Guia do Usuário do Lenovo XClarity Orchestrator

Versão 2.1

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 Orchestrator.

Segunda Edição (Julho 2024)

Conteúdo

Resumo de alterações

As versões subsequentes do software de gerenciamento do Lenovo XClarity Orchestrator oferecem suporte a novos aprimoramentos e correções de software.

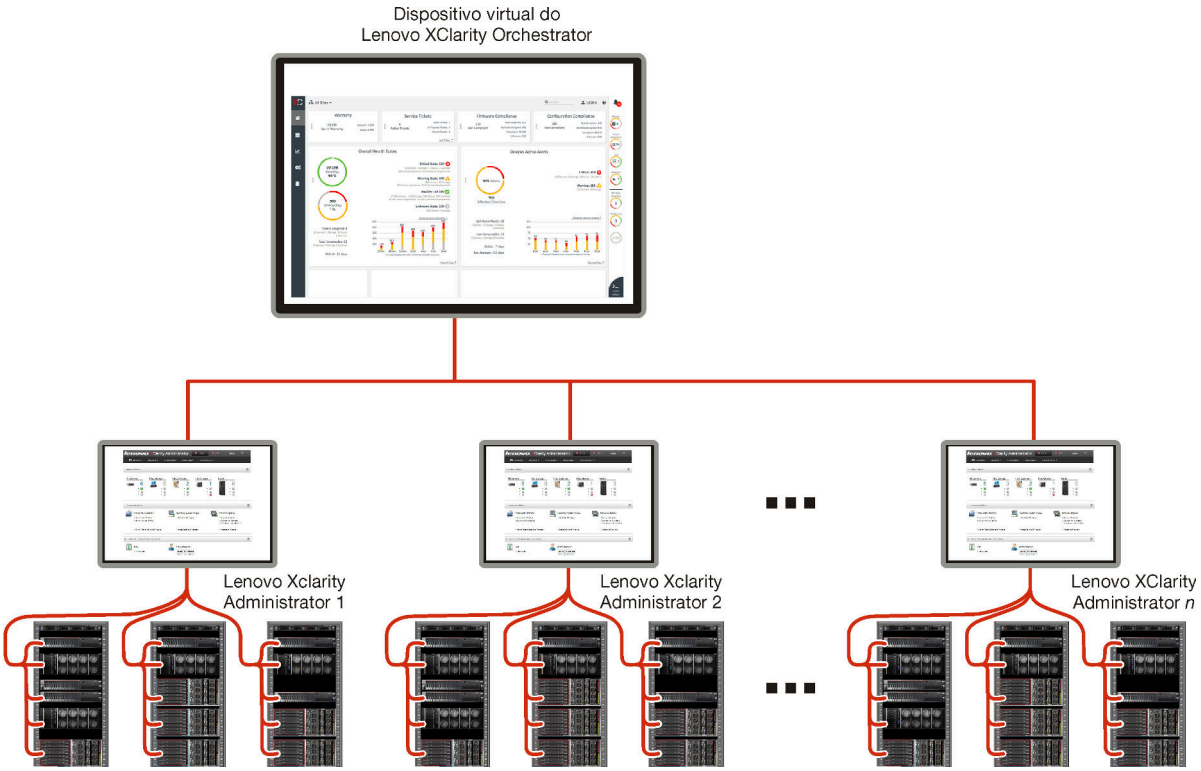
Consulte o arquivo de histórico de alterações (*.chg) fornecido no pacote de atualizações para obter informações sobre as correções.

Esta versão oferece suporte aos seguintes aprimoramentos feitos no software de gerenciamento. Para obter informações sobre alterações nas versões anteriores, consulte O que há de novona documentação online do XClarity Orchestrator.

Função	Descrição
Administrando	É possível reiniciar o servidor do orquestrador na interface do usuário (consulte Reiniciando o XClarity Orchestrator).
Gerenciando recursos	O Lenovo XClarity Management Hub 2.0 é um novo gerenciador de dispositivos leve que você pode usar para gerenciar servidores Lenovo ThinkSystem e ThinkEdge (consulte Conectando gerenciadores de recursos). É possível gerenciar um grande número de servidores usando a opção de gerenciamento em massa (consulte Gerenciando servidores). É possível gerenciar servidores usando nomes de domínio totalmente qualificados (consulte Gerenciando servidores).
Monitorando recursos e atividades	Os dados do inventário de memória agora são exibidos em um formato tabular (consulte Visualizando detalhes de dispositivos). É possível exibir uma lista de todos os trabalhos planejados (consulte Monitorando trabalhos).
Fornecimento de recursos	É possível programar uma atualização de firmware para ser executada em uma data e hora específicas (consulte Aplicando e ativando atualizações aos servidores gerenciados).

Capítulo 1. Visão geral do Lenovo XClarity Orchestrator

O Lenovo XClarity Orchestrator fornece monitoramento, gerenciamento, provisionamento e análise centralizados para ambientes com um grande número de dispositivos. Ele utiliza os gerenciadores de recursos existentes (como o Lenovo XClarity Administrator e o Schneider Electric EcoStruxure IT Expert) em vários locais para exibir a integridade geral, coletar inventário de dispositivo e resumos de integridade, pesquisar detalhes do dispositivo, exibir eventos e logs de auditoria e aplicar atualizações a recursos gerenciados.



Saiba mais:

- Visão geral do XClarity Orchestrator
- Recursos de gerenciamento

Monitoramento centralizado e gerenciamento de recursos

O XClarity Orchestrator fornece uma única interface para monitorar e gerenciar gerenciadores de recursos e os dispositivos gerenciados por meio desses gerenciadores de recursos.

- Exibições resumidas do funcionamento de seus recursos gerenciados, incluindo gerenciadores de recursos, dispositivos e recursos de infraestrutura (como PDUs e UPSs)
- Resumo e exibições detalhadas do funcionamento do componente, inventário de ativos, status de garantia e consultorias para dispositivos em diversos locais
- Agregação de alertas e eventos críticos, criação de alertas personalizados e encaminhamento de eventos para aplicativos externos
- Controle de ciclo de vida para dispositivos gerenciados (incluindo operações de energia)
- Inicialização em contexto na interface do usuário para gerenciadores de recursos e dispositivos gerenciados a partir das páginas de resumo do dispositivo

Fornecimento de atualizações

É possível usar o XClarity Orchestrator para manter níveis atuais de software nos recursos gerenciados. É possível usar o catálogo de atualizações para saber quais níveis de software estão disponíveis, usar as políticas de conformidade de atualização para identificar quais recursos precisam ser atualizados com base em critérios personalizados e, em seguida, implantar as atualizações desejadas nesses recursos. O XClarity Orchestrator garante que o software seja provisionado nos recursos de destino, na ordem correta.

O XClarity Orchestrator oferece suporte às seguintes operações de provisionamento.

- Implantando atualizações nos gerenciadores de recursos do Lenovo XClarity Administrator.
- Implantação de atualizações de firmware em dispositivos gerenciados pelo XClarity Administrator.

Para obter mais informações sobre o fornecimento de atualizações, consulte Fornecimento de atualizações para recursos gerenciados.

Fornecimento da configuração do servidor

É possível fornecer rapidamente servidores gerenciados usando uma configuração consistente. As configurações (como Baseboard Management Controller e configurações UEFI) são salvas como um padrão que pode ser aplicado a vários servidores.

O XClarity Orchestrator não implanta padrões de configuração diretamente em servidores gerenciados. Em vez disso, ele envia uma solicitação ao gerenciador de recursos aplicável para iniciar um trabalho para executar a implantação e, em seguida, monitora o andamento da solicitação.

Para obter mais informações sobre o fornecimento de configurações de servidor, consulte Fornecimento das configurações do servidor.

