Lenovo XClarity Administrator Guia de Instalação e Planejamento de Ambientes Docker

Versão 4.0.0

Nota

Antes de usar estas informações e o produto ao qual elas dão suporte, leia os avisos gerais e legais do na documentação online do XClarity Administrator.

Primeira edição (Fevereiro 2023)

Conteúdo

Figuras

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.

Para obter informações sobre todo o hardware suportado (incluindo servidores, chassis e comutadores Flex), consulte Pré-requisitos de hardware e software.

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

O hardware a seguir é compatível nesta versão.

- **Servidores e dispositivos**
  - ThinkAgile HX630 V3 (7D6M)
  - ThinkAgile HX645 V3 (7D9M)
  - ThinkAgile HX650 V3 (7D6N)
  - ThinkAgile HX665 V3 (7D9N)
  - ThinkAgile MX630 V3 (7D6U)
  - ThinkAgile MX650 V3 (7D6S)
  - ThinkAgile VX630 V3 (7D6X, 7Z63)
  - ThinkAgile VX635 V3 (7D9V)
  - ThinkAgile VX645 V3 (7D9K)
  - ThinkAgile VX650 V2-DPU (7Z63)
  - ThinkAgile VX650 V3 (7D6W)
  - ThinkAgile VX650 V3-DPU (7D6W)
  - ThinkAgile VX655 V3 (7D9W)
  - ThinkAgile VX665 V3 (7D9L)
  - ThinkAgile VX850 V3 (7DDK)
  - ThinkEdge SE350 V2 (7DA9)
  - ThinkEdge SE455 V3 (7DBY)
  - ThinkEdge SE360 V2 (7DAM)
  - ThinkSystem SD555 V3 (7DDP, 7DDQ)
  - ThinkSystem SD650 V3 (7D7M)
  - ThinkSystem SD650-I V3 (7D7L)
  - ThinkSystem SD650-N V3(7D7L)
  - ThinkSystem SD665 V3 (7D9P)
  - ThinkSystem SD665-N V3 (7DAZ)
  - ThinkSystem SR630 V3 (7D72, 7D73, 7D74)
  - ThinkSystem SR635 V3 (7D9G, 7D9H)
  - ThinkSystem SR645 V3 (7D9C, 7D9D)
  - ThinkSystem SR650 V3 (7D75, 7D76, 7D77)
  - ThinkSystem SR655 V3 (7D9E, 7D9F)
  - ThinkSystem SR665 V3 (7D9B, 7D9A)
  - ThinkSystem SR675 V3 (7D9Q, 7D9R)
  - ThinkSystem SR850 V3 (7D96, 7D97, 7D98)
  - ThinkSystem SR860 V3 (7D93, 7D94, 7D95)
  - ThinkSystem SR950 V3 (7DC4, 7DC5, 7DC6)
  - ThinkSystem ST650 V3 (7D7A, 7D7B)
- **Dispositivos de armazenamento**

  - Matriz All Flash ThinkSystem DE6400F (7DB6)
  - Matriz flash híbrida ThinkSystem DE6400H (7DB6)
  - Matriz All Flash ThinkSystem DE6600F (7DB7)
  - Matriz flash híbrida ThinkSystem DE6600H (7DB7)
- **Comutadores**
  - Comutador SAN ThinkSystem DB730S FC (7D9J)
  - Diretor ThinkSystem DB400D FC SAN (6684)
  - Diretor ThinkSystem DB800D FC SAN (6682)

Esta versão oferece suporte aos seguintes aprimoramentos de planejamento ou instalação no software de gerenciamento.

Função	Descrição
Planejamento e instalação	Removido ssh-rsa e adicionados ssh-ed25519, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 e ecdsa-sha2-nistp521 à lista de algoritmos de chave do host compatíveis (consulte Gerenciamento de criptografia).

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 na documentação online do XClarity Administrator.

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 na documentação online do XClarity Administrator.

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 na documentação online do XClarity Administrator.

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 o XClarity Administrator na documentação online do XClarity Administrator.

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 na documentação online do XClarity Administrator.

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 Implantando uma imagem do sistema operacional na documentação online do XClarity Administrator.

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 na documentação online do XClarity Administrator.

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 na documentação online do XClarity Administrator.

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 na documentação online do XClarity Administrator.

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 na documentação online do XClarity Administrator.

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 na documentação online do XClarity Administrator.

- **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 na documentação online do XClarity Administrator.

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 na documentação online do XClarity Administrator.

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.

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**

Capítulo 2. Planejando o XClarity Administrator

Antes de instalar o Lenovo XClarity Administrator, revise as seguintes considerações para ajudá-lo a planejar a instalação e o gerenciamento dia a dia.

Licenças e a versão de avaliação gratuita de 90 dias

O Lenovo XClarity Administrator oferece uma licença de avaliação de 90 dias gratuita que permite o uso integral de todos os recursos disponíveis por tempo limitado.

É possível determinar os status das licenças, incluindo o número de dias restam da licença de avaliação, clicando no menu de ações do usuário (

) na barra de título do XClarity Administrator e clicando em **Sobre**.

O XClarity Administrator é compatível com a seguinte licença.

- **Lenovo XClarity Pro**. Cada licença fornece as autorizações a seguir para um único dispositivo.
  - Serviço e suporte para Lenovo XClarity Integrator
  - Serviço e suporte para XClarity Administrator
  - Funções avançadas em XClarity Administrator:
    - Configurando servidores com Padrões de Configuração
    - Implementando Sistemas Operacionais
    - Relatando problemas de XClarity Administrator usando call home (alertas de Call Home para hardware não são afetados.)

Você deve comprar uma licença para cada dispositivo gerenciado que ofereça suporte às funções avançadas. Uma licença não está vinculada a um dispositivo específico.

A conformidade com a licença é determinada com base no número de dispositivos gerenciados que oferecem suporte para as funções avançadas. O número de dispositivos gerenciados não deve exceder o número total de licenças em todas as chaves de licença ativas. Se o XClarity Administrator não estiver em conformidade com as licenças instaladas (por exemplo, se as licenças expirarem ou se o gerenciamento de dispositivos adicionais exceder o número total de licenças ativas), você terá um período de carência de 90 dias para instalar as licenças apropriadas. Cada vez que o XClarity Administrator se torna incompatível, o período de cortesia é redefinido para 90 dias. Se o período de cortesia (incluindo a avaliação gratuita) terminar antes que as licenças estejam em conformidade, as funções avançadas serão desativadas para todos os dispositivos.

Notas:

- Os recursos de configuração do servidor e de implantação do sistema operacional são desabilitados quando o período de carência expira.
- O recurso Call Home para problemas do XClarity Administrator (recurso Call Home do software) é desabilitado quando as licenças estão fora de conformidade. Não há nenhum período de carência para esse recurso. No entanto, o Call Home para alertas de hardware não é afetado.

Se licenças já estiverem instaladas, novas licenças *não* serão necessárias para fazer a atualização para uma nova versão do XClarity Administrator.

Para obter informações sobre a aquisição de licenças do Lenovo XClarity Pro, entre em contato com um representante da Lenovo ou parceiro de negócios autorizado.

Para obter mais informações sobre como instalar a licença, consulte Instalando a licença de habilitação com funcionalidade completa na documentação online do XClarity Administrator.

Pré-requisitos de hardware e software

O dispositivo de gerenciamento Lenovo XClarity Administrator é executado em uma máquina virtual em um sistema host.

Requisitos do hipervisor

Ambientes de contêiner

O ambiente de contêiner a seguir é compatível com a execução do XClarity Administrator como um contêiner.

- Docker v20.10.9
- Docker-compose v1.29.2

Hipervisores

Os hipervisores a seguir são compatíveis com a execução do XClarity Administrator como um dispositivo virtual.

- Hipervisor Citrix v8.2
- Citrix XenServer v7.6
- CentOS 7 e 8[1]
- Microsoft Windows Server 2022 com Hyper-V instalado
- Microsoft Windows Server 2019 com Hyper-V instalado
- Microsoft Windows Server 2016 com Hyper-V instalado
- Microsoft Windows Server 2012 R2 com Hyper-V instalado
- Microsoft Windows Server 2012 com Hyper-V instalado
- Nutanix Acropolis Hypervisor (AHV)
- Red Hat v8.x com Kernel-based Virtual Machine (KVM) v2.12.0 instalado
- Red Hat v7.x com KVM v1.2.17 instalado
- Ubuntu 20.04.2 LTS com KVM v4.2.3 instalado
- VMware ESXi 7.0, U1, U2 e U3
- VMware ESXi 6.7, U1, U2[2] e U3

Notas:

1. O CentOS Linux não é mais atualizado pela Red Hat. Considere migrar para o Red Hat Enterprise Linux (consulte Página da Web Red Hat: como converter do CentOS ou Oracle Linux em RHEL).
2. Para VMware ESXi 6.7 U2, você deve usar a imagem ISO VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso ou posterior.

Para VMware e Citrix, a máquina virtual está disponível como um modelo OVF. Para o Hyper-V e o Nutanix AHV, a máquina virtual é uma imagem de disco virtual (VHD). Para CentOS e KVM, a máquina virtual está disponível no formato qcow2.

Importante: Para ambientes Hyper-V executados em convidados Linux com uma base de 2.6 Kernel e que usam grandes quantidades de memória para o dispositivo virtual, você deve desabilitar o uso de memória não uniforme (NUMA) no Painel Configurações do Hyper-V do Gerenciador Hyper-V. Alterar essa configuração requer reiniciar o serviço Hyper-V, que também reinicia todas as máquinas virtuais em execução. Se essa configuração não estiver desabilitada, o dispositivo virtual XClarity Administrator poderá ter problemas durante a inicialização inicial.

Requisitos de Hardware

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 na documentação online do XClarity Administrator.

Requisitos de Software

- **Servidor do orquestrador**

  Se você gerenciar um grande número de dispositivos usando várias instâncias do XClarity Administrator, será possível centralizar o monitoramento, o gerenciamento, o fornecimento e a análise usando o Lenovo XClarity Orchestrator. OXClarity Orchestrator é compatível com um número ilimitado de instâncias do XClarity Administrator que gerenciam coletivamente um máximo de **10.000** dispositivos não ThinkEdge-Client.

  Para gerenciar instâncias do XClarity Administratorv4.0 ou posteriores usando o Lenovo XClarity Orchestrator, o XClarity Orchestrator v2.0 ou posterior é necessário.

- **Servidor de autenticação**

  Se você optar por usar um servidor de autenticação externo, apenas o Microsoft Active Directory em execução no Windows Server 2008 ou posterior terá suporte.

  Se você optar por usar um provedor de identidade SAML, apenas o Microsoft Active Directory Federation Services (AD FS) versões 2.0 ou posterior em execução no Windows Server 2012 ou posterior terá suporte.

- **Servidor NTP**

  Deve-se usar um servidor Network Time Protocol (NTP) para garantir que os registros de data e hora de todos os eventos e alertas recebidos dos dispositivos gerenciados sejam sincronizados com o XClarity Administrator. Certifique-se de que o servidor NTP esteja acessível na rede de gerenciamento (geralmente a interface Eth0).

  Dica: Considere usar o sistema host no qual o XClarity Administrator esteja instalado como o servidor NTP. Se fizer isso, garanta que o sistema host esteja acessível na rede de gerenciamento.

Recursos gerenciáveis

Uma única instância do XClarity Administrator pode gerenciar, monitorar e provisionar no máximo **1.000** dispositivos físicos.

É possível encontrar uma lista completa de dispositivos e opções compatíveis (como E/S, DIMM e adaptadores de armazenamento), níveis mínimos de firmware necessários e considerações de limitações a partir do Página da Web Suporte do XClarity Administrator – Compatibilidade clicando na guia **Compatibilidade** e, em seguida, clicando no link para os tipos de dispositivo apropriados.

Para obter informações gerais sobre a configuração e opções de hardware de um dispositivo específico, consulte o Página da Web do Lenovo Server Proven.

Restrição: Se o sistema host no qual o XClarity Administrator estiver instalado for um servidor de rack gerenciado ou um nó de cálculo, você não poderá usar o XClarity Administrator para aplicar atualizações de firmware a esse sistema host nem a todo o chassi simultaneamente. Quando as atualizações de firmware forem aplicadas ao sistema host, o sistema host deverá ser reiniciado. Reiniciar o sistema host também reiniciará o XClarity Administrator, tornando o XClarity Administrator indisponível para concluir as atualizações no sistema host.

Navegadores da Web suportados

A interface da Web do XClarity Administrator funciona com os navegadores da Web a seguir.
- 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)

Firewalls e servidores proxy

Algumas funções do Lenovo XClarity Administrator, incluindo atualizações do servidor de gerenciamento, atualizações, serviço e suporte de firmware, requerem acesso à Internet. Se você tiver firewalls em sua rede, configure os firewalls para ativar o servidor de gerenciamento XClarity Administrator para executar essas operações. Se o servidor de gerenciamento não tiver acesso direto à Internet, configure o XClarity Administrator para usar um servidor proxy.

Firewalls

Verifique se as seguintes portas e nomes DNS estão abertas no firewall.

Nota: Os endereços IP estão sujeitos a mudanças. Use os nomes DNS quando possível.

Tabela 1. Conexões à Internet Necessárias

Nome DNS	Endereço IPv4	Endereço IPv6	Portas	Protocolos
Baixar chaves de ativação da licença				
fod.lenovo.com	N/D	N/D	443	https
Baixar boletins de serviço				
download.lenovo.com/servers/LXCA_Bulletin_Service.json	N/D	N/D	443 e 80	https
Baixar atualizações (do servidor de gerenciamento, as atualizações de firmware, UpdateXpress System Packs (drivers de dispositivo do SO) e pacotes do repositório)				
datacentersupport.lenovo.com	N/D	N/D	443 e 80	https
download.lenovo.com	N/D	N/D	443 e 80	https
filedownload.lenovo.com	N/D	N/D	443 e 80	https
support.lenovo.com	N/D	N/D	443 e 80	https e http
supportapi.lenovo.com	N/D	N/D	443 e 80	https
Baixar o firmware (Flex System x220, x222, x240, x280 X6, x440, x480 X6, x880 X6, alguns comutadores Flex, e somente CMMs de primeira geração)				
www.ibm.com	129.42.56.216, 129.42.58.216, 129.42.60.216, 129.42.160.51, 207.25.252.19-7	N/D	443 e 80	https e http
www-03.ibm.com	204.146.30.17	N/D	443 e 80	https e http
download3.boulder.ibm.com	170.225.126.2-4	N/D	443	https
download4.boulder.ibm.com	170.225.126.4-3	N/D	443 e 80	https e http
delivery04-bld.dhe.ibm.com	170.225.126.4-5	N/D	443 e 80	https e http
delivery04-mul.dhe.ibm.com	170.225.126.4-6	N/D	443 e 80	https e http
delivery04.dhe.ibm.com	170.225.126.4-4	N/D	443 e 80	https e http
Fazer upload de dados de serviço para o Lenovo Support (Call Home)				
soaus.lenovo.com	3.222.8.29, 52.6.14.20	N/D	443	https
logupload.lenovo.com/BLL/Logupload.ashx	N/D	N/D	443 e 80	https
Fazer upload de dados de serviço para o Recurso de Upload da Lenovo				

Tabela 1. Conexões à Internet Necessárias (continuação)

Nome DNS	Endereço IPv4	Endereço IPv6	Portas	Protocolos
logupload.lenovo.com/BLL/Logupload.ashx	N/D	N/D	443 e 80	https
Baixar informações sobre garantia				
ibase.lenovo.com (mundial)	N/D	N/D	443 e 80	https e http
service.lenovo.com.cn (Apenas China)	114.247.140.2-12 (Apenas China)	N/D	83	http
supportapi.lenovo.com	N/D	N/D	443 e 80	https e http

Atenção: Para os usuários na China, para recuperar informações sobre garantia para dispositivos gerenciados usando o XClarity Administrator, é necessário fazer upgrade para o XClarity Administrator v1.3.1 ou posterior.

Servidor proxy

Se o servidor de gerenciamento não tiver acesso direto à Internet, certifique-se de que o servidor de gerenciamento esteja configurado para usar um servidor proxy HTTP (consulte Configurando o acesso à rede).

- 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.

Disponibilidade de porta

Várias portas devem estar disponíveis, dependendo de como os firewalls são implementados em seu ambiente. Se as portas necessárias estiverem bloqueadas ou forem usadas por outro processo, algumas funções do Lenovo XClarity Administrator poderão não funcionar.

Para determinar quais portas devem ser abertas com base em seu ambiente, examine as seguintes seções. As tabelas nessas seções incluem informações sobre como a cada porta é usada em XClarity Administrator, o dispositivo gerenciado que é afetado, o protocolo (TCP ou UDP) e a direção do fluxo de tráfego. O tráfego de *entrada* identifica fluxos do dispositivo gerenciado ou sistemas externos para XClarity Administrator, por isso as portas precisam ser abertas no aparelho XClarity Administrator. *Saída* tráfego flui do XClarity Administrator para o dispositivo gerenciado.

- Acesso ao servidor XClarity Administrator
- Acesso entre o XClarity Administrator e os dispositivos gerenciados
- Acesso entre XClarity Administrator e rede de dados para implantação do SO e atualizações de driver de dispositivo

Acesso ao servidor XClarity Administrator

Se o servidor XClarity Administrator e todos os dispositivos gerenciados estiverem por trás de um firewall e você planeja acessar esses dispositivos de um navegador que está fora do firewall, as portas do XClarity Administrator deverão ficar abertas. Se estiver usando SNMP e SMTP para gerenciamento de eventos,

também poderá ser necessário garantir que as portas usadas pelo servidor XClarity Administrator para o encaminhamento de eventos estejam abertas.

O servidor XClarity Administrator ouve e responde pelas portas que estão listadas na tabela a seguir.

Notas:

- XClarity Administrator é um aplicativo RESTful que se comunica com segurança por TCP na porta 443.
- O XClarity Administrator pode ser configurado para estabelecer conexões de saída com vários serviços externos, como LDAP, SMTP ou syslog. Essas conexões podem exigir portas adicionais que normalmente podem ser configuradas pelo usuário e não estão incluídas nesta lista. Essas conexões podem requerer acesso a um servidor domain name service (DNS) na porta TCP ou UDP 53 para resolver nomes de servidor externo.

Comunicação	**Dispositivo XClarity Administrator**	**Servidores de autenticação externos**	**Serviços de encaminhamento de eventos**	**Serviços Lenovo (incluindo Call Home)**
Saída (portas abertas em sistemas externos)	• DNS – TCP/UDP na porta **53**	• LDAP – TCP na porta **389**[1] • LDAPS – TCP na porta **636** • Autenticação SAML – TCP nas portas **3268, 3269**	• Servidor FTP – TCP na porta **21**[1] • Servidor de emails (SMTP) – UDP na porta **25**[1] • REST Web Service (HTTP) – UDP na porta **80**[1] • Gerenciador SNMP – UDP na porta **161**[2], **162**[1] • MS Azure – UDP na porta **443**[1] • Syslog – UDP na porta **514**[1] • Push da Apple[3] – TCP nas portas **443, 2195, 5223** • Push do Google[4] – TCP nas portas **443, 5288, 5299, 5230**	• Garantia (somente na China) – TCP na porta **83**[5] • HTTPS (Call Home) – TCP na porta **443**
Entrada (portas abertas no dispositivo XClarity Administrator)	• HTTPS – TCP na porta **443**	Não aplicável	• SNMP – UDP na porta **161**	Não aplicável

1. Esta é a porta padrão. É possível configurar essa porta na interface do usuário.
2. Essa porta é usada quando o encaminhamento de eventos SNMP com autenticação do usuário está configurado.
3. Abra essa porta quando o Wi-Fi estiver atrás de um firewall ou um Access Point Name (APN) privado para dados celulares. Uma conexão direta e sem proxy é necessária para servidores APN nessa porta. Essa porta é usada como um failback apenas por Wi-Fi quando os dispositivos não podem acessar o serviço de Notificações por Push da Apple na porta 5223. O intervalo de endereços IP é 17.0.0.0/8.

4. Para obter o intervalo de endereços IP, consulte o Google ASN 15169. O domínio é android.googleapis.com.
5. Embora não seja necessário fora da China, o XClarity Administrator pode tentar se conectar a esse serviço em outros países.

Acesso entre o XClarity Administrator e os dispositivos gerenciados

Se os dispositivos gerenciados (como nós de cálculo ou servidores de rack) estiverem atrás de um firewall e se você pretender gerenciar esses dispositivos a partir de um servidor XClarity Administrator que está fora desse firewall, você deverá garantir que todas as portas envolvidas com comunicações entre XClarity Administrator e o Baseboard Management Controller em cada dispositivo gerenciado estejam abertas.

Caso pretenda instalar sistemas operacionais nos dispositivos gerenciados usando o XClarity Administrator, certifique-se de rever a lista de portas em Acesso entre XClarity Administrator e rede de dados para implantação do SO e atualizações de driver de dispositivo.

- **Chassi Flex CMM**

Comunicação	**Chassi Flex CMMs**
Saída (portas abertas em sistemas externos)	– SLP – UDP/TCP na porta **427** – CIM HTTP – TCP na porta **5988**[2] – CIM HTTPS – TCP na porta **5989** – Comando TCP – TCP na porta **6090**[2] – Comando TCP seguro – TCP na porta **6091**
Entrada (portas abertas no dispositivo XClarity Administrator)	– SFTP – TCP na porta **22**[1] – HTTPS de indicações de CIM – TCP **9090** – LDAPS – TCP nas portas **50637**

1. Esta porta é usada para transferir atualizações de firmware usando SFTP.
2. Por padrão, o gerenciamento é executado por portas seguras. As portas não seguras são opcionais.

- **Servidores e nós de cálculo**

Comunicação	ThinkSystem e ThinkAgile	System x	Flex System	ThinkServer
Saída (portas abertas em sistemas externos)	– SFTP – TCP na porta **115** – SLP – UDP/TCP na porta **427** – HTTPS – TCP na porta **443** – Descoberta de SSDP – UDP na porta **1900** – Controle remoto – TCP na porta **3888**[4] – KVM remoto – TCP na porta**3889**[4] – CIM HTTPS – TCP na porta **5989** – Atualizações de firmware – TCP na porta **6990**[5]	– SLP – UDP/TCP na porta **427** – HTTPS – TCP na porta **443** – IPMI – TCP na porta **623** – Controle remoto – TCP na porta **3888**[4] – KVM remoto – TCP na porta **3889**[4] – CIM HTTP – TCP na porta **5988**[3] – CIM HTTPS – TCP na porta **5989**[3] – Atualizações de firmware – TCP na porta **6990**[5]	– SLP – UDP/TCP na porta **427** – Controle remoto – TCP na porta **3888**[4] – KVM remoto – TCP na porta **3889**[1, 4] – CIM HTTP – TCP na porta **5988**[3] – CIM HTTPS – TCP na porta **5989**[3] – Atualizações de firmware – TCP na porta **6990**[5]	– Traps SNMP – UDP na porta **162** – IPMI – UDP na porta **623**
Entrada (portas abertas no dispositivo XClarity Administrator)	– SFTP – TCP na porta **22**[2] – HTTPS – TCP na porta **443** – Descoberta de SSDP – UDP na porta **1900** – Atualizações de firmware – TCP na porta **6990**[5] – HTTPS de indicações de CIM – TCP **9090** – LDAPS – TCP nas portas **50636**[6]**,50637**	– SFTP – TCP na porta **22**[2] – HTTPS – TCP na porta **443** – Atualizações de firmware – TCP na porta **6990**[5] – HTTPS de indicações de CIM – TCP **9090** – LDAPS – TCP nas portas **50636**[6]**,50637**	– SFTP – TCP na porta **22**[2] – HTTPS – TCP na porta **443** – Atualizações de firmware – TCP na porta **6990**[5] – HTTPS de indicações de CIM – TCP **9090** – LDAPS – TCP nas portas **50636**[6]**,50637**	– Traps SNMP – UDP na porta **162**

1. Essa porta precisa estar aberta apenas para servidores com IMM2.
2. Esta porta é usada para transferir atualizações de firmware usando SFTP.
3. Por padrão, o gerenciamento é executado por portas seguras. As portas não seguras são opcionais.
4. O controle remoto e o KVM remoto são iniciados no navegador da Web, não no servidor XClarity Administrator.
5. Essa porta é usada para conectar-se ao SO da BMU para transferir arquivos e executar os comandos de atualização.
6. Esta porta é necessária para configurar servidores usando padrões de configuração.

- **Comutadores Flex e do rack**

Comunicação	Comutadores do rack	Comutadores Flex
Saída (portas abertas em sistemas externos)	– SSH – TCP na porta **22**[1, 3] – SNMP – UDP na porta **161**[2] – SLP – UDP/TCP na porta **427**[6] – HTTPS – TCP na porta **443**[7]	– SSH – TCP na porta **22**[3] – SNMP – UDP na porta **161**[5]
Entrada (portas abertas no dispositivo XClarity Administrator)	– SFTP – TCP na porta **22**[4] – Traps SNMP – TCP nas portas **162**[2]	– SFTP – TCP na porta **22**[4] – Traps SNMP – TCP na porta **162**[2]

1. Para comutadores do rack ENOS, essa porta é usada para configurar as credenciais do recurso Parte superior da pilha (HoS) usadas entre os comutadores CMM e Flex, ativar o slot de firmware e limpar as chaves de host SSH antes de operações de transferência de arquivos SFTP.
2. Essa porta deverá estar aberta no aparelho XClarity Administrator (entrada) quando os comutadores RackSwitch estiverem em uma rede diferente do XClarity Administrator, para que o XClarity Administrator possa receber eventos para esses dispositivos.
3. Essa porta é usada para gerenciamento (SSH).
4. Esta porta é usada para transferir atualizações de firmware usando SFTP.
5. Para comutadores de rack ENOS, essa porta é usada para transferir dados do inventário.
6. Essa porta é usada para descoberta.
7. Esta porta é usada para aplicar atualizações de firmware.

- **Dispositivos de armazenamento**

Comunicação	Dispositivos de armazenamento
Saída (portas abertas em sistemas externos)	– FTP – TCP na porta **21** – SFTP – TCP na porta **22**[2] – SLP – UDP/TCP na porta **427** – HTTPS – TCP na porta **443**[1]
Entrada (portas abertas no dispositivo XClarity Administrator)	– HTTPS – TCP na porta **443**[2] – Traps SNMP – UDP na porta **115**

1. Esta porta é usada para transferir atualizações de firmware.
2. Esta porta é usada para transferir e aplicar atualizações de firmware.

Acesso entre XClarity Administrator e rede de dados para implantação do SO e atualizações de driver de dispositivo

Comunicação	Implantação do SO[1, 2, 3]	Atualizações de drivers de dispositivo do SO[2]
Saída (portas abertas em sistemas externos)		• WinRM sobre HTTP – TCP na porta **5985**[5] • WinRM sobre HTTPS – TCP na porta **5986**[6]
Entrada (portas abertas no dispositivo XClarity Administrator)	• Comunicação SMB – TCP na porta **445**[4] • HTTPS (Exceto ThinkServer) – TCP na porta **8443**[6]	• Comunicação SMB – TCP na porta **445**[4]

1. Se você configurou o XClarity Administrator para usar uma rede de implantação do sistema operacional, as portas devem ser abertas nessa rede.
2. Para obter uma lista de portas que devem estar disponíveis para implantar sistemas operacionais, consulte Disponibilidade da porta para sistemas operacionais implantados na documentação online do XClarity Administrator. Por exemplo, se a implantação do sistema operacional estiver configurada para usar a rede de dados (eth1), essas portas deverão estar abertas nessa rede.
3. Cada instância do XClarity Administrator tem uma Autoridade de Certificação (CA) exclusiva que é usada somente para implantação do SO. Essa CA assina um certificado que é usado para o servidor de destino na porta 8443. Quando a implantação do SO é iniciada, o certificado da CA é incluído na imagem do SO que é enviada por push para o servidor de destino. Como parte do processo de implantação, esse servidor se conecta novamente à porta 8443 e verifica o certificado que essa porta fornece durante o handshake porque elas têm o certificado da CA.
4. Essa porta é usada para transferir arquivos de driver do Windows.
5. Essa porta é usada para conectar-se ao servidor de destino WinRM.
6. Essa porta é usada para trocar dados entre o SO de destino e o XClarity Administrator, incluindo imagens do SO e status.

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.

Considerações de rede

Ao planejar a instalação do Lenovo XClarity Administrator, considere a topologia de rede que é implementada em seu ambiente e como o XClarity Administrator se ajusta a essa topologia.

Importante: Configure os dispositivos e os componentes de forma a minimizar as alterações de endereço IP. Considere utilizar endereços IP estáticos em vez de Dynamic Host Configuration Protocol (DHCP). Se o DHCP for usado, certifique-se de que as alterações de endereço IP sejam minimizadas.

Limitações de configuração de IP

Para as seguintes funções e dispositivos gerenciados, interfaces de rede devem ser configuradas com um endereço IPv4. Endereços IPv6 não têm suporte.

- Atualizações de firmware para dispositivos Lenovo Storage
- Servidores ThinkServer
- Dispositivos de armazenamento Lenovo

O gerenciamento de dispositivos RackSwitch usando link IPv6 local por meio da porta de dados ou porta de gerenciamento não tem suporte.

A conversão de endereço de rede (NAT), que remapeia um espaço de endereço IP em outro, não é suportada.

Tipos de rede

Em geral, a maioria dos ambientes implementa os seguintes tipos de rede. Com base em seus requisitos, é possível implementar apenas uma dessas redes ou implementar as três.

- **Rede de gerenciamento**

A rede de gerenciamento está reservada geralmente para comunicações entre o Lenovo XClarity Administrator e os processadores de gerenciamento para dispositivos gerenciados. Por exemplo, a rede de gerenciamento pode ser configurada para incluir o XClarity Administrator, os CMMs para cada chassi gerenciado e o Baseboard Management Controller de cada servidor que o XClarity Administrator gerencia.

- **Rede de dados**

  A rede de dados é normalmente usada para comunicação entre sistemas operacionais instalados nos servidores e a intranet corporativa, a Internet ou ambos.

- **Rede de implantação do sistema operacional**

  Em alguns casos, uma rede de implantação do sistema operacional é configurada para separar as comunicações necessárias para implantar sistemas operacionais nos servidores. Se estiver implementada, essa rede geralmente inclui o XClarity Administrator e todos os hosts de servidores.

  Em vez de implementar uma rede de implantação do sistema operacional separada, você pode optar por combinar essa funcionalidade na rede de gerenciamento ou na rede de dados.

Configurações de rede

É possível configurar o Lenovo XClarity Administrator para usar uma ou duas interfaces de rede.

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.

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)

Dados únicos e rede de gerenciamento

Nesta topologia de rede, as comunicações de gerenciamento, as comunicações de dados e a implantação do sistema operacional ocorrem na mesma rede. Esta topologia é referida como uma rede *convergida*.

Importante: Implementar uma rede de gerenciamento e de dados compartilhada que inclui o chassi pode causar interrupções no tráfego, como conjuntos sendo descartados ou problemas de conectividade de rede de gerenciamento, dependendo da configuração de rede (por exemplo, tráfego de servidores com uma alta prioridade e tráfego de controladores de gerenciamento que tenham baixa prioridade). A rede de gerenciamento usa o tráfego UDP além do TCP. O tráfego UDP pode ter uma prioridade inferior quando o tráfego de rede for alto.

