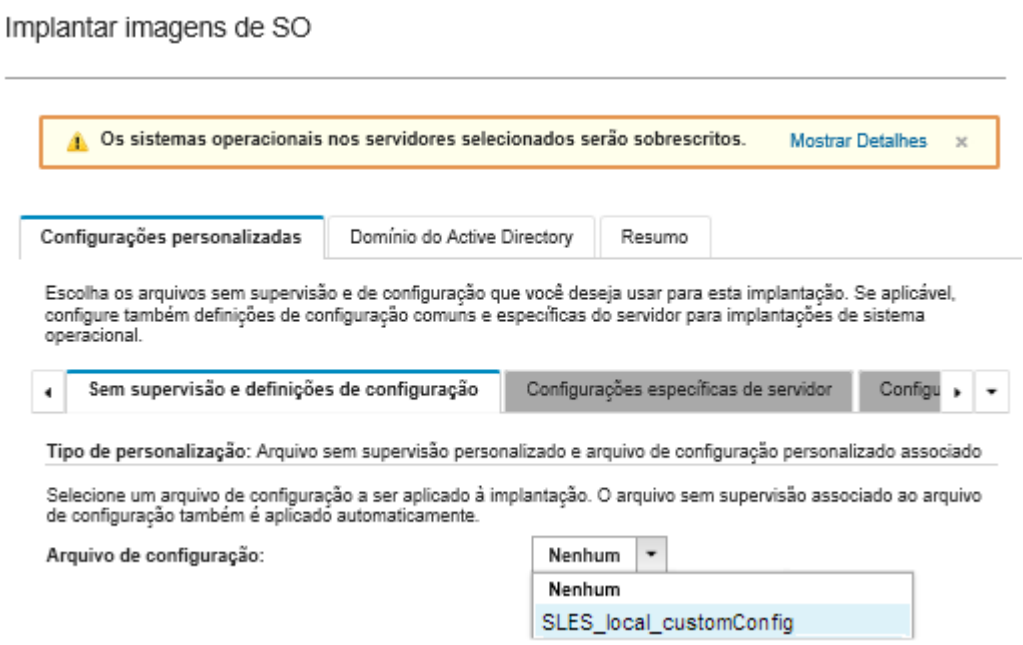
1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar Sistema Operacional: Implantar Imagens do SO.
2. Para cada servidor de destino:
   a. Selecione o servidor.
   b. Clique em **Alterar Selecionado → Configurações de Rede** e especifique o nome do host, endereço IP, as configurações de DNS, MTU e VLAN para o servidor.

      Dica: As configurações de VLAN estão disponíveis apenas quando o modo VLAN é definido em **Configurações Globais → Atribuição de IP → Usar VLANs**.
   c. Selecione o perfil da imagem do SO personalizada (por exemplo, <*base_OS*>|<*timestamp*>`_SLES personalizado para idioma do SO e do teclado e servidor NTP`) na lista suspensa na coluna **Imagem para implantação**

      Nota: Certifique-se de que todos os servidores de destino usem o mesmo perfil personalizado.
   d. Selecione o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional na coluna **Armazenamento**.

      Nota: Para garantir que as implantações do sistema operacional foram feitas com êxito, remova qualquer armazenamento do servidor gerenciado, exceto o armazenamento que será escolhido para a implantação do sistema operacional.
   e. Verifique se o status da implantação para o servidor selecionado é **Pronto**.
3. Selecione todos os servidores de destino e clique no ícone **Implantar imagem** () para iniciar a implementação do sistema operacional.
4. Na guia **Configurações personalizadas**, clique na subguia **Sem supervisão e definições de configuração** e selecione o arquivo de definições de configuração personalizado (por exemplo, `SLES_locale_customConfig`).

   Nota: O arquivo sem supervisão personalizado associado é selecionado automaticamente.



5. Na subguia **Configurações específicas do servidor**, selecione o servidor de destino, o código do idioma do SO e o código do idioma do teclado.
6. Na subguia **Configurações comuns**, clique em **Adicionar** para especificar o endereço IP até três de servidores de NTP.
7. Na guia **Resumo**, revise as configurações.
8. Clique em **Implantar** para implantar o sistema operacional.

Implantando o VMware ESXi v6.7 com Lenovo Customization em um disco local usando um endereço IP estático

Neste cenário, o VMware ESXi v6.7 é instalado com o sistema operacional Lenovo Customization no disco local usando o endereço IP estático do servidor host. É usado um perfil de imagem de SO personalizado que inclui um arquivo sem supervisão com macros predefinidas. Esse perfil personalizado pode ser selecionado na página Implantar imagens de SO. Os valores conhecidos são substituídos para as macros predefinidas no arquivo sem supervisão personalizado, e o instalador do VMware ESXi kickstart usa esses valores no arquivo sem supervisão para configurar o sistema operacional.

Antes de iniciar

Esse cenário usa os seguintes arquivos de amostra.

- ESXi_staticIP_customUnattend.cfg. Esse arquivo sem supervisão personalizado usa os valores em macros predefinidas.

Procedimento

Para implantar o VMware ESXi v6.7 usando perfil de imagem de SO personalizado, conclua as seguintes etapas.

Etapa 1. Baixe o VMware vSphere® Hypervisor (ESXi) com o sistema operacional Lenovo Customization do site Suporte VMware – Página da Web de downloads para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando imagens do sistema operacional.

1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
2. Clique na guia **Imagens do SO**.
3. Clique no ícone **Importar** ().
4. Clique em **Importação Local**.
5. Clique em **Procurar** para encontrar e selecionar a imagem do ESXi a ser importada (por exemplo, `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Clique em **Importar** para fazer o upload da imagem do SO no repositório de imagens do SO.
7. Aguarde a conclusão da importação.

Etapa 2. Modifique o arquivo sem supervisão (kickstart) do ESXi para adicionar as macros predefinidas necessárias e outras macros predefinidas quando aplicável, como o endereço IP, gateway, configurações de nome de host e DNS e, em seguida, importe o arquivo personalizado para o repositório de imagens do SO. Para obter mais informações, consulte Importando arquivos sem supervisão personalizados.

Somente para ESXi e RHEL, o XClarity Administrator fornece a macro **#predefined.unattendSettings.networkConfig#**, que adiciona todas as configurações de rede que estão definidas na interface do usuário ao arquivo sem supervisão. Como esse exemplo especifica uma configuração (**--addvmportgroup**) que não está definida na interface do usuário, a macro **#predefinedunattendSettings.storageConfig#** não é usada no arquivo sem supervisão de exemplo. Em vez disso, as configurações de rede são incluídas individualmente no arquivo e as macros **#predefined.hostPlatforms.networkSettings.**<*setting*>**#** são usadas.

Somente para ESXi e RHEL, o XClarity Administrator também fornece a macro **#predefined.unattendSettings.storageConfig#**, que adiciona todas as configurações de armazenamento que estão definidas na interface do usuário ao arquivo sem supervisão. Como esse exemplo especifica configurações (**--novmfsondisk** e **–ignoressd**) que não estão definidas na interface do usuário, a macro **#predefinedunattendSettings.storageConfig#** não é usada no arquivo sem supervisão de exemplo. Em vez disso, as configurações de armazenamento são adicionadas individualmente e **--firstdisk=local** é codificado permanentemente no arquivo.

Nota: O XClarity Administrator fornece algumas macros básicas, como inserção de driver OOB, relatório de status, scripts pós-instalação e software personalizado. No entanto, para aproveitar essas macros predefinidas, especifique as seguintes macros no arquivo sem supervisão personalizado. O arquivo de exemplo já contém as macros necessárias. Como a seção firstboot % está incluída, a ordem dessas macros predefinidas é importante. Para obter mais informações, consulte Importando arquivos sem supervisão personalizados.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

O arquivo de exemplo já contém as macros necessárias e as macros predefinidas adicionais para especificar dinamicamente configurações de rede para o servidor de destino. Para obter mais informações sobre como adicionar macros para arquivos sem supervisão, consulte Inserindo macros predefinidas e personalizadas para um arquivo sem supervisão.

Para obter informações adicionais sobre macros personalizadas disponíveis, consulte Macros predefinidas.

Para importar o arquivo sem supervisão personalizado, conclua estas etapas.

1. Clique na guia **Arquivos sem supervisão**.
2. Clique no ícone **Importar** ().
3. Clique em **Importação Local**.

4. Selecione `ESXi` do sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o arquivo sem supervisão a ser importado (por exemplo, `ESXi_staticIP_customUnattend.cfg`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO

Etapa 3. Crie um perfil de imagem do SO personalizado que inclua o arquivo sem supervisão personalizado. Para obter mais informações, consulte Criando um perfil da imagem do SO personalizada.

1. Clique na guia **Imagens do SO**.
2. Selecione o perfil de imagem de SO a ser personalizado (por exemplo, `Virtualization`).
3. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Criar Perfil Personalizado.
4. Na guia **Geral**:
   a. Insira um nome para o perfil (por exemplo, `ESXi personalizado usando IP estático`).
   b. Use o valor padrão para o campo **Caminho de dados e arquivo personalizado**.
   c. Selecione **Apenas arquivos sem supervisão** para o tipo de personalização.
   d. Clique em **Avançar**.
5. Na guia **Não supervisionar arquivos**, selecione o arquivo sem supervisão (por exemplo, `ESXi_staticIP_customUnattend.cfg`) e clique em **Avançar**.
6. Na guia **Resumo**, revise as configurações.
7. Clique em **Personalizar** para criar o perfil de imagem do SO personalizado.

Etapa 4. Implante o perfil de imagem do SO personalizado no servidor de destino. Para obter mais informações, consulte Implantando uma imagem do sistema operacional.

1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar Sistema Operacional: Implantar Imagens do SO.
2. Para cada servidor de destino:
   a. Selecione o servidor.
   b. Clique em **Alterar Selecionado → Configurações de Rede** e especifique o nome do host, endereço IP, as configurações de DNS, MTU e VLAN para o servidor.

      Dica:

      - As configurações de VLAN estão disponíveis apenas quando o modo VLAN é definido em **Configurações Globais → Atribuição de IP → Usar VLANs**.
      - As configurações de rede que você especifica na caixa de diálogo Configurações de Rede são incluídas no arquivo sem supervisão em tempo de execução usando as macros **#predefined.hostPlatforms.networkSettings.**<*setting*>**#**.

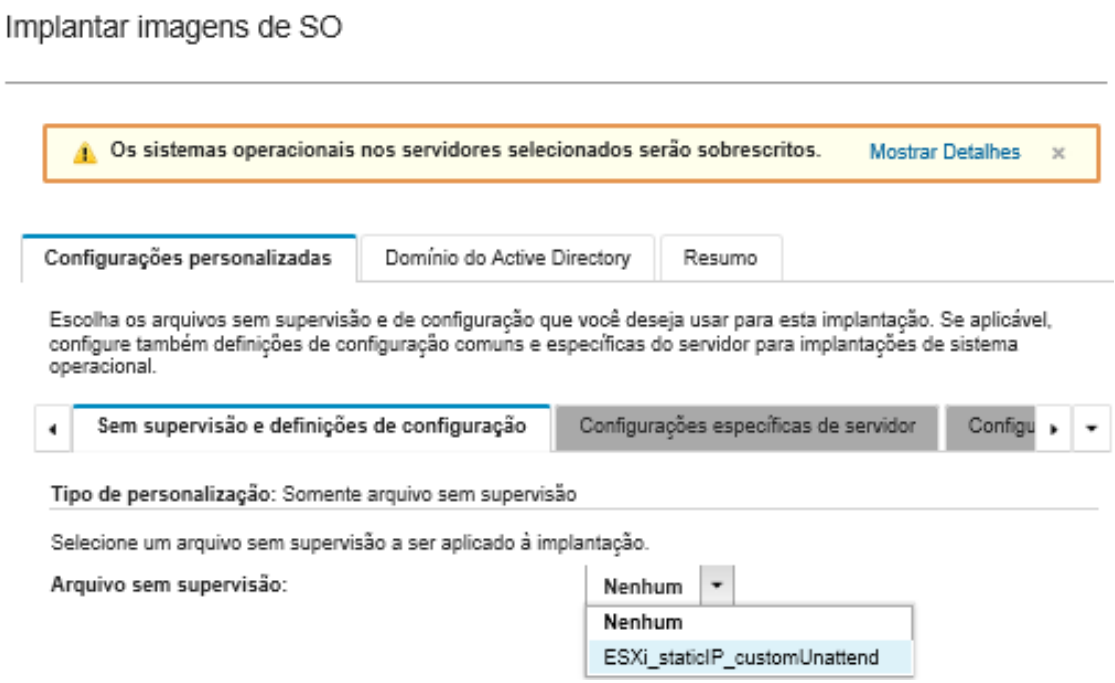
   c. Selecione o perfil da imagem do SO personalizada (por exemplo, <*base_OS*>|<*timestamp*>`_ESXi personalizado usando IP estático`) na lista suspensa na coluna **Imagem para implantação**.

      Nota: Certifique-se de que todos os servidores de destino usem o mesmo perfil personalizado.

   d. (Opcional) Clique no ícone **Chave de Licença** ( ) e especifique a chave de licença a ser usada para ativar o sistema operacional após a sua instalação.
   e. Verifique se o status da implantação para o servidor selecionado é **Pronto**.

Nota: Como **--firstdisk=local** é especificada no arquivo sem supervisão, você não precisa especificar o local de armazenamento preferencial na coluna **Armazenamento**. A configuração na interface do usuário é ignorada.

3. Selecione todos os servidores de destino e clique no ícone **Implantar imagem** ( ) para iniciar a implementação do sistema operacional.
4. Na guia **Configurações personalizadas**, clique na subguia **Sem supervisão e definições de configuração** e selecione o arquivo sem supervisão personalizado (por exemplo, `ESXi_staticIP_customUnattend.cfg`).



5. Na guia **Resumo**, revise as configurações.
6. Clique em **Implantar** para implantar o sistema operacional.

Implantando o VMware ESXi v6.7 com Lenovo Customization com um código do idioma configurável e as credenciais do segundo usuário

Neste cenário é instalado o VMware ESXi v6.7 com o sistema operacional Lenovo Customization com um idioma configurável habilitado para o código do idioma do teclado e as credenciais de um segundo usuário do ESXi. Este exemplo também usa as configurações de rede e armazenamento básicas que são definidas na interface do usuário. Um perfil personalizado de imagem do SO é usado para incluir um arquivo sem supervisão (com macros predefinidas e personalizadas) e um arquivo de definições de configuração para selecionar a senha. Esse perfil personalizado pode ser selecionado na página Implantar imagens de SO. Em seguida, a senha pode ser especificada na guia **Configurações personalizadas**. O valor especificado é substituído para a macro personalizada no arquivo sem supervisão personalizado, e o instalador do ESXi usa esses valores no arquivo sem supervisão para configurar o sistema operacional.