Fornecendo sistemas operacionais

É possível usar o XClarity Orchestrator para implantar imagens do sistema operacional em vários servidores.

O XClarity Orchestrator não implanta diretamente o sistema operacional em servidores gerenciados. Em vez disso, ele envia uma solicitação ao gerenciador de recursos XClarity Administrator aplicável para iniciar um trabalho para executar a atualização e, em seguida, monitora o andamento da solicitação.

Nota: O recurso de implantação do SO requer o XClarity Administrator v4.0 ou posterior.

Para obter mais informações sobre o fornecimento de configurações de servidor, consulte Fornecendo sistemas operacionais.

Aprendizado de máquina de Business Intelligence e análise preditiva

O XClarity Orchestrator pode se conectar a serviços de terceiros (como Splunk) para aprendizado de máquina de Business Intelligence e análise preditivas a fim de:

- Coletar e exibir dados de tendência (como utilização do processador e memória, consumo de energia, temperatura, acesso não autorizado, eventos repetidos e perdidos e tempo médio entre processos como atualizações de firmware e reinicializações do sistema)
- Usa dados métricos para prever falhas (como eventos repetidos e relatórios de integridade)
- Crie relatórios de análise personalizados com base em dados existentes, incluindo alertas, eventos, inventário de dispositivos e métricas de dispositivo.
- Defina regras de alerta personalizadas que, quando ativadas, geram alertas quando há condições específicas em seu ambiente.

Saiba mais:  Recursos de análise e preditivos

Para obter mais informações sobre a análise preditiva, consulte Analisando tendências e prevendo problemas.

Serviço e Suporte

O XClarity Orchestrator pode ser configurado para coletar e enviar arquivos de diagnóstico automaticamente ao Suporte Lenovo usando Call Home quando determinados eventos que podem ser reparados ocorrerem em recursos gerenciados. Também é possível coletar arquivos de diagnóstico manualmente, abrir um registro de problemas e enviar arquivos de diagnóstico ao Suporte Lenovo Center.

Para obter mais informações sobre serviço e suporte, consulte Trabalhando com serviço e suporte.

Documentação

A documentação online é atualizada regularmente, em inglês. Consulte Documentação online do XClarity Orchestrator para obter as informações e os procedimentos mais atuais.

A documentação online está disponível nos seguintes idiomas.
- Inglês (en)
- Chinês simplificado (zh-CN)
- Chinês tradicional (zh-TW)
- Francês (fr)
- Alemão (de)
- Italiano (it)
- Japonês (ja)
- Coreano (ko)
- Português do Brasil (pt-BR)
- Russo (ru)
- Espanhol (es)
- Tailandês (th)

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

- Adicione <*language_code*> após `https://pubs.lenovo.com/lxco/`, por exemplo, para exibir a documentação online em chinês simplificado.
  `https://pubs.lenovo.com/lxco/zh-CN/`

Efetuando login no XClarity Orchestrator

Faça login na interface da Web do Lenovo XClarity Orchestrator de um sistema que tenha conectividade de rede com o dispositivo virtual do XClarity Orchestrator.

Antes de iniciar

Use um dos seguintes navegadores da Web suportados. Para obter mais informações, consulte Hardware e software suportados na documentação online do XClarity Orchestrator.
- Chrome 80.0 ou posterior
- Firefox ESR 68.6.0 ou posterior
- Microsoft Edge 40.0 ou posterior
- Safari 13.0.4 ou posterior (em execução no macOS 10.13 ou posterior)

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

Ao usar uma conta de usuário LDAP, você pode fazer login usando o nome de usuário ou username@domain (por exemplo, `user1@company.com`).

O XClarity Orchestrator desconecta automaticamente as sessões do usuário que estão inativas por um determinado período e sessões do usuário que foram abertas por um determinado período, independentemente da atividade. Os seguintes valores padrão são definidos pelo XClarity Orchestrator.

- Se você não clicou nem digitou na interface do usuário por ***30*** *minutos*, sua sessão de usuário está restrita às operações somente leitura. Se você tentar modificar dados, a sessão do usuário será desconectada automaticamente.
- Se você não tiver exibido ativamente dados por ***1440*** *minutos* (24 horas), sua sessão de usuário será desconectada automaticamente.
- Depois de ***24*** *horas*, as sessões do usuário são desconectadas automaticamente, independentemente da atividade do usuário.

Procedimento

Para fazer login na interface da Web do XClarity Orchestrator, conclua as seguintes etapas.

1. Aponte seu navegador para o endereço IP do dispositivo virtual do XClarity Orchestrator.

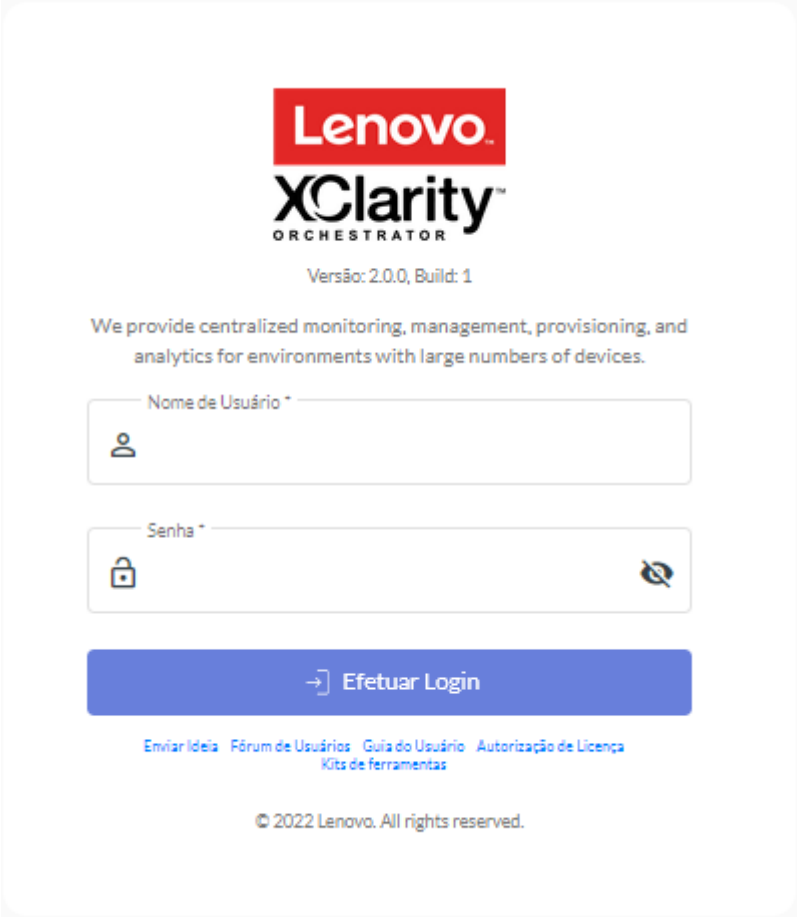
   - **Usando endereços IPv4 estáticos**Se você especificou um endereço IPv4 durante a instalação, use esse endereço IPv4 para acessar a interface da Web usando o seguinte URL.
     `https://{IPv4_address}/#/login.html`

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

   - **Usando um servidor DHCP no mesmo domínio de transmissão como XClarity Orchestrator**Se um servidor DHCP estiver configurado no mesmo domínio de transmissão como XClarity Orchestrator, use o endereço IPv4 exibido no console do dispositivo virtual do XClarity Orchestrator para acessar a interface da Web usando o seguinte URL.
     `https://{IPv4_address}/#/login.html`

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

   A página de login inicial é exibida.