Quando você instalar o Lenovo XClarity Administrator, defina a interface de rede eth0 usando as seguintes considerações:

- 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.

- É possível configurar o XClarity Administrator em qualquer sistema que atenda aos requisitos do XClarity Administrator, incluindo um servidor gerenciado apenas quando implementar uma topologia de rede de gerenciamento e dados únicos ou uma topologia de rede de gerenciamento e dados separados virtualmente. No entanto, não é possível usar o XClarity Administrator para aplicar atualizações de firmware a esse servidor gerenciado. Mesmo assim, apenas alguns firmwares são aplicados com ativação imediata, e o XClarity Administrator força o servidor de destino a reiniciar, o que reinicia também o XClarity Administrator. Quando aplicado com ativação atrasada, apenas alguns firmwares são aplicados quando o host do XClarity Administrator é reiniciado.

É possível também configurar uma segunda interface de rede para se conectar à mesma rede do XClarity Administrator para oferecer suporte à redundância.

A figura a seguir mostra uma implementação de exemplo para uma topologia de rede convergida.

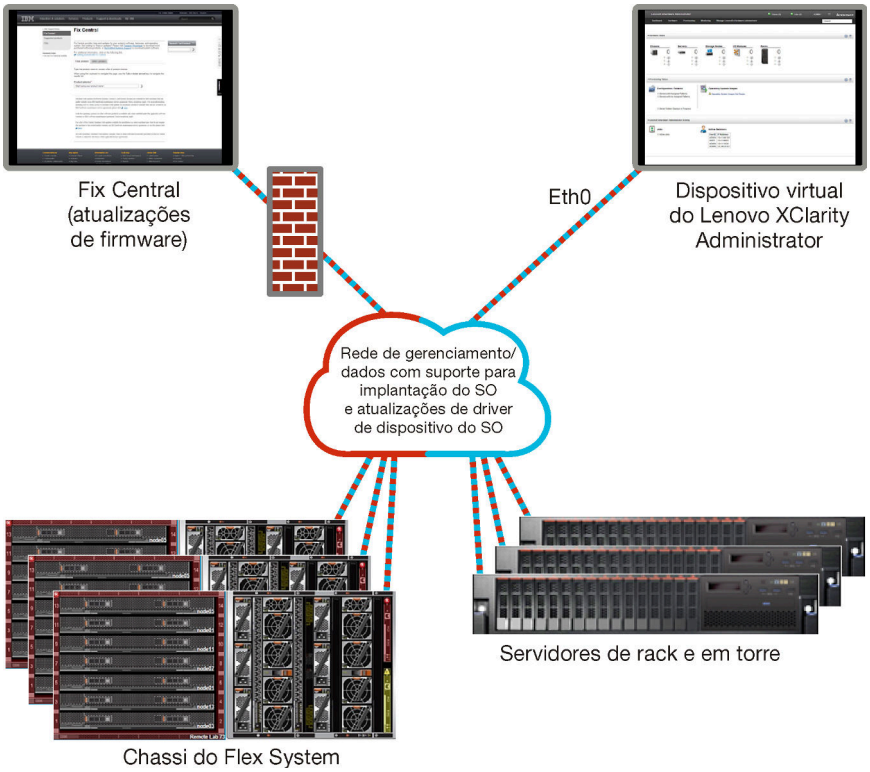


Figura 1. Implementação de exemplo de uma rede única para gerenciamento, dados e implantação do sistema operacional

Dados separados fisicamente e rede de gerenciamento

Nesta topologia de rede, a rede de gerenciamento e a rede de dados são redes fisicamente separadas, e a rede de implantação do sistema operacional é configurada como parte da rede de gerenciamento ou da rede de dados.

Quando instalar o Lenovo XClarity Administrator, defina as configurações de rede usando as seguintes considerações:

- 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.

O Figura 2 "Implementação de exemplo de redes de gerenciamento e de dados separados fisicamente com a rede de sistema operacional como parte da rede de dados" na página 25 mostra um exemplo de implementação de redes de gerenciamento e redes de dados separadas na qual a rede de implantação do sistema operacional é configurada como parte da rede de dados.

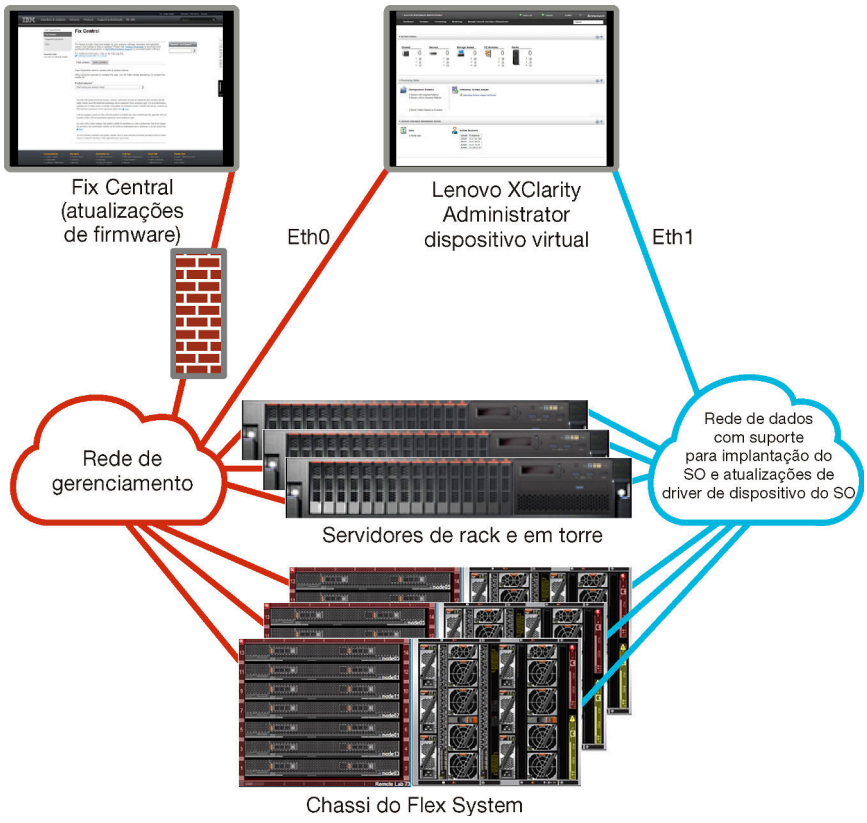


Figura 2. Implementação de exemplo de redes de gerenciamento e de dados separados fisicamente com a rede de sistema operacional como parte da rede de dados

O Figura 3 "Implementação de exemplo de redes de gerenciamento e de dados separados fisicamente com a rede de sistema operacional como parte da rede de gerenciamento" na página 26 mostra um exemplo de outra implementação de redes de gerenciamento e redes de dados separadas na qual a rede de implantação do sistema operacional é configurada como parte da rede de gerenciamento. Nessa implementação, o XClarity Administrator não precisa de conectividade com a rede de dados.

Nota: Se a rede de implantação do sistema operacional não tiver acesso à rede de dados, configure uma interface adicional nos servidores para fornecer conectividade a partir do sistema operacional do host no servidor para a rede de dados, se necessário.

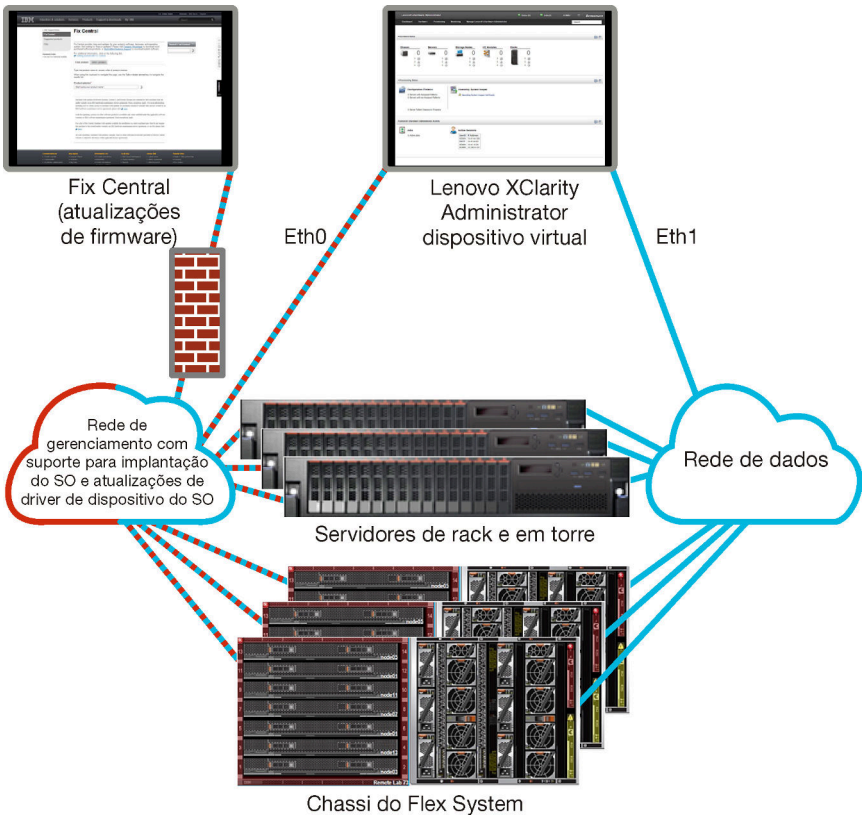


Figura 3. Implementação de exemplo de redes de gerenciamento e de dados separados fisicamente com a rede de sistema operacional como parte da rede de gerenciamento

Dados separados virtualmente e rede de gerenciamento

Nesta topologia, a rede de dados e de gerenciamento são separadas virtualmente. Os pacotes da rede de dados e os pacotes da rede de gerenciamento são enviados pela mesma conexão física. A marcação de VLAN é usada em todos os pacotes de dados da rede de gerenciamento para manter o tráfego entre duas redes separadas.

Nota: Se o Lenovo XClarity Administrator estiver instalado em um host em execução em um servidor gerenciado em um chassi, você não poderá usar o XClarity Administrator para aplicar atualizações de firmware a esse chassi inteiro de uma vez. Quando as atualizações de firmware forem aplicadas, o sistema host deverá ser reiniciado.

Quando instalar o XClarity Administrator, defina as configurações de rede usando as seguintes considerações:

- 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.
- É possível configurar o XClarity Administrator em qualquer sistema que atenda aos requisitos do XClarity Administrator, incluindo um servidor gerenciado apenas quando implementar uma topologia de rede de gerenciamento e dados únicos ou uma topologia de rede de gerenciamento e dados separados virtualmente. No entanto, não é possível usar o XClarity Administrator para aplicar atualizações de firmware a esse servidor gerenciado. Mesmo assim, apenas alguns firmwares são aplicados com ativação imediata, e o XClarity Administrator força o servidor de destino a reiniciar, o que reinicia também o XClarity Administrator. Quando aplicado com ativação atrasada, apenas alguns firmwares são aplicados quando o host do XClarity Administrator é reiniciado.

O Figura 4 "Implementação de exemplo de redes de gerenciamento e dados separados virtualmente com a rede de sistema operacional como parte da rede de dados" na página 28 mostra um exemplo de implementação de redes de gerenciamento e redes de dados separadas virtualmente na qual a rede de implantação do sistema operacional é configurada como parte da rede de dados. Neste exemplo, o XClarity Administrator está instalado em um servidor gerenciado em um chassi.

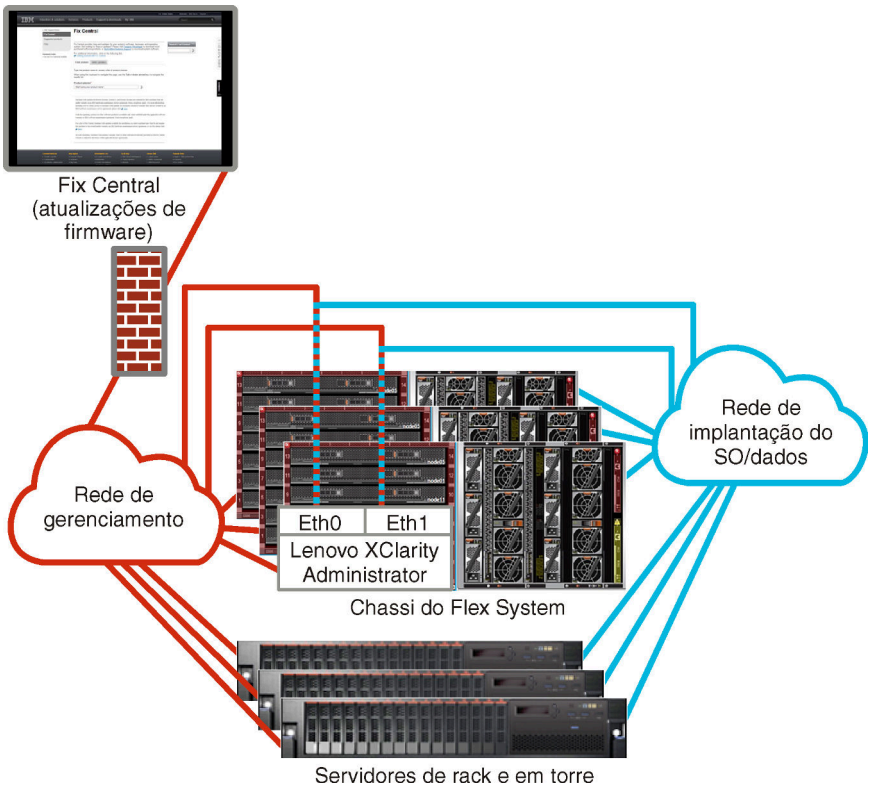


Figura 4. Implementação de exemplo de redes de gerenciamento e dados separados virtualmente com a rede de sistema operacional como parte da rede de dados

O Figura 5 "Implementação de exemplo de redes de gerenciamento e dados separados virtualmente com a rede de sistema operacional como parte da rede de gerenciamento" na página 29 mostra um exemplo de implementação de redes de gerenciamento e redes de dados separadas virtualmente na qual a rede de implantação do sistema operacional é configurada como parte da rede de gerenciamento, e o XClarity Administrator é instalado em um servidor gerenciado em um chassi. Nessa implementação, o XClarity Administrator não precisa de conectividade com a rede de dados.

Nota: Se a rede de implantação do sistema operacional não tiver acesso à rede de dados, configure uma interface adicional nos servidores para fornecer conectividade a partir do sistema operacional do host no servidor para a rede de dados, se necessário.

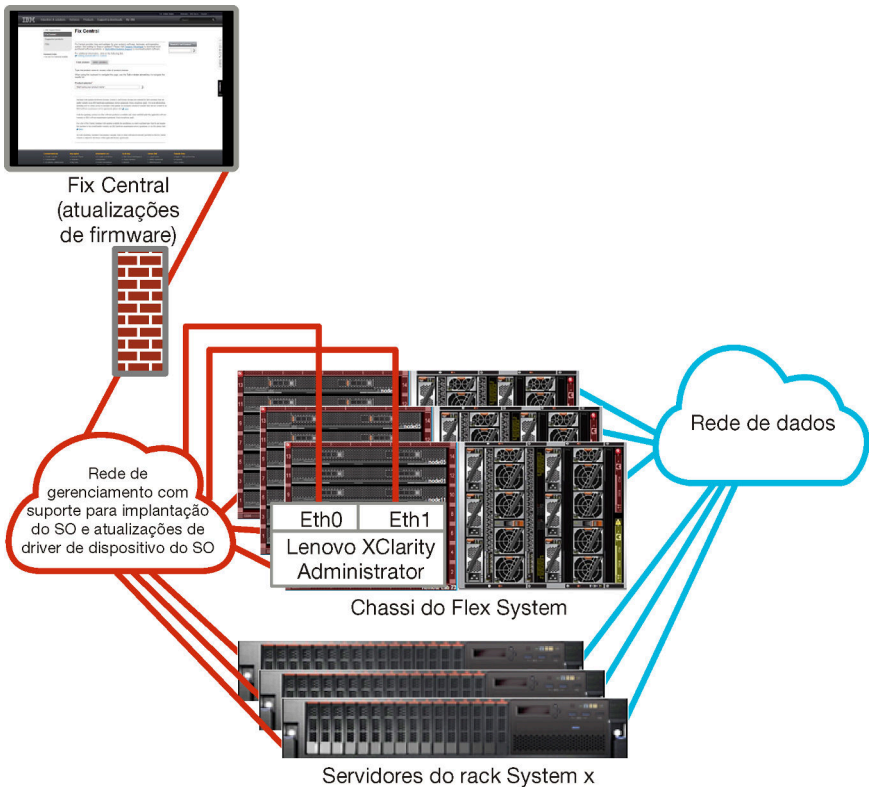


Figura 5. Implementação de exemplo de redes de gerenciamento e dados separados virtualmente com a rede de sistema operacional como parte da rede de gerenciamento

Rede somente de gerenciamento

Nessa topologia, o Lenovo XClarity Administrator tem acesso apenas à rede de gerenciamento. Ele não tem acesso à rede de dados. Entretanto, o XClarity Administrator deve ter acesso à rede de implantação do sistema operacional se você pretende implantar imagens de sistema operacional do XClarity Administrator em servidores gerenciados.

Quando você instalar XClarity Administrator e definir as configurações de rede, a interface de rede eth0 deverá ser configurada para:

- 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.

É possível também configurar uma segunda interface de rede para se conectar à mesma rede do XClarity Administrator para oferecer suporte à redundância.

O Figura 6 "Implementação de exemplo de uma rede somente de gerenciamento sem suporte para implantação do sistema operacional." na página 30 mostra uma implementação de exemplo para uma rede somente de gerenciamento na qual a implantação do sistema operacional do XClarity Administrator não tem suporte.

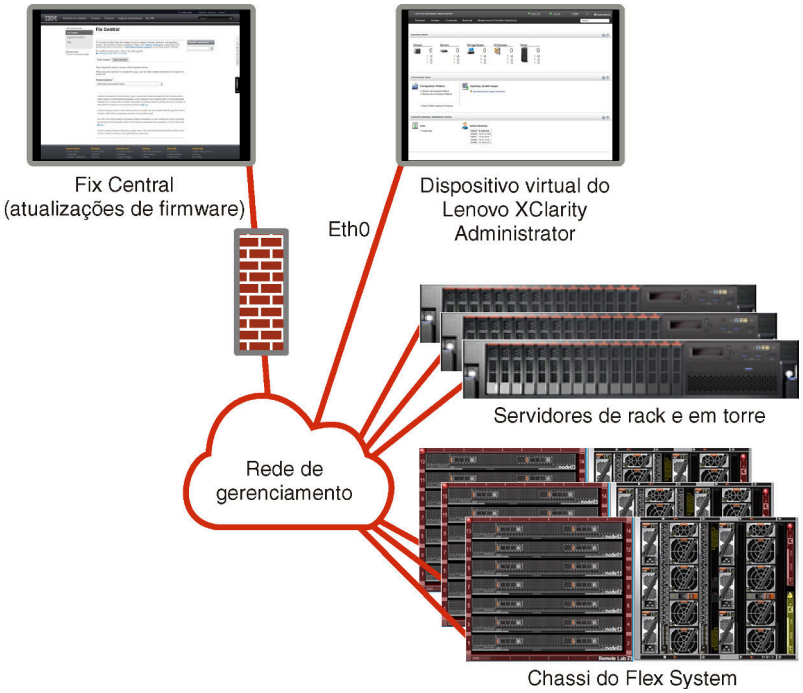


Figura 6. Implementação de exemplo de uma rede somente de gerenciamento sem suporte para implantação do sistema operacional.

O Figura 6 "Implementação de exemplo de uma rede somente de gerenciamento sem suporte para implantação do sistema operacional." na página 30 mostra uma implementação de exemplo de uma rede somente de gerenciamento na qual a implantação do sistema operacional do XClarity Administrator tem suporte.

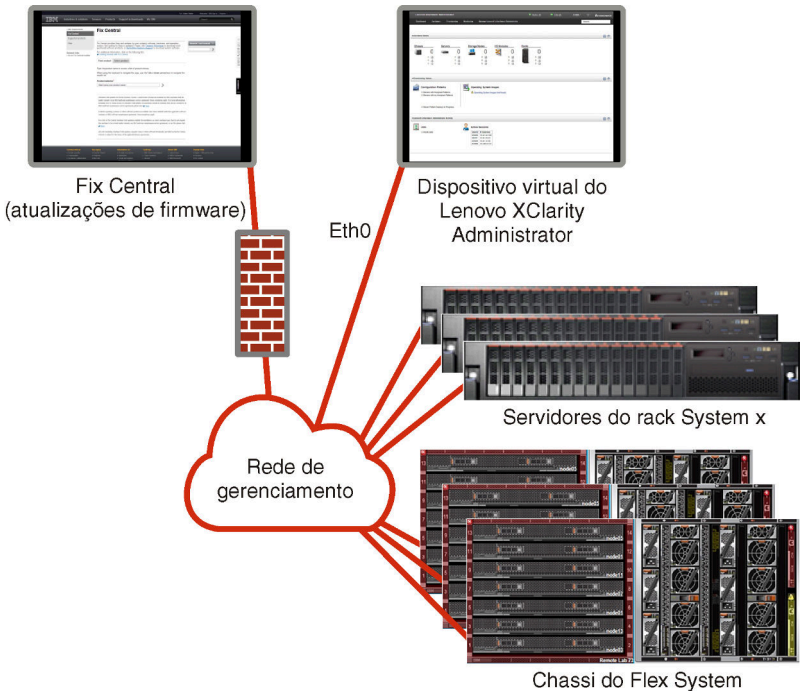


Figura 7. Implementação de exemplo de uma rede somente de gerenciamento com suporte para implantação do sistema operacional.

Considerações sobre segurança

Plano de segurança do Lenovo XClarity Administrator e de todos os dispositivos gerenciados.

Gerenciamento de 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.

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 Recuperando o gerenciamento de chassi com um CMM após uma falha no servidor de gerenciamento e Recuperando o gerenciamento do servidor em torre ou do rack após uma falha no servidor de gerenciamento na documentação online do XClarity Administrator.

Notas:

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

- 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.

Para obter mais informações sobre o encapsulamento, consulte Habilitando o encapsulamento na documentação online do XClarity Administrator.

Gerenciamento de criptografia

O gerenciamento de criptografia é composto por modos e protocolos de comunicação que controlam a maneira como a comunicação segura é manipulada entre o Lenovo XClarity Administrator e os dispositivos gerenciados (como chassis, servidores e comutadores Flex).

Algoritmos criptográficos

O XClarity Administrator oferece suporte a TLS 1.2 e algoritmos criptográficos mais fortes para conexões de rede seguras.

Para aumentar a segurança, apenas criptografias extremamente fortes são suportadas. Os sistemas operacionais cliente e os navegadores da Web devem oferecer suporte a um dos pacotes de criptografia a seguir.
- SSH-ED25519
- SSH-ED25519-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP256
- ECDSA-SHA2-NISTP256-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP384
- ECDSA-SHA2-NISTP384-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP521
- ECDSA-SHA2-NISTP521-CERT-V01@OPENSSH.COM
- RSA-SHA2-512
- RSA-SHA2-256
- RSA-SHA2-384

Modos criptográficos do servidor de gerenciamento

Essa configuração determina o modo a ser usado para comunicações seguras do servidor de gerenciamento.

- **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 na documentação online do XClarity Administrator). 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 800-131A na documentação online do XClarity Administrator.

Para obter mais informações sobre a configuração dos modos de segurança no servidor de gerenciamento, consulte Configurando o modo de criptografia e protocolos de comunicação na documentação online do XClarity Administrator.

Modos de segurança para os servidores gerenciados

Essa configuração determina o modo a ser usado para comunicações seguras dos servidores gerenciados.

- **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.

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

Para obter mais informações sobre a configuração dos modos de segurança no servidor gerenciado, consulte Definindo as configurações de segurança de um servidor na documentação online do XClarity Administrator.

Certificados de segurança

O 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.

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.

Para obter mais informações sobre certificados, consulte Trabalhando com certificados de segurança na documentação online do XClarity Administrator.

Autenticação

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.

Para obter mais informações sobre servidores de autenticação, consulte Gerenciando o servidor de autenticação na documentação online do XClarity Administrator.

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 Gerenciando servidores na documentação online do XClarity Administrator).

    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 do usuário 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 de chassi com um CMM após uma falha no servidor de gerenciamento e Recuperando o gerenciamento do servidor em torre ou do rack após uma falha no servidor de gerenciamento na documentação online do XClarity Administrator.

Contas do usuário e grupos de função

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

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.

Para obter mais informações sobre contas do usuários e grupos de função, consulte Gerenciando contas de usuário na documentação online do XClarity Administrator.

Segurança da conta do usuário

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

Para obter mais informações sobre configurações de segurança da conta, consulte Alterando as configurações de segurança de conta do usuário na documentação online do Lenovo XClarity Administrator.

Considerações sobre alta disponibilidade

Para configurar a alta disponibilidade para o Lenovo XClarity Administrator, use recursos de alta disponibilidade que façam parte do sistema operacional do host ou do ambiente de contêiner.

Docker

É possível usar o Docker Datacenter para configurar um ambiente de alta disponibilidade para contêineres do XClarity Administrator em execução no Docker Engine. Para obter mais informações sobre a alta disponibilidade do Docker Datacenter, consulte Página da Web Arquitetura e aplicativos de alta disponibilidade com o Docker Datacenter.

Citrix

Use a função de alta disponibilidade fornecida para o ambiente Citrix. Para obter mais informações, consulte Implementando alta disponibilidade (Citrix) na documentação online do XClarity Administrator.

KVM (CentOS, RedHat e Ubuntu)

É possível usar o OpenStack, ou se você já tiver um ambiente de alta disponibilidade, continue usando seus processos internos. Para obter mais informações sobre a alta disponibilidade do OpenStack, consulte Implementando alta disponibilidade (KVM) na documentação online do XClarity Administrator.

Microsoft Hyper-V

Use a função de alta disponibilidade fornecida para o ambiente ESXi. Para obter informações, consulte Implementando alta disponibilidade (Microsoft Hyper-V) na documentação online do XClarity Administrator.

Nutanix AHV

use a função de alta disponibilidade da máquina virtual fornecida para o ambiente Nutanix AHV. Para obter mais informações, consulte Implementando alta disponibilidade (Nutanix) na documentação online do XClarity Administrator.

VMware ESXi

Em um ambiente de alta disponibilidade VMware, diversos hosts são configurados como um cluster. O armazenamento compartilhado é usado para disponibilizar a imagem de disco de uma máquina virtual (VM) para os hosts no cluster. A VM é executada apenas em um host de cada vez. Quando há um problema com a VM, outra instância dessa VM é iniciada em um host de backup.

O VMware High Availability requer os seguintes componentes:

- No mínimo, dois hosts nos quais o ESXi esteja instalado. Esses hosts se tornam parte do cluster VMware.
- Um terceiro host no qual o VMware vCenter esteja instalado.

  Dica: Instale uma versão do VMware vCenter que seja compatível com as versões do ESXi instaladas nos hosts que serão usados no cluster.

  O VMware vCenter pode ser instalado em um dos hosts usados no cluster. Entretanto, se esse host estiver desligado ou não puder ser usado, você também perderá acesso à interface VMware vCenter.
- O armazenamento compartilhado (datastores) que pode ser acessado por todos os hosts no cluster. É possível usar qualquer tipo de armazenamento compartilhado ao qual o VMware ofereça suporte. O datastore é usado pela VMware para determinar se será necessário efetuar failover de uma VM em outro host (pulsação).

Para obter detalhes sobre como configurar um cluster do VMware High Availability, consulte Implementando alta disponibilidade (VMware ESXi) na documentação online do XClarity Administrator.

Features on Demand

O Features on Demand ativa recursos sem requerer a instalação de hardware nem a compra de novo equipamento. Essa ativação é feita adquirindo e instalando a chave Features on Demand correspondente.

Para usar as operações de controle remoto ou implantação de sistema operacional no Lenovo XClarity Administrator, você deve habilitar o nível XClarity Controller Enterprise ou a Atualização Avançada do MM para servidores que não são fornecidos com esses recursos já ativados por padrão. Essas operações também requerem que uma chave Features on Demand para presença remota seja instalada nos servidores ThinkSystem, Converged e System x. 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 na documentação online do XClarity Administrator).

Algumas funções avançadas do servidor são ativadas usando chaves Features on Demand. Se os recursos tiverem definições configuráveis expostas durante a configuração do UEFI, você poderá definir a configuração usando Padrões de Configuração. No entanto, a configuração resultante não será ativada até que a chave Features on Demand correspondente seja instalada.

Nota: Não é possível instalar nem gerenciar chaves Features on Demand de XClarity Administrator; entretanto, você poderá exibir a lista de chaves Features on Demand instaladas atualmente em servidores gerenciados. Para obter mais informações sobre como exibir chaves Features on Demand instaladas, consulte Visualizando chaves do Feature on Demand na documentação online do XClarity Administrator.

Para adquirir e instalar chaves Features on Demand:

1. Compre a atualização do Features on Demand usando o número de peça apropriado.

Você pode adquirir chaves do Portal da web Features on Demand. Quando sua compra estiver concluída, você receberá um código de autorização por e-mail.

2. No Portal da web Features on Demand, insira o código de autorização recebido, juntamente com o identificador exclusivo do servidor que você planeja atualizar.
3. Baixe a chave de ativação no formato de um arquivo .KEY.
4. Faça upload da chave de ativação no controlador de gerenciamento do servidor.
5. Reinicie o servidor. Quando a reinicialização for concluída, o recurso será ativado.

Para obter mais informações sobre chaves Features on Demand, consulte Usando o Lenovo Features on Demand.

Capítulo 3. Instalando o Lenovo XClarity Administrator

Há algumas maneiras diferentes de conectar dispositivos gerenciáveis à rede e configurar o dispositivo virtual Lenovo XClarity Administrator para gerenciar esses dispositivos. Use as informações nesta seção como guia para configurar dispositivos gerenciáveis e instalar o XClarity Administrator

Esta seção descreve como configurar várias topologias comuns. Esta seção não abrange todas as topologias de rede possíveis.

Atenção: Para gerenciar dispositivos, o XClarity Administrator deve ter acesso à rede de gerenciamento.

Saiba mais:

- Instalando o Lenovo XClarity Administrator no VMware vCenter
- Instalando o Lenovo XClarity Administrator no VMware vSphere
- Instalando o Lenovo XClarity Administrator no Windows Hyper-V
- Instalando o Lenovo XClarity Administrator no Red Hat KVM

Dados únicos e rede de gerenciamento

Nesta topologia de rede, as redes de dados e de gerenciamento são a mesma rede.

Antes de iniciar

Verifique se todas as portas apropriadas estão ativadas, incluindo as portas necessárias para XClarity Administrator (consulte Disponibilidade de porta).

Verifique se o firmware mínimo necessário está instalado em cada dispositivo 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: Configure os dispositivos e os componentes de forma a minimizar as alterações de endereço IP. Considere utilizar endereços IP estáticos em vez de Dynamic Host Configuration Protocol (DHCP). Se o DHCP for usado, certifique-se de que as alterações de endereço IP sejam minimizadas.