Antes de iniciar

Esse cenário usa os seguintes arquivos de amostra.

- ESXi_locale_customConfig.json. Esse arquivo de configuração personalizado solicita o código do idioma do teclado e as credenciais para o segundo usuário do ESXi.
- ESXi_locale_customUnattend.cfg. Esse arquivo assistido personalizado usa os valores em macros personalizadas e predefinidas que são definidas no arquivo de configuração.

Procedimento

Para implantar o VMware ESXi v6.7 usando perfil de imagem de SO personalizado, conclua as seguintes etapas.

Etapa 1. Baixe o VMware vSphere® Hypervisor (ESXi) com o sistema operacional Lenovo Customization do site Suporte VMware – Página da Web de downloads para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando imagens do sistema operacional.

1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
2. Clique na guia **Imagens do SO**.
3. Clique no ícone **Importar** ( ).
4. Clique em **Importação Local**.
5. Clique em **Procurar** para encontrar e selecionar a imagem do ESXi a ser importada (por exemplo, `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Clique em **Importar** para fazer o upload da imagem do SO no repositório de imagens do SO.
7. Aguarde a conclusão da importação.

Etapa 2. Crie um arquivo de configuração personalizado e importe o arquivo para o repositório de imagens do SO.

O arquivo de definições de configuração é um arquivo JSON que descreve os dados que precisam ser coletados dinamicamente durante o processo de implantação do SO. Para esse cenário, queremos escolher o código do idioma do teclado, o ID do usuário e a senha para o segundo usuário do ESXi a ser usado para cada implantação do SO. Para obter mais informações sobre criação de arquivo de configuração, consulte Macros personalizadas.

Para importar o arquivo de configuração, conclua estas etapas. Para obter mais informações, consulte Importando definições de configuração personalizadas.

1. Clique na guia **Arquivos de configuração**.
2. Clique no ícone **Importar** ( ).
3. Clique em **Importação Local**.
4. Selecione `ESXi` do sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o arquivo de definições de configuração para importar (por exemplo, `ESXi_locale_customConfig.json`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO

   Nota: Quando você importar o arquivo de definições de configuração personalizada, XClarity Administrator cria uma macro personalizada para cada configuração no arquivo. Você pode adicioná-las para o arquivo sem supervisão. Durante a implantação do SO, as macros são substituídas por valores reais.

Etapa 3. Modifique o arquivo sem supervisão ESXi (kickstart) para especificar o código do idioma do sistema operacional e do teclado e as credenciais do segundo usuário do ESXi e, então, importe o arquivo personalizado para o repositório de imagens do SO. Para obter mais informações, consulte Importando arquivos sem supervisão personalizados.

Adicione os comandos para definir a localização do teclado, por exemplo:

```
# Set the keyboard locale
keyboard ''
```

Adicione os comandos para criar um segundo usuário do ESXi. No exemplo a seguir, *<user_id>* e *<password>* serão substituídos pelas macros personalizadas na próxima etapa.

```
#Create second user
/usr/lib/vmware/auth/bin/adduser -D -h /tmp <user_id>
echo <password> | /usr/lib/vmware/auth/bin/passwd <user_id> --stdin
/bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root <user_id> false Admin true
```

Para importar o arquivo sem supervisão personalizado, conclua estas etapas.

1. Clique na guia **Arquivos sem supervisão**.
2. Clique no ícone **Importar** ().
3. Clique em **Importação Local**.
4. Selecione `ESXi` do sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o arquivo sem supervisão a ser importado (por exemplo, `ESXi_locale_customUnattend.cfg`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO

Etapa 4. Associar o arquivo sem supervisão personalizado com o arquivo de configurações personalizadas e inclua as predefinidas e personalizadas macros necessárias (configurações) do arquivo de definições de configuração no arquivo sem supervisão. Para obter mais informações, consulte Associando um arquivo sem supervisão a um arquivo de configuração e Inserindo macros predefinidas e personalizadas para um arquivo sem supervisão.

Dica:

- Como opção, você pode associar o arquivo sem supervisão com o arquivo de definições de configuração personalizado e adicionar macros ao importar o arquivo sem supervisão.
- O XClarity Administrator fornece algumas macros básicas, como inserção de driver OOB, relatório de status, scripts pós-instalação e software personalizado. No entanto, para aproveitar essas macros predefinidas, especifique as seguintes macros no arquivo sem supervisão personalizado. O arquivo de exemplo já contém as macros necessárias. Como a seção firstboot % está incluída, a ordem dessas macros predefinidas é importante. Para obter mais informações, consulte Importando arquivos sem supervisão personalizados.
  ```
  #predefined.unattendSettings.preinstallConfig#
  #predefined.unattendSettings.postinstallConfig#
  ```
- O XClarity Administrator também fornece macros que inserem todas as configurações de rede e local de armazenamento que são definidas na interface do usuário. Essas macros são úteis quando apenas as configurações básicas são necessárias para a implantação. O arquivo de exemplo já contém as macros necessárias.
  ```
  #predefined.unattendSettings.networkConfig#
  #predefined.unattendSettings.storageConfig#
  ```

Para obter mais informações sobre como adicionar macros para arquivos sem supervisão, consulte Inserindo macros predefinidas e personalizadas para um arquivo sem supervisão. Para obter informações adicionais sobre macros personalizadas disponíveis, consulte Macros predefinidas.

Para associar o arquivo sem supervisão personalizado ao arquivo de configuração personalizado, execute estas etapas.

1. Na guia **Não supervisionar arquivos**, selecione o arquivo com supervisão personalizado (por exemplo, `ESXi_locale_customUnattend.cfg`).
2. Clique no ícone **Associar um arquivo de configuração** () para exibir a caixa de diálogo Associar um arquivo sem supervisão.
3. Selecione o arquivo de configuração para associar ao arquivo sem supervisão (por exemplo, `ESXi_locale_customConfig`).

4. Selecione **Personalizada** da lista suspensa **Macros disponíveis**.
5. Adicione a macro personalizada para especificar o código do idioma do teclado colocando o cursor entre aspas simples após o teclado e, em seguida, clicando em **keyboard_locale**.

   Exemplo:

   ```
   # Set the keyboard locale
   keyboard '#keyboard_locale#'
   ```

6. Adicione a macro personalizada para especificar o ID do segundo usuário colocando o cursor em cada local onde você deseja adicionar o ID do usuário e, em seguida, clicando em **second_user_id**. No arquivo de exemplo, substitua cada ocorrência de <*user_id*> pela macro personalizada.

   Exemplo:

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo <password> | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```

7. Adicione a macro personalizada para especificar a senha do segundo usuário colocando o cursor no local onde você deseja adicionar a senha e, em seguida, clicando em **second_user_password**. No arquivo de exemplo, substitua <*password*> pela macro personalizada.

   Exemplo:

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo #second_user_password# | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```

8. Clique em **Associar** para associar os arquivos e salvar as alterações no arquivo sem supervisão.

Etapa 5. Crie um perfil de imagem do SO personalizado que inclui as definições de configuração personalizadas e arquivos não atendidos. Para obter mais informações, consulte Criando um perfil da imagem do SO personalizada.

1. Clique na guia **Imagens do SO**.
2. Selecione o perfil de imagem de SO a ser personalizado (por exemplo, `Virtualization`).
3. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Criar Perfil Personalizado.
4. Na guia **Geral**:
   a. Insira um nome para o perfil (por exemplo, `ESXi personalizado usando o código do idioma e as credenciais do segundo usuário`).
   b. Use o valor padrão para o campo **Caminho de dados e arquivo personalizado**.
   c. Selecione **Arquivos de definições de configuração e sem supervisão associados** para o tipo de personalização.
   d. Clique em **Avançar**.
5. Na guia **Não supervisionar arquivos**, selecione o arquivo sem supervisão (por exemplo, `ESXi_locale_customUnattend.cfg`) e clique em **Avançar**.

   O arquivo de definições de configuração associados é selecionado automaticamente.
6. Na guia **Resumo**, revise as configurações.
7. Clique em **Personalizar** para criar o perfil de imagem do SO personalizado.

Etapa 6. Implante o perfil de imagem do SO personalizado no servidor de destino. Para obter mais informações, consulte Implantando uma imagem do sistema operacional.

1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar Sistema Operacional: Implantar Imagens do SO.

2. Para cada servidor de destino:
   a. Selecione o servidor.
   b. Clique em **Alterar Selecionado → Configurações de Rede** e especifique o nome do host, endereço IP, as configurações de DNS, MTU e VLAN para o servidor.

      Dica:

      - As configurações de VLAN estão disponíveis apenas quando o modo VLAN é definido em **Configurações Globais → Atribuição de IP → Usar VLANs**.
      - As configurações de rede que você especifica na caixa de diálogo Configurações de Rede são incluídas no arquivo sem supervisão em tempo de execução usando a macro **#predefined.hostPlatforms.networkConfig#**.

   c. Selecione o perfil da imagem do SO personalizada (por exemplo, <*base_OS*>|<*timestamp*>_ESXi personalizado usando o código do idioma e as credenciais do segundo usuário) na lista suspensa na coluna **Imagem para implantação**.

      Nota: Certifique-se de que todos os servidores de destino usem o mesmo perfil personalizado.

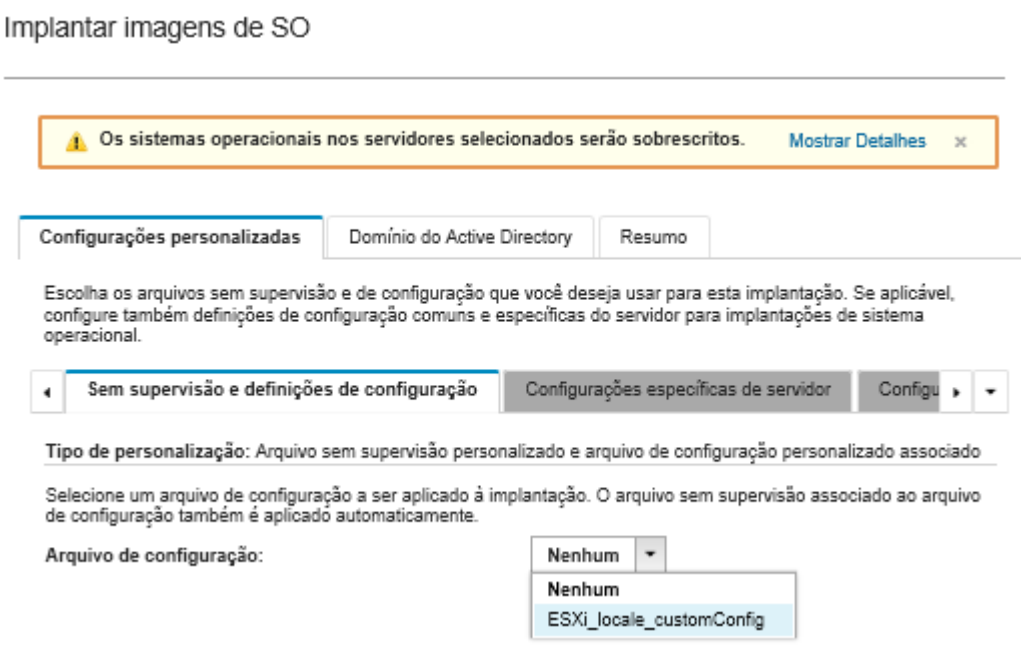
   d. (Opcional) Clique no ícone **Chave de Licença** () e especifique a chave de licença a ser usada para ativar o sistema operacional após a sua instalação.
   e. Selecione o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional na coluna **Armazenamento**.

      Notas:

      - Para garantir que as implantações do sistema operacional foram feitas com êxito, remova qualquer armazenamento do servidor gerenciado, exceto o armazenamento que será escolhido para a implantação do sistema operacional.
      - As configurações de armazenamento que você especifica na caixa de diálogo Configurações de armazenamento são incluídas no arquivo sem supervisão em tempo de execução usando a macro **#predefined.hostPlatforms.storageConfig#**.

   f. Verifique se o status da implantação para o servidor selecionado é **Pronto**.
3. Selecione todos os servidores de destino e clique no ícone **Implantar imagem** () para iniciar a implementação do sistema operacional.
4. Na guia **Configurações personalizadas**, clique na subguia **Sem supervisão e definições de configuração** e selecione o arquivo de definições de configuração personalizado (por exemplo, ESXi_locale_customConfig).

   Nota: O arquivo sem supervisão personalizado associado é selecionado automaticamente.



5. Na subguia **Configurações específicas do servidor**, selecione o código do idioma do teclado e as credenciais para o segundo usuário do ESXi.
6. Na guia **Resumo**, revise as configurações.
7. Clique em **Implantar** para implantar o sistema operacional.

Implantação do Windows 2016 com recursos personalizados

Este cenário instala o sistema operacional Windows 2016 e diversos recursos adicionais. Um perfil personalizado que inclui um arquivo sem supervisão personalizado é usado. O perfil personalizado pode ser selecionado na página Implantar imagens de SO.

Antes de iniciar

Esse cenário usa os seguintes arquivos de amostra.

- Windows_installFeatures_customUnattend.xml. Esse arquivo sem supervisão personalizado instala os recursos WindowsMediaPlayer e BitLocker, e usa macros predefinidas para valores dinâmicos.

Procedimento

Para implantar o Windows 2016 com recursos personalizados, conclua as etapas a seguir.

Etapa 1. Baixe o sistema operacional Windows 2016 japonês para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando imagens do sistema operacional.

1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
2. Clique na guia **Imagens do SO**.
3. Clique no ícone **Importar** ( ).
4. Clique em **Importação Local**.
5. Clique em **Procurar** para localizar e selecionar a imagem do SO que você deseja importar (por exemplo, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Clique em **Importar** para fazer o upload da imagem do SO no repositório de imagens do SO.

7. Aguarde a conclusão da importação. Isso pode levar alguns minutos.

Etapa 2. Baixe o arquivo do pacote do Windows 2016 para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando drivers de dispositivo.

O arquivo do pacote contém os drivers de dispositivo mais recentes e os arquivos de inicialização WinPE que você pode adicionar aos perfis de imagens do SO personalizados. Esse cenário usa um arquivo de inicialização personalizado, para que o arquivo de inicialização do pacote não seja usado.

1. Clique na guia **Arquivos de Driver**.
2. Clique em **Downloads → Arquivos do Pacote Windows** para acessar a página da Web do Suporte Lenovo e baixe o arquivo do pacote do Windows 2016 para o sistema local.
3. Clique no ícone **Importar** ().
4. Clique em **Importação Local**.
5. Clique em **Procurar** para localizar e selecionar a imagem do SO que você deseja importar (por exemplo, `bundle_win2016_20180126130051.zip`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.
7. Aguarde a conclusão da importação. Isso pode levar alguns minutos.

Etapa 3. Modifique o arquivo sem supervisão do Windows para instalar os recursos adicionais (como WindowsMediaPlayer e BitLocker) e importe o arquivo personalizado para o repositório de imagens do SO.