Na página de login, é possível executar as seguintes ações:

- Envie ideias para o XClarity Orchestrator no Web site de concepção do Lenovo XClarity ou clicando em **Enviar ideia**.
- Faça perguntas e encontre respostas no Site do fórum da comunidade do Lenovo XClarity clicando em **Fórum de Usuários**.
- Encontre informações sobre como usar o XClarity Orchestrator clicando em **Guia do Usuário**.
- Encontre e gerencie todas as licenças da Lenovo do Portal da web Features on Demand clicando em **Autorização de Licença**.
- Encontre informações sobre as APIs disponíveis clicando em **Kits de ferramentas**.

2. Selecione o idioma desejado na lista suspensa Idioma.

   Nota: Alguns parâmetros de configuração e os dados que são fornecidos pelos gerenciadores de recursos e dispositivos gerenciados podem estar disponíveis apenas em inglês.

3. Insira um ID de usuário e senha válidos, e clique em **Fazer login**.Na primeira vez que uma conta de usuário específica for usada para fazer login no XClarity Orchestrator, será necessário alterar a senha. Por padrão, as senhas devem conter **8** – **256** caracteres e devem atender aos critérios a seguir.

   Importante: É recomendável usar senhas fortes de 16 ou mais caracteres.

   - Deve conter pelo menos um caractere alfabético e não deve ter mais de dois caracteres sequenciais, incluindo sequências de caracteres alfabéticos, dígitos e teclas de teclado QWERTY (por exemplo, "abc", "123" e "asd" não são permitidos)
   - Deve conter pelo menos um número

- Deve conter pelo menos dois dos caracteres a seguir.
  - Caracteres alfabéticos maiúsculos (A – Z)
  - Caracteres alfabéticos minúsculos (a – z)
  - Caracteres especiais ; @ _ ! ' $ & +

  Caracteres de espaço em branco não são permitidos.
- Não deve repetir nem reverter o nome do usuário.
- Não deve conter mais de dois caracteres consecutivos (por exemplo, "aaa", "111" e "..." não são permitidos).

Depois de concluir

A página de painel do XClarity Orchestrator é exibida com um resumo da integridade e das atividades dos recursos em seu ambiente.

Você pode executar as seguintes ações no menu **Conta do usuário** ( ) no canto superior direito da interface da Web do XClarity Orchestrator.

- Altere a senha do usuário atual clicando em **Alterar senha**.
- Faça logout da sessão atual clicando em **Fazer logout**. A página de login do XClarity Orchestrator será exibida.

  Na página login, é possível clicar no link **Autorização de Licença** para abrir o Portal da web Features on Demand, onde é possível localizar e gerenciar todas as licenças de produtos da Lenovo.
- Envie ideias para o XClarity Orchestrator no Web site de concepção do Lenovo XClarity ou clicando em **Enviar ideia**.
- Faça perguntas e encontre respostas no Site do fórum da comunidade do Lenovo XClarity clicando em **Fórum de Usuários**.
- Baixe o XClarity Orchestratorkit de ferramentas PowerShell (LXCOPSTool) clicando em **Kits de ferramentas**. O kit de ferramentas LXCOPSTool fornece uma biblioteca de cmdlets para automatizar o fornecimento e gerenciamento de recursos em uma sessão do Microsoft PowerShell.
- Encontre informações sobre como usar o XClarity Orchestrator usando o sistema de ajuda integrado, clicando em **Ajuda**.

  A documentação online é atualizada regularmente, em inglês. Consulte Documentação online do XClarity Orchestrator para obter as informações e os procedimentos mais atuais.
- Exiba informações sobre a versão do XClarity Orchestrator clicando em **Sobre**.

  Na caixa de diálogo Sobre, é possível encontrar links para exibir o **Contrato de Licença do Usuário Final**, as **Licenças de Código Aberto** e a **Declaração de Privacidade da Lenovo**.
- Altere o idioma da interface do usuário clicando em **Alterar idioma**. Os seguintes idiomas são suportados.
  - Inglês (en)
  - Chinês simplificado (zh-CN)
  - Chinês tradicional (zh-TW)
  - Francês (fr)
  - Alemão (de)
  - Italiano (it)
  - Japonês (ja)
  - Coreano (ko)
  - Português do Brasil (pt-BR)
  - Russo (ru)
  - Espanhol (es)
  - Tailandês (th)

Dicas e técnicas de interface do usuário

Considere estas dicas e técnicas ao usar a interface do usuário do Lenovo XClarity Orchestrator e do Lenovo XClarity Management Hub.

Importando arquivos

É possível importar arquivos arrastando e soltando os arquivos em uma caixa de diálogo Importar.

Quando você importa um arquivo, um pop-up expansível aparece no canto inferior direito da interface do usuário com informações sobre o progresso e o status de cada processo de importação. Ícones no pop-up ajudam a identificar rapidamente o status do processo para cada importação. Depois que uma importação é concluída com êxito, um trabalho é iniciado para validar o arquivo. Se ocorrer um erro durante o processo de importação, uma mensagem de erro será listada na caixa de diálogo pop-up para ajudar você a resolver rapidamente o problema.

Quando o pop-up estiver recolhido, é possível clicar e segurar o ícone **Arrastar** (⋮⋮) para mover o pop-up para uma posição diferente.

Clique em **Limpar tudo** para limpar a lista de processos de importação concluídos. Se todos os processos de importação estiverem concluídos, o pop-up será oculto.

Inserindo texto em campos de texto

Os caracteres que podem ser inseridos em alguns campos de texto são restritos. A lista a seguir descreve os caracteres permitidos.

- **Nomes**. Inclui todas as letras e caracteres numéricos nos idiomas suportados e os caracteres especiais @ - _ + / [ ] . , : e espaço.
- **Descrições**. Inclui todas as letras e caracteres numéricos nos idiomas suportados e os caracteres especiais @ - _ % & * + = / ( ) { } [ ] . , : e espaço.
- **Senhas**. Para contas de usuários locais, as senhas podem ser caracteres **8** – **256** por padrão, embora 16 ou mais caracteres sejam recomendados. Não há restrições de caracteres para senhas. Entretanto, senhas requerem determinados tipos de caracteres e limitam algumas sequências para segurança.
  - Deve conter pelo menos um caractere alfabético e não deve ter mais de dois caracteres sequenciais, incluindo sequências de caracteres alfabéticos, dígitos e teclas de teclado QWERTY (por exemplo, "abc", "123" e "asd" não são permitidos)
  - Deve conter pelo menos um número
  - Deve conter pelo menos dois dos caracteres a seguir.
    - Caracteres alfabéticos maiúsculos (A – Z)
    - Caracteres alfabéticos minúsculos (a – z)
    - Caracteres especiais ; @ _ ! ' $ & +

    Caracteres de espaço em branco não são permitidos.
  - Não deve repetir nem reverter o nome do usuário.
  - Não deve conter mais de dois caracteres consecutivos (por exemplo, "aaa", "111" e "..." não são permitidos).

Expandindo e reduzindo o painel de navegação

O painel de navegação é reduzido por padrão, mostrando somente ícones que representam itens de menu específicos. É possível clicar em um ícone para expandir temporariamente o painel de navegação e o menu para esse ícone. Quando você move o cursor para fora do painel de navegação, o painel é reduzido para que apenas os ícones sejam exibidos.

Para manter o painel de navegação permanentemente expandido, clique no ícone **Expandir** (). É possível reduzir o painel de navegação clicando no ícone **Reduzir** ().

Determinando o escopo da interface do usuário

Por padrão, o XClarity Orchestrator exibe dados de *todos os recursos*. É possível limitar o escopo dos dados exibidos na sessão de usuário atual a apenas os recursos que estão em gerenciadores de recursos e grupos específicos usando o menu suspenso **Escopo atual** na parte superior da página. No menu suspenso, é possível exibir a lista de gerenciadores de recursos e grupos no escopo atual em **Minha lista de escopo**, clique em **Alterar escopo** para exibir uma caixa de diálogo na qual você cria um escopo personalizado com vários gerenciadores de recursos e grupos ou selecione **Todos os Recursos** para alterar o escopo para visualizar todos os recursos.