Sobre esta tarefa

Para dispositivos virtuais, toda a comunicação entre o XClarity Administrator e a rede ocorre na interface de rede eth0 no host. Para contêineres, é possível usar um nome personalizado; entretanto, esse cenário usa eth0.

Importante: Implementar uma rede de gerenciamento e de dados compartilhada que inclui o chassi pode causar interrupções no tráfego, como conjuntos sendo descartados ou problemas de conectividade de rede de gerenciamento, dependendo da configuração de rede (por exemplo, tráfego de servidores com uma alta prioridade e tráfego de controladores de gerenciamento que tenham baixa prioridade). A rede de gerenciamento usa o tráfego UDP além do TCP. O tráfego UDP pode ter uma prioridade inferior quando o tráfego de rede for alto.

A figura a seguir ilustra uma maneira de configurar seu ambiente caso a rede de dados e a rede de gerenciamento sejam a mesma rede. Os números na figura correspondem às etapas numeradas nas próximas seções.

Nota: Esta figura não descreve as opções de cabeamento que podem ser necessárias para seu ambiente. Esta figura mostra apenas os requisitos de opção de cabeamento para servidores de rack, comutadores de rack, comutadores Flex e CMMs, pois eles estão relacionados à configuração de uma rede de gerenciamento/dados únicos.

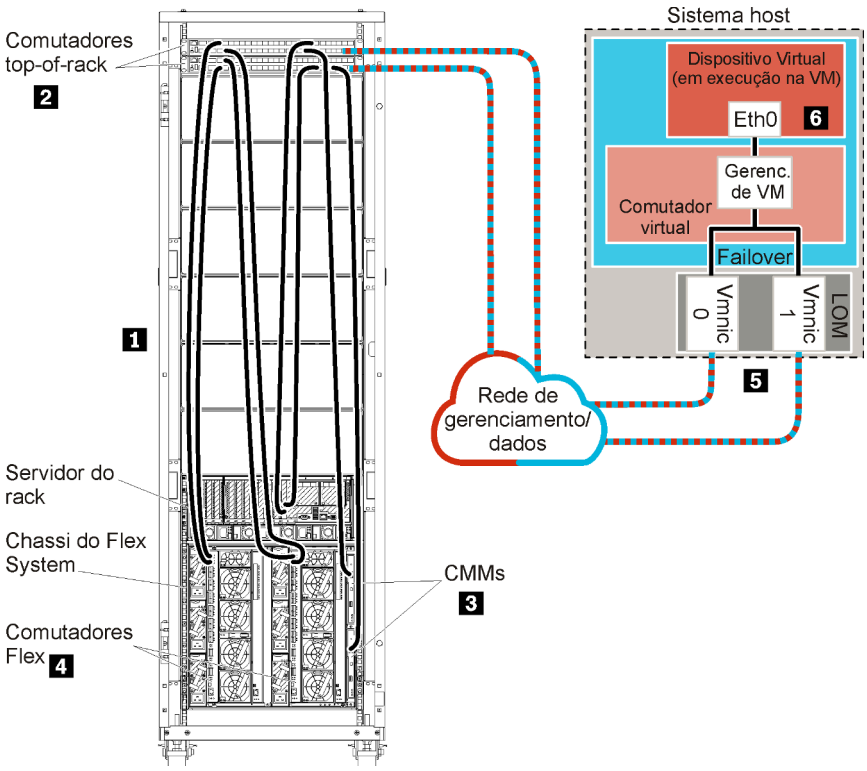


Figura 8. Exemplo de topologia de rede de gerenciamento e dados únicos para um dispositivo virtual

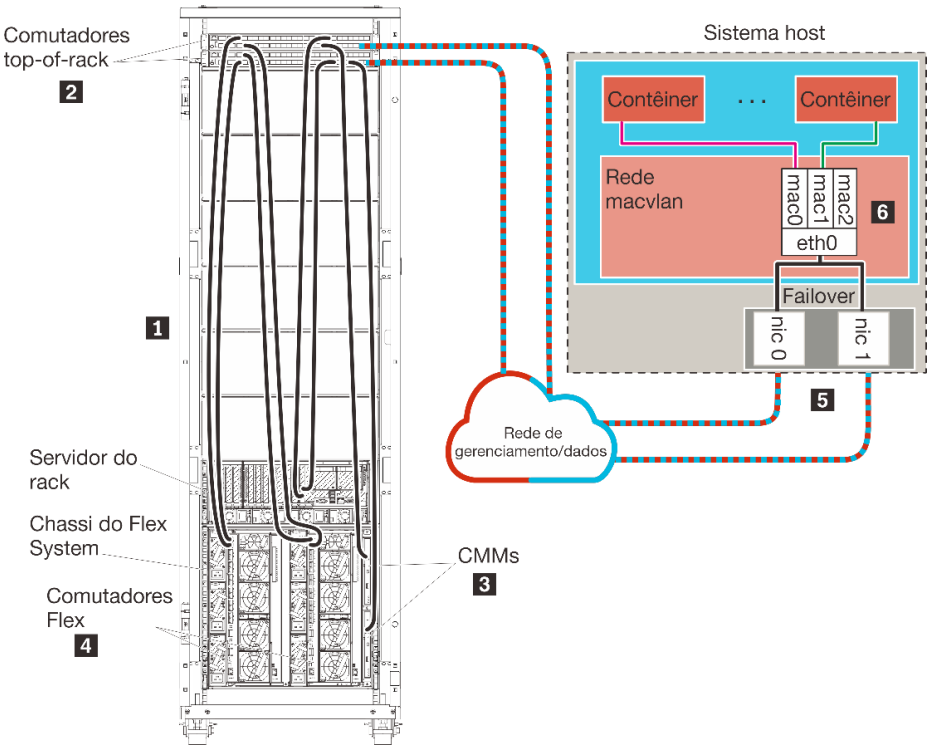


Figura 9. Exemplo de topologia de rede de gerenciamento e dados únicos para contêineres

Importante: É possível configurar o XClarity Administrator em qualquer sistema que atenda aos requisitos para XClarity Administrator, incluindo um servidor gerenciado. Se você usa um servidor gerenciado para o host do XClarity Administrator:

- Deve implementar uma topologia de rede de gerenciamento e dados separados virtualmente ou uma topologia de rede de gerenciamento e dados únicos.
- Não pode usar XClarity Administrator para aplicar atualizações de firmware a esse servidor gerenciado. Mesmo quando apenas alguns firmwares são aplicados com ativação imediata, o XClarity Administrator força o servidor de destino a reiniciar, o que reinicia também o XClarity Administrator. Quando aplicado com ativação adiada, apenas alguns firmwares são aplicados quando o host do XClarity Administrator é reiniciado.
- Se você usar um servidor em um chassi do Flex System, garanta que o servidor esteja configurado para ligar automaticamente. É possível definir essa opção na interface da Web do CMM clicando em **Gerenciamento de Chassi → Nós de Cálculo**, selecionando o servidor e **Ativação Automática** para o **Modo de Ativação Automática**.

Caso pretenda instalar o XClarity Administrator para gerenciar o chassi existente e os servidores de rack que já foram configurados, vá para Etapa 5: Instalar e configurar o host.

Para obter informações adicionais sobre o planejamento dessa topologia, incluindo informações sobre configurações de rede e configuração de Eth0 e Eth1, consulte Dados únicos e rede de gerenciamento.

Etapa 1: Passe o cabo do chassi, dos servidores de rack e do host do Lenovo XClarity Administrator nos comutadores top-of-rack

Conecte o chassi, os servidores de rack e o host do XClarity Administrator aos comutadores top-of-rack para ativar a comunicação entre os dispositivos e a rede.

Procedimento

Conecte cada comutador Flex e CMM em cada chassi, cada servidor de rack e no host do XClarity Administrator aos dois comutadores top-of-rack. É possível escolher qualquer porta nos comutadores top-of-rack.

A figura a seguir é um exemplo que ilustra o cabeamento do chassi (Comutadores Flex e CMMs), servidores de rack e host do XClarity Administrator para comutadores top-of-rack.

Nota: Esta figura não descreve as opções de cabeamento que podem ser necessárias para seu ambiente. Esta figura mostra apenas os requisitos de opção de cabeamento para servidores de rack, comutadores de rack, comutadores Flex e CMMs, pois eles estão relacionados à configuração de uma rede de gerenciamento/dados únicos.

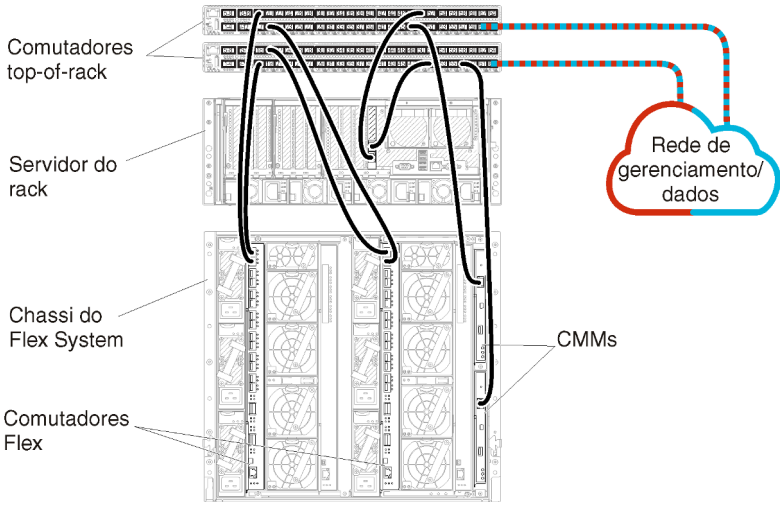


Figura 10. Exemplo de cabeamento de uma rede de gerenciamento e de dados únicos

Etapa 2: Configurar comutadores top-of-rack

Configure os comutadores top-of-rack.

Antes de iniciar

Além dos requisitos de configuração típicos para comutadores top-of-rack, verifique se todas as portas apropriadas estão ativadas, incluindo portas externas ao Comutadores Flex, servidores de rack e rede, e portas internas ao CMM, servidores de rack e rede.

Procedimento

As etapas de configuração podem variar, dependendo do tipo de comutador de rack instalado.

Para obter informações sobre como configurar comutadores top-of-rack da Lenovo, consulte Comutadores de rack na documentação online do System x. Se outro comutador top-of-rack estiver instalado, consulte a documentação fornecida com esse comutador.

Etapa 3: Configurar Chassis Management Modules (CMMs)

Configure o Chassis Management Module (CMM) primário no chassi para gerenciar todos os dispositivos no chassi.

Sobre esta tarefa

Para obter informações detalhadas sobre como configurar um CMM, consulte Configurando componentes do chassi na documentação online do Flex System.

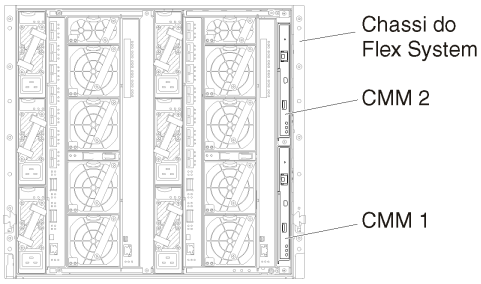
Além disso, consulte as etapas 4.1 a 4.5 do pôster de instrução fornecido com o chassi.

Procedimento

Conclua as etapas a seguir para configurar o CMM.

Se dois CMMs estiverem instalados, configure apenas o CMM *primário*, que sincroniza automaticamente a configuração com o CMM de espera.

Etapa 1. Conecte um cabo Ethernet do CMM no compartimento 1 a uma estação de trabalho do cliente para criar uma conexão direta.



Para conectar-se ao CMM pela primeira vez, talvez seja necessário alterar as propriedades de Internet Protocol na estação de trabalho do cliente.

Importante: Verifique se a sub-rede da estação de trabalho do cliente é a mesma sub-rede do CMM. A sub-rede dos CMM padrão é 255.255.255.0. O endereço IP escolhido para a estação de trabalho do cliente deve estar na mesma rede do CMM (por exemplo, 192.168.70.0 a 192.168.70.24).

Etapa 2. Para iniciar a interface de gerenciamento do CMM, abra um navegador da Web na estação de trabalho do cliente e direcione-o ao endereço IP do CMM.

Notas:

- Certifique-se de usar uma conexão segura e inclua **https** no URL (por exemplo, https://192.168.70.100). Se você não incluir https, receberá um erro de página não encontrada.
- Se você usar o endereço IP padrão 192.168.70.100, a interface de gerenciamento do CMM poderá levar alguns minutos para estar disponível. Esse atraso ocorre porque o CMM tenta obter um endereço DHCP por dois minutos antes de voltar para o endereço estático padrão.

Etapa 3. Faça login na interface de gerenciamento do CMM usando o ID do usuário padrão `USERID` e a senha `PASSWORD`. Depois de fazer login, você deve alterar a senha padrão.

Etapa 4. Conclua o Assistente de Configuração Inicial do CMM para especificar os detalhes do seu ambiente. O Assistente de Configuração Inicial inclui as seguintes opções:

- Veja o inventário e a integridade do chassi.
- Importe a configuração de um arquivo de configuração existente.
- Defina as configurações gerais do CMM.
- Configure data e hora do CMM.

Dica: Ao instalar o XClarity Administrator, configure XClarity Administrator e todos os chassis gerenciados pelo XClarity Administrator para um servidor NTP.

- Configure as informações de IP do CMM.
- Configure a política de segurança do CMM.
- Configure o Sistema de Nomes de Domínio (DNS).
- Configure os encaminhadores de eventos.

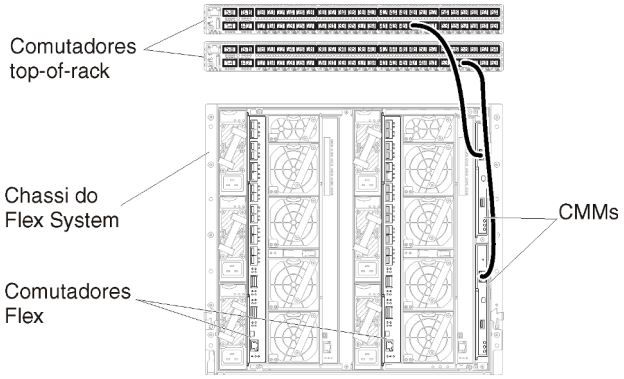
Etapa 5. Após salvar as configurações do assistente de configuração e aplicar as alterações, configure os endereços IP de todos os componentes no chassi.

Consulte a etapa 4.6 do pôster de instrução fornecido com o chassi.

Nota: Você deve redefinir o processador de gerenciamento de sistemas para cada nó de cálculo e reiniciar os comutadores Flex para mostrar os novos endereços IP.

Etapa 6. Reinicie o CMM usando a interface de gerenciamento do CMM.

Etapa 7. Durante a reinicialização do CMM, conecte um cabo da porta Ethernet no CMM à rede.



Etapa 8. Faça login na interface de gerenciamento do CMM usando o novo endereço IP.

Depois de concluir

Também é possível configurar o CMM para suportar redundância. Use o sistema de ajuda do CMM para saber mais sobre os campos disponíveis em cada uma das seguintes páginas.

- Configure o failover para o CMM se houver uma falha de hardware no CMM primário. Na interface de gerenciamento do CMM, clique em **Gerenciamento do Módulo de Gerenciamento → Propriedades → Failover Avançado**.
- Configure o failover em resultado de um problema de rede (uplink). Na interface de gerenciamento do CMM, clique em **Gerenciamento do Módulo de Gerenciamento → Rede**, clique na guia **Ethernet** e, em seguida, em **Ethernet Avançada**. No mínimo, selecione **Failover em caso de perda de link de rede física**.

Etapa 4: Configurar o Comutadores Flex

Configure Comutadores Flex (módulos de E/S) em cada chassi.

Antes de iniciar

Verifique se todas as portas apropriadas estão ativadas, incluindo portas externas do comutador Flex ao comutador top-of-rack e portas internas no CMM.

Se os comutadores Flex estiverem configurados para obter configurações de rede dinâmicas (endereço IP, gateway e endereço DNS) via DHCP, garanta que os comutadores Flex tenham configurações consistentes (por exemplo, verifique se os endereços IP estão na mesma sub-rede que o CMM).

Importante: Para cada chassi do Flex System, verifique se o tipo de malha da placa de expansão em cada servidor no chassi é compatível com o tipo de malha de todos os comutadores Flex no mesmo chassi. Por exemplo, se os comutadores Ethernet estiverem instalados em um chassi, todos os servidores desse chassi deverão ter conectividade Ethernet por meio do conector LAN na placa-mãe ou uma placa de expansão Ethernet. Para obter mais informações sobre como configurar comutadores Flex, consulte Configurando módulos de E/S na documentação online do Flex Systems.

Procedimento

As etapas de configuração podem variar, dependendo do tipo de Comutadores Flex instalado. Para obter mais informações sobre cada Comutadores Flex compatível, consulte Comutadores de rede do Flex System na documentação online do Flex Systems.

Normalmente, é necessário configurar os comutadores Flex nos compartimentos 1 e 2 de comutador Flex.

Dica: O compartimento 2 do comutador Flex é o terceiro compartimento do módulo olhando da traseira do chassi.

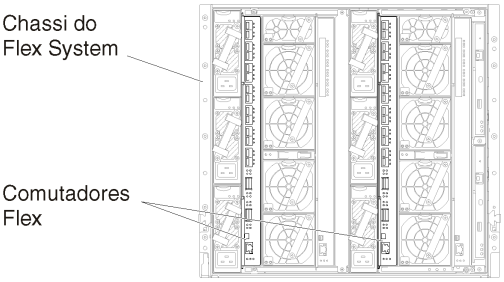


Figura 11. Locais de Comutador Flex em um chassi

Etapa 5: Instalar e configurar o host

É possível instalar o Docker em qualquer servidor que atenda aos requisitos para o Lenovo XClarity Administrator.

Antes de iniciar

É possível usar o Docker Datacenter para configurar um ambiente de alta disponibilidade para contêineres do XClarity Administrator em execução no Docker Engine. Para obter mais informações sobre a alta disponibilidade do Docker Datacenter, consulte Página da Web Arquitetura e aplicativos de alta disponibilidade com o Docker Datacenter.

Verifique se o host satisfaz os pré-requisitos definidos em Pré-requisitos de hardware e software.

Verifique se o sistema do host está na mesma rede que os dispositivos que deseja gerenciar.

Importante: É possível configurar o XClarity Administrator em qualquer sistema que atenda aos requisitos para XClarity Administrator, incluindo um servidor gerenciado. Se você usa um servidor gerenciado para o host do XClarity Administrator:

- Deve implementar uma topologia de rede de gerenciamento e dados separados virtualmente ou uma topologia de rede de gerenciamento e dados únicos.

- Não pode usar XClarity Administrator para aplicar atualizações de firmware a esse servidor gerenciado. Mesmo quando apenas alguns firmwares são aplicados com ativação imediata, o XClarity Administrator força o servidor de destino a reiniciar, o que reinicia também o XClarity Administrator. Quando aplicado com ativação adiada, apenas alguns firmwares são aplicados quando o host do XClarity Administrator é reiniciado.
- Se você usar um servidor em um chassi do Flex System, garanta que o servidor esteja configurado para ligar automaticamente. É possível definir essa opção na interface da Web do CMM clicando em **Gerenciamento de Chassi → Nós de Cálculo**, selecionando o servidor e **Ativação Automática** para o **Modo de Ativação Automática**.

Procedimento

Instale e configure o Docker no host usando as instruções que são fornecidas com a distribuição do Docker.

Etapa 6. Instalar e configurar um XClarity Administrator

Instale e configure o contêiner do Lenovo XClarity Administrator no host do Docker que acabou de ser instalado.

Antes de iniciar

O sistema host físico deve atender aos requisitos mínimos de hardware e software (consulte Pré-requisitos de hardware e software).

Verifique se todas as portas apropriadas estão ativadas, incluindo portas exigidas pelo XClarity Administrator (consulte Disponibilidade de porta).

Verifique se o sistema do host está na mesma rede que os dispositivos que deseja gerenciar.

Verifique se o SO do host e o XClarity Administrator usam o mesmo servidor NTP.

O XClarity Administrator permite que um nome personalizado da rede seja usado para gerenciamento de dados, gerenciamento de hardware e implantação do SO (consulte Configurações de rede). Este exemplo no procedimento a seguir usa eth0.

Verifique se uma rede macvlan está carregada no kernel no sistema host. Para verificar se ela está carregada, use o comando **lsmod | grep macvlan**. Para carregar a macvlan no kernel, execute o comando **modprobe macvlan**.

Use um nome exclusivo e endereço IP para cada contêiner ao executar vários contêineres do XClarity Administrator no mesmo host.

Se você pretende gerenciar o ThinkServer e outros dispositivos legados, o Docker deve estar habilitado para dar suporte ao IPv6.

1. Edite o arquivo /etc/docker/daemon.json, defina a chave **ipv6** como true e defina a chave **fixed-cidr-v6** como sua sub-rede IPv6. Veja a seguir um exemplo de arquivo daemon.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Recarregue o arquivo de configuração do Docker executando o comando a seguir.
```
systemctl reload docker
```

Nota: O XClarity Administrator *não é* executado como um contêiner privilegiado.

Procedimento

Para instalar um contêiner do XClarity Administrator usando a composição do Docker, conclua as etapas a seguir.

Etapa 1. Baixe a imagem do dispositivo virtual do XClarity Administrator, o arquivo de ambiente e o arquivo YAML do Página da Web de download do XClarity Administrator para uma estação de trabalho do cliente. Faça login no Web site e, em seguida, use a tecla de acesso que foi fornecida para baixar a imagem.

Etapa 2. Importe a imagem de contêiner do XClarity Administrator para seu host do docker executando o comando a seguir.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Etapa 3. Edite o arquivo `docker_compose.env` e atualize as variáveis de ambiente a seguir.

- **CONTAINER_NAME**. Nome exclusivo do contêiner, usado para criar volumes de docker para cada instância do XClarity Administrator (por exemplo, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Endereço estático IPv4 para o contêiner (por exemplo, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Opcional) Caminho para o compartilhamento remoto que pode ser usado para armazenar backups do XClarity Administrator. Deve ser `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Opcional) Caminho para o compartilhamento remoto que pode ser usado como um repositório remoto para atualizações de firmware. Deve ser `/mnt/fw_share`.

Veja a seguir um exemplo de arquivo de ambiente.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Etapa 4. Edite o `docker_compose.yml` e atualize as propriedades a seguir.

- Defina a propriedade **image** como o nome do arquivo de imagem de instalação usado na etapa 2.

  Nota: É possível alterar o nome do arquivo de imagem (por exemplo, para "mais recente") usando o comando `docker tag`.
- Se você deseja usar compartilhamentos remotos como um repositório de firmware remoto e armazenar backups do XClarity Administrator, defina o ponto de montagem do host para cada compartilhamento remoto na propriedade **volumes**.
- Defina a propriedade **dns** como o endereço IP dos servidores DNS.
- O contêiner compartilha o conjunto de recursos de processador e memória que estão disponíveis para o host. Opcionalmente, defina limites de uso de recurso configurando as propriedades **cpus** e **memória**.
- Defina a propriedade **parent** como o nome da interface de rede no sistema host que deve ser usada como a interface pai para a interface macvlan no contêiner. Essa interface deve ter acesso direto à sub-rede atribuída ao contêiner.
- Defina a **sub-rede** e o **gateway** de acordo com a topologia de rede. Normalmente, a sub-rede e o gateway se destinam à rede de gerenciamento, à qual pertence o ${ADDRESS}.
- Se você deseja dar suporte ao IPv6, defina a propriedade **enable_ipv6** como true, defina a propriedade **ipv6_address** como o endereço IPv6 e adicione outro conjunto de propriedades de **sub-rede** e **gateway** de acordo com sua topologia de rede (geralmente para rede de gerenciamento à qual o endereço IPv6 pertence).

Nota: O XClarity Administrator usa macvlan para configurar a rede de contêineres. Para obter mais informações, consulte o Usar a página da Web de redes macvlan

Veja a seguir um arquivo YML de exemplo, com IPv6 habilitado.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat
```