Na seção "manutenção" do arquivo sem supervisão do Windows, adicione os recursos do Windows a serem instalados, por exemplo,

```
<servicing>
   <package action="configure">
      <assemblyIdentity name="Microsoft-Windows-Foundation-Package" version="10.0.14393.0"
                        processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
                        language=""></assemblyIdentity>
      <selection name="Microsoft-Hyper-V" state="true"></selection>
      <selection name="MultipathIo" state="true"></selection>
      <selection name="FailoverCluster-PowerShell" state="true"></selection>
      <selection name="FailoverCluster-FullServer" state="true"></selection>
      <selection name="FailoverCluster-CmdInterface" state="true"></selection>
      <selection name="FailoverCluster-AutomationServer" state="true"></selection>
      <selection name="FailoverCluster-AdminPak" state="true"></selection>
      <selection name="MicrosoftWindowsPowerShellRoot" state="true"></selection>
      <selection name="MicrosoftWindowsPowerShell" state="true"></selection>
      <selection name="ServerManager-Core-RSAT" state="true"></selection>
      <selection name="WindowsMediaPlayer" state="true"></selection>
      <selection name="BitLocker" state="true"></selection>
   </package>
</servicing>
```

Notas:

- Essas marcas estão no arquivo sem supervisão de amostra.
- Ao usar um arquivo sem supervisão personalizado, o XClarity Administrator não fornece vários dos recursos normais disponíveis quando você usa um arquivo sem supervisão predefinido. Por exemplo, os destinos `<DiskConfiguration>`, `<ImageInstall>`, `<ProductKey>` e `<UserAccounts>` para administrador, `<Interfaces>` para rede e a lista `<package>` para recursos de instalação devem ser especificados no arquivo sem supervisão personalizado que está sendo carregado.

Para importar o arquivo sem supervisão personalizado, conclua estas etapas. Para obter mais informações, consulte Importando arquivos sem supervisão personalizados.

1. Clique na guia **Arquivos sem supervisão**.
2. Clique no ícone **Importar** ().
3. Clique em **Importação Local**.
4. Selecione `Windows` para o sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o arquivo sem supervisão personalizado a ser importado (por exemplo, `Windows_installFeatures_customUnattend.xml`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.

O XClarity Administrator fornece algumas macros básicas, como inserção de driver OOB, relatório de status, scripts pós-instalação e software personalizado. No entanto, para aproveitar essas macros predefinidas, especifique as seguintes macros no arquivo sem supervisão personalizado.

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

O arquivo de exemplo já contém o código para instalar os recursos adicionais, as macros necessárias e outras macros que são necessárias para entrada dinâmica. Para obter mais informações sobre como adicionar macros para arquivos sem supervisão, consulte Inserindo macros predefinidas e personalizadas para um arquivo sem supervisão.

Para obter informações adicionais sobre macros personalizadas disponíveis, consulte Macros predefinidas.

Etapa 4. Crie um perfil de imagem do SO personalizado que inclui o arquivo sem supervisão. Para obter mais informações, consulte Criando um perfil da imagem do SO personalizada.

1. Clique na guia **Imagens do SO**.
2. Selecione o perfil a ser personalizado (por exemplo, `win2016-x86_64-install-Datacenter_Virtualization`).
3. Clique no ícone **Criar** () para exibir a caixa de diálogo Criar Perfil Personalizado.
4. Na guia **Geral**:
   a. Insira um nome para o perfil (por exemplo, `Windows personalizado com recursos`).
   b. Use o valor padrão para o campo **Caminho de dados e arquivo personalizado**.
   c. Selecione **Apenas arquivos sem supervisão** para o tipo de personalização.
   d. Clique em **Avançar**.
5. Na guia **Opções de Driver**, clique em **Próximo**. Os drivers de dispositivo de entrada são incluídos por padrão.
6. Na guia **Opções de inicialização**, clique em **Avançar**. O arquivo de inicialização do WinPE predefinido é marcado por padrão.
7. Na guia **Software**, clique em **Próximo**.
8. Na guia **Não supervisionar arquivos**, selecione o arquivo sem supervisão personalizado (por exemplo, `Windows_installFeatures_customUnattend.xml`) e clique em **Avançar**.
9. Na guia **Scripts de instalação**, clique em **Próximo**.
10. Na guia **Resumo**, revise as configurações.
11. Clique em **Personalizar** para criar o perfil de imagem do SO personalizado.

Etapa 5. Implante o perfil de imagem do SO personalizado nos servidores de destino. Para obter mais informações, consulte Implantando uma imagem do sistema operacional.

1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar Sistema Operacional: Implantar Imagens do SO.
2. Para cada servidor de destino:
   a. Selecione o servidor.
   b. Clique em **Alterar Selecionado → Configurações de Rede** e especifique o nome do host, endereço IP, máscara de sub-rede, gateway, DNS, MTU e VLAN para o servidor.

      Dica: As configurações de VLAN estão disponíveis apenas quando o modo VLAN é definido em **Configurações Globais → Atribuição de IP → Usar VLANs**.
   c. Selecione o perfil da imagem do SO personalizada (por exemplo, <*base_OS*>|<*timestamp*>_`Windows personalizado com recursos`) na lista suspensa na coluna **Imagem para implantação**.

      Nota: Certifique-se de que todos os servidores de destino usem o mesmo perfil personalizado.
   d. (Opcional) Clique no ícone **Chave de Licença** () e especifique a chave de licença a ser usada para ativar o sistema operacional após a sua instalação.
   e. Selecione o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional na coluna **Armazenamento**.

      Nota: Para garantir que as implantações do sistema operacional foram feitas com êxito, remova qualquer armazenamento do servidor gerenciado, exceto o armazenamento que será escolhido para a implantação do sistema operacional.
   f. Verifique se o status da implantação para o servidor selecionado é **Pronto**.
3. Selecione todos os servidores de destino e clique no ícone **Implantar imagem** () para iniciar a implementação do sistema operacional.
4. Na guia **Configurações personalizadas**, clique na subguia **Sem supervisão e definições de configuração** e selecione o arquivo sem supervisão personalizado (por exemplo, `Windows_installFeatures_customUnattend.xml`).
5. (Opcional) Na guia **Domínio do Active Directory**, especifique as informações para incluir um domínio do Active Directory como parte de uma implantação de imagem do Windows (consulte Integração com Windows Active Directory).
6. Na guia **Resumo**, revise as configurações.
7. Clique em **Implantar** para implantar o sistema operacional.

Implantação do Windows 2016 com software personalizado

Este cenário instala o sistema operacional Windows 2016 juntamente com o software personalizado (Java e Eclipse IDE). Um perfil personalizado que inclui o software personalizado e scripts pós-instalação é usado para instalar e configurar o software personalizado. Os pacotes de software personalizados são copiados para o host durante a implantação e disponibilizados para o script pós-instalação personalizado a ser usado.

Antes de iniciar

Esse cenário usa os seguintes arquivos de amostra.

- jre-8u151-windows-x64-with-configfile.zip. Este é o arquivo de instalação para Java para o Eclipse.
- eclipse-java-oxygen-1a-win32-x86_64.zip Este é o arquivo de instalação para o Eclipse IDE.
- Windows_installSoftware_customScript.ps1 Este script pós-instalação cria um usuário para iniciar o Eclipse e instala o Eclipse IDE e o Java.

Notas:

- Os scripts de instalação do Windows podem estar em um dos seguintes formatos: Arquivo de comando (. cmd), PowerShell (. ps1)
- Arquivos de software e scripts de instalação são instalados do caminho de dados e arquivos personalizado que você especificar durante a implantação. O caminho de arquivos e dados personalizado padrão é `C:\lxca`.

Procedimento

Para implantar o Windows 2016 com software personalizado, conclua as etapas a seguir.

Etapa 1. Baixe o sistema operacional Windows 2016 japonês para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando imagens do sistema operacional.

1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
2. Clique na guia **Imagens do SO**.
3. Clique no ícone **Importar** ( ).
4. Clique em **Importação Local**.
5. Clique em **Procurar** para localizar e selecionar a imagem do SO que você deseja importar (por exemplo, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Clique em **Importar** para fazer o upload da imagem do SO no repositório de imagens do SO.
7. Aguarde a conclusão da importação. Isso pode levar alguns minutos.

Etapa 2. Baixe o arquivo do pacote do Windows 2016 para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando drivers de dispositivo.

O arquivo do pacote contém os drivers de dispositivo mais recentes e os arquivos de inicialização WinPE que você pode adicionar aos perfis de imagens do SO personalizados. Esse cenário usa um arquivo de inicialização personalizado, para que o arquivo de inicialização do pacote não seja usado.

1. Clique na guia **Arquivos de Driver**.
2. Clique em **Downloads → Arquivos do Pacote Windows** para acessar a página da Web do Suporte Lenovo e baixe o arquivo do pacote do Windows 2016 para o sistema local.
3. Clique no ícone **Importar** ( ).
4. Clique em **Importação Local**.
5. Clique em **Procurar** para localizar e selecionar a imagem do SO que você deseja importar (por exemplo, `bundle_win2016_20180126130051.zip`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.
7. Aguarde a conclusão da importação. Isso pode levar alguns minutos.

Etapa 3. Baixe o software personalizado no sistema local e importar os arquivos para o repositório de imagens do SO. Para obter mais informações, consulte Importando software personalizado.

1. Clique na guia **Software**.
2. Clique no ícone **Importar** ( ).
3. Clique em **Importação Local**.
4. Selecione `Windows` para o sistema operacional.

5. Clique em **Procurar** para localizar e selecionar o arquivo de configurações a ser importado (por exemplo, `jre-8u151-windows-x64-with-configfile.zip`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.
7. Clique no ícone **Importar** () novamente.
8. Clique em **Importação Local**.
9. Selecione `Windows` para o sistema operacional.
10. Clique em **Procurar** para localizar e selecionar o arquivo de configurações a ser importado (por exemplo, `eclipse-java-oxygen-1a-win32-x86_64.zip`).
11. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.

Etapa 4. Crie um script pós-instalação personalizado e importe o arquivo para o repositório de imagens do SO.

Adicione comandos para instalar o software, por exemplo:

```
Write-Output "Install Java...."
Invoke-Command -ScriptBlock
        {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
        [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg]
        /s}

Write-Output "Install Eclipse..."
$eclipseDir="C:\Users\Administrator\Desktop\eclipse"
New-Item -ItemType directory -Path $eclipseDir
Expand-Archive -LiteralPath
        "#predefined.otherSettings.deployDataAndSoftwareLocation#\eclipse-java-oxygen-1a-win32-x86_64.zip"
        -DestinationPath $eclipseDir
```

Observe que esse comando usa a macro predefinida para o caminho para os dados extraídos e arquivos de software (**predefined.otherSettings.deployDataAndSoftwareLocation**).

É possível também incluir os comandos para enviar mensagens personalizadas para as tarefas de login no XClarity Administrator, conforme mostrado no arquivo de exemplo. Para obter mais informações, consulte Adicionando relatório de status personalizado aos scripts de instalação.

Para importar o script de instalação personalizado, conclua estas etapas. Para obter mais informações, consulte Importando scripts de instalação personalizados.

1. Clique na guia **Scripts de instalação**.
2. Clique no ícone **Importar** ().
3. Clique em **Importação Local**.
4. Selecione `Windows` para o sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o arquivo sem supervisão a ser importado (por exemplo, `Windows_installSoftware_customScript.ps1`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.

Etapa 5. Crie um perfil de imagem do SO personalizado que inclui o arquivo sem supervisão personalizado. Para obter mais informações, consulte Criando um perfil da imagem do SO personalizada.

1. Clique na guia **Imagens do SO**.
2. Selecione o perfil de imagem de SO a ser personalizado (por exemplo, `Datacenter virtualization`).
3. Clique no ícone **Criar** () para exibir a caixa de diálogo Criar Perfil Personalizado.
4. Na guia **Geral**:

a. Insira um nome para o perfil (por exemplo, `Windows personalizado com software`).
b. Use o valor padrão para o campo **Caminho de dados e arquivo personalizado**.
c. Selecione **Nenhum** para o tipo de personalização.
d. Clique em **Avançar**.

5. Na guia **Opções de Driver**, clique em **Próximo**. Os drivers de dispositivo de entrada são incluídos por padrão.
6. Na guia **Opções de inicialização**, clique em **Avançar**. O arquivo de inicialização do WinPE predefinido é marcado por padrão.
7. Na guia **Software**, selecione os arquivos de instalação de software (por exemplo, `jre-8u151-windows-x64-with-configfile.zip` e `eclipse-java-oxygen-1a-win32-x86_64.zip`) e clique em **Avançar**.
8. Na guia **Scripts de instalação**, selecione os scripts de instalação (por exemplo, `Windows_installSoftware_customScript.ps1`) e clique em **Avançar**.
9. Na guia **Resumo**, revise as configurações.
10. Clique em **Personalizar** para criar o perfil de imagem do SO personalizado.

Etapa 6. Implante o perfil de imagem do SO personalizado nos servidores de destino. Para obter mais informações, consulte Implantando uma imagem do sistema operacional.

1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar Sistema Operacional: Implantar Imagens do SO.
2. Para cada servidor de destino:
   a. Selecione o servidor.
   b. Clique em **Alterar Selecionado → Configurações de Rede** e especifique o nome do host, endereço IP, as configurações de DNS, MTU e VLAN para o servidor.

      Dica: As configurações de VLAN estão disponíveis apenas quando o modo VLAN é definido em **Configurações Globais → Atribuição de IP → Usar VLANs**.
   c. Selecione o perfil da imagem do SO personalizada (por exemplo, <*base_OS*>|<*timestamp*>`_Windows personalizado com software`) na lista suspensa na coluna **Imagem para implantação**

      Nota: Certifique-se de que todos os servidores de destino usem o mesmo perfil personalizado.
   d. (Opcional) Clique no ícone **Chave de Licença** () e especifique a chave de licença a ser usada para ativar o sistema operacional após a sua instalação.
   e. Selecione o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional na coluna **Armazenamento**.

      Nota: Para garantir que as implantações do sistema operacional foram feitas com êxito, remova qualquer armazenamento do servidor gerenciado, exceto o armazenamento que será escolhido para a implantação do sistema operacional.
   f. Verifique se o status da implantação para o servidor selecionado é **Pronto**.
3. Selecione todos os servidores de destino e clique no ícone **Implantar imagem** () para iniciar a implementação do sistema operacional.
4. Na guia **Resumo**, revise as configurações.
5. Clique em **Implantar** para implantar o sistema operacional.

Implantação do Windows 2016 para japonês

Este cenário instala o sistema operacional Windows 2016 em diversos servidores com japonês habilitado para o teclado e a localização do sistema operacional. Um perfil personalizado que inclui um arquivo de inicialização WinPE personalizado e arquivo sem supervisão. O perfil personalizado pode ser selecionado na página Implantar imagens de SO.