O escopo selecionado é persistente apenas na sessão do usuário atual. É possível abrir várias sessões de usuário, cada uma com exibições diferentes do painel, recursos, eventos e dados de alertas.

Nota: Os Gerenciadores de Recursos VMware vRealize Operations Manager não estão incluídos na lista de gerenciadores de recursos, pois eles não gerenciam dispositivos no XClarity Orchestrator.

Visualizando mais ou menos dados por página

Altere o número de linhas exibidas em uma tabela por página usando a lista suspensa **Linhas por página** na parte inferior de cada tabela. É possível exibir 10, 15, 25 ou 50 linhas.

Localizando dados em listas grandes

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

- Classifique as linhas da tabela clicando no cabeçalho da coluna.
- Limite o escopo dos dados exibidos na sessão de usuário atual a apenas os recursos que estão em um gerenciador de recursos ou grupo específico usando o menu suspenso **Escopo atual** na parte superior da página (consulte "Determinando o escopo da interface do usuário" acima).
- Crie dinamicamente um subconjunto de listas com base nos dados encontrados em colunas específicas usando os campos de entrada **Filtros**. É possível filtrar colunas mostradas e ocultas. Também é possível salvar as consultas de filtro que você deseja usar regularmente.
- Refine ainda mais o subconjunto inserindo texto (como um nome ou endereço IP) no campo **Pesquisar** para localizar os dados encontrados em qualquer coluna disponível.

  Dica: separe várias pesquisas usando uma vírgula. Por exemplo, "180,190" exibe todas as linhas que contêm 180 ou 190 em qualquer uma das colunas disponíveis.
- Marque a caixa de seleção no cabeçalho da tabela para marcar ou desmarcar todos os itens listados na tabela.

Visualizando dados da tabela

Atualize as tabelas de dados clicando no ícone **Atualizar** ().

Expanda ou reduza cada linha para mostrar ou ocultar os subdetalhes das tabelas com linhas expansíveis (como nos cartões Trabalhos e Gerenciamento do Repositório). Também é possível clicar no ícone **Reduzir Tudo** () para ocultar os subdetalhes de todas as linhas.

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

Exportando dados da tabela

Exporte os dados na tabela atual para o sistema local clicando no ícone **Exportar dados** (). É possível optar por exportar todas as páginas, a página atual ou as linhas selecionadas, escolher o formato de arquivo (XLSX, CSV ou JSON) e escolher se deve incluir todas as colunas ou apenas colunas visíveis. Para o formato CSV, você também pode escolher como separar os dados (usando ponto-e-vírgula, tabulação ou uma barra vertical).

Dica: Para o formato JSON, os carimbos de data e hora nos dados exportados refletem o fuso horário definido para o XClarity Orchestrator, não o sistema local. Para formatos CSV e XLSX, os carimbos de data e hora são convertidos no fuso horário do usuário, que é exibido na interface da Web.

Quando você exporta dados, um pop-up expansível aparece no canto inferior direito da interface do usuário com informações sobre o progresso e o status. Ícones no pop-up ajudam a identificar rapidamente o status do processo para cada exportação. Se ocorrer um erro durante o processo de exportação, uma mensagem de erro será listada na caixa de diálogo pop-up para ajudar você a resolver rapidamente o problema.

Quando o pop-up estiver recolhido, é possível clicar e segurar o ícone **Arrastar** () para mover o pop-up para uma posição diferente.

Clique em **Limpar tudo** para limpar a lista de processos de exportação concluídos. Se todos os processos de exportação estiverem concluídos, o pop-up será oculto.

Configurar colunas da tabela

Configure tabelas para mostrar as informações mais importantes para você.

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

Alterando o idioma da interface do usuário

Você pode alterar o idioma da interface do usuário ao fazer login.

Depois de fazer login, é possível alterar o idioma clicando no menu **Conta do usuário** () e, em seguida, em **Alterar idioma**.

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

Obtendo Ajuda

Há várias maneiras para obter ajuda com a interface do usuário.

- Passe o cursor sobre o ícone **Ajuda** () em algumas páginas para exibir um pop-up com detalhes adicionais sobre um campo específico.
- Clique no link **Saiba mais** em algumas páginas para abrir o sistema de ajuda e obter mais informações no contexto.
- Obtenha ajuda sobre como executar ações específicas na interface do usuário clicando no menu **Conta do usuário** () e, em seguida, clique em **Ajuda**.A documentação online é atualizada regularmente, em inglês. Consulte Documentação online do XClarity Orchestrator para obter as informações e os procedimentos mais atuais.

Capítulo 2. Administração de XClarity Orchestrator

Várias atividades administrativas estão disponíveis, como definir configurações do sistema, como data e hora e acesso à rede, conectar gerenciadores de recursos, gerenciar servidores de autenticação e acesso do usuário e gerenciar certificados de segurança.

Conectando gerenciadores de recursos

O Lenovo XClarity Orchestrator monitora e gerencia dispositivos por meio de Gerenciadores de Recursos e Aplicativos.

Antes de iniciar

Você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** é atribuída.

O XClarity Orchestrator pode oferecer suporte a um número ilimitado de gerenciadores de recursos que gerenciam, coletivamente, um máximo de 10,000 dispositivos no total.

Verifique se o Gerenciador de Recursos é compatível (consulte Hardware e software suportados na documentação online do XClarity Orchestrator.).

Verifique se os gerenciadores de recursos estão online e acessíveis na rede no XClarity Orchestrator.

Assegure-se de que a conta do usuário que você usa para autenticação no gerenciador de recursos tenha os privilégios corretos. No XClarity Administrator, as contas do usuário devem ser atribuídas à função **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-hw-admin** ou **lxc-recovery**.

Certifique-se de que o gerenciador de recursos não tenha o número máximo de encaminhadores de eventos suportados. O XClarity Orchestrator cria um encaminhador de eventos no gerenciador de recursos quando uma conexão é criada para esse gerenciador de recursos.

Ao conectar um Gerenciador de Recursos que tenha um certificado assinado externamente:

- Garanta que seja um certificado X.509 v3. O XClarity Orchestrator não consegue se conectar a um Gerenciador de Recursos que tenha um certificado v1 assinado externamente.
- Verifique se os detalhes do certificado incluem os requisitos a seguir.
  - O uso da chave deve conter
    - Contrato de chave
    - Assinatura digital
    - Criptografia de chave
  - O uso da chave aprimorada deve conter
    - Servidor de autenticação (1.3.6.1.5.5.7.3.1)
    - Autenticação do cliente (1.3.6.1.5.5.7.3.2)

Sobre esta tarefa

O XClarity Orchestrator comporta os Gerenciadores de Recursos e Aplicativos a seguir.

- **Lenovo XClarity Management Hub 2.0**. Gerencia, monitores e provisiona dispositivos ThinkSystem e ThinkAgile. Um agente UDC deve ser instalado em cada dispositivo ThinkEdge Client para permitir a comunicação entre o dispositivo e o XClarity Orchestrator.

Importante: O processo de registro XClarity Management Hub 2.0 é diferente de outro Gerenciador de Recursos. Para obter instruções detalhadas, consulte Conectando o XClarity Management Hub 2.0 ao XClarity Orchestrator na documentação online do XClarity Orchestrator.

- **Lenovo XClarity Management Hub**. Gerencia, monitora e provisiona dispositivos ThinkEdge Client. Um agente UDC deve ser instalado em cada dispositivo ThinkEdge Client para permitir a comunicação entre o dispositivo e o XClarity Orchestrator.