```
networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
```

Etapa 5. Implante a imagem no docker executando o comando a seguir, em que <*ENV_FILENAME*> é o nome do arquivo de variáveis do ambiente criado na etapa 2.
COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file` <*ENV_FILENAME*> `up -d`

Depois de concluir

Faça login e configure o XClarity Administrator (consulte Acessando a interface da Web do Lenovo XClarity Administrator pela primeira vez e Configurando Lenovo XClarity Administrator).

Redes de gerenciamento e dados separados fisicamente

Nesta topologia, as redes de dados e de gerenciamento são separadas fisicamente. A comunicação de gerenciamento entre Lenovo XClarity Administrator e a rede ocorre na interface de rede Eth0 no host. A comunicação de dados ocorre na interface de rede Eth1.

Antes de iniciar

Verifique se todas as portas apropriadas estão ativadas, incluindo as portas necessárias para XClarity Administrator (consulte Disponibilidade de porta).

Verifique se o firmware mínimo necessário está instalado em cada dispositivo 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: Configure os dispositivos e os componentes de forma a minimizar as alterações de endereço IP. Considere utilizar endereços IP estáticos em vez de Dynamic Host Configuration Protocol (DHCP). Se o DHCP for usado, certifique-se de que as alterações de endereço IP sejam minimizadas.

Sobre esta tarefa

A figura a seguir ilustra uma maneira de configurar seu ambiente quando as redes de dados e de gerenciamento são fisicamente diferentes. Os números na figura correspondem às etapas numeradas nas próximas seções.

Nota: Esta figura não descreve as opções de cabeamento que podem ser necessárias para seu ambiente. Em vez disso, essa figura mostra apenas os requisitos de opção de cabeamento para comutadores Flex, CMMs e servidores de rack, pois eles estão relacionados dados separados fisicamente e redes de gerenciamento.

Dica: Em vez de configurar dois comutadores físicos remotos conectados a cada rede para redundância (totalizando quatro comutadores), é possível configurar um único comutador físico conectado a cada rede (totalizando dois comutadores). Nesse caso, cada comutador seria conectado às duas redes, e você

implementaria duas VLANs: uma para a rede de dados e uma para a rede de gerenciamento, para segregar o tráfego de dados.

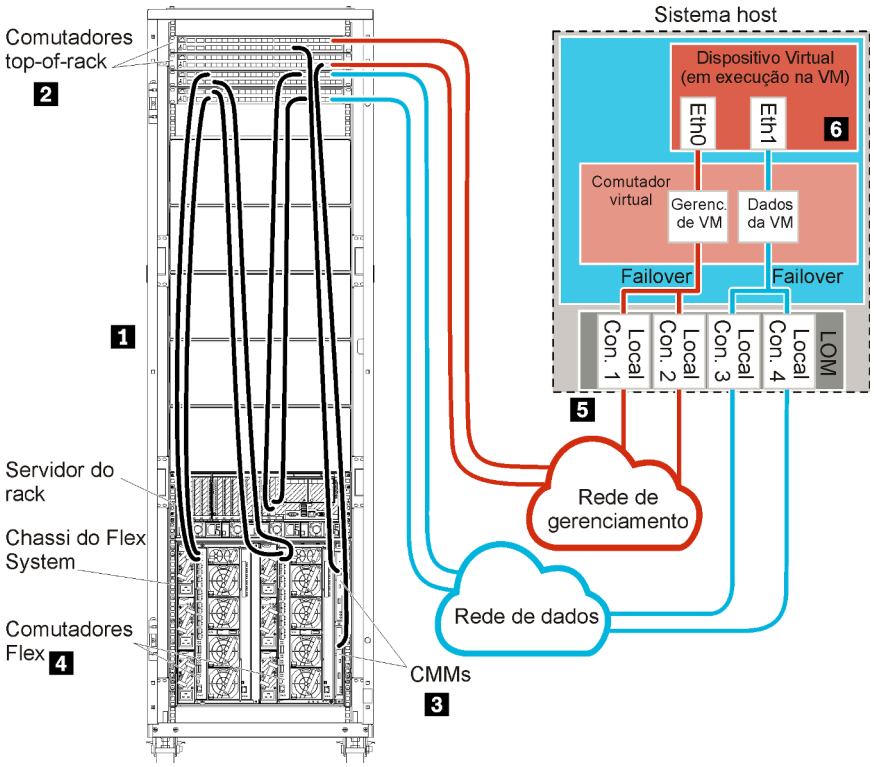


Figura 12. Exemplo de topologia de rede de gerenciamento e dados separados fisicamente para um dispositivo virtual

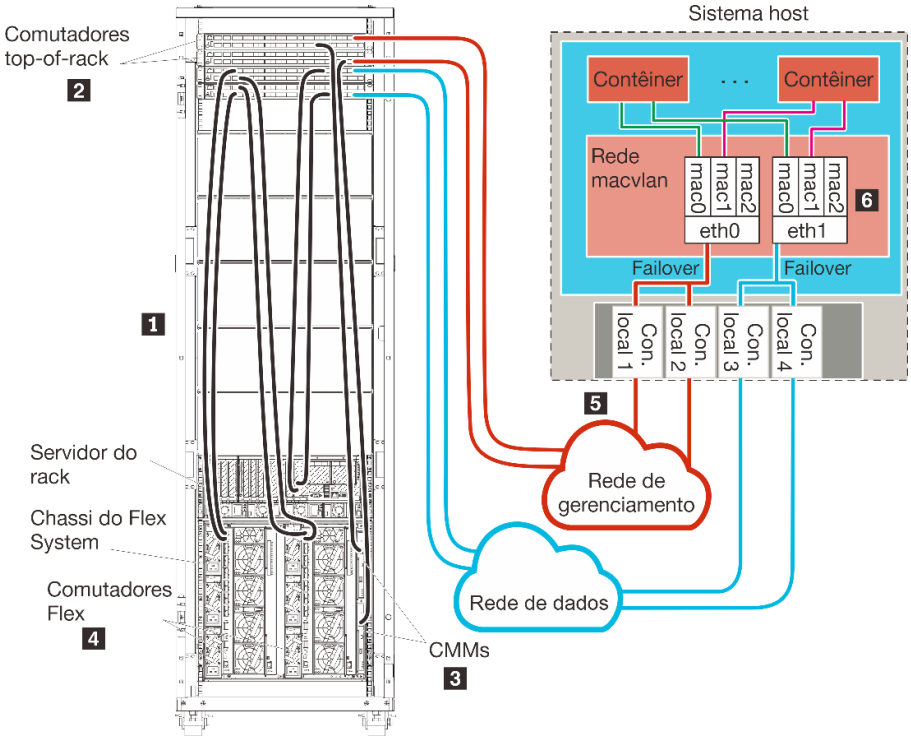


Figura 13. Exemplo de topologia de rede de gerenciamento e dados separados fisicamente para contêineres

Caso pretenda instalar o XClarity Administrator para gerenciar o chassi existente e os servidores de rack que já foram configurados, vá para Etapa 5: Instalar e configurar o host.

Para obter informações adicionais sobre o planejamento dessa topologia, incluindo informações sobre configurações de rede e configuração de Eth0 e Eth1, consulte Dados separados fisicamente e rede de gerenciamento.

Etapa 1: Passe o cabo do chassi, dos servidores de rack e do host do Lenovo XClarity Administrator nos comutadores top-of-rack

Conecte o chassi, os servidores de rack e o host do XClarity Administrator aos comutadores top-of-rack para ativar a comunicação entre os dispositivos e as redes.

Procedimento

Conecte cada comutador Flex e CMM em cada chassi, cada servidor de rack e no host do XClarity Administrator aos dois comutadores top-of-rack. É possível escolher qualquer porta nos comutadores top-of-rack.

A figura a seguir é um exemplo que ilustra o cabeamento do chassi (Comutadores Flex e CMMs), servidores de rack e host do XClarity Administrator para comutadores top-of-rack.

Nota: Esta figura não descreve as opções de cabeamento que podem ser necessárias para seu ambiente. Em vez disso, essa figura mostra apenas os requisitos de opção de cabeamento para comutadores Flex, CMMs e servidores de rack, pois eles estão relacionados dados separados fisicamente e redes de gerenciamento.

Dica: Em vez de configurar dois comutadores físicos remotos conectados a cada rede para redundância (totalizando quatro comutadores), é possível configurar um único comutador físico conectado a cada rede (totalizando dois comutadores). Nesse caso, cada comutador seria conectado às duas redes, e você implementaria duas VLANs: uma para a rede de dados e uma para a rede de gerenciamento, para segregar o tráfego de dados.

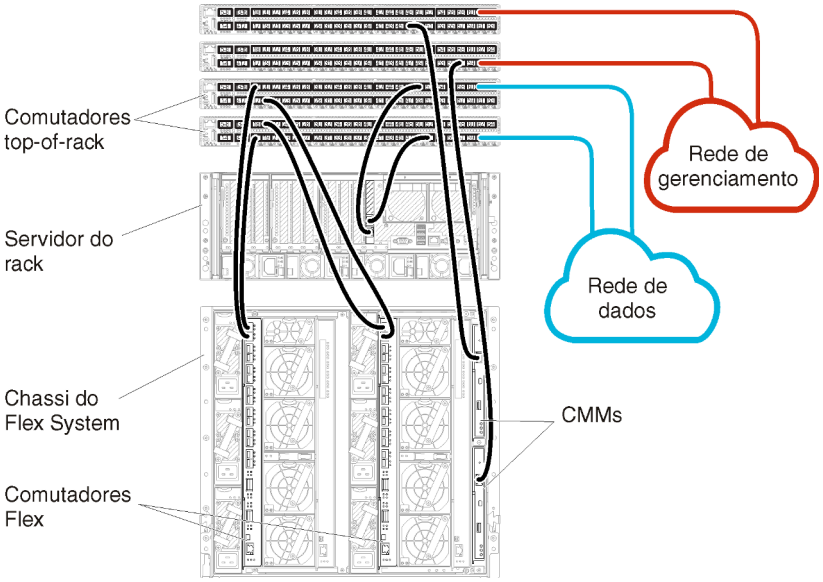


Figura 14. Exemplo de cabeamento de dados separados fisicamente e redes de gerenciamento

Etapa 2: Configurar comutadores top-of-rack

Configure os comutadores top-of-rack.

Antes de iniciar

Além dos requisitos de configuração típicos para comutadores top-of-rack, verifique se todas as portas apropriadas estão ativadas, incluindo portas externas ao Comutadores Flex, servidores de rack e rede, e portas internas ao CMM, servidores de rack e rede.

Procedimento

As etapas de configuração podem variar, dependendo do tipo de comutador de rack instalado.

Para obter informações sobre como configurar comutadores top-of-rack da Lenovo, consulte Comutadores de rack na documentação online do System x. Se outro comutador top-of-rack estiver instalado, consulte a documentação fornecida com esse comutador.

Etapa 3: Configurar Chassis Management Modules (CMMs)

Configure o Chassis Management Module (CMM) primário no chassi para gerenciar todos os dispositivos no chassi.

Sobre esta tarefa

Para obter informações detalhadas sobre como configurar um CMM, consulte Configurando componentes do chassi na documentação online do Flex System.

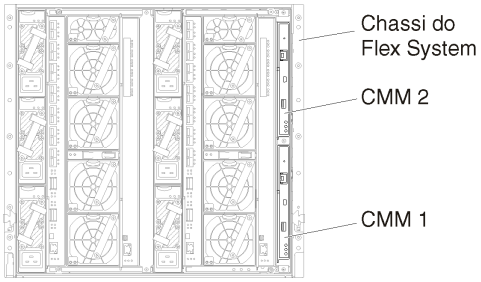
Além disso, consulte as etapas 4.1 a 4.5 do pôster de instrução fornecido com o chassi.

Procedimento

Conclua as etapas a seguir para configurar o CMM.

Se dois CMMs estiverem instalados, configure apenas o CMM *primário*, que sincroniza automaticamente a configuração com o CMM de espera.

Etapa 1. Conecte um cabo Ethernet do CMM no compartimento 1 a uma estação de trabalho do cliente para criar uma conexão direta.



Para conectar-se ao CMM pela primeira vez, talvez seja necessário alterar as propriedades de Internet Protocol na estação de trabalho do cliente.

Importante: Verifique se a sub-rede da estação de trabalho do cliente é a mesma sub-rede do CMM. A sub-rede dos CMM padrão é 255.255.255.0. O endereço IP escolhido para a estação de trabalho do cliente deve estar na mesma rede do CMM (por exemplo, 192.168.70.0 a 192.168.70.24).

Etapa 2. Para iniciar a interface de gerenciamento do CMM, abra um navegador da Web na estação de trabalho do cliente e direcione-o ao endereço IP do CMM.

Notas:

- Certifique-se de usar uma conexão segura e inclua **https** no URL (por exemplo, https://192.168.70.100). Se você não incluir https, receberá um erro de página não encontrada.
- Se você usar o endereço IP padrão 192.168.70.100, a interface de gerenciamento do CMM poderá levar alguns minutos para estar disponível. Esse atraso ocorre porque o CMM tenta obter um endereço DHCP por dois minutos antes de voltar para o endereço estático padrão.

Etapa 3. Faça login na interface de gerenciamento do CMM usando o ID do usuário padrão `USERID` e a senha `PASSWORD`. Depois de fazer login, você deve alterar a senha padrão.

Etapa 4. Conclua o Assistente de Configuração Inicial do CMM para especificar os detalhes do seu ambiente. O Assistente de Configuração Inicial inclui as seguintes opções:

- Veja o inventário e a integridade do chassi.
- Importe a configuração de um arquivo de configuração existente.
- Defina as configurações gerais do CMM.
- Configure data e hora do CMM.

  Dica: Ao instalar o XClarity Administrator, configure XClarity Administrator e todos os chassis gerenciados pelo XClarity Administrator para um servidor NTP.
- Configure as informações de IP do CMM.
- Configure a política de segurança do CMM.
- Configure o Sistema de Nomes de Domínio (DNS).
- Configure os encaminhadores de eventos.

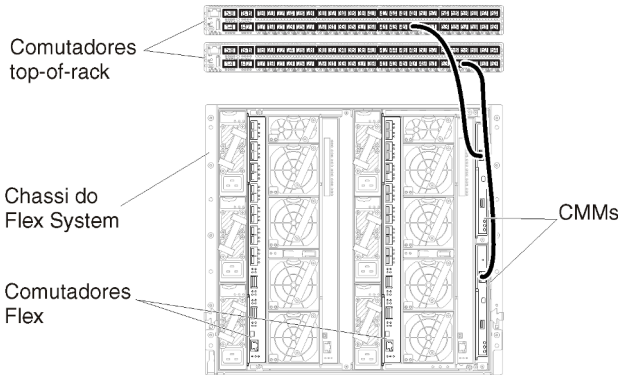
Etapa 5. Após salvar as configurações do assistente de configuração e aplicar as alterações, configure os endereços IP de todos os componentes no chassi.

Consulte a etapa 4.6 do pôster de instrução fornecido com o chassi.

Nota: Você deve redefinir o processador de gerenciamento de sistemas para cada nó de cálculo e reiniciar os comutadores Flex para mostrar os novos endereços IP.

Etapa 6. Reinicie o CMM usando a interface de gerenciamento do CMM.

Etapa 7. Durante a reinicialização do CMM, conecte um cabo da porta Ethernet no CMM à rede.



Etapa 8. Faça login na interface de gerenciamento do CMM usando o novo endereço IP.

Depois de concluir

Também é possível configurar o CMM para suportar redundância. Use o sistema de ajuda do CMM para saber mais sobre os campos disponíveis em cada uma das seguintes páginas.

- Configure o failover para o CMM se houver uma falha de hardware no CMM primário. Na interface de gerenciamento do CMM, clique em **Gerenciamento do Módulo de Gerenciamento → Propriedades → Failover Avançado**.
- Configure o failover em resultado de um problema de rede (uplink). Na interface de gerenciamento do CMM, clique em **Gerenciamento do Módulo de Gerenciamento → Rede**, clique na guia **Ethernet** e, em seguida, em **Ethernet Avançada**. No mínimo, selecione **Failover em caso de perda de link de rede física**.

Etapa 4: Configurar o Comutadores Flex

Configure o Comutadores Flex em cada chassi.

Antes de iniciar

Verifique se todas as portas apropriadas estão ativadas, incluindo portas externas do comutador Flex ao comutador top-of-rack e portas internas no CMM.

Se os comutadores Flex estiverem configurados para obter configurações de rede dinâmicas (endereço IP, gateway e endereço DNS) via DHCP, garanta que os comutadores Flex tenham configurações consistentes (por exemplo, verifique se os endereços IP estão na mesma sub-rede que o CMM).

Importante: Para cada chassi do Flex System, verifique se o tipo de malha da placa de expansão em cada servidor no chassi é compatível com o tipo de malha de todos os comutadores Flex no mesmo chassi. Por exemplo, se os comutadores Ethernet estiverem instalados em um chassi, todos os servidores desse chassi deverão ter conectividade Ethernet por meio do conector LAN na placa-mãe ou uma placa de expansão Ethernet. Para obter mais informações sobre como configurar comutadores Flex, consulte Configurando módulos de E/S na documentação online do Flex Systems.

Procedimento

As etapas de configuração podem variar, dependendo do tipo de Comutadores Flex instalado. Para obter mais informações sobre cada Comutadores Flex compatível, consulte Comutadores de rede do Flex System na documentação online do Flex Systems.

Normalmente, é necessário configurar os comutadores Flex nos compartimentos 1 e 2 de comutador Flex.

Dica: O compartimento 2 do comutador Flex é o terceiro compartimento do módulo olhando da traseira do chassi.

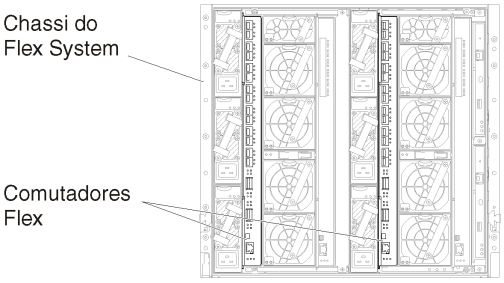


Figura 15. Locais de Comutador Flex em um chassi

Etapa 5: Instalar e configurar o host

É possível instalar o Docker em qualquer servidor que atenda aos requisitos para o Lenovo XClarity Administrator.

Antes de iniciar

É possível usar o Docker Datacenter para configurar um ambiente de alta disponibilidade para contêineres do XClarity Administrator em execução no Docker Engine. Para obter mais informações sobre a alta disponibilidade do Docker Datacenter, consulte Página da Web Arquitetura e aplicativos de alta disponibilidade com o Docker Datacenter.

Verifique se o host satisfaz os pré-requisitos definidos em Pré-requisitos de hardware e software.

Verifique se o sistema do host está na mesma rede que os dispositivos que deseja gerenciar.

Importante: É possível configurar o XClarity Administrator em qualquer sistema que atenda aos requisitos para XClarity Administrator, incluindo um servidor gerenciado. Se você usa um servidor gerenciado para o host do XClarity Administrator:

- Deve implementar uma topologia de rede de gerenciamento e dados separados virtualmente ou uma topologia de rede de gerenciamento e dados únicos.
- Não pode usar XClarity Administrator para aplicar atualizações de firmware a esse servidor gerenciado. Mesmo quando apenas alguns firmwares são aplicados com ativação imediata, o XClarity Administrator força o servidor de destino a reiniciar, o que reinicia também o XClarity Administrator. Quando aplicado com ativação adiada, apenas alguns firmwares são aplicados quando o host do XClarity Administrator é reiniciado.
- Se você usar um servidor em um chassi do Flex System, garanta que o servidor esteja configurado para ligar automaticamente. É possível definir essa opção na interface da Web do CMM clicando em **Gerenciamento de Chassi → Nós de Cálculo**, selecionando o servidor e **Ativação Automática** para o **Modo de Ativação Automática**.

Procedimento

Instale e configure o Docker no host usando as instruções que são fornecidas com a distribuição do Docker.

Etapa 6. Instalar e configurar o XClarity Administrator

Instale e configure o contêiner do Lenovo XClarity Administrator no host do Docker que acabou de ser instalado.

Antes de iniciar

O sistema host físico deve atender aos requisitos mínimos de hardware e software (consulte Pré-requisitos de hardware e software).

Verifique se todas as portas apropriadas estão ativadas, incluindo portas exigidas pelo XClarity Administrator (consulte Disponibilidade de porta).

Verifique se o sistema do host está na mesma rede que os dispositivos que deseja gerenciar.

Verifique se o SO do host e o XClarity Administrator usam o mesmo servidor NTP.

O XClarity Administrator permite que um nome personalizado da rede seja usado para gerenciamento de dados, gerenciamento de hardware e implantação do SO (consulte Configurações de rede). Este exemplo no procedimento a seguir usa eth0.

O XClarity Administrator permite que um nome personalizado da rede seja usado para gerenciamento de dados e hardware e a rede usada para implantação do SO (consulte Configurações de rede). Este exemplo no procedimento a seguir usa eth0 e eth1 respectivamente

Verifique se uma rede macvlan está carregada no kernel no sistema host. Para verificar se ela está carregada, use o comando **lsmod | grep macvlan**. Para carregar a macvlan no kernel, execute o comando **modprobe macvlan**.

Use um nome exclusivo e endereço IP para cada contêiner ao executar vários contêineres do XClarity Administrator no mesmo host.

Se você pretende gerenciar o ThinkServer e outros dispositivos legados, o Docker deve estar habilitado para dar suporte ao IPv6.

1. Edite o arquivo /etc/docker/daemon.json, defina a chave **ipv6** como true e defina a chave **fixed-cidr-v6** como sua sub-rede IPv6. Veja a seguir um exemplo de arquivo daemon.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Recarregue o arquivo de configuração do Docker executando o comando a seguir.
```
systemctl reload docker
```

Nota: O XClarity Administrator *não é* executado como um contêiner privilegiado.

Procedimento

Para instalar um contêiner do XClarity Administrator usando a composição do Docker, conclua as etapas a seguir.

Etapa 1. Baixe a imagem do dispositivo virtual do XClarity Administrator, o arquivo de ambiente e o arquivo YAML do Página da Web de download do XClarity Administrator para uma estação de trabalho do cliente. Faça login no Web site e, em seguida, use a tecla de acesso que foi fornecida para baixar a imagem.

Etapa 2. Importe a imagem de contêiner do XClarity Administrator para seu host do docker executando o comando a seguir.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Etapa 3. Edite o arquivo `docker_compose.env` e atualize as variáveis de ambiente a seguir.

- **CONTAINER_NAME**. Nome exclusivo do contêiner, usado para criar volumes de docker para cada instância do XClarity Administrator (por exemplo, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Endereço estático IPv4 para o contêiner (por exemplo, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Opcional) Caminho para o compartilhamento remoto que pode ser usado para armazenar backups do XClarity Administrator. Deve ser `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Opcional) Caminho para o compartilhamento remoto que pode ser usado como um repositório remoto para atualizações de firmware. Deve ser `/mnt/fw_share`.

Veja a seguir um exemplo de arquivo de ambiente.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
```

```
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Etapa 4. Edite o `docker_compose.yml` e atualize as propriedades a seguir.

- Defina a propriedade **image** como o nome do arquivo de imagem de instalação usado na etapa 2.

  Nota: É possível alterar o nome do arquivo de imagem (por exemplo, para "mais recente") usando o comando `docker tag`.
- Se você deseja usar compartilhamentos remotos como um repositório de firmware remoto e armazenar backups do XClarity Administrator, defina o ponto de montagem do host para cada compartilhamento remoto na propriedade **volumes**.
- Defina a propriedade **dns** como o endereço IP dos servidores DNS.
- O contêiner compartilha o conjunto de recursos de processador e memória que estão disponíveis para o host. Opcionalmente, defina limites de uso de recurso configurando as propriedades **cpus** e **memória**.
- Defina a propriedade **parent** como o nome da interface de rede no sistema host que deve ser usada como a interface pai para a interface macvlan no contêiner. Essa interface deve ter acesso direto à sub-rede atribuída ao contêiner.
- Defina a **sub-rede** e o **gateway** de acordo com a topologia de rede. Normalmente, a sub-rede e o gateway se destinam à rede de gerenciamento, à qual pertence o ${ADDRESS}.
- Se você deseja dar suporte ao IPv6, defina a propriedade **enable_ipv6** como true, defina a propriedade **ipv6_address** como o endereço IPv6 e adicione outro conjunto de propriedades de **sub-rede** e **gateway** de acordo com sua topologia de rede (geralmente para rede de gerenciamento à qual o endereço IPv6 pertence).

Veja a seguir um arquivo YML de exemplo, com IPv6 habilitado.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan1:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2000::2"
      lan2:
```

```
          ipv4_address: 192.0.1.3
          ipv6_address: "2001:8003:7d51:2003::2"
      dns:
        - 192.0.40.10
        - 192.0.50.11
      deploy:
        resources:
          limits:
            cpus: "2.0"
            memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan1:
    name: lan1
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eno1
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
  lan2:
    name: lan2
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: virbr0
    ipam:
      config:
        - subnet: 192.0.122.0/24
        - subnet: "2001:8003:7d51:2005::/80"
```

Etapa 5. Implante a imagem no docker executando o comando a seguir, em que <*ENV_FILENAME*> é o nome do arquivo de variáveis do ambiente criado na etapa 2.
COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d`

Depois de concluir

Faça login e configure o XClarity Administrator (consulte Acessando a interface da Web do Lenovo XClarity Administrator pela primeira vez e Configurando Lenovo XClarity Administrator).

Dados separados virtualmente e topologia de rede de gerenciamento

Nesta topologia, a rede de dados e de gerenciamento são separadas virtualmente. Os pacotes da rede de dados e os pacotes da rede de gerenciamento são enviados pela mesma conexão física. A marcação de VLAN em todos os pacotes de dados da rede de gerenciamento é usada para manter o tráfego entre duas redes separadas.

Antes de iniciar

Verifique se todas as portas apropriadas estão ativadas, incluindo as portas necessárias para XClarity Administrator (consulte Disponibilidade de porta).

Verifique se o firmware mínimo necessário está instalado em cada dispositivo 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 os IDs de VLAN estão configurados para a rede de dados e a rede de gerenciamento. Opcionalmente, ative a marcação de VLAN no Comutadores Flex se implementar a marcação no Comutadores Flex ou ative nos comutadores top-of-rack se implementar a marcação nos comutadores top-of-rack.

Defina as portas às quais os CMMs estão conectados como pertencentes à VLAN de gerenciamento.

Importante: Configure os dispositivos e os componentes de forma a minimizar as alterações de endereço IP. Considere utilizar endereços IP estáticos em vez de Dynamic Host Configuration Protocol (DHCP). Se o DHCP for usado, certifique-se de que as alterações de endereço IP sejam minimizadas.

Sobre esta tarefa

A figura a seguir ilustra uma maneira de configurar seu ambiente para que a rede de gerenciamento seja separada da rede virtual. Os números na figura correspondem às etapas numeradas nas próximas seções.

Nota: Esta figura não descreve as opções de cabeamento que podem ser necessárias para seu ambiente. Em vez disso, essa figura mostra apenas os requisitos de opção de cabeamento para comutadores Flex, CMMs e servidores de rack, pois eles estão relacionados dados separados virtualmente e redes de gerenciamento.

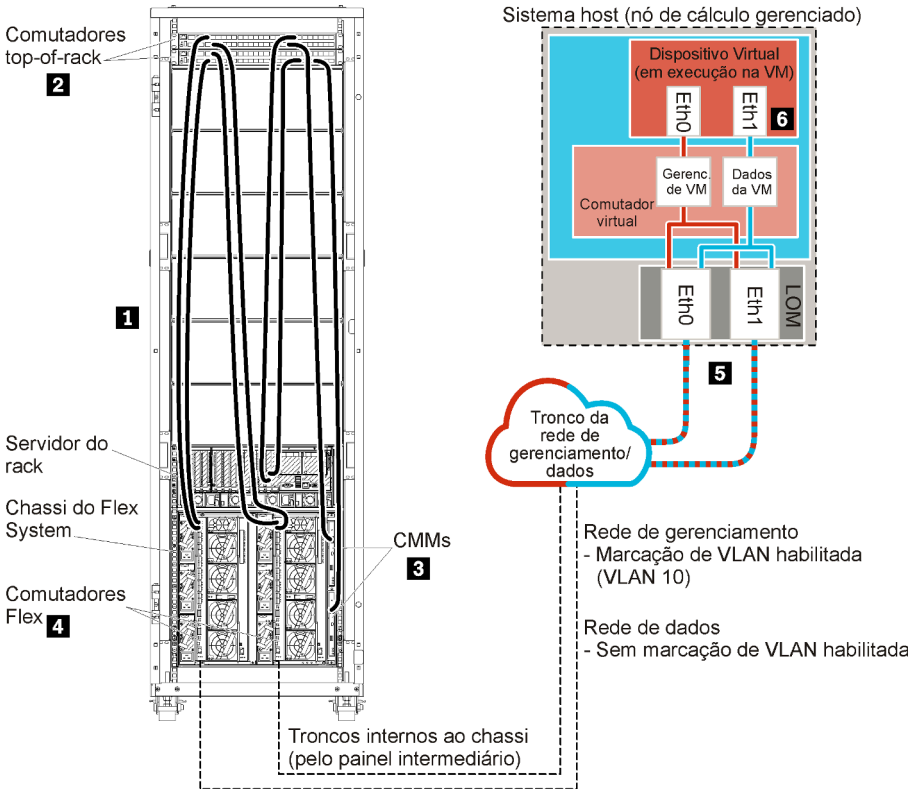


Figura 16. Exemplo de topologia de rede de gerenciamento e dados separados virtualmente para um dispositivo virtual

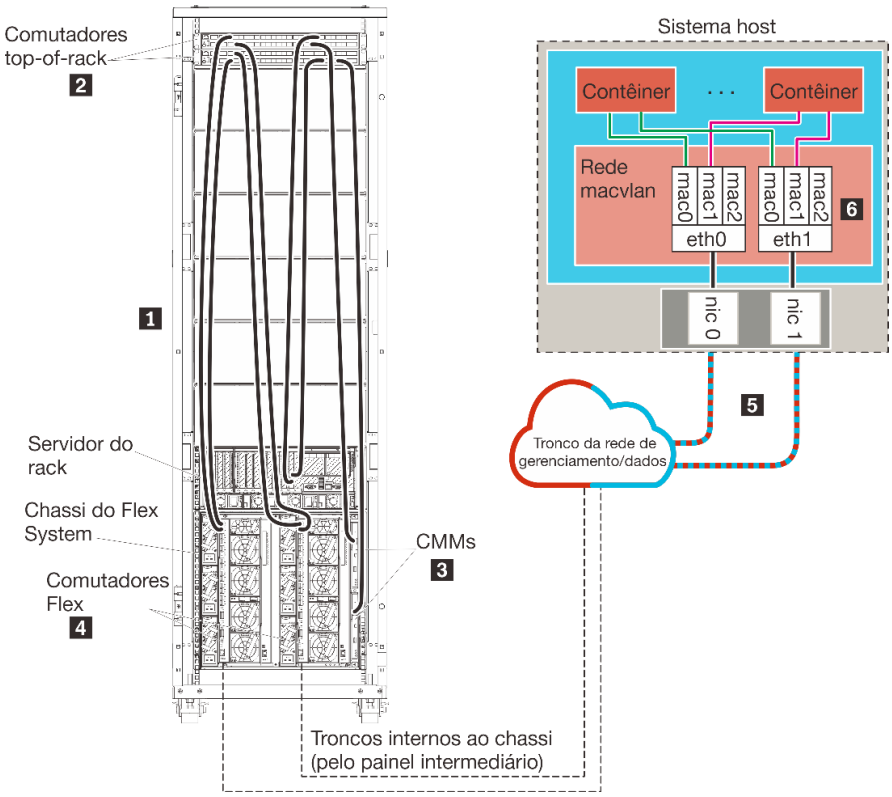


Figura 17. Exemplo de topologia de rede de gerenciamento e dados separados virtualmente para contêineres

Neste cenário, o XClarity Administrator está instalado em um servidor em um chassi do Flex System que está sendo gerenciado pelo XClarity Administrator.

Importante: É possível configurar o XClarity Administrator em qualquer sistema que atenda aos requisitos para XClarity Administrator, incluindo um servidor gerenciado. Se você usa um servidor gerenciado para o host do XClarity Administrator:

- Deve implementar uma topologia de rede de gerenciamento e dados separados virtualmente ou uma topologia de rede de gerenciamento e dados únicos.
- Não pode usar XClarity Administrator para aplicar atualizações de firmware a esse servidor gerenciado. Mesmo quando apenas alguns firmwares são aplicados com ativação imediata, o XClarity Administrator força o servidor de destino a reiniciar, o que reinicia também o XClarity Administrator. Quando aplicado com ativação adiada, apenas alguns firmwares são aplicados quando o host do XClarity Administrator é reiniciado.
- Se você usar um servidor em um chassi do Flex System, garanta que o servidor esteja configurado para ligar automaticamente. É possível definir essa opção na interface da Web do CMM clicando em **Gerenciamento de Chassi → Nós de Cálculo**, selecionando o servidor e **Ativação Automática** para o **Modo de Ativação Automática**.

Também neste cenário, todos os dados são enviados pelas mesmas conexões físicas. A separação entre a rede de gerenciamento e a rede de dados é realizada pela marcação de VLAN. Nesse caso, tags específicas que correspondem à rede de gerenciamento são anexadas aos pacotes de dados de entrada para assegurar que sejam roteados para as interfaces apropriadas. As tags serão removidas dos pacotes de dados de saída.

A marcação de VLAN pode ser ativada em um destes dispositivos:

- **Comutadores top-of-rack**. As tags de VLAN que correspondem à rede de gerenciamento são adicionadas aos pacotes à medida que entram no comutador top-of-rack e são transmitidas pelo Comutadores Flex e em servidores no chassi do Flex System. Na rota de retorno, as tags de VLAN são removidas porque são enviadas do comutador top-of-rack para controladores de gerenciamento.
- **Comutadores Flex**. As tags de VLAN que correspondem à rede de gerenciamento são adicionadas aos pacotes à medida que entram no Comutadores Flex e são transmitidas para os servidores em um chassi do Flex System. Na rota de retorno, as tags de VLAN são adicionadas pelos servidores e transmitidas ao Comutadores Flex, que as remove durante o encaminhamento para os controladores de gerenciamento.

A opção por implementar a marcação de VLAN é baseada nas necessidades e na complexidade de seu ambiente.

Caso pretenda instalar o XClarity Administrator para gerenciar o chassi existente e os servidores de rack que já foram configurados, vá para Etapa 5: Instalar e configurar o host.

Para obter informações adicionais sobre o planejamento dessa topologia, incluindo informações sobre configurações de rede e configuração de Eth0 e Eth1, consulte Dados separados virtualmente e rede de gerenciamento.

Etapa 1: Passe o cabo do chassi e dos servidores de rack nos comutadores top-of-rack

Conecte o chassi e os servidores de rack no mesmo comutador top-of-rack para ativar a comunicação entre os dispositivos.

Procedimento

Conecte cada comutador Flex e CMM em cada chassi e cada servidor de rack aos dois comutadores top-of-rack. É possível escolher qualquer porta nesse comutador top-of-rack.

A figura a seguir é um exemplo que ilustra o cabeamento do chassi (comutadores Flex e CMMs) e de servidores de rack para comutadores top-of-rack quando o Lenovo XClarity Administrator é instalado em um servidor em um chassi que será gerenciado por XClarity Administrator.

Nota: Esta figura não descreve as opções de cabeamento que podem ser necessárias para seu ambiente. Em vez disso, essa figura mostra apenas os requisitos de opção de cabeamento para comutadores Flex, CMMs e servidores de rack, pois eles estão relacionados dados separados virtualmente e redes de gerenciamento.

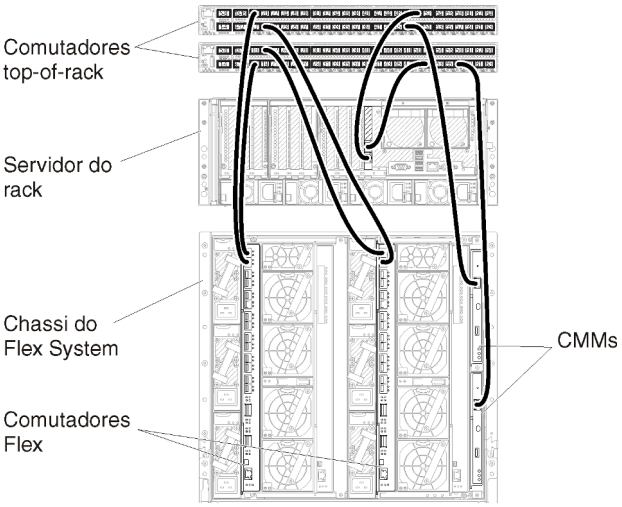


Figura 18. Exemplo de cabeamento de dados separados virtualmente e redes de gerenciamento

Etapa 2: Configurar comutadores top-of-rack

Configure os comutadores top-of-rack.

Antes de iniciar

Além dos requisitos de configuração típicos para comutadores top-of-rack, verifique se todas as portas apropriadas estão ativadas, incluindo portas externas ao Comutadores Flex, servidores de rack e rede, e portas internas ao CMM, servidores de rack e rede.

É possível implementar a marcação de VLAN em comutadores Flex ou comutadores top-of-rack, dependendo das necessidades e da complexidade de seu ambiente. Se você implementar a marcação nos comutadores top-of-rack, ative a marcação de VLAN nos comutadores top-of-rack.

Verifique se os IDs de VLAN estão configurados para as redes de gerenciamento e de dados.

Procedimento

As etapas de configuração podem variar, dependendo do tipo de comutador de rack instalado.

A figura a seguir é um cenário de exemplo que ilustra a marcação de VLAN que é implementada nos comutadores top-of-rack e ativada apenas na rede de gerenciamento. A VLAN de gerenciamento é configurada como VLAN 10.

Nesse cenário, você deve definir as portas às quais os CMMs estão conectados como pertencentes à VLAN de gerenciamento.

Nota: Também é possível ativar a marcação de VLAN na rede de dados para configurar uma VLAN de dados.