Antes de iniciar

Esse cenário usa os seguintes arquivos de amostra.

- `WinPE_64_ja.zip`. Esse arquivo de inicialização (WinPE) personalizado do Windows instala a localização japonesa.
- Windows_locale_customUnattend.xml. Esse arquivo sem supervisão personalizado usa o arquivo WinPE para instalar japonês.

Notas: O arquivo sem supervisão personalizado de exemplo assume o seguinte:

- O servidor tem apenas um disco visível (disco 0) e ainda não tem uma partição do sistema nele.
- O modo de IPv4 estático é usado e define um IP estático (que é usado como uma macro predefinida no arquivo sem supervisão personalizado).

Procedimento

Para implantar o Windows 2016 japonês em servidores de destino usando um perfil de imagem de SO personalizado, conclua as seguintes etapas.

Etapa 1. Baixe o sistema operacional Windows 2016 japonês para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando imagens do sistema operacional.

1. Na barra de menus XClarity Administrator, clique em **Fornecimento → Gerenciar Imagens de SO** para exibir a página Implantar Sistema Operacional: Gerenciar Imagens de SO.
2. Clique na guia **Imagens do SO**.
3. Clique no ícone **Importar** ( ).
4. Clique em **Importação Local**.
5. Clique em **Procurar** para localizar e selecionar a imagem do SO que você deseja importar (por exemplo, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Clique em **Importar** para fazer o upload da imagem do SO no repositório de imagens do SO.
7. Aguarde a conclusão da importação. Isso pode levar alguns minutos.

Etapa 2. Baixe o arquivo do pacote do Windows 2016 para o sistema local e importe a imagem para o repositório de imagens do SO. Para obter mais informações, consulte Importando drivers de dispositivo.

O arquivo do pacote contém os drivers de dispositivo mais recentes e os arquivos de inicialização WinPE que você pode adicionar aos perfis de imagens do SO personalizados. Esse cenário usa um arquivo de inicialização personalizado, para que o arquivo de inicialização do pacote não seja usado.

1. Clique na guia **Arquivos de Driver**.
2. Clique em **Downloads → Arquivos do Pacote Windows** para acessar a página da Web do Suporte Lenovo e baixe o arquivo do pacote do Windows 2016 para o sistema local.
3. Clique no ícone **Importar** ( ).
4. Clique em **Importação Local**.

5. Clique em **Procurar** para localizar e selecionar a imagem do SO que você deseja importar (por exemplo, `bundle_win2016_20180126130051.zip`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.
7. Aguarde a conclusão da importação. Isso pode levar alguns minutos.

Etapa 3. Crie um arquivo de inicialização do WinPE personalizado para japonês durante a instalação do WinPE e importe o arquivo para o repositório de imagens do SO.

O XClarity Administrator usa um arquivo de inicialização predefinido do Windows PreInstallation (WinPE) para instalar o sistema operacional Windows. A localidade usada com esse arquivo de inicialização predefinido é inglês (en-US). Se você desejar alterar a localização que é usada durante a instalação do Windows, crie um arquivo de inicialização do WinPE personalizado com a localização desejada e atribua esse arquivo de inicialização personalizado ao seu perfil personalizado.

Para obter informações sobre como inserir localização no WinPE, consulte Windows WinPE: página da Web Adicionar pacotes.

Importante: Especificar um idioma diferente do inglês no arquivo de inicialização do WinPE não altera o local do SO final que está sendo implantado. Isso só altera a localidade que é mostrada durante a configuração e a instalação do Windows.

Para criar um arquivo de inicialização do WinPE personalizado que inclui japonês, conclua estas etapas. Para obter mais informações, consulte Criando um arquivo de inicialização (WinPE).

1. Usando um ID de usuário com autoridade de administrador, execute o comando do ADK "Deployment and Imaging Tools Environment." Uma sessão de comando é exibida.
2. Na sessão do comando, altere para o diretório onde os arquivos `genimage.cmd` e `starnet.cmd` foram baixados (por exemplo, `C:\customwim`).
3. Garanta que nenhuma imagem montada anteriormente esteja no host executando o seguinte comando:
   ```
   dism /get-mountedwiminfo
   ```
   Se houver imagens montadas, rejeite-as executando o seguinte comando:
   ```
   dism /unmount-wim /MountDir:C:\<mount_path> /Discard
   ```
4. Se estiver adicionando drivers de dispositivo predefinidos a um perfil personalizado do Windows copie os arquivos dos drivers de dispositivo brutos no formato .inf no sistema host no diretório `C:\drivers`.
5. Execute o seguinte comando ao gerar o arquivo de inicialização, no formato .wim, e espere alguns minutos pela conclusão.
   ```
   genimage.cmd amd64 <ADK_Version>
   ```
   Em que <*ADK_Version*> é um dos valores a seguir.
   - **8.1**. Para Windows 2012 R2
   - **10**. Para Windows 2016

   Esse comando cria o arquivo de inicialização com o nome `C:\WinPE_64\media\Boot\WinPE_64.wim`.
6. Monte o arquivo de inicialização executando o seguinte comando:
   ```
   DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount
   ```
7. Se você estiver incluindo drivers de dispositivo predefinidos diretamente no arquivo de inicialização, conclua as seguintes etapas.
   a. Crie a estrutura de diretório a seguir, em que <*os_release*> é `2012R2` ou `2016`
      ```
      drivers\<os_release>\
      ```

b. Copie os drivers de dispositivo, no formato .inf, em um diretório dentro desse caminho, por exemplo:
`drivers\<os_release>\<driver1>\<driver1_files>`

c. Copie o diretório `drivers` no diretório montado, por exemplo:
`C:\WinPE_64\mount\drivers`

8. **Opcional:** faça personalizações adicionais no arquivo de inicialização, como adicionar pastas, arquivos, scripts de inicialização, pacotes de idioma e aplicativos. Para obter mais informações sobre personalização de arquivos de inicialização, consulte Site WinPE: Montar e personalizar.
9. Adicione os pacotes de japonês, por exemplo.
10. Exiba pacotes instalados para assegurar que os pacotes específicos em japonês estejam instalados.

```
Dism /Add-Package /Image:"C:\WinPE_64\mount"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment
and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\ja-jp\lp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-DismCmdlets_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-NetFx_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-PowerShell_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-RNDIS_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-Scripting_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-StorageWMI_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WDS-Tools_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WMI_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\WinPE-FontSupport-JA-JP.cab"
```

11. Revise as Configurações Padrão na imagem.

```
Dism /Get-Packages /Image:"C:\WinPE_64\mount"
```

12. Desmonte a imagem executando o seguinte comando.

```
DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit
```

13. Compacte o conteúdo do diretório `C:\WinPE_64\media` em um arquivo zip chamado `WinPE_64_ja.zip`.
14. Importe o arquivo .zip no XClarity Administrator (consulte Importar arquivos de inicialização).
    a. Clique na guia **Arquivos de Inicialização**.
    b. Clique no ícone **Importar** ().
    c. Clique em **Importação Local**.
    d. Selecione `Windows` para o sistema operacional.
    e. Clique em **Procurar** para localizar e selecionar o arquivo de inicialização personalizado (por exemplo, `WinPE_64_ja.zip`).
    f. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.

Etapa 4. Modifique o arquivo sem supervisão do Windows para especificar que japonês está incluído na imagem do SO e importe o arquivo personalizado para o repositório de imagens do SO.

Na senha "windowsPE" de instalação do Windows, adicione japonês como o idioma do sistema operacional e a localização, por exemplo:

```
<settings pass="windowsPE">
   <component name="Microsoft-Windows-International-Core-WinPE" processorArchitecture="amd64"
              publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
              xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <SetupUILanguage>
         <UILanguage>ja-JP</UILanguage>
      </SetupUILanguage>
      <SystemLocale>ja-JP</SystemLocale>
      <UILanguage>ja-JP</UILanguage>
      <UserLocale>ja-JP</UserLocale>
      <InputLocale>0411:00000411</InputLocale>
   </component>
</settings>
```

Nota: Ao usar um arquivo sem supervisão personalizado, o XClarity Administrator não fornece vários dos recursos normais disponíveis quando você usa um arquivo sem supervisão predefinido. Por exemplo, os destinos `<DiskConfiguration>`, `<ImageInstall>`, `<ProductKey>` e `<UserAccounts>` para administrador, `<Interfaces>` para rede e a lista `<package>` para recursos de instalação devem ser especificados no arquivo sem supervisão personalizado que está sendo carregado.

O XClarity Administrator fornece algumas macros básicas, como inserção de driver OOB, relatório de status, scripts pós-instalação e software personalizado. No entanto, para aproveitar essas macros predefinidas, especifique as seguintes macros no arquivo sem supervisão personalizado.

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

O arquivo de exemplo já contém as macros necessárias. Para obter mais informações sobre como adicionar macros para arquivos sem supervisão, consulte Inserindo macros predefinidas e personalizadas para um arquivo sem supervisão. Para obter informações adicionais sobre macros personalizadas disponíveis, consulte Macros predefinidas.

Para importar o arquivo sem supervisão personalizado, conclua estas etapas. Para obter mais informações, consulte Importando arquivos sem supervisão personalizados.

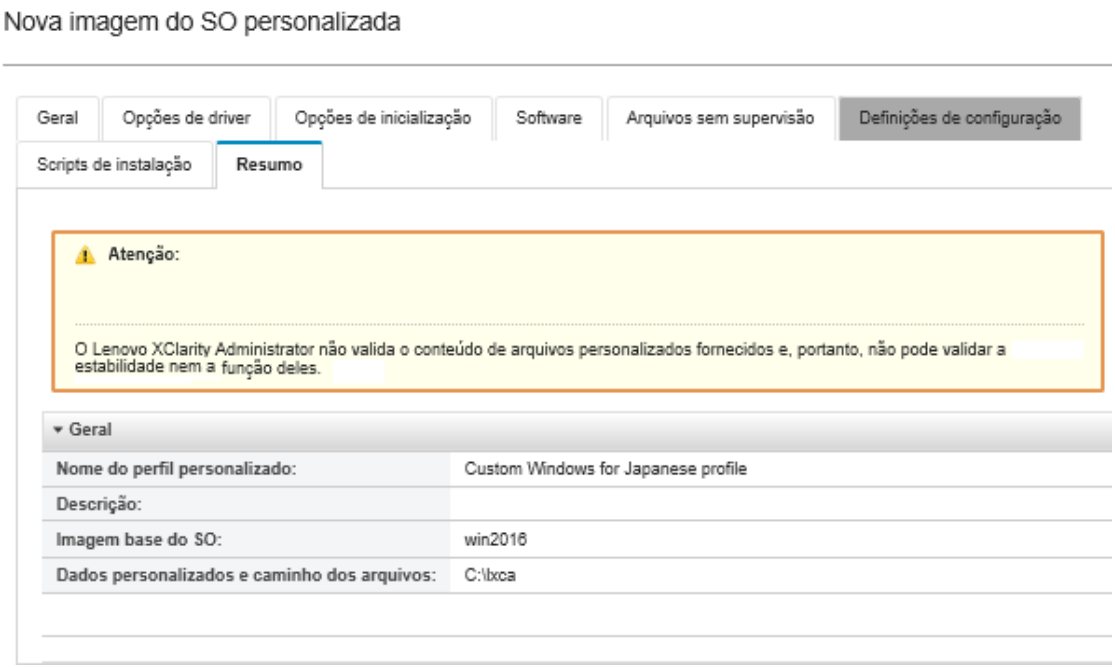
1. Clique na guia **Arquivos sem supervisão**.
2. Clique no ícone **Importar** ( ).
3. Clique em **Importação Local**.
4. Selecione `Windows` para o sistema operacional.
5. Clique em **Procurar** para localizar e selecionar o arquivo sem supervisão personalizado a ser importado (por exemplo, `Windows_locale_customUnattend.xml`).
6. Clique em **Importar** para fazer o upload do arquivo no repositório de imagens do SO.

Etapa 5. Crie um perfil de imagem do SO personalizado que inclui o arquivo de inicialização (WinPE) personalizado e o arquivo sem supervisão. Para obter mais informações, consulte Criando um perfil da imagem do SO personalizada.

1. Clique na guia **Imagens do SO**.
2. Selecione o perfil a ser personalizado (por exemplo, `win2016-x86_64-install-Datacenter_Virtualization`).
3. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Criar Perfil Personalizado.
4. Na guia **Geral**:
   a. Insira um nome para o perfil (por exemplo, `Perfil do Windows personalizado para japonês`).
   b. Use o valor padrão para o campo **Caminho de dados e arquivo personalizado**.
   c. Selecione **Apenas arquivos sem supervisão** para o tipo de personalização.

d. Clique em **Avançar**.

5. Na guia **Opções de Driver**, clique em **Próximo**. Os drivers de dispositivo de entrada são incluídos por padrão.
6. Na guia **Arquivos de Inicialização**, selecione o arquivo de inicialização personalizado (por exemplo, `WinPE_64_ja`) e clique em **Avançar**.
7. Na guia **Software**, clique em **Próximo**.
8. Na guia **Não supervisionar arquivos**, selecione o arquivo sem supervisão personalizado (por exemplo, `Windows_locale_customUnattend.xml`) e clique em **Avançar**.
9. Na guia **Scripts de instalação**, clique em **Próximo**.
10. Na guia **Resumo**, revise as configurações.



11. Clique em **Personalizar** para criar o perfil de imagem do SO personalizado.

Etapa 6. Implante o perfil de imagem do SO personalizado nos servidores de destino. Para obter mais informações, consulte Implantando uma imagem do sistema operacional.

1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO** para exibir a página Implantar Sistema Operacional: Implantar Imagens do SO.
2. Para cada servidor de destino:
   a. Selecione o servidor.
   b. Clique em **Alterar Selecionado → Configurações de Rede** e especifique o nome do host, endereço IP, máscara de sub-rede, gateway, DNS, MTU e VLAN para o servidor.

      Dica: As configurações de VLAN estão disponíveis apenas quando o modo VLAN é definido em **Configurações Globais → Atribuição de IP → Usar VLANs**.
   c. Selecione o perfil da imagem do SO personalizada (por exemplo, <*base_OS*>|<*timestamp*>_`Perfil do Windows personalizado para japonês`) na lista suspensa na coluna **Imagem para implantação**.

      Nota: Certifique-se de que todos os servidores de destino usem o mesmo perfil personalizado.