  Importante: O processo de registro XClarity Management Hub é diferente de outro Gerenciador de Recursos. Para obter instruções detalhadas, consulte Conectando o XClarity Management Hub ao XClarity Orchestrator na documentação online do XClarity Orchestrator.
- **Lenovo XClarity Administrator**. Gerencia, monitora e provisiona dispositivos Lenovo com Baseboard Management Controllers.
- **Schneider Electric EcoStruxure IT Expert**. Gerencia e monitora recursos de infraestrutura.
- **VMware vRealize Operations Manager**.

Quando você conecta um Gerenciador de Recursos XClarity Management Hub ou XClarity Administrator, XClarity Orchestrator:

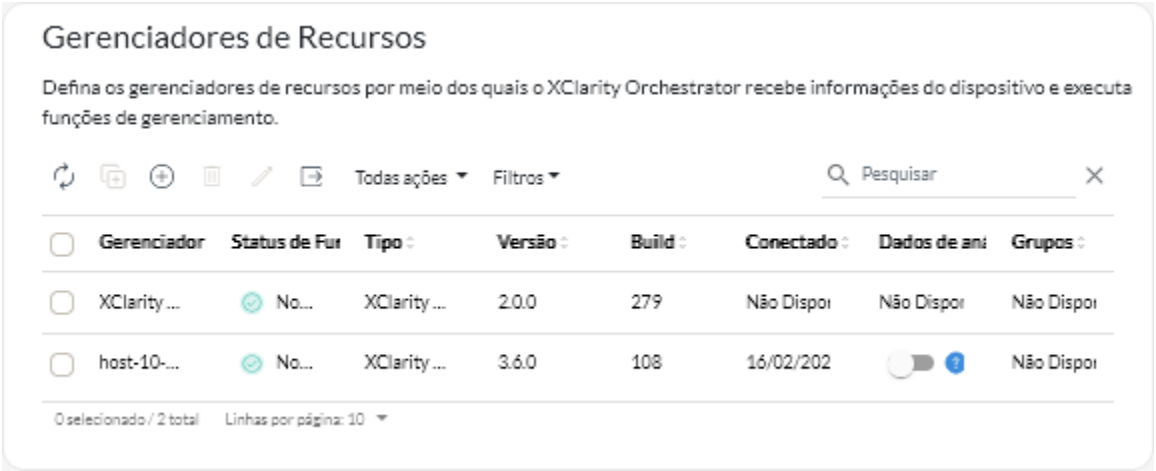
- Recupera informações sobre todos os dispositivos que são gerenciados pelo gerenciador de recursos.
- Cria e ativa um encaminhador de evento (para um serviço da Web REST) no servidor de gerenciamento para monitorar e encaminhar eventos ao XClarity Orchestrator.

O endereço de rede (endereço IP ou nome do host) fornecido é usado como o nome do gerenciador.

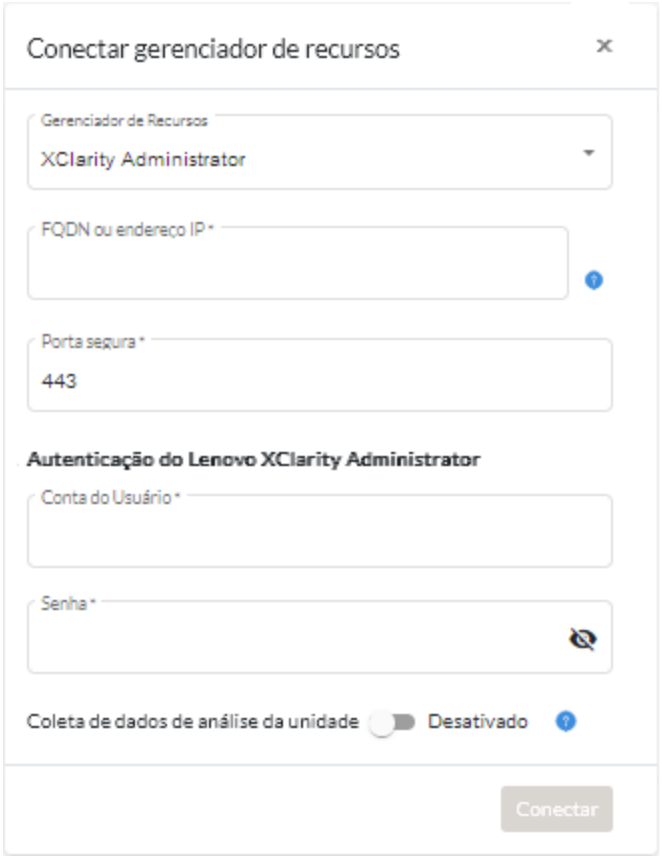
Procedimento

Para conectar um Gerenciador de Recursos ou Aplicativos, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Recursos (⚙) → Gerenciador de Recursos** para exibir a placa Gerenciadores de Recursos.



Etapa 2. Clique no ícone **Conectar** (⊕) para exibir o gerenciador de recursos. A caixa de diálogo Conectar gerenciador de recursos.



Etapa 3. Selecione o tipo de Gerenciador de Recursos e preencha as informações a seguir.

- XClarity Management Hub 2.0 ou **XClarity Management Hub**
  1. Insira a chave de registro que foi gerada pela instância do hub de gerenciamento e, em seguida, clique em **Conectar**.Para obter o token de solicitação de registro, faça login no portal do hub de gerenciamento, clique em **Registro** e, em seguida, clique em **Criar chave de registro**.
  2. Copie a chave de registro XClarity Orchestrator gerada.
  3. No portal do hub de gerenciamento, clique em **Registro** e em **Instalar chave de registro**, cole o token de registro XClarity Orchestrator e, em seguida, clique em **Conectar**.
- **XClarity Administrator**
  - Especifique o nome de domínio totalmente qualificado ou o endereço IP (IPv4 ou IPv6).Não há suporte para o uso do nome do host sem o nome do domínio.
  - Como opção, altere a porta do gerenciador de recursos. O padrão é 443.
  - Especifique a conta do usuário e a senha a serem usadas para fazer login no gerenciador de recursos.
  - Opcionalmente, ative a **Coleta de dados de análise da unidade**. Quando habilitados, os dados de análise da unidade são coletados diariamente para dispositivos ThinkSystem e ThinkAgile e são usados para análise preditiva.A coleta de dados de unidade de análise é compatível apenas com o XClarity Administrator v3.3.0 e gerenciadores de recursos posteriores.

    Atenção: O desempenho do sistema poderá ser afetado quando os dados forem coletados.
- **EcoStruxure IT Expert**. Especifique o nome, a chave de token e a URL a ser usada para a conexão.
- **vRealize Operations Manager**

- Especifique o nome de domínio totalmente qualificado ou o endereço IP (IPv4 ou IPv6).Não há suporte para o uso do nome do host sem o nome do domínio.
- Como opção, altere a porta do gerenciador de recursos. O padrão é 443.
- Opcionalmente, selecione a origem da autorização para os usuários e grupos.
- Especifique a conta do usuário e a senha a serem usadas para fazer login no vRealize Operations Manager.

Etapa 4. Clique em **Conectar**.

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 .)

Quando uma conexão é estabelecida com o gerenciador de recursos, o gerenciador é adicionado à tabela.

Etapa 5. Se você escolheu se conectar a um XClarity Management Hub, uma caixa de diálogo, uma caixa de diálogo será exibida com uma chave de registro.

Para concluir a conexão, clique em **Copiar para área de transferência** para copiar a chave de registro. Em seguida, faça login no XClarity Management Hub, clique em **Administração** → **Configuração do hub** e clique em **Instalar chave de registro**. Em seguida, cole a chave de registro e clique em **Enviar**.