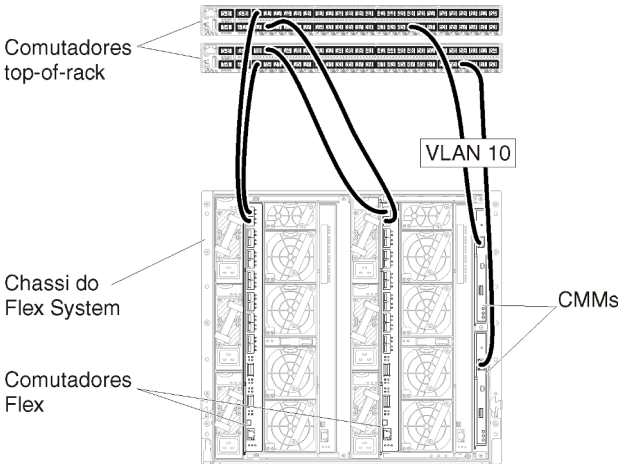


Figura 19. Configuração de exemplo do Comutadores Flex em redes de gerenciamento e dados separados virtualmente (VMware ESXi) nas quais a marcação de VLAN está ativada na rede de gerenciamento

Para obter informações sobre como configurar comutadores top-of-rack da Lenovo, consulte Comutadores de rack na documentação online do System x. Se outro comutador top-of-rack estiver instalado, consulte a documentação fornecida com esse comutador.

Etapa 3: Configurar Chassis Management Modules (CMMs)

Configure o Chassis Management Module (CMM) primário no chassi para gerenciar todos os dispositivos no chassi.

Sobre esta tarefa

Para obter informações detalhadas sobre como configurar um CMM, consulte Configurando componentes do chassi na documentação online do Flex System.

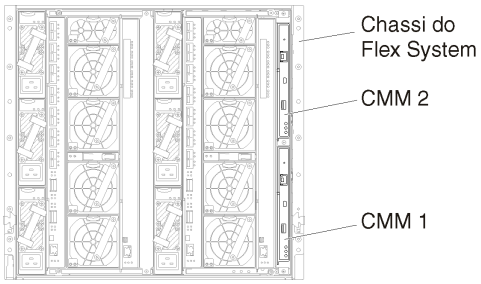
Além disso, consulte as etapas 4.1 a 4.5 do pôster de instrução fornecido com o chassi.

Procedimento

Conclua as etapas a seguir para configurar o CMM.

Se dois CMMs estiverem instalados, configure apenas o CMM *primário*, que sincroniza automaticamente a configuração com o CMM de espera.

Etapa 1. Conecte um cabo Ethernet do CMM no compartimento 1 a uma estação de trabalho do cliente para criar uma conexão direta.



Para conectar-se ao CMM pela primeira vez, talvez seja necessário alterar as propriedades de Internet Protocol na estação de trabalho do cliente.

Importante: Verifique se a sub-rede da estação de trabalho do cliente é a mesma sub-rede do CMM. A sub-rede dos CMM padrão é 255.255.255.0. O endereço IP escolhido para a estação de trabalho do cliente deve estar na mesma rede do CMM (por exemplo, 192.168.70.0 a 192.168.70.24).

Etapa 2. Para iniciar a interface de gerenciamento do CMM, abra um navegador da Web na estação de trabalho do cliente e direcione-o ao endereço IP do CMM.

Notas:

- Certifique-se de usar uma conexão segura e inclua **https** no URL (por exemplo, https://192.168.70.100). Se você não incluir https, receberá um erro de página não encontrada.
- Se você usar o endereço IP padrão 192.168.70.100, a interface de gerenciamento do CMM poderá levar alguns minutos para estar disponível. Esse atraso ocorre porque o CMM tenta obter um endereço DHCP por dois minutos antes de voltar para o endereço estático padrão.

Etapa 3. Faça login na interface de gerenciamento do CMM usando o ID do usuário padrão `USERID` e a senha `PASSWORD`. Depois de fazer login, você deve alterar a senha padrão.

Etapa 4. Conclua o Assistente de Configuração Inicial do CMM para especificar os detalhes do seu ambiente. O Assistente de Configuração Inicial inclui as seguintes opções:

- Veja o inventário e a integridade do chassi.
- Importe a configuração de um arquivo de configuração existente.
- Defina as configurações gerais do CMM.
- Configure data e hora do CMM.

  Dica: Ao instalar o XClarity Administrator, configure XClarity Administrator e todos os chassis gerenciados pelo XClarity Administrator para um servidor NTP.
- Configure as informações de IP do CMM.
- Configure a política de segurança do CMM.
- Configure o Sistema de Nomes de Domínio (DNS).
- Configure os encaminhadores de eventos.

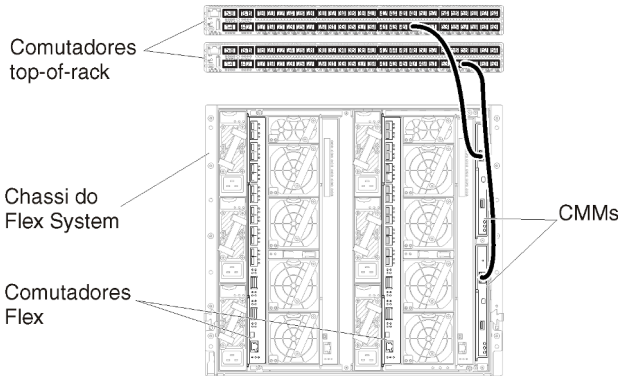
Etapa 5. Após salvar as configurações do assistente de configuração e aplicar as alterações, configure os endereços IP de todos os componentes no chassi.

Consulte a etapa 4.6 do pôster de instrução fornecido com o chassi.

Nota: Você deve redefinir o processador de gerenciamento de sistemas para cada nó de cálculo e reiniciar os comutadores Flex para mostrar os novos endereços IP.

Etapa 6. Reinicie o CMM usando a interface de gerenciamento do CMM.

Etapa 7. Durante a reinicialização do CMM, conecte um cabo da porta Ethernet no CMM à rede.



Etapa 8. Faça login na interface de gerenciamento do CMM usando o novo endereço IP.

Depois de concluir

Também é possível configurar o CMM para suportar redundância. Use o sistema de ajuda do CMM para saber mais sobre os campos disponíveis em cada uma das seguintes páginas.

- Configure o failover para o CMM se houver uma falha de hardware no CMM primário. Na interface de gerenciamento do CMM, clique em **Gerenciamento do Módulo de Gerenciamento → Propriedades → Failover Avançado**.
- Configure o failover em resultado de um problema de rede (uplink). Na interface de gerenciamento do CMM, clique em **Gerenciamento do Módulo de Gerenciamento → Rede**, clique na guia **Ethernet** e, em seguida, em **Ethernet Avançada**. No mínimo, selecione **Failover em caso de perda de link de rede física**.

Etapa 4: Configurar o Comutadores Flex

Configure o Comutadores Flex em cada chassi.

Antes de iniciar

Verifique se todas as portas apropriadas estão ativadas, incluindo portas externas do comutador Flex ao comutador top-of-rack e portas internas no CMM.

É possível implementar a marcação de VLAN em comutadores Flex ou comutadores top-of-rack, dependendo das necessidades e da complexidade de seu ambiente. Se você implementar a marcação nos comutadores Flex, ative a marcação de VLAN nos comutadores Flex.

Verifique se os IDs de VLAN estão configurados para as redes de gerenciamento e de dados.

Importante: Para cada chassi do Flex System, verifique se o tipo de malha da placa de expansão em cada servidor no chassi é compatível com o tipo de malha de todos os comutadores Flex no mesmo chassi. Por exemplo, se os comutadores Ethernet estiverem instalados em um chassi, todos os servidores desse chassi deverão ter conectividade Ethernet por meio do conector LAN na placa-mãe ou uma placa de expansão Ethernet. Para obter mais informações sobre como configurar comutadores Flex, consulte Configurando módulos de E/S na documentação online do Flex Systems.

Procedimento

As etapas de configuração podem variar, dependendo do tipo de Comutadores Flex instalado. Para obter mais informações sobre cada Comutadores Flex compatível, consulte Comutadores de rede do Flex System na documentação online do Flex Systems.

A figura a seguir é um cenário de exemplo que ilustra a marcação de VLAN que é implementada nos comutadores Flex e ativada apenas na rede de gerenciamento. A VLAN de gerenciamento é configurada como VLAN 10.

Nota: Também é possível configurar uma VLAN de dados ativando a marcação de VLAN na rede de dados.

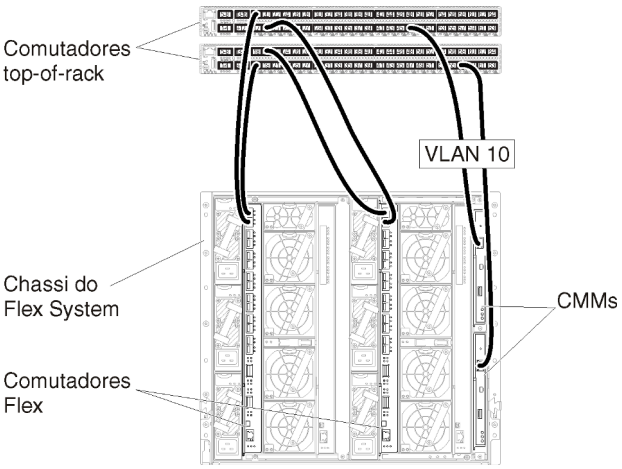


Figura 20. Configuração de exemplo do Comutadores Flex em redes de gerenciamento e dados separados virtualmente (VMware ESXi) nas quais a marcação de VLAN está ativada na rede de gerenciamento

Conclua as seguintes etapas para configurar os comutadores Flex para esse cenário:

Etapa 1. Configure o comutador Flex no compartimento 1 do comutador Flex:

a. Defina a VLAN de gerenciamento (no exemplo, escolhemos VLAN 10) para conter a porta externa onde o cabo é roteado para o comutador top-of-rack de gerenciamento (Ext1).

b. Defina uma porta interna para fazer parte da VLAN 10 (VLAN de gerenciamento). Verifique se o entroncamento de VLAN está ativado nessa porta.

Etapa 2. Configure o comutador Flex no compartimento 2 do comutador Flex:

Dica: O compartimento 2 do comutador Flex é, na verdade, o terceiro compartimento do módulo se você estiver olhando da traseira do chassi:

a. Defina a VLAN de gerenciamento (no exemplo, escolhemos VLAN 10) para conter a porta externa onde o cabo é roteado para o comutador top-of-rack de gerenciamento.

b. Defina uma porta interna para fazer parte da VLAN 10 (VLAN de gerenciamento). Verifique se o entroncamento de VLAN está ativado nessa porta.

Etapa 5: Instalar e configurar o host

É possível instalar o Docker em qualquer sistema que atenda aos requisitos para o Lenovo XClarity Administrator.

Antes de iniciar

É possível usar o Docker Datacenter para configurar um ambiente de alta disponibilidade para contêineres do XClarity Administrator em execução no Docker Engine. Para obter mais informações sobre a alta disponibilidade do Docker Datacenter, consulte Página da Web Arquitetura e aplicativos de alta disponibilidade com o Docker Datacenter.

Verifique se o host satisfaz os pré-requisitos definidos em Pré-requisitos de hardware e software.

Verifique se o sistema do host está na mesma rede que os dispositivos que deseja gerenciar.

Importante: É possível configurar o XClarity Administrator em qualquer sistema que atenda aos requisitos para XClarity Administrator, incluindo um servidor gerenciado. Se você usa um servidor gerenciado para o host do XClarity Administrator:

- Deve implementar uma topologia de rede de gerenciamento e dados separados virtualmente ou uma topologia de rede de gerenciamento e dados únicos.
- Não pode usar XClarity Administrator para aplicar atualizações de firmware a esse servidor gerenciado. Mesmo quando apenas alguns firmwares são aplicados com ativação imediata, o XClarity Administrator força o servidor de destino a reiniciar, o que reinicia também o XClarity Administrator. Quando aplicado com ativação adiada, apenas alguns firmwares são aplicados quando o host do XClarity Administrator é reiniciado.
- Se você usar um servidor em um chassi do Flex System, garanta que o servidor esteja configurado para ligar automaticamente. É possível definir essa opção na interface da Web do CMM clicando em **Gerenciamento de Chassi → Nós de Cálculo**, selecionando o servidor e **Ativação Automática** para o **Modo de Ativação Automática**.

Procedimento

Instale e configure o Docker no host usando as instruções que são fornecidas com a distribuição do Docker.

Etapa 6. Instalar e configurar o XClarity Administrator

Instale e configure o contêiner do Lenovo XClarity Administrator no host do Docker que acabou de ser instalado.

Antes de iniciar

O sistema host físico deve atender aos requisitos mínimos de hardware e software (consulte Pré-requisitos de hardware e software).

Verifique se todas as portas apropriadas estão ativadas, incluindo portas exigidas pelo XClarity Administrator (consulte Disponibilidade de porta).

Verifique se o sistema do host está na mesma rede que os dispositivos que deseja gerenciar.

Verifique se o SO do host e o XClarity Administrator usam o mesmo servidor NTP.

O XClarity Administrator permite que um nome personalizado da rede seja usado para gerenciamento de dados, gerenciamento de hardware e implantação do SO (consulte Configurações de rede). Este exemplo no procedimento a seguir usa eth0.

O XClarity Administrator permite que um nome personalizado da rede seja usado para gerenciamento de dados e hardware e a rede usada para implantação do SO (consulte Configurações de rede). Este exemplo no procedimento a seguir usa eth0 e eth1 respectivamente.

Verifique se uma rede macvlan está carregada no kernel no sistema host. Para verificar se ela está carregada, use o comando **lsmod | grep macvlan**. Para carregar a macvlan no kernel, execute o comando **modprobe macvlan**.

Use um nome exclusivo e endereço IP para cada contêiner ao executar vários contêineres do XClarity Administrator no mesmo host.

Se você pretende gerenciar o ThinkServer e outros dispositivos legados, o Docker deve estar habilitado para dar suporte ao IPv6.

1. Edite o arquivo /etc/docker/daemon.json, defina a chave **ipv6** como true e defina a chave **fixed-cidr-v6** como sua sub-rede IPv6. Veja a seguir um exemplo de arquivo daemon.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Recarregue o arquivo de configuração do Docker executando o comando a seguir.
```
systemctl reload docker
```

Nota: O XClarity Administrator *não é* executado como um contêiner privilegiado.

Procedimento

Para instalar um contêiner do XClarity Administrator usando a composição do Docker, conclua as etapas a seguir.

Etapa 1. Baixe a imagem do dispositivo virtual do XClarity Administrator, o arquivo de ambiente e o arquivo YAML do Página da Web de download do XClarity Administrator para uma estação de trabalho do cliente. Faça login no Web site e, em seguida, use a tecla de acesso que foi fornecida para baixar a imagem.

Etapa 2. Importe a imagem de contêiner do XClarity Administrator para seu host do docker executando o comando a seguir.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Etapa 3. Edite o arquivo `docker_compose.env` e atualize as variáveis de ambiente a seguir.

- **CONTAINER_NAME**. Nome exclusivo do contêiner, usado para criar volumes de docker para cada instância do XClarity Administrator (por exemplo, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Endereço estático IPv4 para o contêiner (por exemplo, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Opcional) Caminho para o compartilhamento remoto que pode ser usado para armazenar backups do XClarity Administrator. Deve ser `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Opcional) Caminho para o compartilhamento remoto que pode ser usado como um repositório remoto para atualizações de firmware. Deve ser `/mnt/fw_share`.

Veja a seguir um exemplo de arquivo de ambiente.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Etapa 4. Edite o `docker_compose.yml` e atualize as propriedades a seguir.

- Defina a propriedade **image** como o nome do arquivo de imagem de instalação usado na etapa 2.

  Nota: É possível alterar o nome do arquivo de imagem (por exemplo, para "mais recente") usando o comando `docker tag`.
- Se você deseja usar compartilhamentos remotos como um repositório de firmware remoto e armazenar backups do XClarity Administrator, defina o ponto de montagem do host para cada compartilhamento remoto na propriedade **volumes**.
- Defina a propriedade **dns** como o endereço IP dos servidores DNS.

- O contêiner compartilha o conjunto de recursos de processador e memória que estão disponíveis para o host. Opcionalmente, defina limites de uso de recurso configurando as propriedades **cpus** e **memória**.
- Defina a propriedade **parent** como o nome da interface de rede no sistema host que deve ser usada como a interface pai para a interface macvlan no contêiner. Essa interface deve ter acesso direto à sub-rede atribuída ao contêiner.
- Defina a **sub-rede** e o **gateway** de acordo com a topologia de rede. Normalmente, a sub-rede e o gateway se destinam à rede de gerenciamento, à qual pertence o ${ADDRESS}.
- Se você deseja dar suporte ao IPv6, defina a propriedade **enable_ipv6** como true, defina a propriedade **ipv6_address** como o endereço IPv6 e adicione outro conjunto de propriedades de **sub-rede** e **gateway** de acordo com sua topologia de rede (geralmente para rede de gerenciamento à qual o endereço IPv6 pertence).

Veja a seguir um arquivo YML de exemplo, com IPv6 habilitado.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan1:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2000::2"
      lan2:
        ipv4_address: 192.0.1.3
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.40.10
      - 192.0.50.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
```

```
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan1:
    name: lan1
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eno1
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
  lan2:
    name: lan2
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: virbr0
    ipam:
      config:
        - subnet: 192.0.122.0/24
          gateway: 192.0.122.1
        - subnet: "2001:8003:7d51:2003::/80"
          gateway: "2001:8003:7d51:2003::1"
```

Etapa 5. Implante a imagem no docker executando o comando a seguir, em que <*ENV_FILENAME*> é o nome do arquivo de variáveis do ambiente criado na etapa 2.

COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file` <*ENV_FILENAME*> `up -d`

Depois de concluir

Faça login e configure o XClarity Administrator (consulte Acessando a interface da Web do Lenovo XClarity Administrator pela primeira vez e Configurando Lenovo XClarity Administrator).

Topologia de rede somente de gerenciamento

Nessa topologia, o Lenovo XClarity Administrator tem apenas a rede de gerenciamento. Ele não tem a rede de dados.

Antes de iniciar

Verifique se todas as portas apropriadas estão ativadas, incluindo:

- Portas necessárias para o XClarity Administrator (consulte Disponibilidade de porta)
- Portas externas à rede
- Portas internas ao CMM

Verifique se o firmware mínimo necessário está instalado em cada dispositivo 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: Configure os dispositivos e os componentes de forma a minimizar as alterações de endereço IP. Considere utilizar endereços IP estáticos em vez de Dynamic Host Configuration Protocol (DHCP). Se o DHCP for usado, certifique-se de que as alterações de endereço IP sejam minimizadas.

Sobre esta tarefa

A figura a seguir ilustra uma maneira de configurar seu ambiente caso o Lenovo XClarity Administrator tenha apenas a rede de gerenciamento (e não a rede de dados). Os números na figura correspondem às etapas numeradas nas próximas seções.

Nota: Esta figura não descreve as opções de cabeamento que podem ser necessárias para seu ambiente. Em vez disso, essa figura mostra apenas os requisitos de opção de cabeamento para comutadores Flex, CMMs e servidores de rack, pois eles estão relacionados à configuração de uma rede somente de gerenciamento.

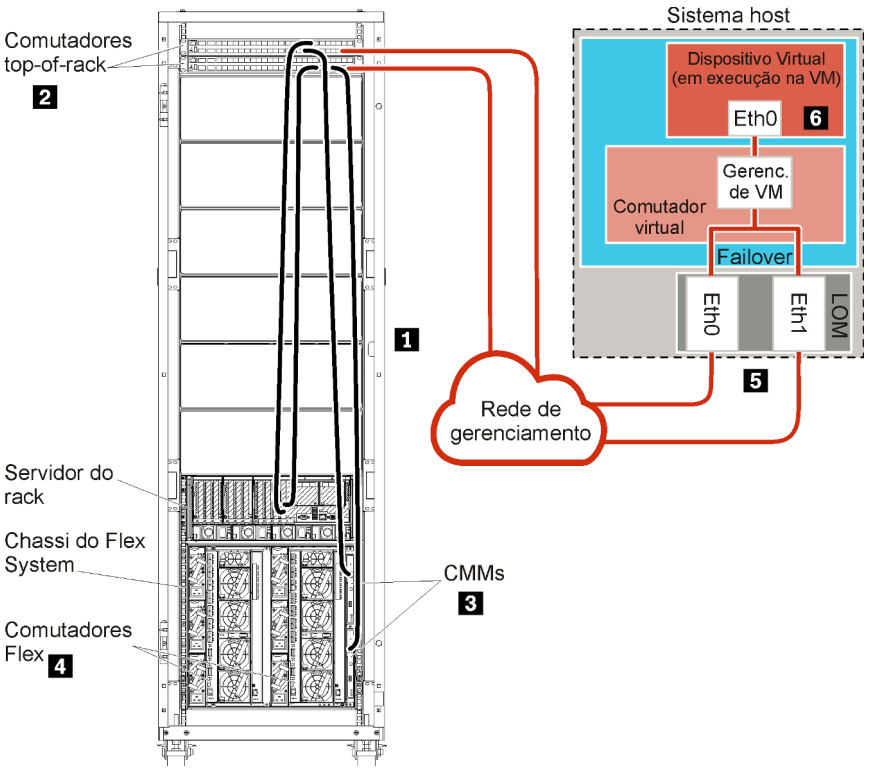


Figura 21. Exemplo de topologia de rede somente de gerenciamento para um dispositivo virtual

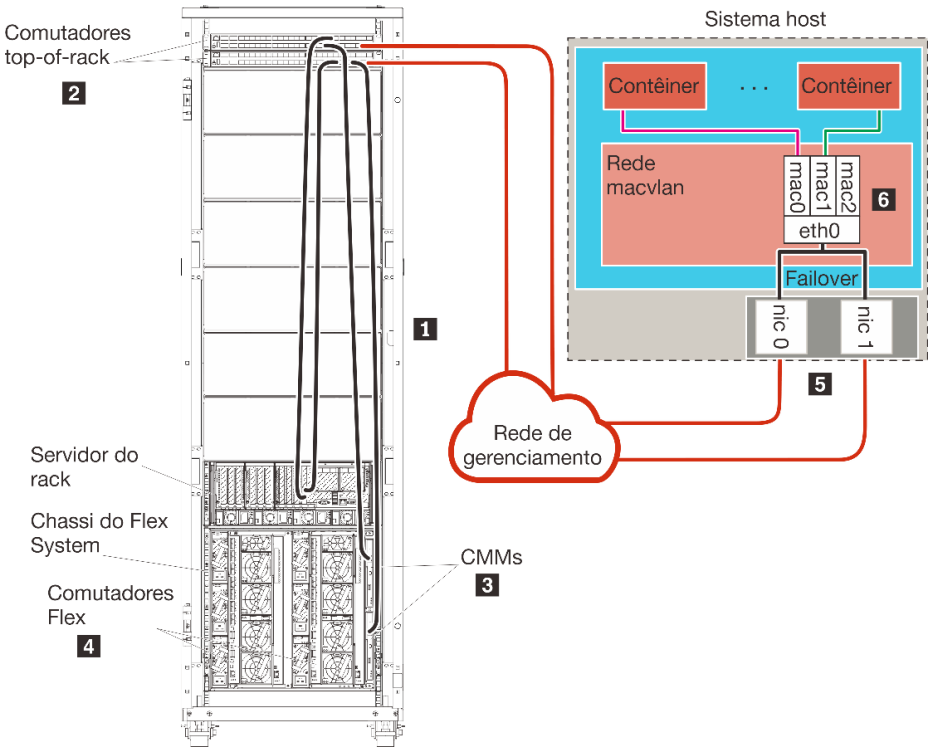


Figura 22. Exemplo de topologia de rede somente de gerenciamento para contêineres

Caso pretenda instalar o XClarity Administrator para gerenciar o chassi existente e os servidores de rack que já foram configurados, vá para Etapa 5: Instalar e configurar o host.

Para obter informações adicionais sobre o planejamento dessa topologia, incluindo informações sobre configurações de rede e configuração de Eth0 e Eth1, consulte Rede somente de gerenciamento.

Etapa 1: Passe o cabo do chassi, dos servidores de rack e do host do Lenovo XClarity Administrator nos comutadores top-of-rack

Conecte o chassi, os servidores de rack e o host do XClarity Administrator aos comutadores top-of-rack para ativar a comunicação entre os dispositivos e a rede.

Procedimento

Conecte cada comutador Flex e CMM em cada chassi, cada servidor de rack e no host do XClarity Administrator aos dois comutadores top-of-rack. É possível escolher qualquer porta nos comutadores top-of-rack.

A figura a seguir é um exemplo que ilustra o cabeamento do chassi (comutadores Flex e CMMs), servidores de rack e host do XClarity Administrator para comutadores top-of-rack.

Nota: Esta figura não descreve as opções de cabeamento que podem ser necessárias para seu ambiente. Em vez disso, essa figura mostra apenas os requisitos de opção de cabeamento para comutadores Flex, CMMs e servidores de rack, pois eles estão relacionados à configuração de uma rede somente de gerenciamento.

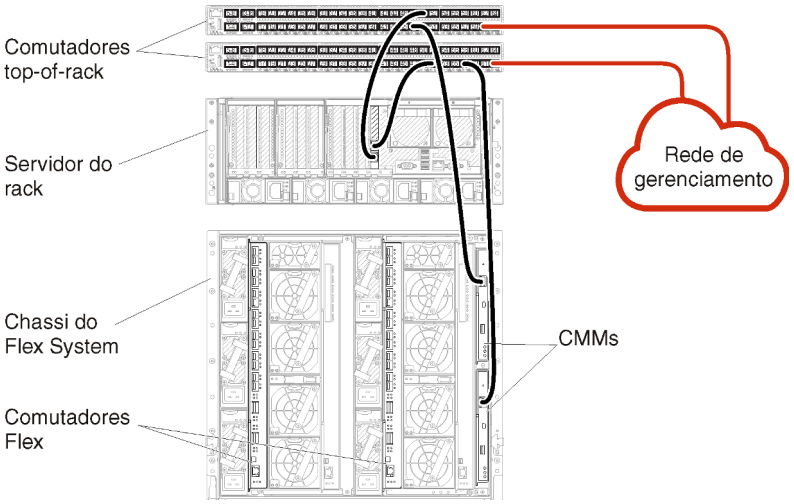


Figura 23. Exemplo de cabeamento para uma rede somente de gerenciamento

Etapa 2: Configurar comutadores top-of-rack

Configure os comutadores top-of-rack.

Antes de iniciar

Além dos requisitos de configuração típicos para comutadores top-of-rack, verifique se todas as portas apropriadas estão ativadas, incluindo portas externas ao Comutadores Flex, servidores de rack e rede, e portas internas ao CMM, servidores de rack e rede.

Procedimento

As etapas de configuração podem variar, dependendo do tipo de comutador de rack instalado.

Para obter informações sobre como configurar comutadores top-of-rack da Lenovo, consulte Comutadores de rack na documentação online do System x. Se outro comutador top-of-rack estiver instalado, consulte a documentação fornecida com esse comutador.

Etapa 3: Configurar Chassis Management Modules (CMMs)

Configure o Chassis Management Module (CMM) primário no chassi para gerenciar todos os dispositivos no chassi.

Sobre esta tarefa

Para obter informações detalhadas sobre como configurar um CMM, consulte Configurando componentes do chassi na documentação online do Flex System.

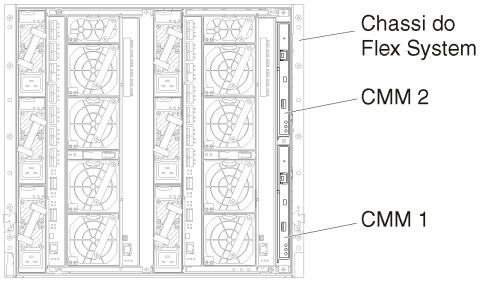
Além disso, consulte as etapas 4.1 a 4.5 do pôster de instrução fornecido com o chassi.

Procedimento

Conclua as etapas a seguir para configurar o CMM.

Se dois CMMs estiverem instalados, configure apenas o CMM *primário*, que sincroniza automaticamente a configuração com o CMM de espera.

Etapa 1. Conecte um cabo Ethernet do CMM no compartimento 1 a uma estação de trabalho do cliente para criar uma conexão direta.



Para conectar-se ao CMM pela primeira vez, talvez seja necessário alterar as propriedades de Internet Protocol na estação de trabalho do cliente.

Importante: Verifique se a sub-rede da estação de trabalho do cliente é a mesma sub-rede do CMM. A sub-rede dos CMM padrão é 255.255.255.0. O endereço IP escolhido para a estação de trabalho do cliente deve estar na mesma rede do CMM (por exemplo, 192.168.70.0 a 192.168.70.24).

Etapa 2. Para iniciar a interface de gerenciamento do CMM, abra um navegador da Web na estação de trabalho do cliente e direcione-o ao endereço IP do CMM.

Notas:

- Certifique-se de usar uma conexão segura e inclua **https** no URL (por exemplo, https://192.168.70.100). Se você não incluir https, receberá um erro de página não encontrada.
- Se você usar o endereço IP padrão 192.168.70.100, a interface de gerenciamento do CMM poderá levar alguns minutos para estar disponível. Esse atraso ocorre porque o CMM tenta obter um endereço DHCP por dois minutos antes de voltar para o endereço estático padrão.

Etapa 3. Faça login na interface de gerenciamento do CMM usando o ID do usuário padrão `USERID` e a senha `PASSWORD`. Depois de fazer login, você deve alterar a senha padrão.

Etapa 4. Conclua o Assistente de Configuração Inicial do CMM para especificar os detalhes do seu ambiente. O Assistente de Configuração Inicial inclui as seguintes opções:

- Veja o inventário e a integridade do chassi.
- Importe a configuração de um arquivo de configuração existente.
- Defina as configurações gerais do CMM.
- Configure data e hora do CMM.

  Dica: Ao instalar o XClarity Administrator, configure XClarity Administrator e todos os chassis gerenciados pelo XClarity Administrator para um servidor NTP.
- Configure as informações de IP do CMM.
- Configure a política de segurança do CMM.
- Configure o Sistema de Nomes de Domínio (DNS).
- Configure os encaminhadores de eventos.

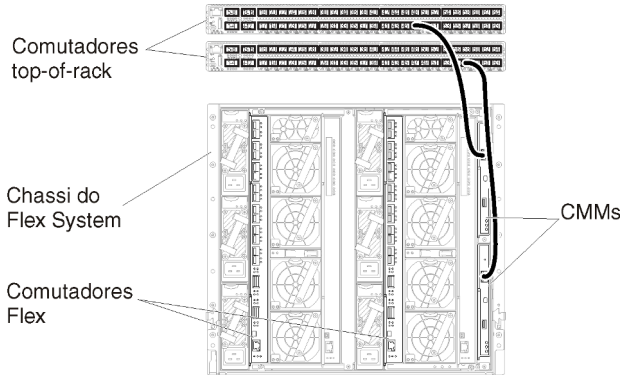
Etapa 5. Após salvar as configurações do assistente de configuração e aplicar as alterações, configure os endereços IP de todos os componentes no chassi.

Consulte a etapa 4.6 do pôster de instrução fornecido com o chassi.

Nota: Você deve redefinir o processador de gerenciamento de sistemas para cada nó de cálculo e reiniciar os comutadores Flex para mostrar os novos endereços IP.

Etapa 6. Reinicie o CMM usando a interface de gerenciamento do CMM.

Etapa 7. Durante a reinicialização do CMM, conecte um cabo da porta Ethernet no CMM à rede.



Etapa 8. Faça login na interface de gerenciamento do CMM usando o novo endereço IP.

Depois de concluir

Também é possível configurar o CMM para suportar redundância. Use o sistema de ajuda do CMM para saber mais sobre os campos disponíveis em cada uma das seguintes páginas.

- Configure o failover para o CMM se houver uma falha de hardware no CMM primário. Na interface de gerenciamento do CMM, clique em **Gerenciamento do Módulo de Gerenciamento → Propriedades → Failover Avançado**.
- Configure o failover em resultado de um problema de rede (uplink). Na interface de gerenciamento do CMM, clique em **Gerenciamento do Módulo de Gerenciamento → Rede**, clique na guia **Ethernet** e, em seguida, em **Ethernet Avançada**. No mínimo, selecione **Failover em caso de perda de link de rede física**.

Etapa 4: Configurar o Comutadores Flex

Configure o Comutadores Flex em cada chassi.

Antes de iniciar

Verifique se todas as portas apropriadas estão ativadas, incluindo portas externas do comutador Flex ao comutador top-of-rack e portas internas no CMM.

Se os comutadores Flex estiverem configurados para obter configurações de rede dinâmicas (endereço IP, gateway e endereço DNS) via DHCP, garanta que os comutadores Flex tenham configurações consistentes (por exemplo, verifique se os endereços IP estão na mesma sub-rede que o CMM).

Importante: Para cada chassi do Flex System, verifique se o tipo de malha da placa de expansão em cada servidor no chassi é compatível com o tipo de malha de todos os comutadores Flex no mesmo chassi. Por exemplo, se os comutadores Ethernet estiverem instalados em um chassi, todos os servidores desse chassi deverão ter conectividade Ethernet por meio do conector LAN na placa-mãe ou uma placa de expansão Ethernet. Para obter mais informações sobre como configurar comutadores Flex, consulte Configurando módulos de E/S na documentação online do Flex Systems.

Procedimento

As etapas de configuração podem variar, dependendo do tipo de Comutadores Flex instalado. Para obter mais informações sobre cada Comutadores Flex compatível, consulte Comutadores de rede do Flex System na documentação online do Flex Systems.

Normalmente, é necessário configurar os comutadores Flex nos compartimentos 1 e 2 de comutador Flex.

Dica: O compartimento 2 do comutador Flex é o terceiro compartimento do módulo olhando da traseira do chassi.

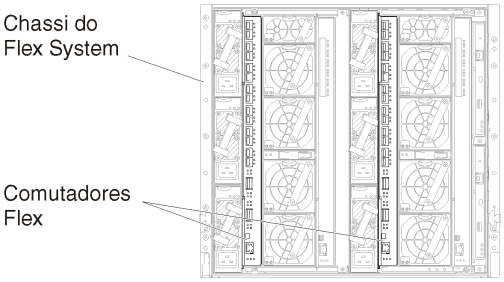


Figura 24. Locais de Comutador Flex em um chassi

Etapa 5: Instalar e configurar o host

É possível instalar o Docker em qualquer sistema que atenda aos requisitos para o Lenovo XClarity Administrator.

Antes de iniciar

É possível usar o Docker Datacenter para configurar um ambiente de alta disponibilidade para contêineres do XClarity Administrator em execução no Docker Engine. Para obter mais informações sobre a alta disponibilidade do Docker Datacenter, consulte Página da Web Arquitetura e aplicativos de alta disponibilidade com o Docker Datacenter.

Verifique se o host satisfaz os pré-requisitos definidos em Pré-requisitos de hardware e software.

Verifique se o sistema do host está na mesma rede que os dispositivos que deseja gerenciar.

Importante: É possível configurar o XClarity Administrator em qualquer sistema que atenda aos requisitos para XClarity Administrator, incluindo um servidor gerenciado. Se você usa um servidor gerenciado para o host do XClarity Administrator:

- Deve implementar uma topologia de rede de gerenciamento e dados separados virtualmente ou uma topologia de rede de gerenciamento e dados únicos.
- Não pode usar XClarity Administrator para aplicar atualizações de firmware a esse servidor gerenciado. Mesmo quando apenas alguns firmwares são aplicados com ativação imediata, o XClarity Administrator força o servidor de destino a reiniciar, o que reinicia também o XClarity Administrator. Quando aplicado com ativação adiada, apenas alguns firmwares são aplicados quando o host do XClarity Administrator é reiniciado.
- Se você usar um servidor em um chassi do Flex System, garanta que o servidor esteja configurado para ligar automaticamente. É possível definir essa opção na interface da Web do CMM clicando em **Gerenciamento de Chassi → Nós de Cálculo**, selecionando o servidor e **Ativação Automática** para o **Modo de Ativação Automática**.

Procedimento

Instale e configure o Docker no host usando as instruções que são fornecidas com a distribuição do Docker.

Etapa 6. Instalar e configurar o XClarity Administrator

Instale e configure o contêiner do Lenovo XClarity Administrator no host do Docker que acabou de ser instalado.

Antes de iniciar

O sistema host físico deve atender aos requisitos mínimos de hardware e software (consulte Pré-requisitos de hardware e software).

Verifique se todas as portas apropriadas estão ativadas, incluindo portas exigidas pelo XClarity Administrator (consulte Disponibilidade de porta).

Verifique se o sistema do host está na mesma rede que os dispositivos que deseja gerenciar.

Verifique se o SO do host e o XClarity Administrator usam o mesmo servidor NTP.

O XClarity Administrator permite que um nome personalizado da rede seja usado para gerenciamento de dados, gerenciamento de hardware e implantação do SO (consulte Configurações de rede). Este exemplo no procedimento a seguir usa eth0.

O XClarity Administrator permite que um nome personalizado da rede seja usado para gerenciamento de dados e hardware (consulte Configurações de rede). Este exemplo no procedimento a seguir usa eth0

Verifique se uma rede macvlan está carregada no kernel no sistema host. Para verificar se ela está carregada, use o comando **lsmod | grep macvlan**. Para carregar a macvlan no kernel, execute o comando **modprobe macvlan**.

Use um nome exclusivo e endereço IP para cada contêiner ao executar vários contêineres do XClarity Administrator no mesmo host.

Se você pretende gerenciar o ThinkServer e outros dispositivos legados, o Docker deve estar habilitado para dar suporte ao IPv6.

1. Edite o arquivo /etc/docker/daemon.json, defina a chave **ipv6** como true e defina a chave **fixed-cidr-v6** como sua sub-rede IPv6. Veja a seguir um exemplo de arquivo daemon.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Recarregue o arquivo de configuração do Docker executando o comando a seguir.
```
systemctl reload docker
```

Nota: O XClarity Administrator *não é* executado como um contêiner privilegiado.

Procedimento

Para instalar um contêiner do XClarity Administrator usando a composição do Docker, conclua as etapas a seguir.

Etapa 1. Baixe a imagem do dispositivo virtual do XClarity Administrator, o arquivo de ambiente e o arquivo YAML do Página da Web de download do XClarity Administrator para uma estação de trabalho do

cliente. Faça login no Web site e, em seguida, use a tecla de acesso que foi fornecida para baixar a imagem.

Etapa 2. Importe a imagem de contêiner do XClarity Administrator para seu host do docker executando o comando a seguir.