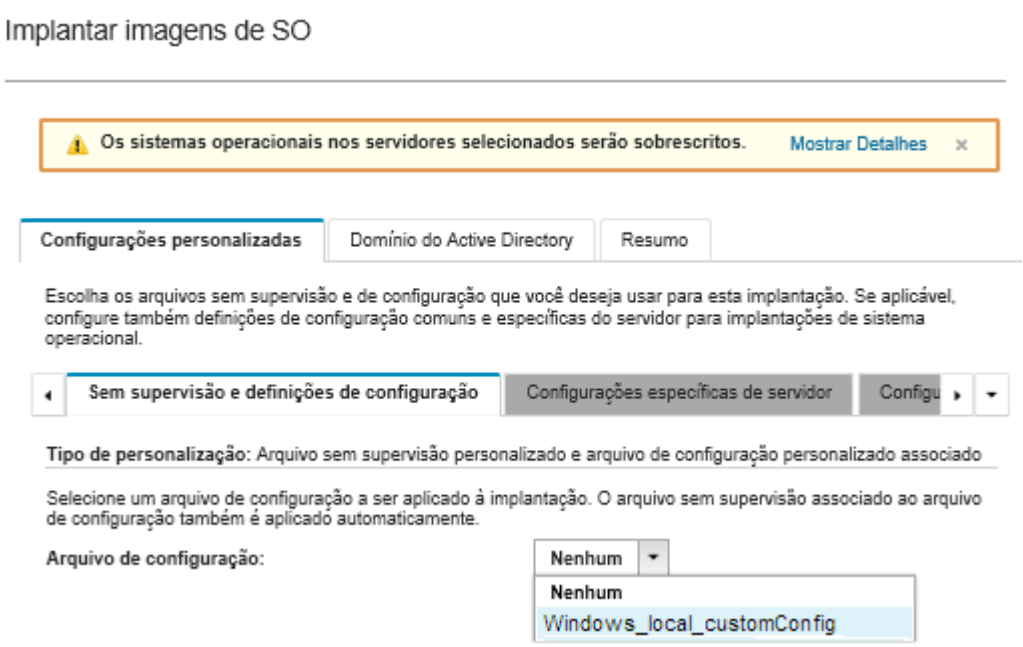
d. (Opcional) Clique no ícone **Chave de Licença** ( ) e especifique a chave de licença a ser usada para ativar o sistema operacional após a sua instalação.

e. Selecione o local de armazenamento preferencial onde você quer implantar a imagem do sistema operacional na coluna **Armazenamento**.

Nota: Para garantir que as implantações do sistema operacional foram feitas com êxito, remova qualquer armazenamento do servidor gerenciado, exceto o armazenamento que será escolhido para a implantação do sistema operacional.

f. Verifique se o status da implantação para o servidor selecionado é **Pronto**.

3. Selecione todos os servidores de destino e clique no ícone **Implantar imagem** ( ) para iniciar a implementação do sistema operacional.
4. Na guia **Configurações personalizadas**, clique na subguia **Sem supervisão e definições de configuração** e selecione o arquivo sem supervisão personalizado (por exemplo, `Windows_locale_customUnattend.xml`).



5. (Opcional) Na guia **Domínio do Active Directory**, especifique as informações para incluir um domínio do Active Directory como parte de uma implantação de imagem do Windows (consulte Integração com Windows Active Directory).
6. Na guia **Resumo**, revise as configurações.
7. Clique em **Implantar** para implantar o sistema operacional.

A caixa de diálogo de instalação do Windows é exibida em japonês.

Após a instalação ser concluída, a página de login do Windows também é exibida em japonês.

Capítulo 16. Cenários completos para configurar novos dispositivos

Use estes cenários completos para descrever como ajudá-lo a usar o Lenovo XClarity Administrator para configurar novos dispositivos de maneira facilmente repetível e consistente.

Implantando o ESXi em um disco rígido local

Use estes procedimentos para implantar o VMware ESXi 5.5 em um disco rígido instalado localmente em um Nó de Cálculo do Flex System x240. Isto ilustra como aprender um padrão de servidor a partir de um servidor existente, como modificar o padrão de categoria da configuração de UEFI estendida para esse padrão de servidor e também como instalar o VMware ESXi.

O VMware ESXi 5.5 requer espaço E/S de memória mapeada (MMIO) para ser configurado com os 4 GB iniciais do sistema. Dependendo da configuração, determinados sistemas tentam usar uma memória maior que 4 GB, o que pode causar uma falha. Para resolver o problema, você poderá aumentar o valor da opção MM Config para 3 GB usando o Setup utility para cada servidor que o VMware ESXi 5.5 irá ser instalado.

Uma alternativa é implantar um padrão de servidor que contém um padrão de categoria UEFI estendida predefinido que está relacionado à virtualização, o qual configura a opção de MM Config e desativa alocação de recurso da PCI de 64 bits.

Implantando um padrão de virtualização predefinido

Um padrão de categoria define as configurações de firmware específicas que podem ser reutilizadas por vários padrões de servidor. Para implantar um padrão predefinido de virtualização, é preciso criar um padrão de servidor e depois aplicar um padrão de UEFI estendida predefinido para esse padrão de servidor. O padrão de servidor pode então ser aplicado a vários servidores do mesmo tipo, como Nó de Cálculo do Flex System x240 ou Flex System x880 X6 Nó de Cálculo.

Sobre esta tarefa

Ao criar um padrão de servidor, é possível escolher se deseja concluir a configuração sozinho ou se deseja aprender os atributos padrões de um servidor existente que já foi configurado. Quando você aprende sobre um novo padrão a partir de um servidor existente, a maioria dos atributos padrão já está definida.

Para obter mais informações sobre os padrões de servidor e os padrões de categoria, consulte Trabalhando com padrões de servidor.

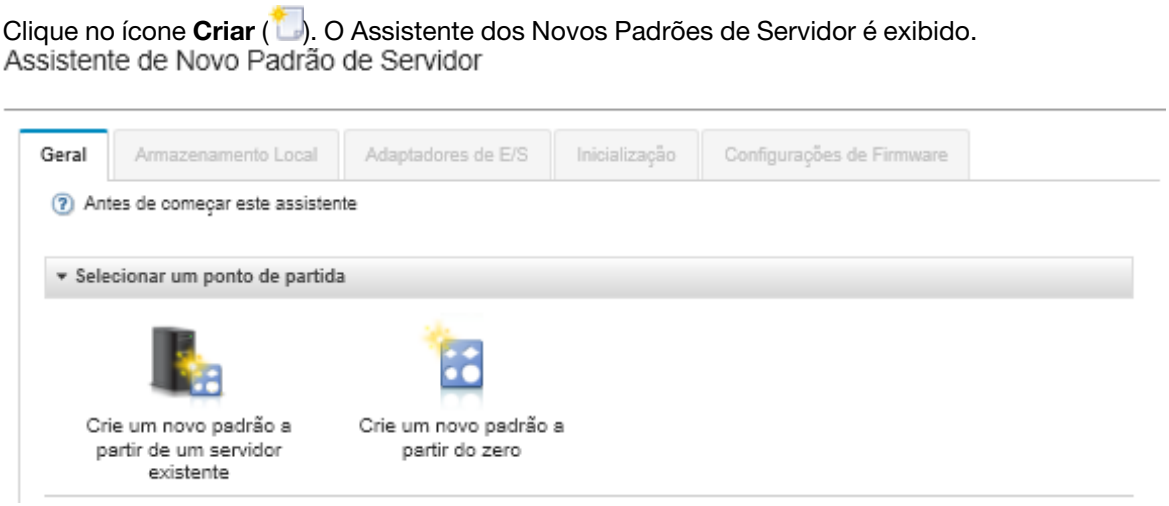
Procedimento

Para aprender um novo padrão a partir de um servidor existente, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Administrator, clique em **Fornecimento → Padrões**. A página Padrões de Configuração: Padrões é exibida.

Etapa 2. Clique na guia **Padrões de Servidor**.

Etapa 3. Clique no ícone **Criar** ( ). O Assistente dos Novos Padrões de Servidor é exibido.



Etapa 4. Clique em **Criar um novo padrão a partir de um servidor existente**. É possível escolher criar um padrão do zero, mas geralmente é mais eficaz criar um padrão a partir de um servidor existente que contém a configuração desejada.

Quando você criar um padrão de servidor a partir de um servidor existente, o XClarity Administrator aprende as configurações de um servidor gerenciado (incluindo a porta estendida, UEFI e configurações do Baseboard Management Controller) e cria dinamicamente padrões de categoria para essas configurações. Se o servidor for novo, o XClarity Administrator aprende as configurações de fábrica. Se o servidor estiver em uso, o XClarity Administrator aprende as configurações personalizadas. É possível alterar as configurações especificamente para o servidor ao qual esse padrão deve ser implantado.

Etapa 5. Selecione o servidor a ser usado como uma configuração base ao criar o padrão.

Nota: Lembre-se que o servidor que você escolher deve ser do mesmo modelo dos servidores aos quais você pretende implantar o padrão de servidor. Este cenário é baseado em escolher um Nó de Cálculo do Flex System x240.

Etapa 6. Insira o nome do novo padrão e forneça uma descrição.

Exemplo:

- Nome: **x240_ESXi_deployment**
- Descrição: **Padrão com configurações de UEFI estendidas apropriadas para a implantação de VMware ESXi**

Etapa 7. Clique em **Avançar** para carregar informações do servidor selecionado.

Etapa 8. Na guia **Armazenamento Local**, selecione **Especificar configuração de armazenamento** e escolha um dos tipos de armazenamento. Em seguida, clique em **Avançar**.

Para obter mais informações sobre configurações de armazenamento local, consulte Definindo o armazenamento local.

Etapa 9. Na guia **Adaptadores de E/S**, insira as informações sobre os adaptadores que estão nos servidores em que você pretende instalar o VMware ESXi.

Quaisquer adaptadores que estavam presentes no servidor usado como base são exibidos.

Se todos os Flex System x240 Nós de Cálculo na sua instalação possuírem os mesmos adaptadores, não será necessário modificar nenhuma configuração desta guia.

Para obter mais informações sobre as configurações de adaptadores de E/S, consulte Definindo adaptadores de E/S.

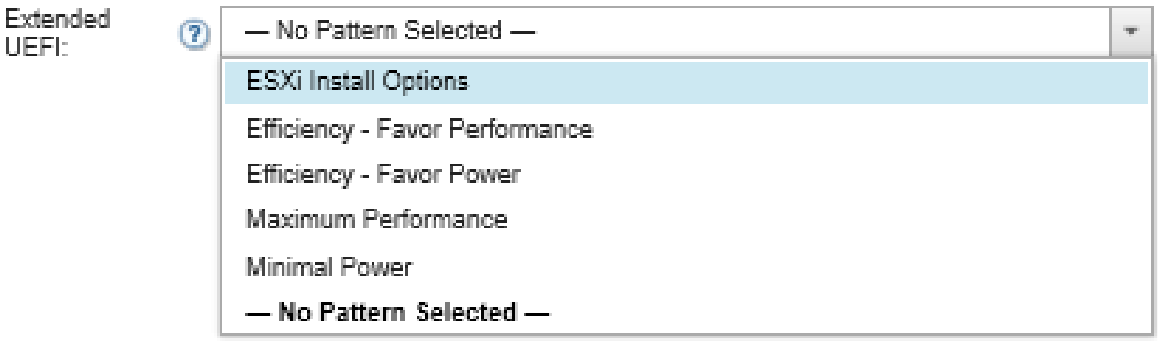
Etapa 10. Clique em **Avançar** para continuar.

Etapa 11. Na guia **Boot**, defina as configurações como ambiente de inicialização somente de legado e ambientes de inicialização de SAN. A menos que você esteja usando um desses ambientes, aceite o padrão, que é **Inicialização Somente de UEFI**, e clique em **Avançar**.

Para obter mais informações sobre configurações de inicialização, consulte Definindo opções de inicialização.

Etapa 12. Na guia **Configurações de Firmware**, especifique as configurações de firmware UEFI e do controlador de gerenciamento que devem ser usadas em servidores de destino quando esse padrão for implantado (por exemplo, selecione **Virtualização x240**).

Nessa guia, é possível escolher um dos padrões de UEFI estendida predefinidos:



Para obter mais informações sobre configurações de firmware, consulte Definindo configurações de firmware.

Etapa 13. Clique em **Salvar e Implantar** para salvar o padrão no XClarity Administrator e implantá-lo nos servidores em que você pretende instalar o VMware ESXi.

Depois de concluir

Depois que um padrão de servidor for implantado em todos os servidores, será possível instalar o sistema operacional nos servidores.

Implantando o VMware ESXi ao Nó de Cálculo do Flex System x240

Use este procedimento como um fluxo de exemplo ilustrando o processo de implantação do sistema operacional ESXi ao Nó de Cálculo do Flex System x240.

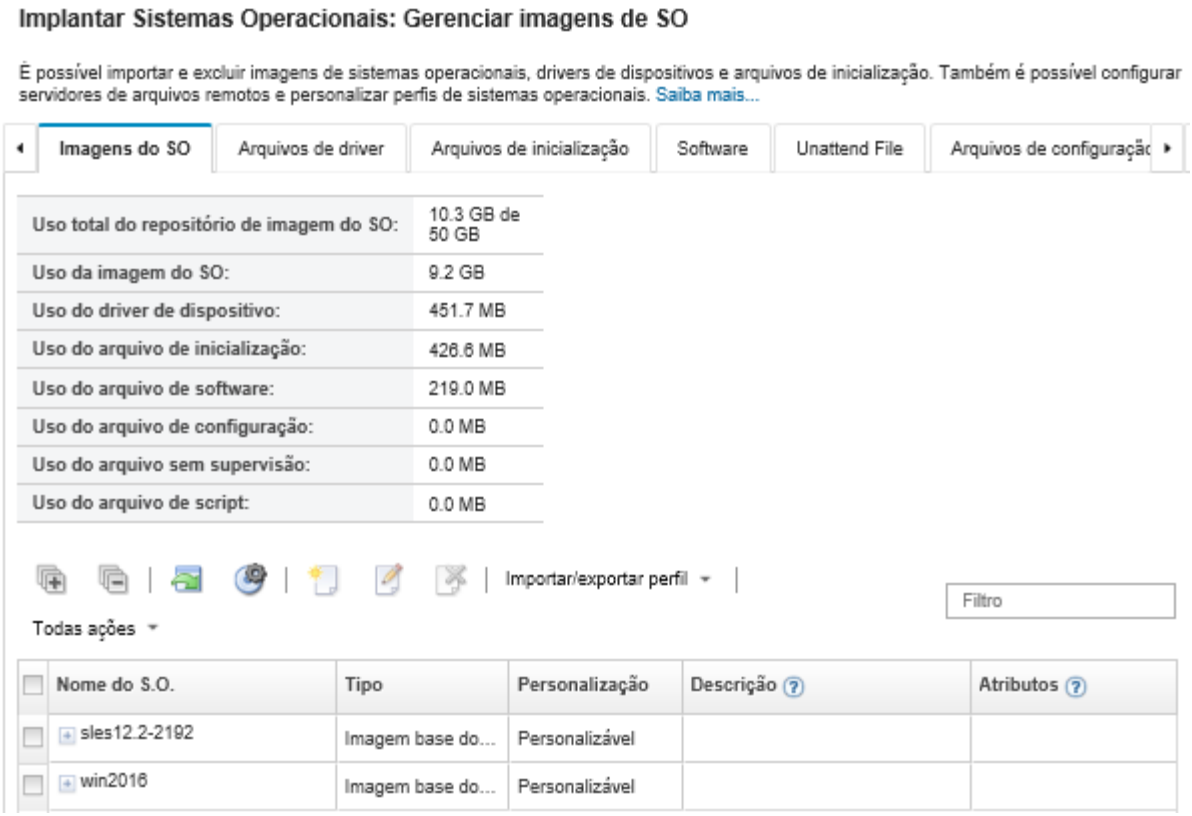
Antes de iniciar

Antes de iniciar este procedimento, certifique-se de que o Lenovo XClarity Administrator esteja gerenciando o chassi em que o Nó de Cálculo do Flex System x240 está instalado.