Depois de concluir

É possível executar as ações a seguir a partir da placa Gerenciadores de Recursos.

- Exibir o status de conexão do gerenciador de recursos na coluna **Status de Funcionamento**.
- Modifique as credenciais e propriedades de um gerenciador de recursos selecionado clicando no ícone **Editar** ( ).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 .)
- Habilite ou desabilite a coleta de dados de análise de unidade para um gerenciador de recursos XClarity Administrator selecionado clicando no ícone **Editar** ( ).

  Nota: A alternância da **Coleta de dados de análise da unidade** é desativada quando o XClarity Administrator tem problemas de conectividade ou credenciais (consulte Perda repentina de conectividade com um gerenciador de recursos na documentação online do XClarity Orchestrator).
- Desconecte e remova o gerenciador de recursos selecionado clicando no ícone **Excluir** ( ).

  Nota: Se o XClarity Orchestrator não puder se conectar ao gerenciador de recursos (por exemplo, se as credenciais estiverem expiradas ou se houver problemas de rede), selecione **Forçar desconexão**.

  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 .)

  Quando o gerenciador de recursos é removido, todos os dispositivos que são gerenciados por esse gerenciador de recursos também são removidos. Isso inclui inventário de dispositivo, logs, dados de métricas e relatórios analíticos.
- Solução de problemas ao conectar um Gerenciador de Recursos (consulte Não é possível estabelecer conexão com um gerenciador de recursosna documentação online do XClarity Orchestrator).

Descobrindo e gerenciando dispositivos

É possível descobrir e gerenciar dispositivos usando o Lenovo XClarity Orchestrator e atribuir o gerenciamento desses dispositivos a um gerenciador de recursos específico.

Antes de iniciar

Para executar esta tarefa, você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** ou **Administrador de Segurança** foi atribuída.

Sobre esta tarefa

O XClarity Orchestrator monitora e gerencia dispositivos por meio de gerenciadores de recursos. Ao conectar um gerenciador de recursos, o XClarity Orchestrator gerencia todos os dispositivos gerenciados por esse gerenciador de recursos.

Também é possível trazer dispositivos para o gerenciamento usando o XClarity Orchestrator. O XClarity Orchestrator lista dispositivos que já foram descobertos (mas não gerenciados) pelos gerenciadores de recursos. Ao gerenciar dispositivos descobertos a partir do XClarity Orchestrator, os dispositivos são gerenciados pelo gerenciador de recursos que o descobriu. Ao descobrir e gerenciar dispositivos manualmente usando endereços IP, nomes de host ou sub-redes, escolha qual gerenciador de recursos deseja usar para gerenciar os dispositivos. O XClarity Management Hub pode ser usado para gerenciar dispositivos ThinkEdge Client. O XClarity Management Hub 2.0 pode ser usado para gerenciar dispositivos ThinkServer. O Lenovo XClarity Administrator pode ser usado para gerenciar servidores, armazenamento, comutadores e chassi.

Notas:

- Se você tentar gerenciar um dispositivo por meio do XClarity Management Hub 2.0 e esse dispositivo já for gerenciado por outro XClarity Management Hub 2.0, o XClarity Orchestrator removerá a conta do usuário de gerenciamento e as assinaturas do dispositivo sem o reconhecimento de gerenciamento antigo e, em seguida, gerenciará o dispositivo novamente por meio do novo hub de gerenciamento. Após esse processo, o dispositivo ainda é gerenciado, mas fica offline no hub de gerenciamento antigo. No entanto, o dispositivo não envia mais dados a ele. Esteja ciente de que você deve cancelar manualmente o gerenciamento dos dispositivos do primeiro hub de gerenciamento pelo portal conectado.
- Se você tentar gerenciar um dispositivo por meio do XClarity Management Hub 2.0 e esse dispositivo já for gerenciado por meio de outro XClarity Administrator, o XClarity Orchestrator removerá a conta do usuário de gerenciamento, as assinaturas e as informações de LDAP e de SSO que estão registradas no XCC pelo XClarity Administrator do dispositivo sem o reconhecimento do XClarity Administrator e, em seguida, gerenciará o dispositivo novamente por meio do novo XClarity Management Hub 2.0. Após esse processo, o dispositivo ainda é gerenciado, mas fica offline no hub XClarity Administrator. No entanto, o dispositivo não envia mais dados a ele. Esteja ciente de que você deve cancelar manualmente o gerenciamento dos dispositivos do XClarity Administrator pelo portal conectado.

Os dispositivos a seguir podem ser descobertos automaticamente pelos gerenciadores de recursos usando um protocolo de descoberta de serviço.
- Servidores e dispositivos ThinkSystem e ThinkAgile
- Servidores ThinkEdge SE
- Chassi do Flex System e dispositivos ThinkSystem e Flex System em um chassi do Flex System
- Servidores em rack e em torre ThinkServer
- Servidores e dispositivos System x, Converged HX e NeXtScale
- Dispositivos de armazenamento

Os dispositivos a seguir *não podem* ser descobertos automaticamente pelos gerenciadores de recursos usando um protocolo de descoberta de serviço. Você deve instalar o agente UDC nesses dispositivos para que eles possam ser descobertos e gerenciados com segurança.

- Cliente ThinkCentre
- Clientes ThinkEdge

Atualmente, não é possível trazer comutadores para o gerenciamento a partir do XClarity Orchestrator. Também não é possível cancelar o gerenciamento de comutadores Flex System a partir do XClarity Orchestrator.

Considerações sobre gerenciamento de dispositivos

Antes de tentar descobrir e gerenciar dispositivos usando o XClarity Orchestrator, revise as considerações a seguir.

- Considerações gerais
- Considerações sobre servidor
- Considerações sobre armazenamento
- Considerações sobre comutadores
- Considerações sobre chassi
- Considerações sobre várias ferramentas de gerenciamento

Considerações gerais

Certifique-se de que o XClarity Orchestrator comporte os dispositivos que você deseja gerenciar.

Verifique se o firmware mínimo necessário está instalado em cada sistema que você deseja gerenciar.

Algumas portas podem estar disponíveis para comunicação com os dispositivos. Assegure-se de todas as portas necessárias estejam disponíveis antes de tentar gerenciar servidores.

O XClarity Orchestrator pode descobrir automaticamente os dispositivos em seu ambiente sondando dispositivos gerenciáveis que estão na mesma sub-rede IP que o XClarity Orchestrator usando um protocolo de descoberta de serviços. Para descobrir dispositivos que estão em outras sub-redes, é possível especificar manualmente endereços IP, nomes de host, intervalo de endereços IP ou sub-redes.

Após os dispositivos serem gerenciados pelo XClarity Orchestrator, o XClarity Orchestrator sonda cada dispositivo de armazenamento gerenciado periodicamente para coletar informações, como inventário, dados vitais do produto e status.

Se o XClarity Orchestrator perder a comunicação com um dispositivo (por exemplo, devido a uma falha de rede ou perda de energia ou se o comutador estiver offline) ao coletar o inventário durante o processo de gerenciamento, o gerenciamento será concluído com êxito. Entretanto, algumas informações de inventário podem estar incompletas. Aguarde o dispositivo entrar online e o XClarity Orchestrator pesquisar o dispositivo quanto ao inventário ou coletar manualmente o inventário no dispositivo na interface do gerenciador de recursos selecionando o dispositivo e clicando em **Todas as Ações → Inventário → Atualizar inventário**.

Os dispositivos podem ser gerenciados apenas por um Gerenciador de Recursos (XClarity Orchestrator, XClarity Management Hub 2.0,XClarity Management Hub ou XClarity Administrator) por vez. Se um dispositivo for gerenciado por um Gerenciador de Recursos, e você desejar gerenciá-lo com outro Gerenciador de Recursos, primeiro cancele o gerenciamento do dispositivo no Gerenciador de Recursos original.