```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Etapa 3. Edite o arquivo `docker_compose.env` e atualize as variáveis de ambiente a seguir.

- **CONTAINER_NAME**. Nome exclusivo do contêiner, usado para criar volumes de docker para cada instância do XClarity Administrator (por exemplo, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Endereço estático IPv4 para o contêiner (por exemplo, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Opcional) Caminho para o compartilhamento remoto que pode ser usado para armazenar backups do XClarity Administrator. Deve ser `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Opcional) Caminho para o compartilhamento remoto que pode ser usado como um repositório remoto para atualizações de firmware. Deve ser `/mnt/fw_share`.

Veja a seguir um exemplo de arquivo de ambiente.

```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Etapa 4. Edite o `docker_compose.yml` e atualize as propriedades a seguir.

- Defina a propriedade **image** como o nome do arquivo de imagem de instalação usado na etapa 2.

  Nota: É possível alterar o nome do arquivo de imagem (por exemplo, para "mais recente") usando o comando `docker tag`.
- Se você deseja usar compartilhamentos remotos como um repositório de firmware remoto e armazenar backups do XClarity Administrator, defina o ponto de montagem do host para cada compartilhamento remoto na propriedade **volumes**.
- Defina a propriedade **dns** como o endereço IP dos servidores DNS.
- O contêiner compartilha o conjunto de recursos de processador e memória que estão disponíveis para o host. Opcionalmente, defina limites de uso de recurso configurando as propriedades **cpus** e **memória**.
- Defina a propriedade **parent** como o nome da interface de rede no sistema host que deve ser usada como a interface pai para a interface macvlan no contêiner. Essa interface deve ter acesso direto à sub-rede atribuída ao contêiner.
- Defina a **sub-rede** e o **gateway** de acordo com a topologia de rede. Normalmente, a sub-rede e o gateway se destinam à rede de gerenciamento, à qual pertence o ${ADDRESS}.
- Se você deseja dar suporte ao IPv6, defina a propriedade **enable_ipv6** como true, defina a propriedade **ipv6_address** como o endereço IPv6 e adicione outro conjunto de propriedades de **sub-rede** e **gateway** de acordo com sua topologia de rede (geralmente para rede de gerenciamento à qual o endereço IPv6 pertence).

Veja a seguir um arquivo YML de exemplo, com IPv6 habilitado.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
```

```
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
```

```
gateway: "2001:8003:7d51:2000::1"
```

Etapa 5. Implante a imagem no docker executando o comando a seguir, em que <*ENV_FILENAME*> é o nome do arquivo de variáveis do ambiente criado na etapa 2.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

Depois de concluir

Faça login e configure o XClarity Administrator (consulte Acessando a interface da Web do Lenovo XClarity Administrator pela primeira vez e Configurando Lenovo XClarity Administrator).

Implementando alta disponibilidade

É possível usar o Docker Datacenter para configurar um ambiente de alta disponibilidade para contêineres do Lenovo XClarity Administrator em execução no Docker Engine.

Para obter mais informações sobre a alta disponibilidade do Docker Datacenter, consulte Página da Web Arquitetura e aplicativos de alta disponibilidade com o Docker Datacenter.

Capítulo 4. Configurando Lenovo XClarity Administrator

Quando você acessa o Lenovo XClarity Administrator pela primeira vez, há diversas etapas que devem ser concluídas para configurar inicialmente o XClarity Administrator.

Saiba mais: XClarity Administrator: Configurando pela primeira vez

Procedimento

Conclua as seguintes etapas para configurar o XClarity Administrator pela primeira vez.

Etapa 1. Acesse a interface da Web do XClarity Administrator.

Etapa 2. Leia e aceite o contrato de licença.

Etapa 3. Crie contas de usuário que tenham autoridade de supervisor.

Dica: considere a possibilidade de criar pelo menos duas contas de usuário com autoridade de supervisor para ter um backup, se necessário.

Etapa 4. Configure o acesso à rede, incluindo endereços IP para as redes de dados e gerenciamento.

Etapa 5. Configure data e hora.

Etapa 6. Defina as configurações de serviço e suporte, incluindo a declaração de privacidade, os dados de uso e hardware, o Suporte Lenovo (Call Home), o Recurso de Upload da Lenovo e garantia do produto.

Etapa 7. Defina configurações de segurança, incluindo servidor de autenticação, grupos de usuários, certificados do servidor e modo de criptografia.

Etapa 8. Gerencie chassis, servidores, comutadores e dispositivos de armazenamento.

Acessando a interface da Web do Lenovo XClarity Administrator pela primeira vez

É possível iniciar a interface da Web do XClarity Administrator em qualquer computador que tenha conectividade de rede com a máquina virtual do XClarity Administrator.

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 etapas a seguir para acessar a interface da Web do XClarity Administrator pela primeira vez.

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.

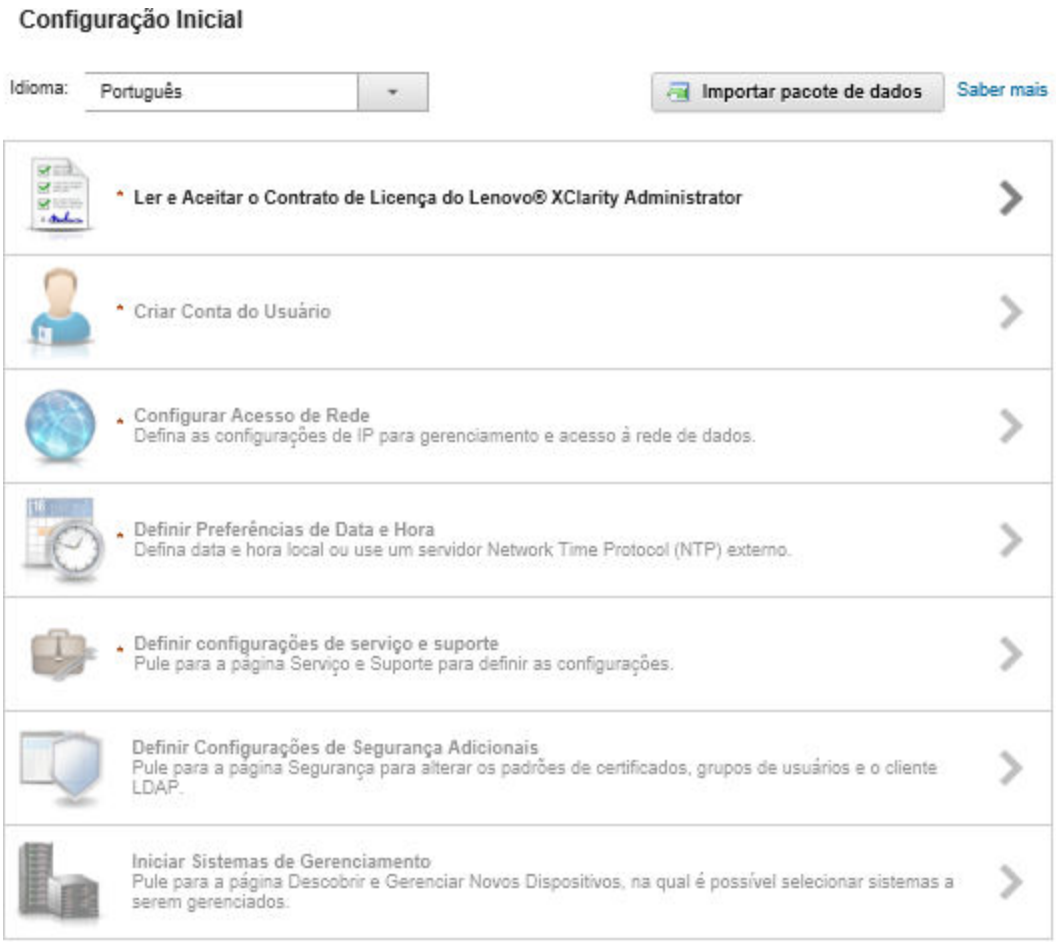
Por exemplo, com base nos exemplos mostrados para Eth0 e o índice da zona, insira o seguinte URL em seu navegador da Web:

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

Etapa 2. Você pode receber notificações de segurança ou certificado na primeira vez em que acessar o Lenovo XClarity Administrator. É possível ignorar os avisos.

Resultados

A página Configuração Inicial é exibida.



Depois de concluir

Conclua as etapas de configuração inicial para configurar o XClarity Administrator (consulte Configurando Lenovo XClarity Administrator).

Criando contas do usuário

As contas do usuário são usadas para gerenciar a autorização e o acesso ao Lenovo XClarity Administrator e a dispositivos que estão em autenticação gerenciada.

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 criar contas do usuário, conclua as etapas a seguir.

Etapa 1. Preencha as informações a seguir na caixa de diálogo Criar Novo Usuário Supervisor.

- 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 na documentação online do XClarity Administrator.
- (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 2. Clique em **Criar**.

Etapa 3. Clique no ícone **Criar** ( ) e repita as etapas anteriores para criar outros usuários.

Etapa 4. Clique em **Retornar à Configuração Inicial**.

Configurando o acesso à rede

Para configurar o acesso à rede, você pode configurar até duas interfaces de rede, o nome do host do Lenovo XClarity Administrator e os servidores DNS a serem usados.

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 3. 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 3. 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 do XClarity Administrator, consulte Considerações de rede.

Procedimento

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

Etapa 1. Na página Configuração Inicial, clique em **Configurar Acesso de Rede**. A página Editar Acesso à Rede é exibida.

Etapa 2. 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 3. Especifique 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 de IP.

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.

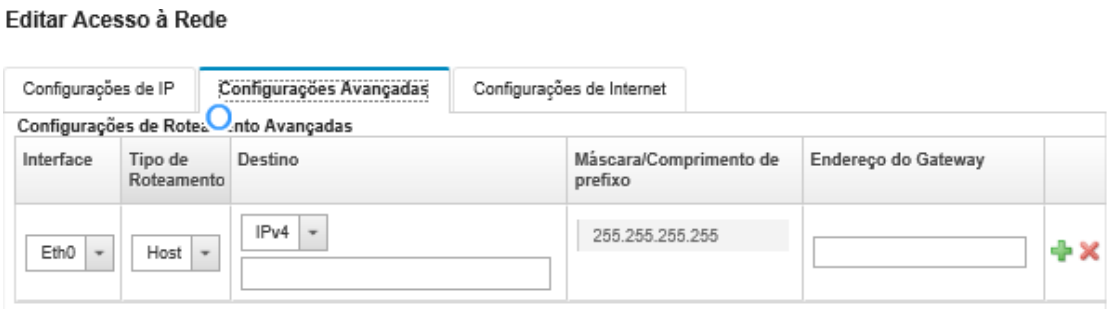
- Para voltar a um gateway fornecido pelo DHCP, desmarque a caixa de seleção **Substituir Gateway**.

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 4. **Opcional:** Defina as configurações avançadas.

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



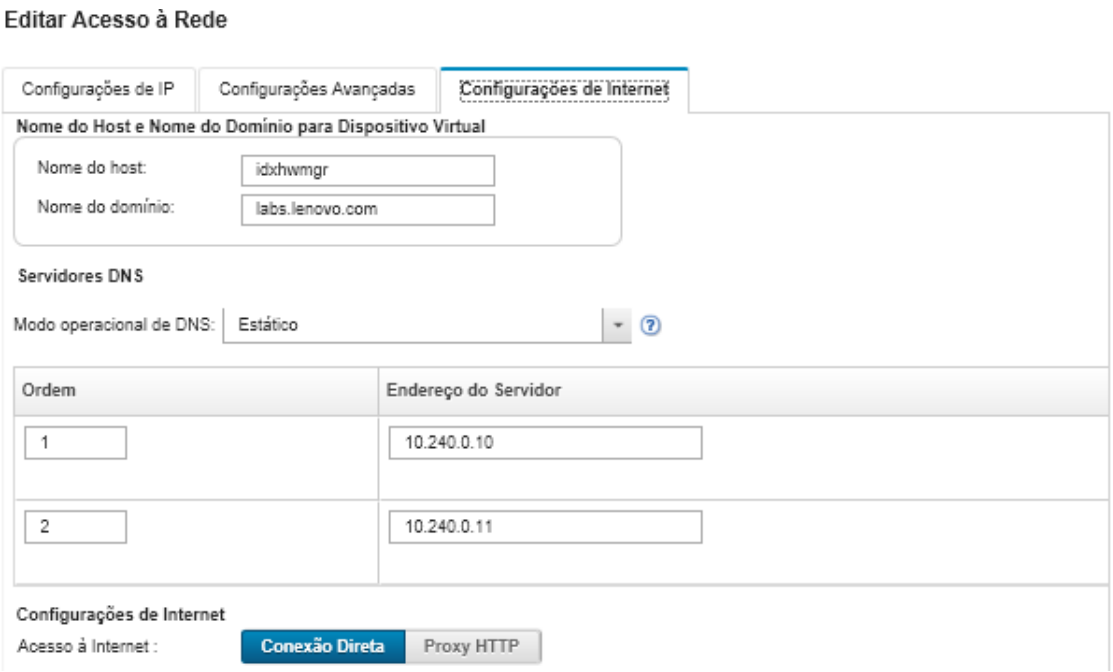
b. Especifique uma ou mais entradas de rota na tabela **Configurações de Roteamento Avançadas** a ser usada por essa interface.

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 5. Opcionalmente, modifique as configurações de DNS e proxy.

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 Trabalhando com trabalhos na documentação online do XClarity Administrator).

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 6. Clique em **Voltar**.

Etapa 7. Clique em **Testar Conexão** para verificar as configurações de rede.

Configurando data e hora

Embora você possa configurar manualmente a data e hora para Lenovo XClarity Administrator, uma abordagem melhor é configurar um servidor Network Time Protocol (NTP) que pode ser usado para sincronização de registros de data e hora entre XClarity Administrator e todos os dispositivos gerenciados.

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.

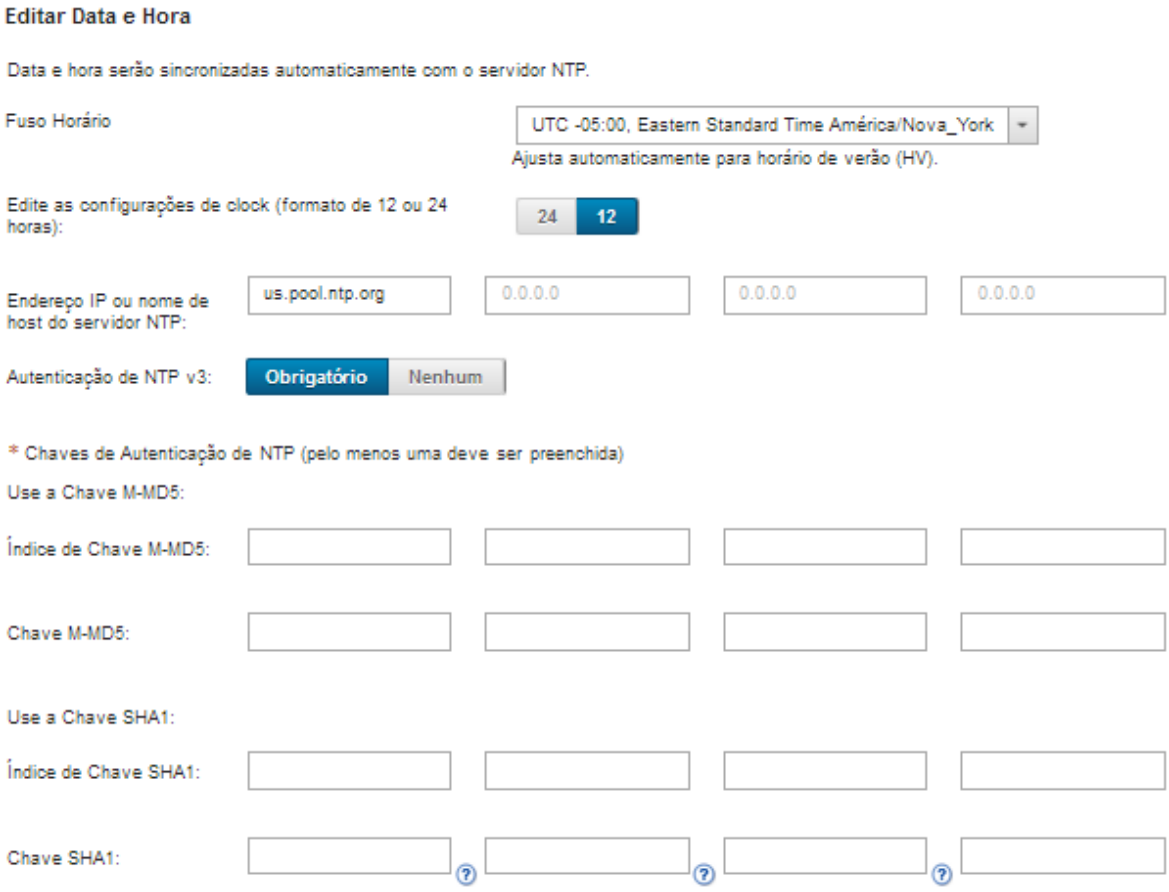
- Para o ESXi, seguindo as instruções no VMware – Página Desabilitar Sincronização de Tempo.

- 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

Para configurar um servidor NTP para o XClarity Administrator, conclua as seguintes etapas.

Etapa 1. Na página Configuração Inicial, clique em **Definir Preferências de Data e Hora**. A página Editar Data e Hora é exibida.



Etapa 2. 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 3. Clique em **Salvar**.

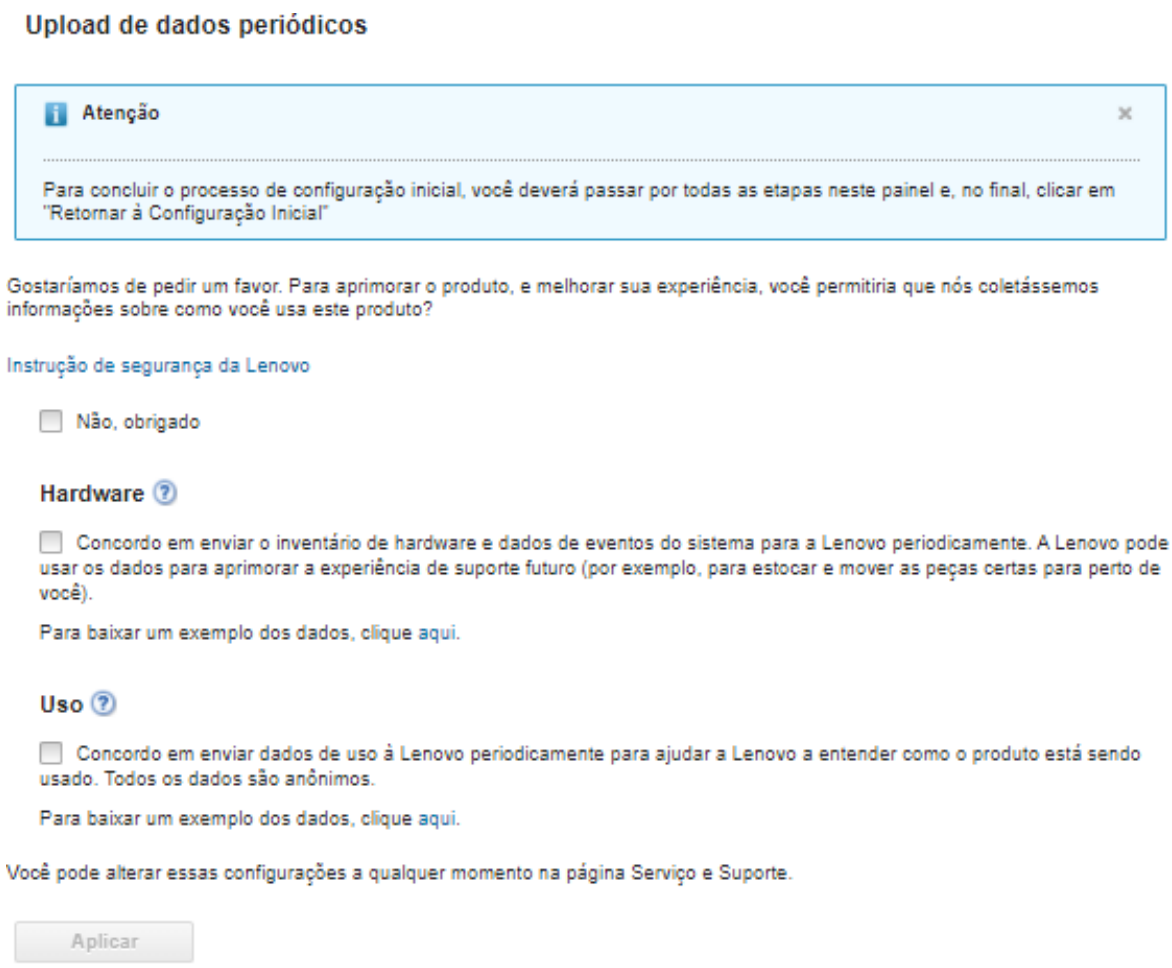
Configurando serviço e suporte

É possível definir as configurações de serviço e suporte, incluindo os dados de uso, o Suporte Lenovo (Call Home), o Recurso de Upload da Lenovo e garantia do produto.

Procedimento

Conclua as seguintes etapas para configurar a segurança.

Etapa 1. Na página Configuração Inicial, clique em **Definir Configurações de Serviço e Suporte**. A página Serviço e Suporte é exibida.



Etapa 2. Leia e aceite o Instrução de privacidade da Lenovo.

Nota: Não é possível coletar e enviar dados para a Lenovo sem primeiro aceitar o Instrução de privacidade da Lenovo. Se você optar por recusar a política de privacidade, poderá examinar e aceitar a política de privacidade posteriormente na página **Serviço e Suporte → Configuração de Call Home**.

Etapa 3. Como opção, permita que o Lenovo XClarity Administrator colete informações de uso e hardware e clique em **Aplicar**.

É possível coletar e enviar os seguintes tipos de dados para a Lenovo.

- **Dados de uso**

  Quando você concorda em enviar dados de uso para a Lenovo, os dados a seguir são coletados e enviados semanalmente. Esses dados *são anônimos*. Nenhum dado privado (incluindo números de série, UUIDs, nomes de host, endereços IP e nomes de usuário) é coletado ou enviado para a Lenovo.
  - Log de ações executadas
  - Lista de eventos que foram gerados e o carimbo de data e hora em que foram gerados
  - Lista de eventos de auditoria que foram gerados e o carimbo de data e hora em que foram gerados
  - Lista de trabalhos que foram executados e informações de êxito ou falha para cada trabalho
  - Métricas do XClarity Administrator, incluindo uso da memória, uso do processador e espaço em disco
  - Dados do inventário limitados sobre todos os dispositivos gerenciados

- **Dados de hardware**

  Quando você concorda em enviar dados de hardware para a Lenovo, os dados a seguir são coletados e enviados periodicamente. Esses dados *não são anônimos*. Os dados de hardware incluem atributos, como UUIDs e números de série. Não incluem endereços IP ou nomes de host.

  - **Dados de hardware diários**. Os dados a seguir são incluídos para cada alteração de inventário.
    - Evento de alteração de inventário (FQXHMDM0001I)
    - Alterações nos dados de inventário do dispositivo associado a esse evento
  - **Dados de hardware semanais**. Os dados do inventário são incluídos para todos os dispositivos gerenciados.

Quando os dados de uso e hardware são enviados para a Lenovo, um evento é registrado no log de auditoria.

É possível alterar essa configuração a qualquer momento e fazer download do último arquivo que foi coletado e enviado para a Lenovo usando os links ao clicar em **Administração → Serviço e Suporte** e ao clicar na guia **Upload de Dados Periódico**.