Procedimento

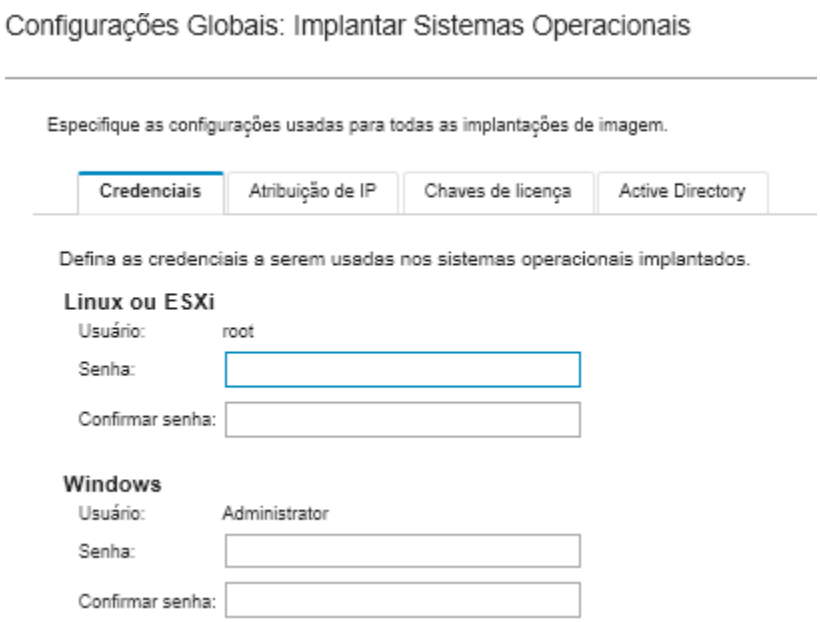
Conclua as seguintes etapas para implantar o sistema operacional ESXi a um Nó de Cálculo do Flex System x240.

Etapa 1. Certifique-se de que a imagem a ser implantada já esteja carregada no Repositório de imagens do SO clicando em **Todas as Ações → Gerenciar imagens de SO** para exibir uma lista de todas as imagens disponíveis.



Etapa 2. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO**. A página Implantar imagens de SO é exibida.

Etapa 3. Defina as configurações globais que devem ser usadas como padrão para as implantações de imagem, clicando em **Todas as Ações → Configurações Globais** para exibir a caixa de diálogo Configurações Globais.



a. Na guia **Credenciais**, insira a senha que deve ser usada pela conta de administrador para acessar o sistema operacional.

b. Na guia **Atribuição de IP**, especifique como o endereço IP do sistema operacional será atribuído ao servidor.

   Se você escolher **Usar Protocolo de Configuração Dinâmica de Host (DHCP)** para atribuir endereços IP, as informações do endereço IP não serão exibidas na caixa de diálogo Editar Configurações de Rede (consulte a etapa Etapa 8 9 na página 626). Se você escolher **Atribuir endereço IP estático (IPv4)**, poderá especificar um endereço IP, uma sub-rede e um gateway, um para cada implantação.

c. Na guia **Chaves de Licença**, insira uma chave de licença de ativação em massa, se desejado.

d. Clique em **OK** para fechar a caixa de diálogo.

Etapa 4. Certifique-se de que o servidor esteja pronto para implantação do sistema operacional, selecionando o servidor no qual o sistema operacional deve ser implantado. Inicialmente, o status de implantação pode ser mostrado como Não Pronto. O status de implantação deve ser Pronto para que você possa implantar um sistema operacional em um servidor.

Dica: é possível escolher vários servidores em diversos chassis do Flex System se você pretende implantar o mesmo sistema operacional em todos os servidores. É possível escolher até 28 servidores.

Etapa 5. Clique na coluna **Imagem para implantação** e selecione VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**).

Etapa 6. Na mesma coluna, clique no ícone **Chave de Licença** ( ) para inserir a chave de licença para essa implantação.

Dica: é possível optar por usar uma chave de ativação em massa que você inseriu na caixa de diálogo Configurações Globais.

Etapa 7. Certifique-se de que **Disco Local** esteja selecionado na coluna Armazenamento.

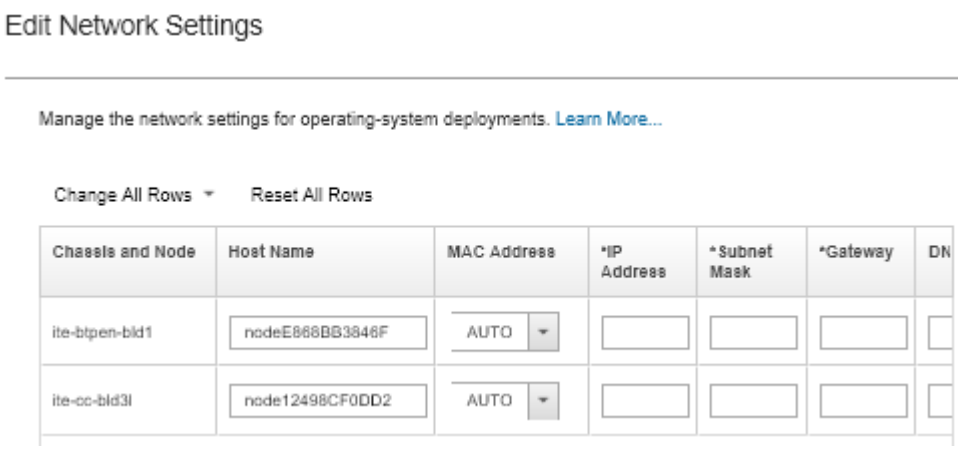
Etapa 8. Clique em **Editar** na coluna **Configurações de Rede** na linha do servidor para definir as configurações de rede que devem ser usadas para essa implantação. A página Editar Configurações de Rede é exibida.

Preencha os campos a seguir:

- Nome do Host
- O endereço MAC da porta no host no qual o sistema operacional será instalado
- Servidores Sistema de Nomes de Domínio (DNS), se necessário
- velocidade da unidade de transmissão máxima (MTU)

Notas: Se você escolher **Atribuir endereço IP estático (IPv4)** na caixa de diálogo Configurações Globais (consulte a etapa Etapa 3 4 na página 624), insira também as informações a seguir:

- Endereço IPv4
- Máscara de Sub-rede
- Gateway



Etapa 9. Clique em **OK** para fechar a caixa de diálogo.

Na página Implantar Imagens de SO, certifique-se de que o servidor mostre um Status de Implantação como Pronto.

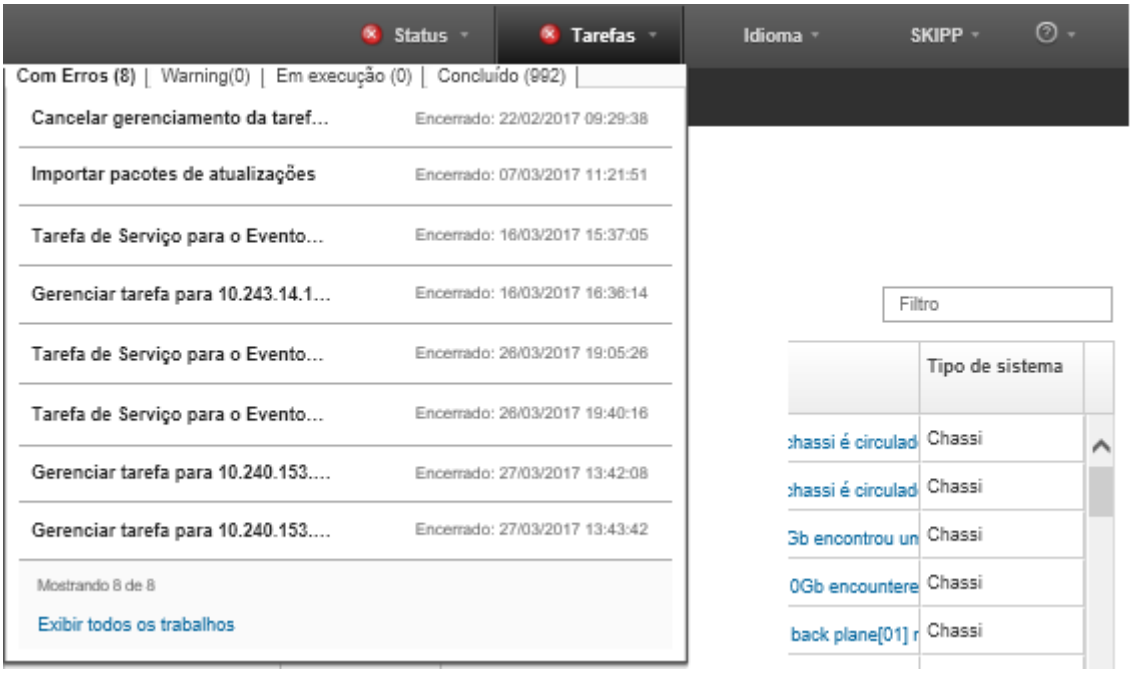
Etapa 10. Implante o sistema operacional, clicando em **Todas as Ações → Implantar imagens**.

Etapa 11. Na página de confirmação, clique em **Implantar** para implantar a imagem.

Se o servidor tiver, atualmente, um sistema operacional, você será advertido sobre o fato de implantar a imagem que substituirá o sistema operacional atual.

Dica: é possível configurar uma sessão de Controle Remoto para observar o progresso da instalação. Clique em **Todas as Ações → Controle Remoto** para iniciar uma sessão de Controle Remoto com o servidor.

Ao implantar o sistema operacional, o Lenovo XClarity Administrator inicia um trabalho para controlar a implantação. Para exibir o status do trabalho de implantação, clique em **Trabalhos** na barra de menus do Lenovo XClarity Administrator. Em seguida, clique na guia **Executar**.

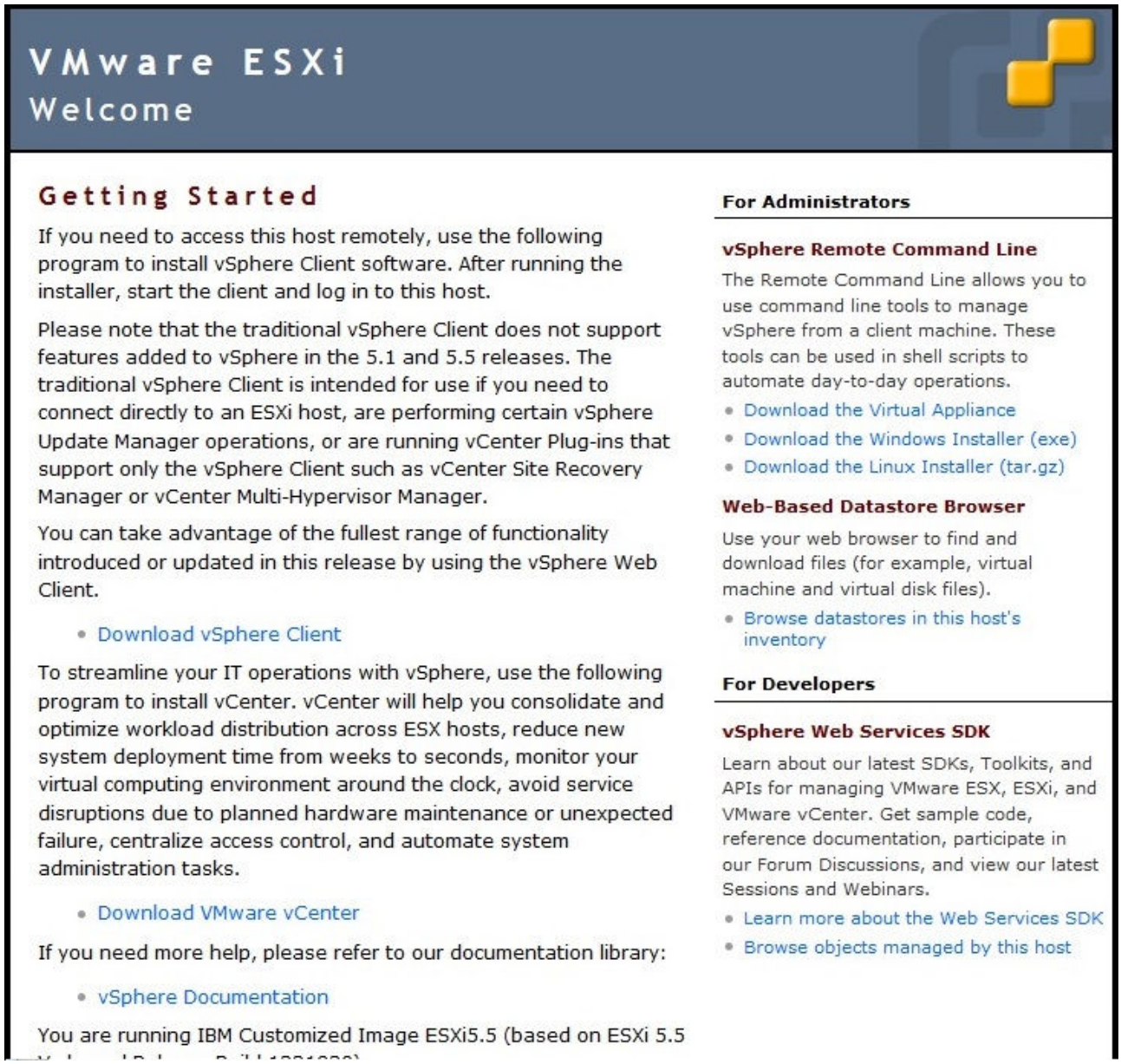


Para obter mais detalhes, como a porcentagem do trabalho realizada, passe o mouse sobre o trabalho em execução.

Resultados

Após a implantação do sistema operacional ser concluída, faça login no endereço IP que você especificou na página Editar Configurações de Rede para continuar com o processo de configuração.

Nota: A licença fornecida com a imagem é uma versão de avaliação gratuita de 60 dias. Você é responsável por cumprir todos os requisitos de licenciamento do VMware.