Se você altera o endereço IP de um dispositivo depois que ele é gerenciado pelo XClarity Orchestrator, reconhece o novo endereço IP e continua gerenciando o servidor. No entanto, o XClarity Orchestrator não reconhece a alteração de endereço IP para alguns servidores. Se o XClarity Orchestrator mostrar que o

servidor está offline após a alteração do endereço IP, gerencie o servidor novamente usando a opção **Forçar gerenciamento**.

Se você remover, substituir ou configurar qualquer adaptador em um dispositivo, reinicie o dispositivo pelo menos uma vez para atualizar as informações de inventário.

Para descobrir um dispositivo que está em uma sub-rede *diferente* do Gerenciador de Recursos, uma das seguintes condições deverá ser atendida:

- Habilite o encaminhamento SLP multicast em comutadores do rack, bem como nos roteadores em seu ambiente. Consulte a documentação que foi fornecida com seu comutador ou roteador específico para determinar se o encaminhamento SLP de multicast está ativado e para encontrar procedimentos para ativá-lo caso esteja desativado.
- Se o SLP estiver desabilitado no dispositivo ou na rede, você poderá usar o método de descoberta DNS adicionando manualmente um registro de serviço (registro do servidor) ao servidor de nomes de domínio (DNS). Exemplo:
  ```
  lxco.company.com  service = 0 0 443 server1.company.com
  ```
  Em seguida, habilite a descoberta de DNS no Baseboard Management Console na interface da Web de gerenciamento clicando em **Configuração BMC → Rede**clicando na guia **DNS**.

Considerações sobre encapsulamento

É possível optar por ativar o encapsulamento no chassi e nos servidores durante o processo de gerenciamento de dispositivos. Quando a configuração de encapsulamento global é ativada e o dispositivo é compatível com o encapsulamento, o gerenciador de recursos se comunica com o dispositivo durante o processo de gerenciamento para alterar o modo de encapsulamento do dispositivo para **encapsulationLite** e modificar as regras de firewall no dispositivo para limitar as solicitações de entrada àquelas do gerenciador de recursos.

Nota: Quando a interface de rede de gerenciamento é configurada para usar o Protocolo de Configuração de Host Dinâmico (DHCP), o gerenciamento de dispositivos com encapsulamento pode ser muito demorado.

A configuração de encapsulamento global é desativada por padrão. Quando desativado, o modo de encapsulamento do dispositivo é definido como **normal** e as regras de firewall não são alteradas durante o processo de gerenciamento de dispositivos.

Atenção: Se o modo de encapsulamento for **encapsulationLite** em dispositivos gerenciados, as seguintes situações poderão causar problemas de comunicação e autenticação entre o gerenciador de recursos e dispositivos gerenciados, tornando os dispositivos gerenciados inacessíveis. Como os dispositivos estão configurados para ignorar solicitações TCP de outras fontes, não é possível acessar esses dispositivos por meio de uma interface de rede. Na maioria dos casos, esses dispositivos não responderão a ping, solicitações SSH ou TELNET.

- Alterações de rede no hipervisor em que o gerenciador de recursos é executado
- Alterações em VLANs (Virtual Local Area Networks) ou tags VLAN
- Alterações permanentes nos endereços IP do dispositivo enquanto o encapsulamento está ativado
- Forçar cancelamento do gerenciamento de um dispositivo enquanto o encapsulamento está ativado
- Perda da máquina virtual do gerenciador de recursos
- Perda de comunicação TCP entre a máquina virtual e os dispositivos gerenciados
- Outros problemas de rede que impedem o gerenciador de recursos de se comunicar diretamente com dispositivos gerenciados enquanto o modo de encapsulamento está ativado

Se ocorrer um problema permanente, conclua uma das ações a seguir para recuperar o acesso aos dispositivos gerenciados anteriormente. Para obter mais informações, consulte Gerenciamento de encapsulamento, Recuperando o gerenciamento com um CMM após uma falha no servidor de gerenciamento e Recuperando o gerenciamento com um CMM após uma falha no servidor de gerenciamento na documentação online do XClarity Administrator.

- Para recuperar o acesso a um IMM gerenciado em que o modo de encapsulamento está ativo, as configurações padrão devem ser carregadas do console local por meio da interface gráfica do usuário UEFI.
- Use a ponte USB para Ethernet para obter acesso dentro da banda ao controlador de gerenciamento e execute o seguinte comando:
  ```
  encaps lite -off
  ```
- Para recuperar o acesso a um CMM gerenciado em que o modo de encapsulamento está ativo, as configurações padrão devem ser carregadas usando o botão de redefinição traseira ou executando o seguinte comando se o console ainda puder ser atingido:
  ```
  accesscontrol -off -T mm[p]
  ```

Considerações sobre servidor

Verifique se CIM sobre HTTPS está ativado no dispositivo. Faça login na interface da Web de gerenciamento do servidor usando a conta do usuário `RECOVERY_ID` Clique em **Configuração BMC → Segurança** e, em seguida, clique na guia **CIM sobre HTTPS** e garanta que **Habilitar CIM sobre HTTPS** esteja selecionado.

Ao executar ações de gerenciamento em um servidor, verifique se o servidor está desligado ou ligado na configuração do BIOS/UEFI ou em um sistema operacional em execução (consulte Executando ações de energia em servidores gerenciados). Se o servidor estiver ligado sem um sistema operacional, o controlador de gerenciamento redefinirá continuamente o servidor para tentar localizar um sistema operacional.

Verifique se as configurações UEFI_Ethernet_* e UEFI_Slot_* estão ativadas nas Configurações UEFI do servidor. Para verificar as configurações, reinicie o servidor e, quando o prompt <F1> Configuração for exibido, pressione **F1** para iniciar o Setup Utility. Acesse **Configurações do Sistema → Dispositivos e Portas de E/S → Habilitar/desabilitar suporte a ROM de opção do adaptador**e, em seguida, localize a seção **Habilitar/desabilitar ROMs de opção de UEFI** para verificar se as configurações estão ativadas. Se suportado, você também poderá usar o recurso Console Remoto na interface de gerenciamento de placa-mãe para examinar e alterar as configurações remotamente.

Se o certificado do servidor do dispositivo for assinado por uma autoridade de certificado externa, garanta que o certificado de autoridade de certificado e todos os certificados intermediários sejam importados para o armazenamento confiável do XClarity Orchestrator (consulte Instalando um certificado de servidor assinado externamente confiável XClarity Orchestrator).

Dispositivos ThinkEdge Client

Os dispositivos ThinkEdge Client não têm Baseboard Management Controllers e, portanto, não são descobertos usando protocolos de descoberta de serviço. Você deve instalar um agente UDC em dispositivos ThinkEdge Client para que os dispositivos possam ser descobertos e gerenciados com segurança pelo Lenovo XClarity Management HubGerenciador de Recursos atribuído. Para obter mais informações, consulte Gerenciando dispositivos ThinkEdge Client.

Servidores ThinkSystem SR635 e SR655

Verifique se um sistema operacional está instalado e o servidor foi inicializado para o SO, mídia inicializável montada ou efishell pelo menos uma vez para que o XClarity Orchestrator possa coletar o inventário desses servidores.

Verifique se a IPMI sobre LAN está ativada. O IPMI sobre LAN é desabilitado por padrão nesses servidores e deve ser habilitado manualmente para que os servidores possam ser gerenciados. Para habilitar o IPMI sobre LAN na interface da Web do ThinkSystem System Manager, clique em **Configurações → Configuração de IPMI**. Talvez seja necessário reiniciar o servidor para ativar a mudança.