Etapa 4. Como opção, clique em **Configuração de Call Home** para configurar a notificação automática de problemas para o Suporte Lenovo (Call Home). Em seguida, clique em **Aplicar e Habilitar** para criar o encaminhador de serviço de Call Home padrão ou clique em **Aplicar somente** para salvar as informações de contato.

Para obter mais informações sobre como configurar a notificação automática de problemas para o Suporte Lenovo, consulte Configurando call home na documentação online do XClarity Administrator.

Etapa 5. Como opção, clique em **Recurso de Upload da Lenovo** para configurar a notificação automática de problemas para o Recurso de Upload da Lenovo. Em seguida, clique em **Aplicar e Habilitar** para criar o encaminhador de serviço do Recurso de Upload da Lenovo padrão ou clique em **Aplicar somente** para salvar as informações de configuração.

Para obter mais informações sobre como configurar a notificação automática de problemas 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.

Etapa 6. Como opção, clique em **Garantia** para ativar as conexões externas necessárias para coletar informações sobre garantia para seus dispositivos gerenciados.

Para obter mais informações sobre como exibir o status da garantia (inclusive garantias estendidas) dos dispositivos gerenciados, consulte Visualizando informações sobre garantia na documentação online do XClarity Administrator.

Etapa 7. Opcionalmente, clique em **Serviço de Boletim Lenovo** para permitir que a Lenovo envie boletins de serviço para o XClarity Administrator e clique em **Aplicar**.

Para obter mais informações sobre os tipos de boletins de serviço que a Lenovo envia, consulte Obtendo boletins da Lenovo na documentação online do XClarity Administrator.

Etapa 8. Especifique a senha de recuperação de serviço que você pode usar para coletar e baixar dados de serviço e os logs se o XClarity Administrator para de responder e não for possível recuperá-lo.

Para obter mais informações sobre a senha de recuperação do serviço, consulte Alterando a senha de recuperação de serviço na documentação online do XClarity Administrator.

Etapa 9. Clique em **Retornar à Configuração Inicial**.

Configurando a segurança

É possível configurar a segurança, incluindo grupos de funções, servidor de autenticação, configurações de segurança da conta de usuário, criptografia e certificados.

Procedimento

Conclua as seguintes etapas para configurar a segurança.

Etapa 1. Na página Configuração Inicial, clique em **Definir Configurações de Segurança Adicionais**. A página Segurança é exibida.

Etapa 2. Crie grupos de funções personalizados para gerenciar a autorização e o acesso aos recursos (consulte Criando um grupo de funções na documentação online do XClarity Administrator).

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

Etapa 3. Configure o servidor de autenticação (consulte Gerenciando o servidor de autenticação na documentação online do XClarity Administrator).

O *servidor de autenticação* é um servidor Microsoft Active Directory (LDAP) que é usado para autenticar as credenciais do usuário. O XClarity Administrator usa um único servidor de autenticação para gerenciamento de usuários central de todos os dispositivos gerenciados (exceto comutadores Flex). Quando um dispositivo é gerenciado por XClarity Administrator, o dispositivo gerenciado e seus componentes instalados (exceto comutadores Flex) são configurados para usar o servidor de autenticação do XClarity Administrator. As contas do usuário definidas no servidor de autenticação são usadas para fazer login no XClarity Administrator, CMMs e Baseboard Management Controller.

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

Etapa 4. Defina configurações de segurança de conta do usuário, que controlam a complexidade da senha, o bloqueio da conta, o tempo limite de inatividade da sessão da Web (consulte Alterando as configurações de segurança de conta do usuário na documentação online do XClarity Administrator).

Etapa 5. Defina a configuração de criptografia que define os modos e protocolos de comunicação que controlam a maneira como as comunicações seguras são manipuladas entre o XClarity Administrator e os dispositivos gerenciados (consulte Configurando o modo de criptografia e protocolos de comunicação na documentação online do XClarity Administrator)

Etapa 6. Se você pretende gerenciar servidores em rack usando a autenticação local em vez da autenticação gerenciada do XClarity Administrator, crie uma ou mais as credenciais armazenadas que correspondem às contas de usuário ativas no dispositivo ou no Active Directory que podem ser usadas para fazer login nos dispositivos durante o processo de gerenciamento. Para obter mais informações sobre credenciais armazenadas, consulte Gerenciando credenciais compartilhadas na documentação online do XClarity Administrator.

Etapa 7. Se você pretende usar um certificado de servidor personalizado que inclua suas próprias informações ou usar um certificado assinado externamente, gerencie e implante o novo certificado antes de começar a gerenciar sistemas. Para obter informações sobre como gerar seu próprio certificado de segurança, consulte Trabalhando com certificados de segurança na documentação online do XClarity Administrator.

Etapa 8. No menu vertical na página Segurança, clique em **Retornar à Configuração Inicial**.

Gerenciando dispositivos

O Lenovo XClarity Administrator pode gerenciar diversos tipos de sistemas, incluindo o chassi do Flex System, servidores em rack e em torre, comutadores RackSwitch e dispositivos de armazenamento. Você pode descobrir e gerenciar facilmente um grande número de dispositivos que estão em seu ambiente importando informações sobre os dispositivos com o uso de um arquivo de importação em massa.

Antes de iniciar

Importante:

- É possível gerenciar no máximo 300 dispositivos ao mesmo tempo. Não inclua mais de 300 dispositivos em um arquivo de importação em massa.
- Depois de iniciar uma operação de gerenciamento de dispositivo, aguarde a conclusão de todo o trabalho de gerenciamento antes de iniciar outra operação de gerenciamento de dispositivo.

Os componentes do chassi (como CMMs, nós de cálculo, comutadores e dispositivos de armazenamento) são descobertos e gerenciados automaticamente ao gerenciar o chassi que os contêm. Não é possível descobrir e gerenciar componentes do chassi separados do chassi.

Algumas portas devem estar disponíveis para comunicação com os CMMs em chassis e Baseboard Management Controllers nos servidores. Assegure-se de que essas portas estejam disponíveis antes de tentar gerenciar sistemas. Para obter mais informações sobre portas, consulte Disponibilidade de porta.

Verifique se o firmware mínimo necessário está instalado em cada sistema 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 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.

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).

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.

Importante:

- 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.
- O encaminhamento SLP multicast deve ser ativado em cada dispositivo de armazenamento para que possa ser descoberto pelo XClarity Administrator.
- Se você pretende usar um certificado de servidor personalizado que inclua suas próprias informações ou usar um certificado assinado externamente, gerencie e implante o novo certificado antes de começar a gerenciar sistemas. Para obter informações sobre como gerar seu próprio certificado de segurança, consulte Trabalhando com certificados de segurança na documentação online do XClarity Administrator.

- 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.
- 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

Sobre esta tarefa

O XClarity Administrator pode descobrir sistemas em seu ambiente procurando dispositivos gerenciáveis que estão na mesma sub-rede IP que XClarity Administrator, usando um endereço IP ou intervalo de endereços IP especificados ou importando informações de uma planilha.

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 Gerenciando servidores na documentação online do XClarity Administrator).

  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.

Após os sistemas serem gerenciados pelo XClarity Administrator, o XClarity Administrator sonda cada sistema gerenciado periodicamente para coletar informações, como inventário, dados vitais do produto e status. É possível exibir e monitorar cada sistema gerenciado e executar ações de gerenciamento (como definir configurações do sistema, implantar imagens de sistema operacional e ligar e desligar o equipamento).

Um sistema pode ser gerenciado somente por um XClarity Administrator por vez. Não há suporte para o gerenciamento por vários gerenciadores. Se um sistema for gerenciado por um XClarity Administrator e você quiser gerenciá-lo com o outro XClarity Administrator, deverá primeiro cancelar o gerenciamento do sistema no XClarity Administrator atual. Em seguida, é possível gerenciar o sistema com outro XClarity Administrator. Para obter mais informações sobre como cancelar o gerenciamento de um sistema, consulte Cancelando o gerenciamento do chassi, Cancelando o gerenciamento de servidores, Cancelando o gerenciamento de um comutador RackSwitch e Cancelando o gerenciamento de um sistema de armazenamento Lenovo Storage na documentação online do XClarity Administrator.

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 sistema é gerenciado (consulte Configurando o modo de criptografia e protocolos de comunicação na documentação online do XClarity Administrator).

Nota: O XClarity Administrator pode ser preenchido previamente com o inventário de hardware para um chassi de demonstração (incluindo CMM, nós de cálculo e comutadores) e para um servidor de rack ou em torre de demonstração que simule hardware real. Os dispositivos de demonstração são preenchidos nas páginas da interface da Web e podem ser usados para demonstrar operações de gerenciamento. No entanto, as operações de gerenciamento falharão. Por exemplo, você pode criar um padrão de configuração e implantar o padrão em um servidor de demonstração, mas a implantação falhará. É possível remover os dispositivos de demonstração cancelando o gerenciamento deles (consulte Cancelando o gerenciamento do chassi e Cancelando o gerenciamento de servidores na documentação online do XClarity Administrator). Após os dispositivos de demonstração serem excluídos, não é possível gerenciá-los novamente.

Procedimento

Para descobrir e gerenciar seus sistemas no XClarity Administrator usando um arquivo de importação em massa, conclua as etapas a seguir.

Nota: Ao gerenciar comutadores usando a importação em massa, o HTTPS é ativado no comutador, e clientes de NTP no comutador são configurados para usar as configurações de NTP do servidor de gerenciamento. Para alterar essa configuração, você deve gerenciar manualmente os comutadores.

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.

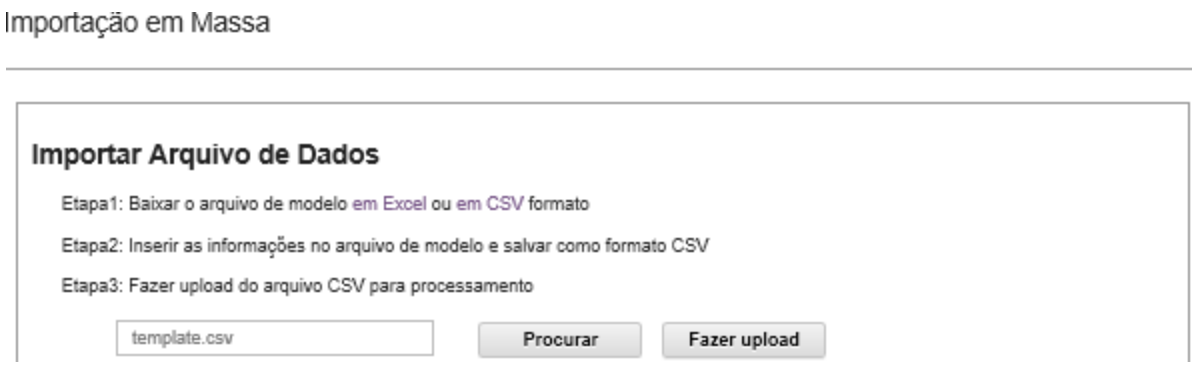
   Notas:

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

   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 Recuperando o gerenciamento de chassi com um CMM após uma falha no servidor de gerenciamento e Recuperando o gerenciamento do servidor em torre ou do rack após uma falha no servidor de gerenciamento na documentação online do XClarity Administrator.

3. Clique em **Importação em Massa**. O assistente de Importação em Massa é exibido.



4. 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.

5. Preencha a planilha de dados no arquivo de modelo e salve o arquivo em formato CSV *delimitado por vírgulas*.

   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 atribui-lo a um dispositivo.

   Para definir os dispositivos no arquivo de importação em massa, complete as seguintes colunas.

   - (Colunas A – C) Para descoberta básica, especifique o tipo de dispositivo e o endereço IP ou número de série atual do dispositivo. Os seguintes tipos são suportados:
     - **filler**. Marcadores para um dispositivo não gerenciado. Na exibição do rack, esse dispositivo é mostrado como o gráfico de preenchimento genérico. Consulte a planilha **Leia-me** no modelo de Excel para ver outros tipos de preenchimento.

- **flexchassis**. Chassi do Flex System 10U
- **server**. Servidores de rack e em torre suportados por XClarity Administrator
- **rack**. Racks 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U e 52U. Outras alturas de rack não são suportadas. 52U é usado por padrão.
- **storage**. Dispositivos de armazenamento
- **comutador**. Comutadores RackSwitch

Nota: Nós de cálculo Flex System, comutadores e dispositivos de armazenamento são considerados parte do processo de descoberta e gerenciamento de chassi.

- (Colunas D - H) Se você optar por usar credenciais inseridas manualmente em vez de credenciais armazenadas (Colunas Z) ou identidade (Colunas AF – AJ), especifique o nome de usuário e a senha atuais. Credenciais inseridas manualmente serão úteis se as credenciais forem diferentes para alguns dispositivos. Se você não especificar credenciais de um ou mais dispositivos no arquivo de importação em massa, as credenciais globais especificadas na caixa de diálogo Importação em Massa serão usadas. Para obter mais informações sobre usuários inseridos manualmente e autenticação gerenciada, consulte Gerenciando contas de usuário na documentação online do XClarity Administrator.

  Notas:

  - Para usar credenciais inseridas manualmente, você deve selecionar a autenticação gerenciada do XClarity Administrator.
  - Alguns campos não se aplicam a alguns dispositivos.
  - (Para chassis) Se você escolher autenticação gerenciada (na coluna AA ou na caixa de diálogo Importação em Massa), será possível especificar a senha de `RECOVERY_ID` na coluna G do arquivo de importação em massa ou na caixa de diálogo Importação em Massa. Se você escolher autenticação local, a senha de recuperação não será permitida; não especifique a senha de recuperação na coluna G do arquivo de importação em massa nem na caixa de diálogo Importação em Massa.
  - (Para servidores de rack) Se você escolher autenticação gerenciada (na coluna AA ou na caixa de diálogo Importação em Massa), será possível especificar opcionalmente uma senha de recuperação na coluna G do arquivo de importação em massa ou na caixa de diálogo Importação em Massa. Se você escolher autenticação local, a senha de recuperação não será permitida; não especifique a senha de recuperação na coluna G do arquivo de importação em massa nem na caixa de diálogo Importação em Massa.
  - (Para comutadores de rack) Dispositivos RackSwitch oferecem suporte apenas a credenciais armazenadas (na coluna Z) para autenticação nos comutadores. Credenciais manuais do usuário não são suportadas.
- (Colunas I -U) É possível opcionalmente fornecer informações adicionais se desejar aplicar alterações ao dispositivo após o gerenciamento bem-sucedido.

  Nota: Alguns campos não se aplicam a alguns dispositivos. Esses campos não se aplicam a comutadores RackSwitch.
- (Colunas V – Z) Como opção, você pode fornecer informações para criação e atribuição de rack, incluindo o nome do rack, o local, a sala, a menor unidade de rack e altura.

  Notas:

  - Ao criar um rack, você deve especificar o nome e a altura do rack. As seguintes alturas de rack são suportadas: Racks 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U e 52U. Outras alturas de rack não são suportadas.

  - Ao criar um filtro genérico, você deve especificar o nome do rack e a altura do preenchimento. As seguintes alturas de preenchimento são suportadas: 1U, 2U e 4U.
  - Ao criar um preenchimento específico, a altura do preenchimento será ignorada. O XClarity Administrator sabe a altura de cada preenchimento específico. Consulte a planilha de modelo para ver tipos e alturas de preenchimento.
  - Ao atribuir um dispositivo ao rack, a altura do dispositivo é ignorada. A altura do dispositivo é recuperada do inventário do dispositivo.
- (Coluna AA) 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.

  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.

  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.
- (Coluna AB) Se você optar por usar as credenciais armazenadas em vez de credenciais inseridas manualmente (colunas D – H)ou identificar (colunas AF – AJ), especifique um ID de credencial armazenada. É possível localizar o ID da credencial armazenada na página Credenciais armazenadas clicando em **Administração → Segurança** no menu do XClarity Administrator e, em seguida, clicando em **Credenciais Armazenadas** na navegação esquerda. Para obter mais informações sobre as credenciais armazenadas e autenticação local, consulte Gerenciando credenciais compartilhadas na documentação online do XClarity Administrator.

  Notas:

  - Os dispositivos RackSwtich oferecem suporte apenas a credenciais armazenadas para autenticação. Credenciais manuais do usuário (na coluna D) não são suportadas.
  - Se você gerenciar um dispositivo usando as credenciais armazenadas e ativar a autenticação gerenciada, não poderá editar essas credenciais armazenadas.
- (Coluna AC) Para chassi e servidores em rack, se você escolher usar a autenticação gerenciada, deverá especificar a senha de RECOVERY_ID na coluna G do arquivo de importação em massa ou na caixa de diálogo Importação em massa. Se você escolher autenticação local, a senha de recuperação não será permitida; não especifique a senha de recuperação na coluna G do arquivo de importação em massa nem na caixa de diálogo Importação em Massa.
- (Coluna AD) Para servidores de rack, opcionalmente, é possível optar por usar autenticação local em vez da autenticação gerenciada do XClarity Administrator especificando FALSE nesta coluna. Para obter mais informações sobre autenticação gerenciada e local, consulte Gerenciando o servidor de autenticação na documentação online do XClarity Administrator.

- (Coluna AE) Você pode especificar uma lista de grupos de funções com permissão para exibir e gerenciar o dispositivo. É possível especificar apenas grupos de funções aos quais o usuário atual pertence.

  Nota: Se você adicionar dispositivos a um chassi gerenciado, os novos dispositivos pertencerão os mesmos grupos de funções do chassi.

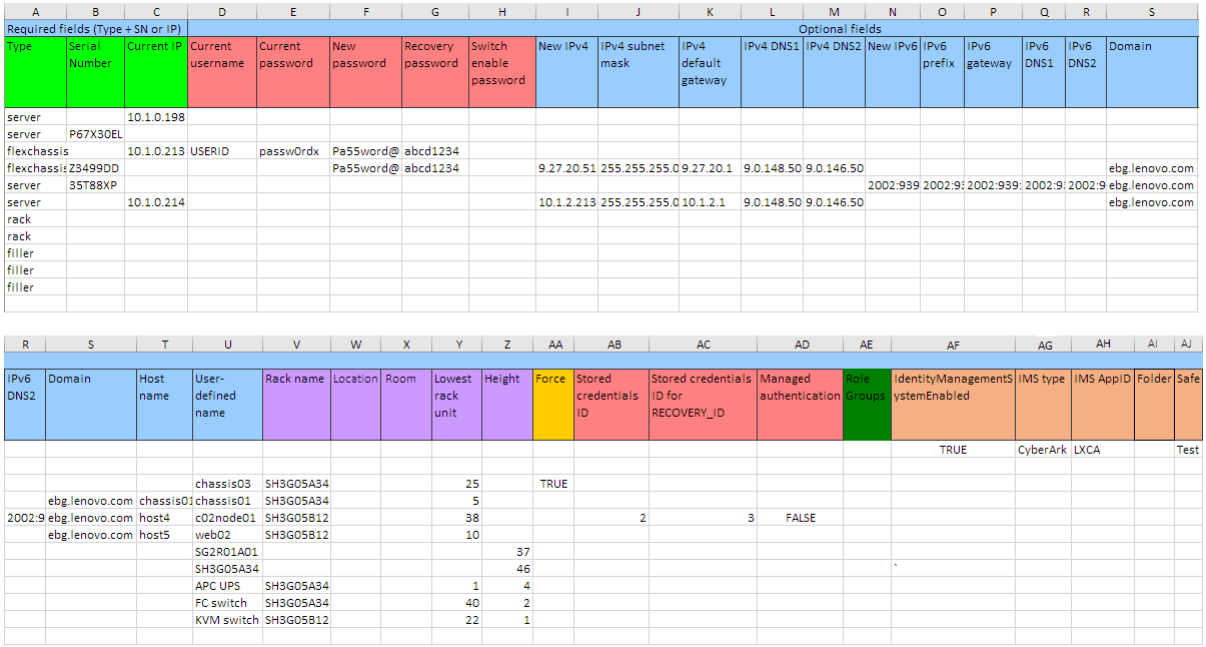
- (Coluna AF – AJ) Se você optar por usar um sistema de gerenciamento de identidade em vez de credenciais inseridas manualmente (Colunas D – H) ou credenciais armazenadas (Colunas AB), especifique o endereço IP ou o nome do host do servidor gerenciado, nome do usuário e, opcionalmente, ID do aplicativo, cofre e 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.

A figura a seguir mostra um arquivo de importação em massa de exemplo:



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Required fields (Type + SN or IP)			Optional fields															
Type	Serial Number	Current IP	Current username	Current password	New password	Recovery password	Switch enable password	New IPv4	IPv4 subnet mask	IPv4 default gateway	IPv4 DNS1	IPv4 DNS2	New IPv6	IPv6 prefix	IPv6 gateway	IPv6 DNS1	IPv6 DNS2	Domain
server		10.1.0.198																
server	P67X30EL																	
flexchassis		10.1.0.213	USERID	passw0rdx	Pa55word@	abcd1234												
flexchassis	Z3499DD				Pa55word@	abcd1234		9.27.20.51	255.255.255.0	9.27.20.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
server	3ST88XP												2002:939	2002:9	2002:939:	2002:9	2002:9	ebg.lenovo.com
server		10.1.0.214						10.1.2.213	255.255.255.0	10.1.2.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
rack																		
rack																		
filler																		
filler																		
filler																		

R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ
IPv6 DNS2	Domain	Host name	User-defined name	Rack name	Location	Room	Lowest rack unit	Height	Force	Stored credentials ID	Stored credentials ID for RECOVERY_ID	Managed authentication	Role Groups	IdentityManagementSystemEnabled	IMS type	IMS AppID	Folder	Safe
														TRUE	CyberArk	LXCA		Test
			chassis03	SH3G05A34			25		TRUE									
	ebg.lenovo.com	chassis01	chassis01	SH3G05A34			5											
2002:9	ebg.lenovo.com	host4	c02node01	SH3G05B12			38			2	3	FALSE						
	ebg.lenovo.com	host5	web02	SH3G05B12			10											
			SG2R01A01					37										
			SH3G05A34					46										
			APC UPS	SH3G05A34			1	4										
			FC switch	SH3G05A34			40	2										
			KVM switch	SH3G05B12			22	1										

6. 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.
7. Clique em **Fazer upload** para fazer upload e validar o arquivo.
8. Clique em **Avançar** para exibir a página Resumo de Entrada com uma lista de dispositivos a serem gerenciados.

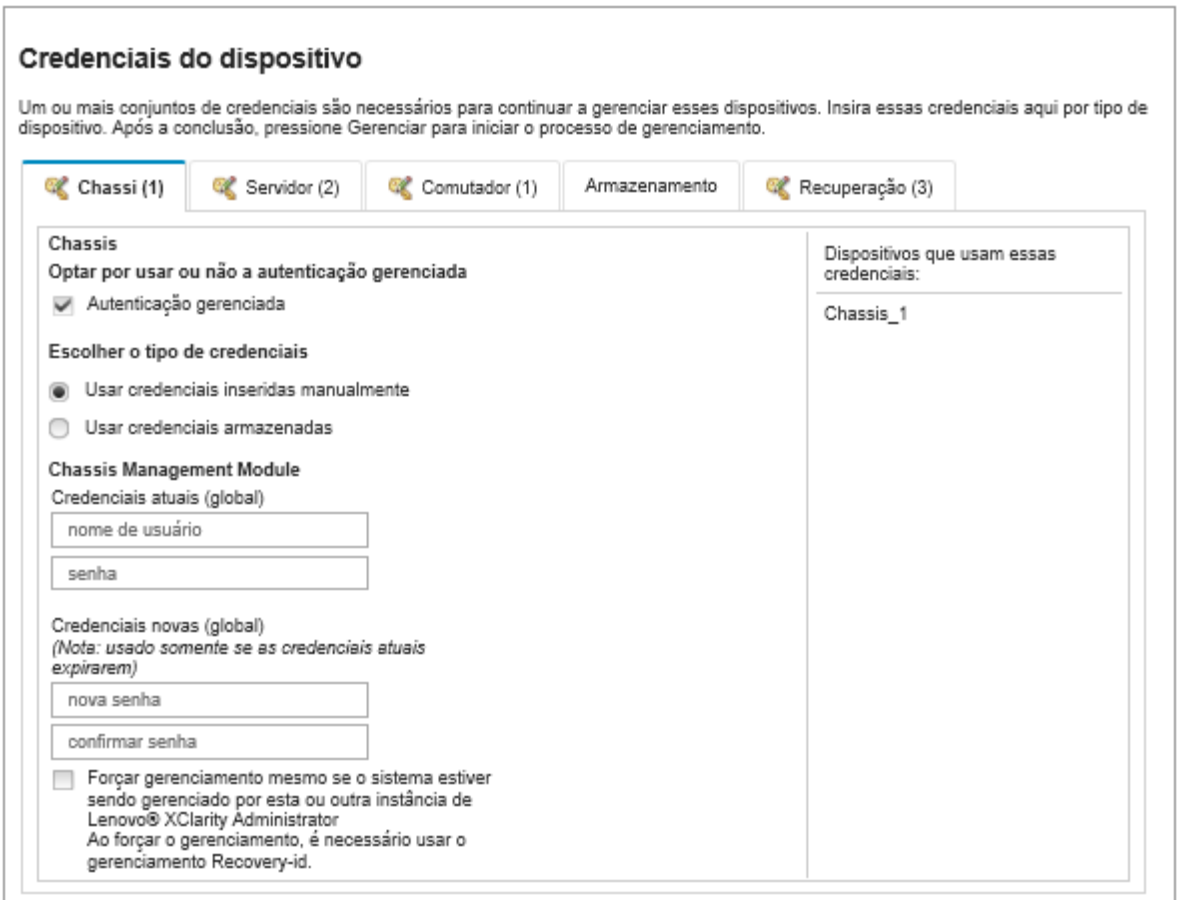
9. Revise o resumo de dispositivos que deseja gerenciar.

   Selecione **Mostrar somente as linhas com problemas** para listar linhas com dados incompletos. Corrija todos os problemas no arquivo de importação em massa e clique em **Voltar** para fazer upload do arquivo CSV corrigido.

   Notas:

   - Se os dados necessários não forem fornecidos no arquivo de importação em massa, os dispositivos associados não serão gerenciados.
   - A página Resumo de Entrada sinaliza linhas que não têm informações de credenciais. Se você não especificar credenciais no arquivo de importação em massa, as credenciais globais especificadas no assistente Importação em Massa serão usadas.

10. Clique em **Avançar** para exibir a página Credenciais do Dispositivo.



11. **Opcional:** 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.

    Se você optar por usar as credenciais globais, as credenciais de um tipo de dispositivo específico deverão ser as mesmas para todos os dispositivos do mesmo tipo que não têm credenciais inseridas no arquivo de importação em massa. Por exemplo, as credenciais do CMM devem ser as mesmas para todos os chassis e as credenciais de gerenciamento de armazenamento devem ser as mesmas para todos os dispositivos de armazenamento. Se as credenciais não forem as mesmas, você deverá inserir credenciais no arquivo de importação em massa.

    - **Chassi**. Especifique o modo de autenticação e o tipo de credenciais. Especifique as credenciais atuais para fazer login em todos os chassis definidos no arquivo de importação em massa. Especifique a nova senha a ser usada se as credenciais atuais do CMM tiverem expirado.

      Se você forçar o gerenciamento de um chassi, especifique a conta RECOVERY_ID e a senha para as credenciais do dispositivo.

    - **Servidores**. Especifique o modo de autenticação e o tipo de credenciais. Especifique as credenciais atuais para fazer login em todos os servidores em rack e em torre definidos no arquivo de importação em massa. Especifique a nova senha a ser usada se as credenciais atuais do Baseboard Management Controller tiverem expirado.

      Se você forçar o gerenciamento de um servidor, especifique a conta RECOVERY_ID e a senha para as credenciais do dispositivo.

- **Comutadores**. Especifique as credenciais armazenadas para fazer login em todos os comutadores RackSwitch definidos no arquivo de importação em massa. Se definido, especifique também a senha "enable" usada para entrar no Modo Privilegiado/Exec do comutador.
- **Armazenamento**. Especifique as credenciais atuais para fazer login em todos os dispositivos de armazenamento definidos no arquivo de importação em massa.
- **Recuperação**. Especifique a senha de recuperação para fazer login em todos os servidores e chassis definidos no arquivo de importação em massa.

  É possível optar por usar uma conta de usuário local ou credencial de recuperação armazenada. Em qualquer um dos casos, o nome do usuário é sempre `RECOVERY_ID`.

  Quando uma senha é especificada, a conta de `RECOVERY_ID` é criada no dispositivo, e todas as contas de usuário locais são desativadas.

  – Para o chassi, a senha de recuperação será necessária.
  – Para servidores, a senha de recuperação é opcional se você optar por usar autenticação gerenciada e não é permitida se você optar por usar autenticação local.
  – 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.

As informações que você especificar no arquivo de importação em massa substituem informações semelhantes que você especificar na página Credenciais do Dispositivo.

Como opção, é possível optar por forçar o gerenciamento de cada tipo de dispositivo se:

- Os dispositivos forem atualmente gerenciados por outro sistema de gerenciamento, como outra instância do XClarity Administrator ou IBM Flex System Manager
- O XClarity Administrator tiver sido desligado, mas o gerenciamento dos dispositivos não tiver sido cancelado antes do desligamento
- O gerenciamento dos dispositivos não tiver sido cancelado corretamente, e a assinatura do CIM não tiver sido apagada

Nota: Se o dispositivo for gerenciado por outra instância do XClarity Administrator, o dispositivo dará a impressão de ser gerenciado pela instância original por um período após o gerenciamento forçado ocorrer. Você pode cancelar o gerenciamento do dispositivo para removê-lo da instância original do XClarity Administrator.

12. 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 documentação online do XClarity Administrator.

    Se XClarity Administrator não conseguir fazer login em um dispositivo usando as credenciais especificadas no arquivo de importação em massa ou as credenciais globais especificadas na caixa de diálogo, o gerenciamento desse dispositivo falhará e XClarity Administrator passará para o próximo dispositivo no arquivo de importação em massa.

    Notas: 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.

13. Se o arquivo de importação em massa incluir um chassi novo, valide e altere as configurações de rede de gerenciamento para o chassi inteiro (incluindo nós de cálculo e comutadores Flex) e configure 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 mais informações, consulte Alterando as configurações de IP de gerenciamento de um chassi e Configurando servidores com o XClarity Administrator na documentação online do XClarity Administrator.

Depois de concluir

Após gerenciar os sistemas, será possível executar as seguintes ações:

- Descobrir e gerenciar sistemas adicionais (consulte Gerenciando chassi, Gerenciando racks, Gerenciando servidores, Gerenciando dispositivos de armazenamento e Gerenciando comutadores na documentação online do Lenovo XClarity Administrator).
- Configurar as informações do sistema, o armazenamento local, os adaptadores de E/S, as configurações de inicialização e as configurações de firmware criando e implantando padrões de servidor (consulte Configurando servidores com o XClarity Administrator na documentação online do Lenovo XClarity Administrator).
- Implantar imagens do sistema operacional nos servidores que ainda não tenham um sistema operacional instalado (consulte Implantando uma imagem do sistema operacional na documentação online do XClarity Administrator).
- Atualizar o firmware em dispositivos que não estão em conformidade com as políticas atuais (consulte Atualizando firmware em dispositivos gerenciados na documentação online do XClarity Administrator).
- Adicionar os sistemas gerenciados recentemente ao rack adequado para refletir o ambiente físico (consulte Gerenciando racks na documentação online do XClarity Administrator).
- Monitorar o status e os detalhes de hardware (consulte Visualizando o status de um servidor gerenciado na documentação online do XClarity Administrator).
- Monitorar eventos e alertas (consulte Trabalhando com eventos e Trabalhando com alertas na documentação online do XClarity Administrator).
- 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.