Implantando o ESXi ao armazenamento SAN

Use estes procedimentos para implantar o VMware ESXi 5.5 aos volumes SAN conectados aos servidores.

Ao implantar um sistema operacional ao SAN, o sistema operacional será implantado no primeiro destino de inicialização de SAN configurado em um padrão de servidor. Além disso, um disco rígido local não pode ser ativado no servidor que estará inicializando a partir do SAN. Isto deve ser desativado ou removido se houver um disco rígido presente.

Implantando um padrão de servidor para suportar a inicialização de SAN

Ao criar e implantar um padrão de servidor para suportar a inicialização de um sistema a partir de SAN, certifique-se de identificar o destino de inicialização de SAN e os adaptadores que fazem parte do servidor.

Procedimento

Para criar e implantar um padrão de servidor que suporta a implantação do sistema operacional no armazenamento SAN, conclua as seguintes etapas.

Etapa 1. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Padrões**. A página Padrões de Configuração: Padrões é exibida.

Etapa 2. Para identificar os IDs de LUN e de WWPN dos volumes de armazenamento onde o sistema operacional deve ser implantado, crie um padrão de categoria.

a. Clique na guia **Padrões de Categoria**.

b. Clique em **Padrões de Destino de Inicialização do Fibre Channel** e, em seguida, clique no ícone **Criar** ( ).

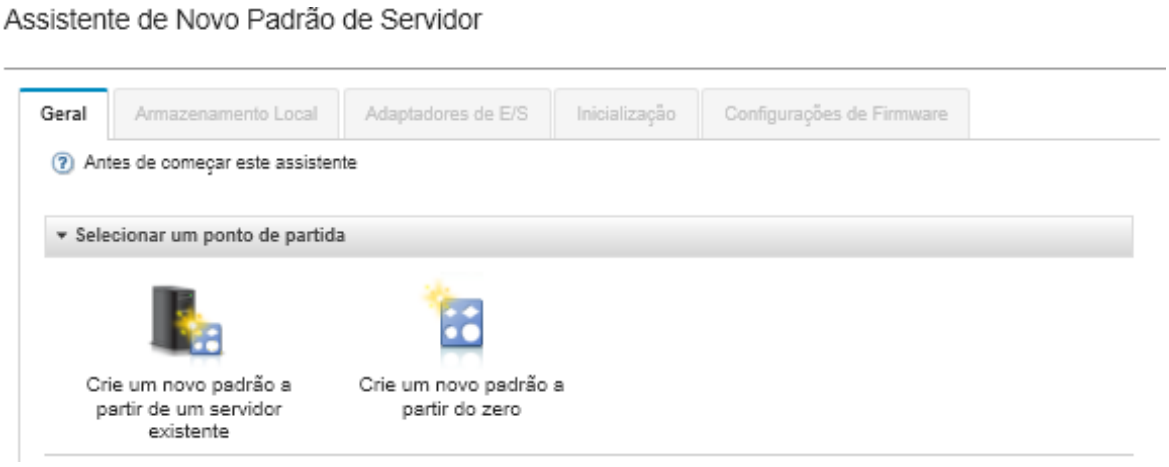
c. Insira o WWPN do destino de armazenamento.

Nota: Clique em **Permitir Vários Identificadores de LUN** para atribuir vários identificadores LUN de destino aos mesmos volumes de armazenamento.

d. Clique em **Criar** para criar o padrão. O destino é exibido na lista de Padrões de Destino de Inicialização do Fibre Channel.

Etapa 3. Clique na guia **Padrões de Servidor** para criar um padrão.

Etapa 4. Clique no ícone **Criar** ( ). O Assistente dos Novos Padrões de Servidor é exibido.



Etapa 5. Clique em **Criar um novo padrão a partir do zero**.

Etapa 6. Na guia **Geral**:

- Selecione **Nós de cálculo Flex** para o fator forma.

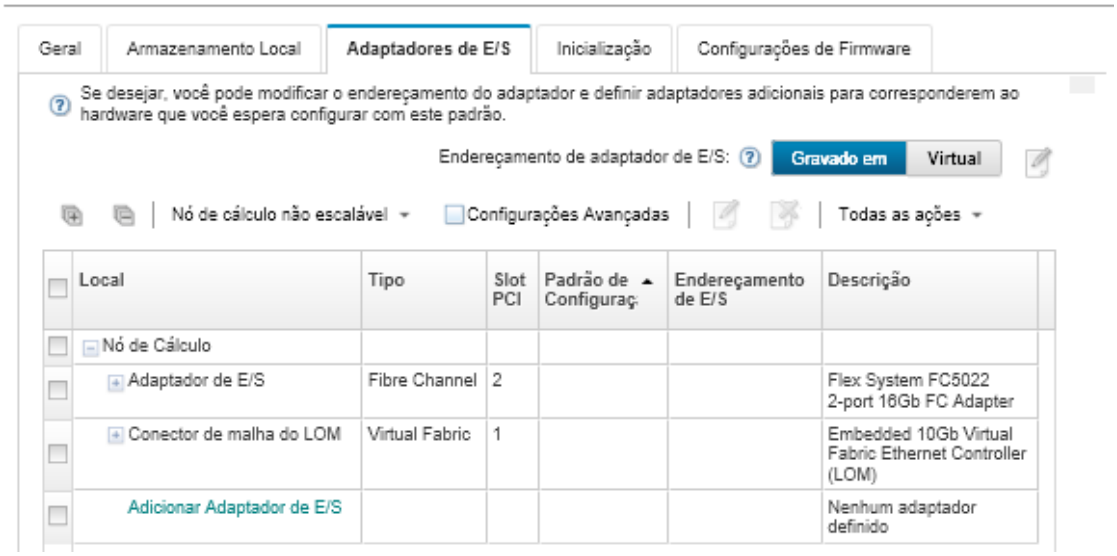
- Especifique um nome padrão (**x240_san_boot**) e descrição.
- Clique em **Avançar**.

Etapa 7. Na guia **Armazenamento Local**, considere desativar o adaptador de armazenamento local se estiver usando um sistema sem disco para melhorar o tempo de inicialização relacionado à verificação de unidades locais. Em seguida, clique em **Avançar**.

Etapa 8. Na guia **Adaptadores de E/S**, adicione as placas de Ethernet e Fibre Channel. Certifique-se de que estejam nos slots PCI apropriados.

a. Para cada placa, clique em **Adicionar Adaptador de E/S**, escolha o slot PCI onde a placa está localizada e selecione a placa.

Nota: Certifique-se de especificar uma placa Ethernet e uma placa Fibre Channel.



b. Verifique se o endereçamento do adaptador de E/S está configurado como **Virtual**. Clique no ícone **Editar** para especificar a configuração a ser usada para o endereçamento virtual de Ethernet (MAC) e o endereçamento virtual de Fibre Channel (WWN).

Nota: Na página Editar Endereçamento Virtual, é possível usar o endereço MAC gravado na placa Ethernet, desativando o endereçamento virtual. Entretanto, para selecionar e utilizar um padrão de destino de inicialização Fibre Channel, você deverá usar o endereçamento virtual para o adaptador Fibre Channel.

c. Clique em **Avançar**.

Etapa 9. Na guia **Boot**, inclua o padrão de destino de inicialização de SAN criado anteriormente.

a. Na guia **Inicialização de SAN**, escolha o padrão de destino de inicialização de SAN definido.

b. Clique em **Avançar**.

Etapa 10. Na guia **Configurações de Firmware**, defina todos os padrões de categoria adicionais que devem ser incluídos nesse padrão de servidor. É possível configurar os seguintes padrões de categoria.

- **Informações do sistema** (consulte Definindo configurações de informações do sistema)
- **Interface de gerenciamento** (consulte Definindo configurações de interface de gerenciamento)
- **Dispositivo e portas de E/S** (consulte Definindo configurações de dispositivos e portas de E/S

- **BMC estendida**. É possível escolher as configurações do Baseboard Management Controller que foram detectadas anteriormente (consulte Definindo configurações estendidas do controlador de gerenciamento).
- **UEFI estendida**. É possível escolher as configurações predefinidas ou UEFI que foram detectadas anteriormente (consulte Definindo configurações UEFI estendidas).

Etapa 11. Clique em **Salvar e Implantar** para salvar o padrão no Lenovo XClarity Administrator e implantá-lo nos servidores em que você pretende instalar o VMware ESXi.

Depois de concluir

Considere as seguintes etapas após o padrão de servidor ser implantado nos servidores.

1. Obtenha os endereços WWPN virtualizados que foram criados e inclua-os à zona de armazenamento para que o servidor possa acessar o LUNs de armazenamento definidos.

   Dica: depois de implantar o perfil do servidor, é possível localizar os endereços WWPN virtualizados visualizando o perfil do servidor.

   a. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Perfis de servidor**.
   b. Clique no perfil de servidor implantado (por exemplo, **x240_SAN_boot**). A guia **Mapeamento de Endereço Virtual** exibe a lista de endereços.
2. Implante o sistema operacional no servidor.

Implantando o VMware ESXi ao armazenamento SAN

Use este procedimento como um fluxo de exemplo ilustrando o processo de implantação do sistema operacional ESXi ao armazenamento SAN que é conectado a um servidor.

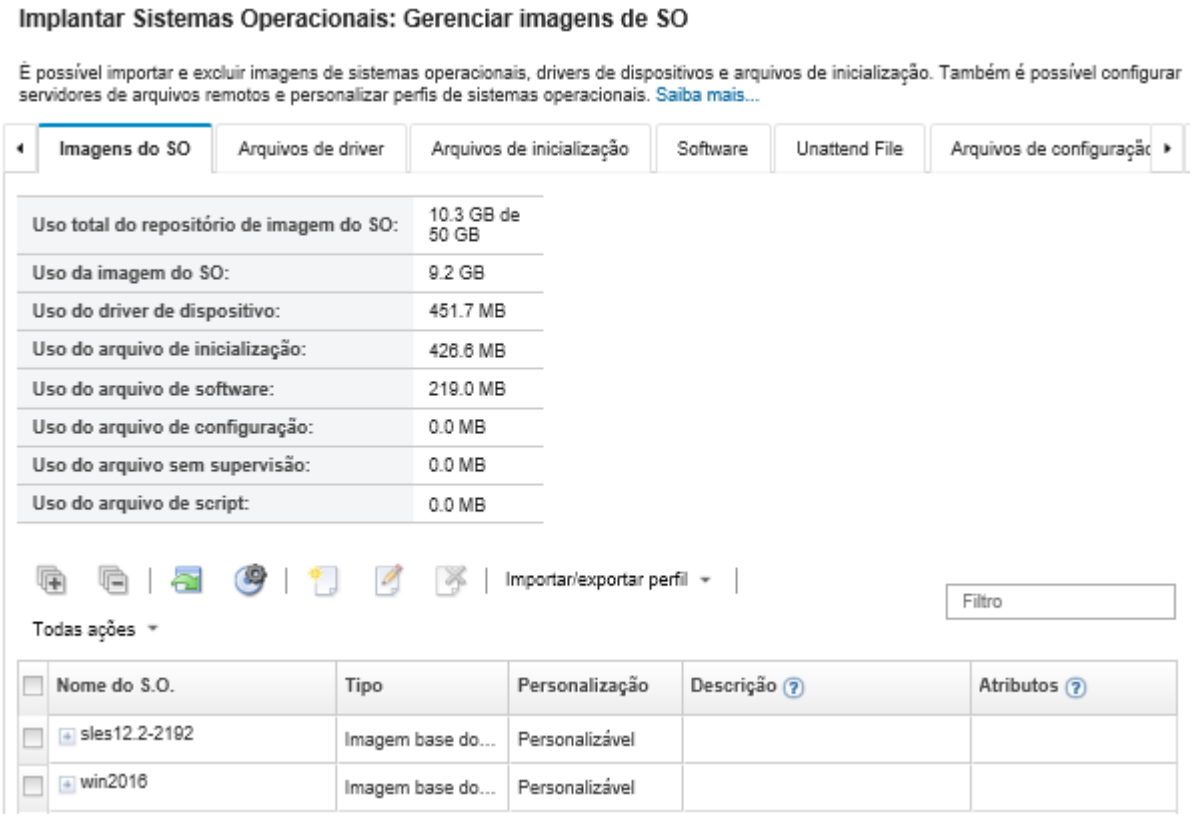
Antes de iniciar

Antes de iniciar este procedimento, certifique-se de que o Lenovo XClarity Administrator esteja gerenciando o chassi em que o Nó de Cálculo do Flex System x220 está instalado.

Procedimento

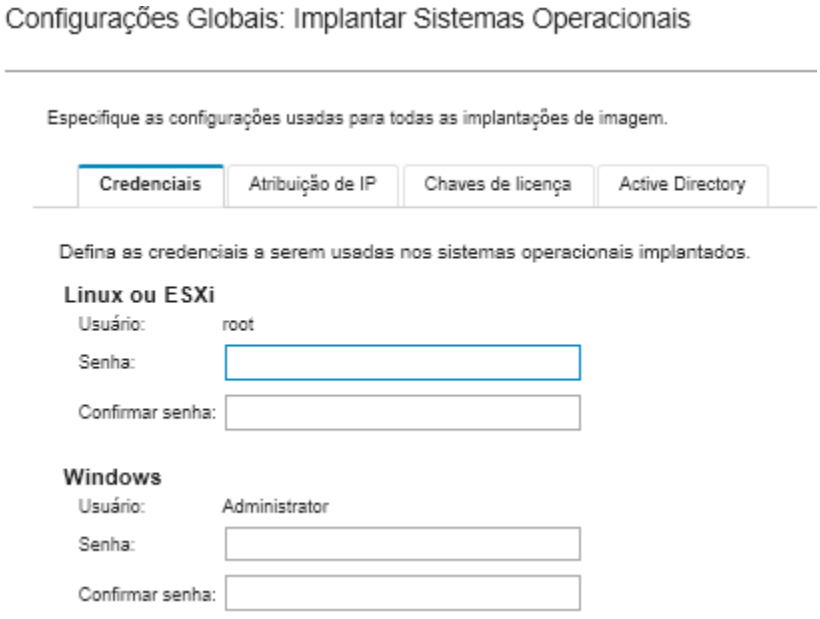
Conclua as seguintes etapas para implantar o sistema operacional ESXi a um Flex System x222 Nó de Cálculo.

Etapa 1. Certifique-se de que a imagem a ser implantada já está carregada no Repositório de imagens do SO clicando em **Todas as Ações → Gerenciar imagens de SO**.



Etapa 2. Na barra de menu do Lenovo XClarity Administrator, clique em **Fornecimento → Implantar imagens de SO**

Etapa 3. Defina as configurações globais que devem ser usadas como padrão para as implantações de imagem, clicando em **Todas as Ações → Configurações Globais** para exibir a caixa de diálogo Configurações Globais: Implantar Sistemas Operacionais.



a. Na guia **Credenciais**, insira a senha que deve ser usada pela conta de administrador para acessar o sistema operacional.

b. Na guia **Atribuição** de IP, especifique como o endereço IP do sistema operacional será atribuído ao servidor.

   Se você escolher **Usar Protocolo de Configuração Dinâmica de Host (DHCP)** para atribuir endereços IP, as informações do endereço IP não serão exibidas na caixa de diálogo Editar Configurações de Rede (consulte a etapa Etapa 8 9 na página 635). Se você escolher **Atribuir endereço IP estático (IPv4)**, poderá especificar um endereço IP, uma sub-rede e um gateway, um para cada implantação.

c. Na guia **Chaves de Licença**, insira uma chave de licença de ativação em massa, se desejado.

d. Clique em **OK** para fechar a caixa de diálogo.

Etapa 4. Certifique-se de que o servidor esteja pronto para implantação do sistema operacional, selecionando o servidor no qual o sistema operacional deve ser implantado. Inicialmente, o status de implantação pode ser mostrado como Não Pronto. O status de implantação deve ser Pronto para que você possa implantar um sistema operacional em um servidor.

Dica: é possível escolher vários servidores de diversos chassis do Flex System se você pretende implantar o mesmo sistema operacional em todos os servidores. É possível escolher até 28 servidores.

Etapa 5. Clique na coluna **Imagem para implantação** e selecione VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**).

Etapa 6. Na mesma coluna, clique no ícone **Chave de Licença** ( ) para inserir a chave de licença para essa implantação.

Dica: é possível optar por usar uma chave de ativação em massa você inseriu na caixa de diálogo Configurações Globais: Implantar Sistemas Operacionais.

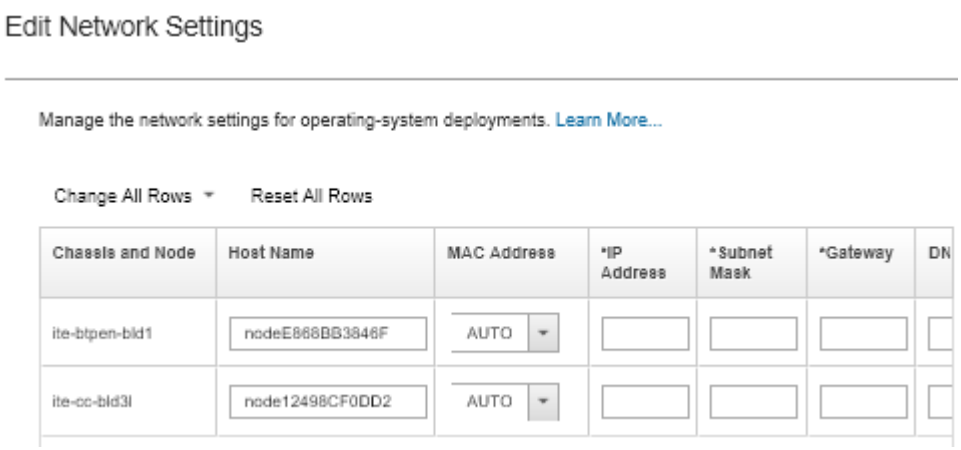
Etapa 7. Na coluna **Armazenamento**, selecione o armazenamento SAN o qual o sistema operacional deve ser implantado.

O armazenamento está listado como:
`LUN: <LUN_VALUE>  WWPN: <WWPN_VALUE>`

Etapa 8. Clique em **Editar** na coluna **Configurações de Rede** na linha do servidor para definir as configurações de rede que devem ser usadas para essa implantação. A página Editar Configurações de Rede é exibida.

Preencha os campos a seguir:
- Nome do Host
- O endereço MAC da porta no qual o sistema operacional será instalado
- Servidores Sistema de Nomes de Domínio (DNS), se necessário
- Velocidade da Unidade de Transmissão Máxima (MTU)

Notas: Se você escolher **Atribuir endereço IP estático (IPv4)** na caixa de diálogo Configurações Globais: Implantar Sistemas Operacionais (etapa Etapa 3 4 na página 633), insira também as informações a seguir:
- Endereço IPv4
- Máscara de Sub-rede
- Gateway



Etapa 9. Clique em **OK** para fechar a caixa de diálogo.

Na página Implantar imagens de SO, agora o servidor mostra um status de implantação como Pronto.

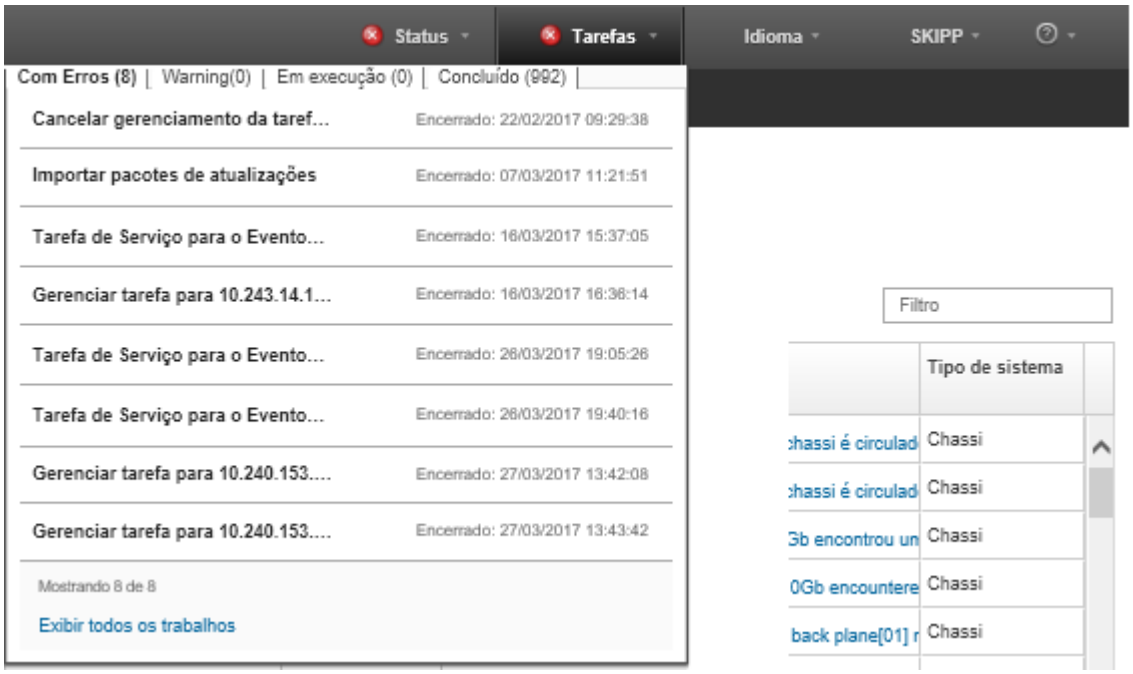
Etapa 10. Implante o sistema operacional, clicando em **Todas as Ações → Implantar imagens**.

Etapa 11. Na página de confirmação, clique em **Implantar** para implantar a imagem.

Se o servidor tiver, atualmente, um sistema operacional, você será advertido sobre o fato de implantar a imagem que substituirá o sistema operacional atual.

Dica: é possível configurar uma sessão de controle remoto para observar o progresso da instalação. Clique em **Todas as ações → Controle Remoto** para iniciar uma sessão de controle remoto com o servidor.

Ao implantar o sistema operacional, o Lenovo XClarity Administrator inicia um trabalho para controlar a implantação. Para exibir o status do trabalho de implantação, clique em **Trabalhos** na barra de menus do Lenovo XClarity Administrator. Em seguida, clique na guia **Executar**.

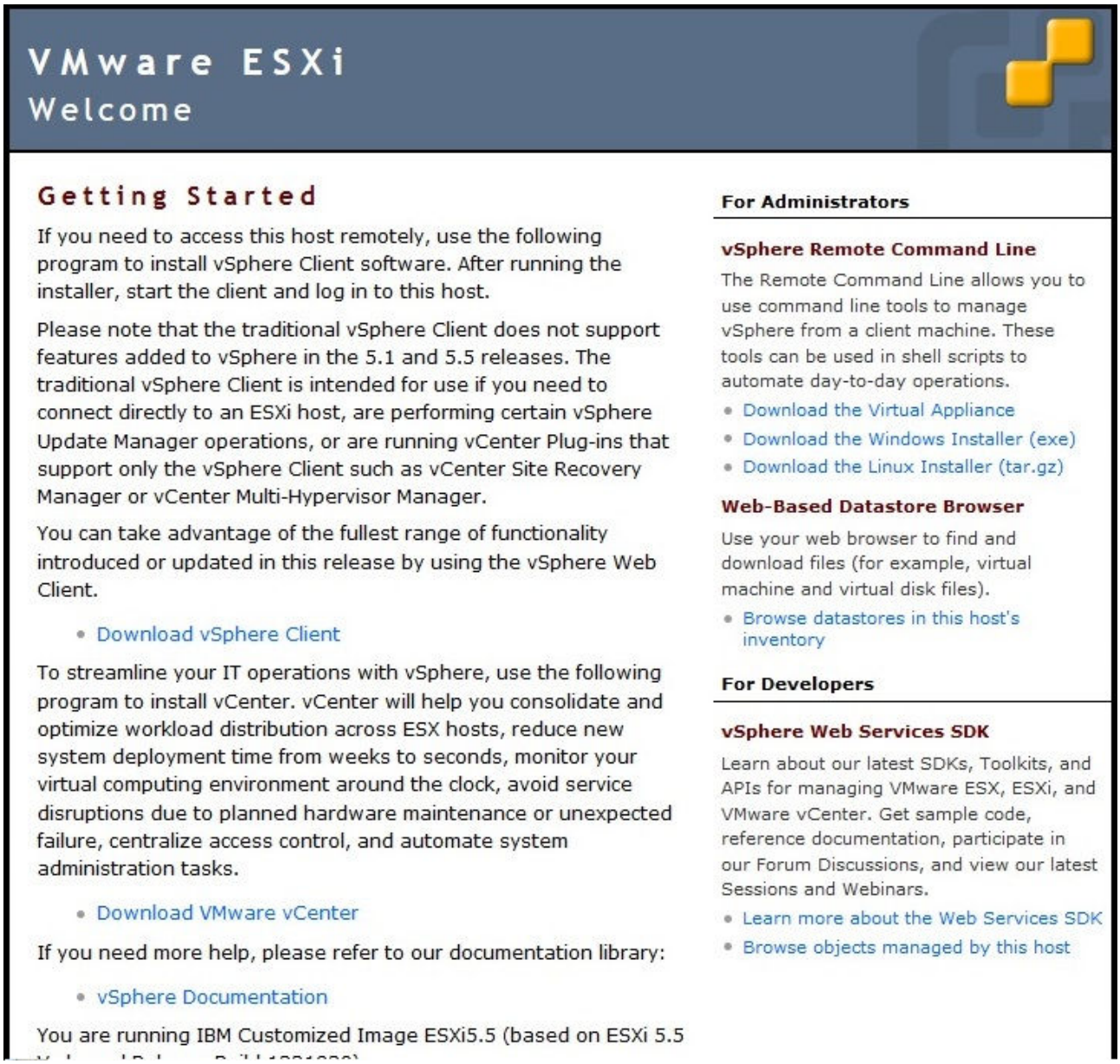


Para obter mais detalhes, como a porcentagem do trabalho realizada, passe o mouse sobre o trabalho em execução.

Resultados

Após a implantação do sistema operacional ser concluída, faça logon no endereço IP que você especificou na página Editar Configurações de Rede para continuar com o processo de configuração.

Nota: A licença fornecida com a imagem é uma versão de avaliação gratuita de 60 dias. Você é responsável por cumprir todos os requisitos de licenciamento do VMware.


VMware ESXi
Welcome
Getting Started
If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.
Please note that the traditional vSphere Client does not support features added to vSphere in the 5.1 and 5.5 releases. The traditional vSphere Client is intended for use if you need to connect directly to an ESXi host, are performing certain vSphere Update Manager operations, or are running vCenter Plug-ins that support only the vSphere Client such as vCenter Site Recovery Manager or vCenter Multi-Hypervisor Manager.
You can take advantage of the fullest range of functionality introduced or updated in this release by using the vSphere Web Client.
Download vSphere Client
To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.
Download VMware vCenter
If you need more help, please refer to our documentation library:
vSphere Documentation
You are running IBM Customized Image ESXi5.5 (based on ESXi 5.5
For Administrators
vSphere Remote Command Line
The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.
Download the Virtual Appliance
Download the Windows Installer (exe)
Download the Linux Installer (tar.gz)
Web-Based Datastore Browser
Use your web browser to find and download files (for example, virtual machine and virtual disk files).
Browse datastores in this host's inventory
For Developers
vSphere Web Services SDK
Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.
Learn more about the Web Services SDK
Browse objects managed by this host

Avisos

É possível que a Lenovo não ofereça os produtos, serviços ou recursos discutidos nesta publicação em todos os países. Consulte um representante Lenovo local para obter informações sobre os produtos e serviços disponíveis atualmente em sua área.

Qualquer referência a produtos, programas ou serviços Lenovo não significa que apenas produtos, programas ou serviços Lenovo possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da Lenovo, poderá ser utilizado em substituição a esse produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer outro produto, programa ou serviço são de responsabilidade do Cliente.

A Lenovo pode ter patentes ou solicitações de patentes pendentes relativas a assuntos descritos nesta publicação. O fornecimento desta publicação não é uma oferta e não fornece uma licença em nenhuma patente ou solicitações de patente. Pedidos devem ser enviados, por escrito, para:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

A LENOVO FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A Lenovo pode fazer aperfeiçoamentos e/ou alterações nos produtos ou programas descritos nesta publicação a qualquer momento sem aviso prévio.

Os produtos descritos nesta publicação não são destinados para uso em implantações ou em outras aplicações de suporte à vida, nas quais o mau funcionamento pode resultar em ferimentos ou morte. As informações contidas nesta publicação não afetam nem alteram as especificações ou garantias do produto Lenovo. Nada nesta publicação deverá atuar como uma licença expressa ou implícita nem como indenização em relação aos direitos de propriedade intelectual da Lenovo ou de terceiros. Todas as informações contidas nesta publicação foram obtidas em ambientes específicos e representam apenas uma ilustração. O resultado obtido em outros ambientes operacionais pode variar.

A Lenovo pode utilizar ou distribuir as informações fornecidas, da forma que julgar apropriada, sem incorrer em qualquer obrigação para com o Cliente.

Referências nesta publicação a Web sites que não são da Lenovo são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses Web sites. Os materiais contidos nesses Web sites não fazem parte dos materiais desse produto Lenovo e a utilização desses Web sites é de inteira responsabilidade do Cliente.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, o resultado obtido em outros ambientes operacionais pode variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão as mesmas em sistemas disponíveis em geral. Além disso, algumas medidas podem ter sido

estimadas através de extrapolação. Os resultados atuais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

Marcas Registradas

Lenovo