Capítulo 5. Registro do XClarity Administrator

Ao registrar sua instância do Lenovo XClarity Administrator, você pode usar os recursos básicos sem receber avisos recorrentes sobre a expiração do teste e licenças não compatíveis. Após o registro, o aviso de licença não conforme não é mais exibido. No entanto, todas as funções que requerem uma licença permanecem desativadas até que você compre e instale licenças com base no número de dispositivos gerenciados.

Sobre esta tarefa

O registro da sua instância do XClarity Administrator não requer o compartilhamento de suas informações de contato. A Lenovo não compartilha as informações fornecidas com outras entidades externas.

Se você instalou licenças para funções avançadas, não precisa registrar sua instância do XClarity Administrator. Para obter mais informações sobre licenças e função avançada, consulte Instalando a licença de habilitação com funcionalidade completa.

Procedimento

Para registrar o XClarity Administrator, conclua as seguintes etapas.

- Se o XClarity Administrator estiver conectado à Internet
  1. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Registro** para exibir a página Registro.
  2. Clique em **Registrar** para registrar uma nova instância do XClarity Administrator.
  3. Preencha o nome da empresa, o número de dispositivos a serem gerenciados pelo XClarity Administrator e o país em que o XClarity Administrator está localizado.
  4. Clique em **Enviar**.
- Se o XClarity Administrator não estiver conectado à Internet
  1. Registre o XClarity Administrator.
     a. Em um navegador da Web, abra o Portal da Web de registro do Lenovo XClarity.
     b. Preencha o nome da empresa, o número de dispositivos a serem gerenciados pelo XClarity Administrator e o país em que o XClarity Administrator está localizado.
     c. Clique em **Enviar** para receber um token de registro.
  2. Na barra de menu do Lenovo XClarity Administrator, clique em **Administração → Registro** para exibir a página Registro.
  3. Clique em **Importar** para importar o token de registro.
  4. Preencha o token de registro que você recebeu na etapa 1.
  5. Clique em **Enviar**.

Capítulo 6. Instalando a licença de habilitação com funcionalidade completa

Após a expiração da versão de avaliação gratuita de 90 dias, você deve comprar e instalar licenças do Lenovo XClarity Pro para todos os dispositivos gerenciados que oferecem suporte a funções avançadas para continuar a usar a implantação de sistema operacional e os recursos da configuração do dispositivo em Lenovo XClarity Administrator. Você deve ter licenças do Lenovo XClarity Pro para *todos* os dispositivos gerenciados para obter serviço e suporte ao XClarity Administrator.

Saiba mais: XClarity Administrator: Instalando a licença

Antes de iniciar

Examine as considerações de licença a seguir.

- Uma licença *não* está vinculada a um dispositivo específico.
- Uma licença de chassi fornece licenças para 14 dispositivos.
- Para servidores complexos escaláveis System x3850 X6 (6241), cada servidor precisa de uma licença separada, independentemente de partições.
- Para servidores complexos escaláveis System x3950 X6 (6241), se não particionados, cada servidor precisará de uma licença separada. Se particionados, cada partição precisará de uma licença separada.
- Os dispositivos a seguir *não oferecem suporte* a funções avançadas e, portanto, *não requerem* licenças para esses recursos; entretanto, uma licença deve ser comprada para cada um desses dispositivos para obter serviço e suporte do XClarity Administrator.
  - Servidores ThinkServer
  - Servidores System x M4
  - Servidores System x X5
  - Servidores System x3850 X6 e x3950 X6 (3837)
  - Dispositivos de armazenamento
  - Comutadores

Você deve ter privilégios **lxc-supervisor** ou **lxc-security-admin** para instalar licenças.

Sobre esta tarefa

O XClarity Administrator é compatível com a seguinte licença.

- **Lenovo XClarity Pro**. Cada licença fornece as autorizações a seguir para um único dispositivo.
  - Serviço e suporte para Lenovo XClarity Integrator
  - Serviço e suporte para XClarity Administrator
  - Funções avançadas em XClarity Administrator:
    - Configurando servidores com Padrões de Configuração
    - Implementando Sistemas Operacionais
    - Relatando problemas de XClarity Administrator usando call home (alertas de Call Home para hardware não são afetados.)

O período de ativação da licença é iniciado quando a licença é comprada e o código de autorização é criado.

A conformidade com a licença é determinada com base no número de dispositivos gerenciados que oferecem suporte para as funções avançadas. O número de dispositivos gerenciados não deve exceder o número total de licenças em todas as chaves de licença ativas. Se o XClarity Administrator não estiver em conformidade com as licenças instaladas (por exemplo, se as licenças expirarem ou se o gerenciamento de dispositivos adicionais exceder o número total de licenças ativas), você terá um período de carência de 90 dias para instalar as licenças apropriadas. Cada vez que o XClarity Administrator se torna incompatível, o período de cortesia é redefinido para 90 dias. Se o período de cortesia (incluindo a avaliação gratuita) terminar antes que as licenças estejam em conformidade, as funções avançadas serão desativadas para todos os dispositivos.

Por exemplo, se você gerenciar um servidor adicional 100 ThinkSystem e 20 comutadores do rack em uma instância existente do XClarity Administrator, terá 90 dias para comprar e instalar 100 licenças adicionais antes que as funções avançadas sejam desativadas na interface do usuário (para todos os dispositivos). As licenças para os 20 comutadores do rack não são necessárias para usar as funções avançadas; no entanto, elas serão necessárias se você desejar serviço e suporte. Se as funções avançadas estiverem desativadas, elas serão reativadas depois que você instalar licenças suficientes para voltar à conformidade.

Se você estiver usando uma licença de avaliação gratuita ou tiver um período de cortesia para se tornar compatível e atualizar para uma versão posterior do XClarity Administrator, a licença de avaliação ou o período de cortesia será redefinido para 90 dias.

Notas:

- Os recursos de configuração do servidor e de implantação do sistema operacional são desabilitados quando o período de carência expira.
- O recurso Call Home para problemas do XClarity Administrator (recurso Call Home do software) é desabilitado quando as licenças estão fora de conformidade. Não há nenhum período de carência para esse recurso. No entanto, o Call Home para alertas de hardware não é afetado.

Se licenças já estiverem instaladas, novas licenças *não* serão necessárias para fazer a atualização para uma nova versão do XClarity Administrator.

É possível determinar os status das licenças, incluindo o número de dias restam da licença de avaliação, clicando no menu de ações do usuário (

) na barra de título do XClarity Administrator e clicando em **Sobre**.

Obtendo Ajuda

- Se você tiver problemas e tiver usado um parceiro de negócios, entre em contato com seu parceiro de negócios para verificar a transação e o direito.
- Se você não receber o comprovante eletrônico de autorização, códigos de autorização ou chaves de ativação ou se eles tiverem sido enviados para outra pessoa, entre em contato com os representantes regionais, de acordo com sua região.
  - ESDNA@lenovo.com (países da América do Norte)
  - ESDAP@lenovo.com (países do Pacífico Asiático)
  - ESDEMEA@lenovo.com (países da Europa, Oriente Médio e Ásia)
  - ESDLA@lenovo.com (países da América Latina)
  - ESDChina@Lenovo.com (China)
- Se as informações sobre a autorização não estiverem corretas, entre em contato com o Suporte Lenovo em SW_override@lenovo.com e inclua as informações a seguir:
  - Número do pedido
  - Suas informações de contato, incluindo endereço de e-mail.
  - O endereço físico
  - Alterações que você deseja que sejam feitas

- Se você tiver problemas ou dúvidas sobre como baixar a licença, entre em contato com o Suporte Lenovo em -eSupport_-_Ops@lenovo.com.

Instalando licenças de aplicação de funcionalidade completa usando a interface da Web do XClarity Administrator

Se o XClarity Administrator tiver acesso à Internet, será possível usar a interface da Web do XClarity Administrator para recuperar licenças para autorização existente e, em seguida, importar e instalar as licenças restauradas.

Antes de iniciar

Entre em contato com seu representante da Lenovo ou o parceiro de negócios autorizado para comprar licenças do Lenovo XClarity Pro com base nas funções que deseja habilitar e no número de dispositivos que deseja gerenciar. Depois que você comprar as licenças, um código de autorização será enviado a você em um e-mail de *prova de autorização eletrônica*. O código de autorização é uma sequência alfanumérica de 22 caracteres, necessária para restaurar e instalar as licenças. Se você não receber o e-mail e tiver comprado as licenças por meio de um parceiro de negócios, entre em contato com seu parceiro de negócios para solicitar o código de autorização.

Você também pode recuperar seus códigos de autorização do Portal da web Features on Demand clicando em **Recuperar código de autorização**.

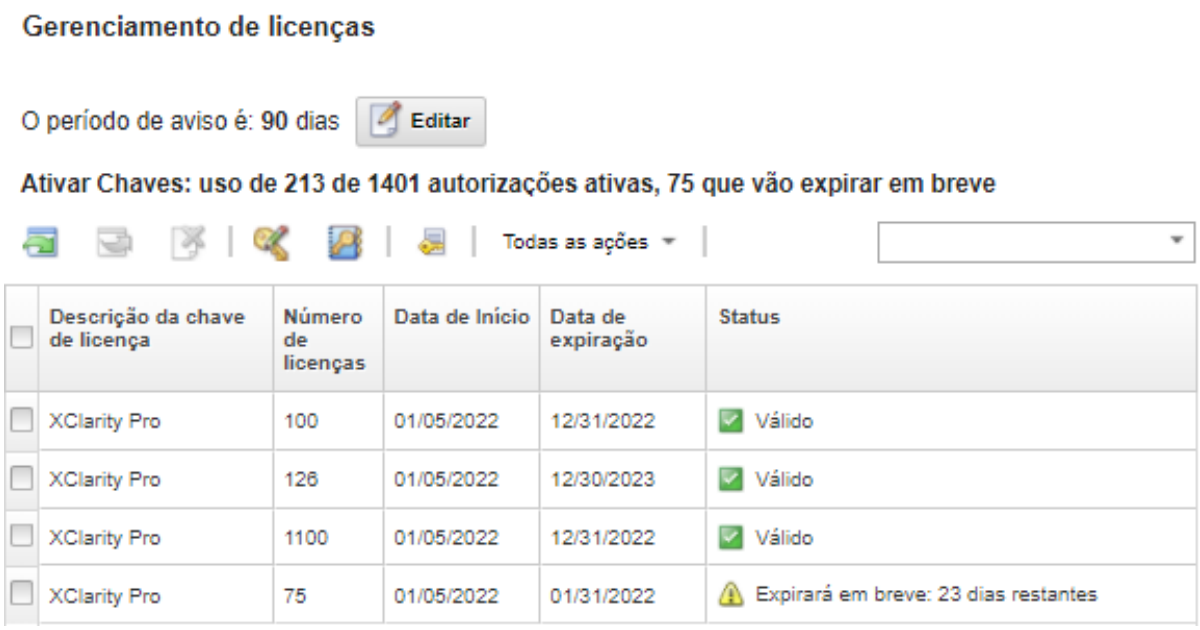
Procedimento

Para instalar licenças do Lenovo XClarity Pro no servidor de gerenciamento, conclua um dos procedimentos a seguir.

- **Restaurar e instalar todas ou um subconjunto de licenças restantes de um único código de autorização**

  É possível restaurar todas ou um subconjunto de licenças disponíveis para um único código de autorização para criar uma chave de ativação de licença, que é um arquivo que contém todas as informações sobre a licença restaurada. É possível então instalar as licenças restauradas usando esse arquivo de chave de ativação de licença.

  1. Na barra de menus do XClarity Administrator, clique em **Administração → Licenças** para exibir a página Gerenciamento de Licenças.



2. Clique no ícone **Solicitar chave de ativação** ( ) para exibir a caixa de diálogo Solicitar chave de ativação.
3. Clique em **Código Único de Autorização**.
4. Insira o código de autorização de 22 caracteres e clique em **Pesquisar** para buscar informações sobre as licenças compradas para o código de autorização especificado no site do Features on Demand.

   Se o código de autorização recebido não for aceito, entre em contato com o Lenovo Support.
5. Insira o número de 10 dígitos do seu cliente Lenovo no campo **Número do cliente da Lenovo**.
6. Insira o número de licenças que deseja resgatar no campo **Resgatar Quantidade** e, em seguida, clique em **Continuar**.

   Para resgatar todas as licenças disponíveis no código de autorização, compare o número no campo **Licenças disponíveis**.

   Se você resgatar um subconjunto de licenças disponíveis, poderá resgatar as licenças restantes posteriormente usando o mesmo código de autorização.

   Dica: cada XClarity Administrator é compatível com até 1.000 dispositivos gerenciados. Portanto, uma única chave de ativação de licença que você pode instalar em uma instância do XClarity Administrator não pode ter mais de 1.000 licenças.
7. Verifique a exatidão das informações de contato e faça modificações se necessário.
8. Clique em **Enviar solicitação** para recuperar as licenças e criar a chave de ativação de licença.
9. Selecione a chave de ativação de licença que contém as licenças a serem instaladas.
10. Clique em **Instalar** para instalar as licenças no servidor de gerenciamento.
11. Clique em **Fechar**.

- **Resgatar e instalar todas as licenças restantes de vários códigos de autorização**

  É possível resgatar todas as licenças restantes para vários códigos de autorização. Uma chave de ativação de licença é criada para cada código de autorização. É possível então instalar as licenças restauradas usando as chaves de ativação de licença. Os códigos de autorização devem ser fornecidos em um arquivo formatado por CSV, usando o modelo fornecido.

1. Na barra de menus do XClarity Administrator, clique em **Administração → Licenças** para exibir a página Gerenciamento de Licenças.
2. Clique no ícone **Solicitar chave de ativação** () para exibir a caixa de diálogo Solicitar chave de ativação.
3. Clique em **Vários Códigos de Autorização**.
4. Clique no link **Baixar Modelo** para abrir um arquivo Excel. Adicione cada código de autorização ao arquivo e salve o arquivo em formato CSV no sistema local.
5. Clique em **Procurar** para encontrar e selecionar o arquivo CSV do código de autorização e, em seguida, clique em **Pesquisar** para obter informações sobre o código de autorização no site do Lenovo Support.
6. Revise as informações sobre a licença comprada e as chaves de ativação de licença disponíveis associadas a cada código de autorização.
7. Insira o número de 10 dígitos do seu cliente Lenovo no campo **Número do cliente da Lenovo**.
8. Verifique a exatidão das informações de contato e faça modificações se necessário. Em seguida, clique em **Continuar**.
9. Selecione **Sim, quero resgatar todos os códigos de autorização válidos** e, em seguida, clique em **Enviar solicitação** para gerar as chaves de ativação de licença.
10. Selecione as chaves de ativação de licença que deseja instalar.
11. Clique em **Instalar** para instalar as chaves de ativação de licença no servidor de gerenciamento.
12. Clique em **Fechar**.

- **Recuperar e instalar licenças recuperadas**

  É possível baixar chaves de ativação de licença para o sistema local de uma instância do XClarity Administrator que tenha acesso ao Portal da web Features on Demand e, em seguida, importar e instalar essas chaves de ativação de licença em outra instância do XClarity Administrator. Isso é útil quando você deseja instalar licenças em uma instância do XClarity Administrator que não tenha acesso à Internet ou quando você reinstalou o XClarity Administrator e precisa restaurar as licenças instaladas.

  1. Na barra de menus do XClarity Administrator, clique em **Administração → Licenças** para exibir a página Gerenciamento de Licenças.
  2. Clique no ícone **Recuperar Histórico** () para exibir a caixa de diálogo Recuperar Histórico.
  3. Insira o número do cliente da Lenovo ou o código de autorização de 22 caracteres.
  4. Clique em **Pesquisar** para recuperar informações sobre licenças disponíveis e recuperadas.

     Se o código de autorização recebido não for aceito, entre em contato com o Lenovo Support.
  5. Selecione os arquivos de chave de licença que deseja instalar.
  6. Clique em **Instalar** para instalar as chaves de ativação de licença em XClarity Administrator.
  7. Clique em **Fechar**.

- **Importar e instalar licenças resgatadas em outra instância do XClarity Administrator**

  Se você resgatou licenças usando uma instância do XClarity Administrator e deseja instalar essas licenças em outra instância do XClarity Administrator ou se ocorrer uma condição de erro que exija restaurar licenças instaladas, será possível importar o arquivo de chave de licença do sistema local para a outra instância do XClarity Administrator.

  1. Em uma instância do XClarity Administrator com acesso às Portal da web Features on Demand, recupere as chaves de ativação de licença de Portal da web Features on Demand e, em seguida, salve as chaves de ativação de licença como um arquivo em seu sistema local.
     a. Na barra de menus do XClarity Administrator, clique em **Administração → Licenças** para exibir a página Gerenciamento de Licenças.

b. Clique no ícone **Recuperar Histórico** () para exibir a caixa de diálogo Recuperar Histórico.
c. Insira o código de autorização de 22 caracteres.
d. Clique em **Pesquisar** para recuperar informações sobre licenças disponíveis e resgatadas para esse código de autorização.

   Se o código de autorização recebido não for aceito, entre em contato com o Lenovo Support.
e. Selecione os arquivos de chaves de ativação de licença que deseja instalar.
f. Clique em **Baixar** para salvar os arquivos de chave de licença no sistema local.

2. Na instância do XClarity Administrator na qual você deseja instalar chaves de ativação de licença:
   a. Na barra de menus do XClarity Administrator, clique em **Administração → Licenças** para exibir a página Gerenciamento de Licenças.
   b. Clique no ícone **Importar e Aplicar** () para importar e instalar as licenças.
   c. Clique em **Procurar** para selecionar as chaves de ativação para as licenças que deseja instalar.

      Para importar várias chaves de ativação de licença, compacte os arquivos .KEY em um arquivo ZIP e selecione-o para importação.
   d. Clique em **Aceitar Licença** para importar e aplicar as licenças.

      Quando a instalação for concluída, as chaves de ativação de licença serão listadas na tabela com o número de licenças instaladas e o período de ativação (datas de início e de expiração).

Depois de concluir

É possível executar as ações a seguir na página Licenças.

- Baixe uma ou mais chaves de ativação de licença específicas para o sistema local clicando no ícone **Exportar** ().

  Nota: Quando você exporta várias chaves de ativação de licença, os arquivos são baixados como um único arquivo ZIP.
- Exclua uma chave de ativação de licença específica clicando no ícone **Excluir** ().
- Configure o período de aviso de licença clicando no botão **Editar** na parte superior da página. O período de aviso de licença é o número de dias antes que as licenças expirem quando o XClarity Administrator dispara um aviso.

Obtendo Ajuda

- Se você tiver problemas e tiver usado um parceiro de negócios, entre em contato com seu parceiro de negócios para verificar a transação e o direito.
- Se você não receber o comprovante eletrônico de autorização, códigos de autorização ou chaves de ativação ou se eles tiverem sido enviados para outra pessoa, entre em contato com os representantes regionais, de acordo com sua região.
  - ESDNA@lenovo.com (países da América do Norte)
  - ESDAP@lenovo.com (países do Pacífico Asiático)
  - ESDEMEA@lenovo.com (países da Europa, Oriente Médio e Ásia)
  - ESDLA@lenovo.com (países da América Latina)
  - ESDChina@Lenovo.com (China)
- Se as informações sobre a autorização não estiverem corretas, entre em contato com o Suporte Lenovo em SW_override@lenovo.com e inclua as informações a seguir:
  - Número do pedido
  - Suas informações de contato, incluindo endereço de e-mail.

  - O endereço físico
  - Alterações que você deseja que sejam feitas
- Se você tiver problemas ou dúvidas sobre como baixar a licença, entre em contato com o Suporte Lenovo em -eSupport_-_Ops@lenovo.com.

Instalando licenças de aplicação de funções completas usando o portal da Web do Features on Demand

Se o XClarity Administrator *não* tiver acesso à Internet, será possível recuperar licenças para códigos de autorização existentes usando o Portal da web Features on Demand de outro sistema que tenha acesso à rede ao XClarity Administrator. Em seguida, é possível usar a interface da Web do XClarity Administrator para importar e instalar as licenças resgatadas.

Procedimento

Para instalar licenças do Lenovo XClarity Pro no servidor de gerenciamento, conclua as etapas a seguir.

Etapa 1. Compre uma licença do Lenovo XClarity Pro para cada dispositivo gerenciado.

Entre em contato com seu representante da Lenovo ou o parceiro de negócios autorizado para comprar licenças do Lenovo XClarity Pro com base nas funções que deseja habilitar e no número de dispositivos que deseja gerenciar. Depois que você comprar as licenças, um código de autorização será enviado a você em um e-mail de *prova de autorização eletrônica*. O código de autorização é uma sequência alfanumérica de 22 caracteres, necessária para restaurar e instalar as licenças. Se você não receber o e-mail e tiver comprado as licenças por meio de um parceiro de negócios, entre em contato com seu parceiro de negócios para solicitar o código de autorização.

Você também pode recuperar seus códigos de autorização do Portal da web Features on Demand clicando em **Recuperar código de autorização**.

Etapa 2. Resgate todas ou um subconjunto de licenças usando o código de autorização. Quando as licenças são resgatadas, um arquivo de chave de ativação de licença é gerado.

1. Abra o Portal da web Features on Demand de um navegador da Web e faça login no portal usando seu endereço de e-mail como seu ID de usuário.
2. Clique em **Solicitar chave de ativação**.
3. Selecione **Inserir um Código Único de Autorização**.
4. Insira o código de autorização de 22 caracteres e clique em **Continuar**.
5. Insira o número do seu cliente Lenovo no campo **Número do Cliente da Lenovo**.
6. Insira o número de licenças que deseja resgatar no campo **Resgatar Quantidade** e, em seguida, clique em **Continuar**.

   Para resgatar todas as licenças disponíveis neste código de autorização, compare o número no campo **Licenças disponíveis**.

   Se você resgatar um subconjunto de licenças disponíveis, poderá resgatar as licenças restantes em outra chave de ativação de licença usando o mesmo código de autorização.

   Dica: cada XClarity Administrator é compatível com até 1.000 dispositivos gerenciados. Portanto, uma única chave de ativação de licença instalada em uma instância do XClarity Administrator não deve ter mais de 1.000 licenças.
7. Siga os comandos para inserir detalhes do produto e informações de contato, e clique em **Continuar** para gerar a chave de ativação de licença.

8. Opcionalmente, especifique destinatários adicionais para receber as chaves de ativação de licença.
9. Clique em **Enviar** para enviar as chaves de ativação de licença.

   A pessoa atribuída à ordem de compra e os destinatários adicionais receberão um e-mail com a chave de ativação de licença. A chave é um arquivo no formato .KEY.

   Nota: Também é possível baixar chaves de ativação de licença (individualmente ou em lote) do Portal da web Features on Demand clicando em **Recuperar Histórico** e usando o número do cliente da Lenovo para encontrar suas chaves de ativação de licença e, em seguida, baixar todos ou um subconjunto de chaves. Em seguida, clique em **E-mail** para enviar por e-mail as chaves para você ou clique em **Baixar** para baixar as chaves no sistema local.

Etapa 3. Importe e instale as licenças em XClarity Administrator.

1. Na barra de menus do XClarity Administrator, clique em **Administração → Licenças** para exibir a página Gerenciamento de Licenças.
2. Clique no ícone **Importar e Aplicar** () para instalar as licenças.
3. Clique em **Procurar** para selecionar o arquivo de chave de ativação de licença para as licenças que deseja instalar.

   Dica: para importar várias chaves de ativação de licença, compacte os arquivos .KEY em um arquivo ZIP e selecione-o para importação.
4. Clique em **Aceitar Licença** para importar e aplicar as licenças.

   Quando a instalação for concluída, a chave de ativação de licença será listada na tabela com o número de licenças instaladas e o período de ativação (datas de início e de expiração).

Depois de concluir

É possível executar as ações a seguir na página Licenças.

- Baixe uma ou mais chaves de ativação de licença específicas para o sistema local clicando no ícone **Exportar** ().

  Nota: Quando você exporta várias chaves de ativação de licença, os arquivos são baixados como um único arquivo ZIP.
- Exclua uma chave de ativação de licença específica clicando no ícone **Excluir** ().
- Configure o período de aviso de licença clicando no botão **Editar** na parte superior da página. O período de aviso de licença é o número de dias antes que as licenças expirem quando o XClarity Administrator dispara um aviso.

Obtendo Ajuda

- Se você tiver problemas e tiver usado um parceiro de negócios, entre em contato com seu parceiro de negócios para verificar a transação e o direito.
- Se você não receber o comprovante eletrônico de autorização, códigos de autorização ou chaves de ativação ou se eles tiverem sido enviados para outra pessoa, entre em contato com os representantes regionais, de acordo com sua região.
  - ESDNA@lenovo.com (países da América do Norte)
  - ESDAP@lenovo.com (países do Pacífico Asiático)
  - ESDEMEA@lenovo.com (países da Europa, Oriente Médio e Ásia)
  - ESDLA@lenovo.com (países da América Latina)
  - ESDChina@Lenovo.com (China)

- Se as informações sobre a autorização não estiverem corretas, entre em contato com o Suporte Lenovo em SW_override@lenovo.com e inclua as informações a seguir:
  - Número do pedido
  - Suas informações de contato, incluindo endereço de e-mail.
  - O endereço físico
  - Alterações que você deseja que sejam feitas
- Se você tiver problemas ou dúvidas sobre como baixar a licença, entre em contato com o Suporte Lenovo em -eSupport_-_Ops@lenovo.com.

Capítulo 7. Atualizando o XClarity Administrator como um

Ao executar o Lenovo XClarity Administrator como um contêiner, use este procedimento de atualização para instalar o software mais recente como um novo contêiner e vincular os volumes do contêiner original ao novo contêiner.

Antes de iniciar

É possível atualizar o XClarity Administrator v4.0 ou posterior apenas em um XClarity Administrator v3.0 ou instância posterior. Se você estiver usando um XClarity Administrator que seja anterior a v3.0, você deverá fazer atualização para v3.0 ou posterior antes de atualizá-lo para v4.0.

Para gerenciar instâncias do XClarity Administratorv4.0 ou posteriores usando o Lenovo XClarity Orchestrator, o XClarity Orchestrator v2.0 ou posterior é necessário. Se você estiver atualizando o XClarity Administrator para v4.0 ou posterior, o XClarity Orchestrator já deverá estar na versão v2.0 ou posterior.

Sobre esta tarefa

O arquivo `docker-compose.yml` usa as variáveis de ambiente a seguir, configuradas durante a instalação do contêiner *original*. Essas variáveis de ambiente também são usadas pelo novo contêiner.

- **CONTAINER_NAME**. Nome exclusivo do contêiner, usado para criar volumes de docker para cada instância do XClarity Administrator (por exemplo, `CONTAINER_NAME=LXCA-203`)

  O XClarity Administrator usa o nome do contêiner para criar os volumes do contêiner. Se você usar o mesmo nome para o novo contêiner, a nova instância do XClarity Administrator usará nos mesmos volumes e, portanto, terá acesso aos mesmos dados e configurações do sistema que a instância original do XClarity Administrator (contêiner).

  Se você alterar o nome do contêiner, novos volumes serão criados para o contêiner, e a nova instância do XClarity Administrator não terá acesso aos mesmos dados e configurações do sistema que a instância original do XClarity Administrator (contêiner). Se você precisar alterar o nome do contêiner ou o endereço IP, faça backup dos dados do sistema e configurações da instância original do XClarity Administrator antes de instalar o novo contêiner e, em seguida, use esse backup para restaurar os dados do sistema e a configuração no novo contêiner.
- **ADDRESS**. Endereço estático IPv4 ou IPv6 para o contêiner (por exemplo, `ADDRESS=192.0.2.0`)

  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.
- **BACKUP_MOUNT** e **FIRMWARE_MOUNT**. (Opcional) Caminhos para os compartilhamentos remotos que podem ser usados para armazenar backups do XClarity Administrator ou usados como repositório remoto para atualizações de firmware. Os caminhos devem ser `/mnt/backup_share` e `/mnt/fw_share`, respectivamente.

Nota: O XClarity Administrator *não é* executado como um contêiner privilegiado.

Procedimento

Para atualizar um contêiner do XClarity Administrator, conclua as etapas a seguir.

Etapa 1. Baixe a imagem do contêiner do XClarity Administrator do Página da Web de download do XClarity Administrator para uma estação de trabalho cliente. Faça login no Web site e, em seguida, use a tecla de acesso que foi fornecida para baixar a imagem.

Etapa 2. Importe a imagem de contêiner do XClarity Administrator para seu host do docker executando o comando a seguir.

```
docker load -i lnvgy_sw_lxca_1l0-3.5.0_anyos_noarch
```

Etapa 3. Edite o mesmo `docker-compose.yml` que foi usado para o contêiner original. Atualize a propriedade da imagem no início do arquivo para apontar para a nova imagem docker na etapa 2. É possível alterar a etiqueta de imagem usando o comando `docker tag`.

Veja a seguir um arquivo yml de exemplo, com IPv6 habilitado.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
```

```
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
```

Etapa 4. Desligue o contêiner *original* executando o comando a seguir.

```
docker-compose -p ${CONTAINER_NAME} down
```

Etapa 5. Implante a *nova* imagem no docker executando o comando a seguir, em que <*ENV_FILENAME*> é o nome do arquivo de variáveis do ambiente.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

Capítulo 8. Desinstalando o XClarity Administrator

Conclua estas etapas para desinstalar um dispositivo virtual Lenovo XClarity Administrator ou um contêiner.

Procedimento

Para desinstalar o dispositivo virtual do XClarity Administrator, conclua as seguintes etapas.

Etapa 1. Cancele o gerenciamento de todos os dispositivos atualmente gerenciados pelo XClarity Administrator (consulte Gerenciando chassi, Gerenciando servidores e Gerenciando comutadores na documentação online do XClarity Administrator).

Etapa 2. Desinstale o XClarity Administrator, dependendo do sistema operacional:

- **Docker-compose**Execute o comando a seguir para parar o contêiner e remover as redes e os volumes.
  ```
  docker-compose down -v
  ```
- **CentOS, Red Hat, Rocky e Ubuntu**
  1. Conecte-se ao host usando o Virtual Machine Manager.
  2. Clique com o botão direito na máquina virtual e clique em **Desligar → Forçar desligamento**.
  3. Clique com o botão direito na máquina virtual novamente e clique em **Excluir**. A caixa de diálogo Confirmação de exclusão é exibida.
  4. Marque todas as caixas de seleção e clique em **Excluir**.
- **ESXi**
  1. Conectar-se ao host pelo VMware vSphere Client.
  2. Clique com o botão direito na máquina virtual e clique em **Potência → Desligar**.
  3. Clique com o botão direito na máquina virtual novamente e clique em **Excluir do Disco**.
- **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 **Desligar**.
  4. Clique com o botão direito na máquina virtual novamente e clique em **Excluir**.