Servidores ThinkServer

O nome do host do servidor deve ser configurado usando um nome de host ou um endereço IP válido para descobrir automaticamente esses servidores.

A configuração de rede deve permitir o tráfego SLP entre XClarity Orchestrator e o servidor.

Unicast SLP é necessário.

Para descobrir automaticamente os servidores ThinkServer, o multicast SLP será necessário. Além disso, SLP deve ser ativado no ThinkServer System Manager (TSM).

Se os servidores ThinkServer estiverem em uma rede diferente do XClarity Orchestrator, verifique se a rede está configurada para permitir UDP de entrada pela porta 162 para que o XClarity Orchestrator possa receber eventos para esses dispositivos.

Servidores System x3950 X6
Esses servidores devem ser gerenciados como dois gabinetes 4U, cada um com seu próprio Baseboard Management Controller.

Para obter mais informações sobre o gerenciamento de servidores, consulte Gerenciando servidores e Gerenciando dispositivos ThinkEdge Client.

Considerações sobre armazenamento

Certifique-se de que os seguintes requisitos sejam atendidos antes de descobrir e gerenciar dispositivos de armazenamento do rack (que não sejam ThinkSystem série DE).

- A configuração de rede deve permitir o tráfego SLP entre Gerenciador de Recursos e o dispositivo de armazenamento em rack.
- Unicast SLP é necessário.
- O SLP multicast é necessário se você deseja que o XClarity Orchestrator descubra automaticamente os dispositivos Lenovo Storage. Além, SLP deve ser ativado no dispositivo de armazenamento em rack.

Para obter mais informações sobre gerenciamento de dispositivos de armazenamento, consulte Gerenciando dispositivos de armazenamento.

Considerações sobre comutadores

O gerenciamento de comutadores de rack usando o XClarity Orchestrator não é compatível atualmente.

Considerações sobre chassi

Ao gerenciar um chassi, todos os dispositivos no chassi também são gerenciados. Não é possível descobrir e gerenciar componentes no chassi independentes do chassi.

A configuração Número de sessões ativas simultâneas para usuários LDAP no CMM deve estar configurada como 0 (zero) para o chassi. Para verificar essa configuração na interface da Web do CMM, clique em **Configuração BMC → Contas do Usuário**, clique em **Configurações globais de login** e depois clique na guia **Geral**.

Verifique se há pelo menos três sessões do modo de comando TCP configuradas para comunicação fora da banda com o CMM. Para obter informações sobre como configurar o número de sessões, consulte Comando tcpcmdmode na documentação online do CMM.

Avalie a possibilidade de implementar endereços IPv4 *ou* IPv6 para todos os CMMs e comutadores Flex System gerenciados pelo XClarity Orchestrator. 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).

Para descobrir um chassi que está em uma sub-rede *diferente* do Gerenciador de Recursos, uma das seguintes condições deverá ser atendida:

- Habilite o encaminhamento SLP multicast em comutadores do rack, bem como nos roteadores em seu ambiente. Consulte a documentação que foi fornecida com seu comutador ou roteador específico para determinar se o encaminhamento SLP de multicast está ativado e para encontrar procedimentos para ativá-lo caso esteja desativado.
- Se o SLP estiver desabilitado no dispositivo ou na rede, você poderá usar o método de descoberta DNS adicionando manualmente um registro de serviço (registro do servidor) ao servidor de nomes de domínio (DNS). Exemplo:
  ```
  lxco.company.com  service = 0 0 443 cmm1.company.com
  ```
  Em seguida, habilite a descoberta de DNS no Baseboard Management Console na interface da Web de gerenciamento clicando em **Configuração BMC → Rede**clicando na guia **DNS**.

Para obter mais informações sobre gerenciamento de chassi, consulte Gerenciando chassi.

Considerações sobre várias ferramentas de gerenciamento

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 Orchestrator.

Dispositivos ThinkSystem, ThinkServer e System x

Caso pretenda usar outro software de gerenciamento para monitorar seus dispositivos gerenciados, crie um usuário local com configurações de SNMP ou IPMI corretas da interface do Baseboard Management Controller. 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 login na interface da Web do controlador de gerenciamento do chassi usando o nome de usuário RECOVERY_ID e a senha.
2. Se a política de segurança for definida como **Seguro**, altere o método de autenticação do usuário.
   a. Clique em **Configuração BMC → Contas do Usuário**.
   b. Clique na guia **Contas**.
   c. Clique nas 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.

Definindo configurações de descoberta globais

Escolha as configurações preferenciais a serem usadas ao descobrir dispositivos.

Procedimento

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Recursos (⚙) → Novos dispositivos** para exibir o cartão Descobrir e gerenciar novos dispositivos .

Etapa 2. Clique no ícone ⚙ **Configuração** para exibir a caixa de diálogo Configurações de descoberta.

Etapa 3. Selecione as configurações de descoberta preferenciais.

- **Descoberta do SLP**Indica se o sistema deve descobrir automaticamente dispositivos usando o Service Location Protocol (SLP).

  Quando habilitado, o XClarity Orchestrator tenta descobrir novos dispositivos a cada 15 minutos e em cada login do usuário.

  Nota: A configuração Descoberta do SLP que você escolher no XClarity Orchestrator substitui todas as configurações de descoberta de SLP escolhidas para instâncias do Lenovo XClarity Administrator que são gerenciadas pelo XClarity Orchestrator.Se a configuração Descoberta do SLP for alterada no Lenovo XClarity Administrator, ela será sincronizada com o XClarity Orchestrator.
- **Encapsulamento em todos os dispositivos gerenciados futuros**Indica se o encapsulamento está habilitado durante o gerenciamento do dispositivo.

  O encapsulamento é desativado por padrão. Quando desativado, o modo de encapsulamento do dispositivo é definido como **normal** e as regras de firewall não são alteradas como parte do processo de gerenciamento.

  Quando o encapsulamento é habilitado e um dispositivo é compatível com o encapsulamento, o XClarity Orchestrator se comunica com o dispositivo (por meio do Gerenciador de Recursos) durante o processo de gerenciamento para alterar o modo de encapsulamento do dispositivo para **encapsulationLite** e modificar as regras de firewall no dispositivo para delimitar as solicitações de entrada àquelas do Gerenciador de Recursos escolhido para gerenciar o dispositivo.

  Atenção: Se o encapsulamento for ativado e o Gerenciamento de Recursos escolhido para gerenciar o dispositivo se tornar indisponível antes do cancelamento do gerenciamento do dispositivo, será necessário executar etapas para desativar o encapsulamento a fim de estabelecer a comunicação com esse dispositivo.
- **Solicitação de registro ativada**Indica se os Gerenciadores de Recursos (Lenovo XClarity Administrator e Lenovo XClarity Management Hub) aceitam solicitações de descoberta de um Baseboard Management Controller quando o controlador de gerenciamento usa DNS para encontrar instâncias do Gerenciador de Recursos. Quando ativado, o controlador de gerenciamento pode se registrar com o Gerenciador de Recursos como um dispositivo descoberto.
- **Limpeza de dispositivos offline**. Indica se o sistema deve cancelar automaticamente o gerenciamento de dispositivos que estão offline por pelo menos a quantidade de tempo especificada pelo **Tempo limite de dispositivos offline**. Quando ativado, o XClarity Orchestrator verifica dispositivos offline a cada hora e cada vez que um usuário faz login no portal.
- **Tempo limite de dispositivos offline**A quantidade de tempo, em horas, que os dispositivos devem ficar offline antes de o gerenciamento ser cancelado automaticamente. Esse valor pode ser de **1 a 24** horas. O valor padrão é **24** horas.

Etapa 4. Clique em **Salvar**.

Gerenciando servidores

É possível usar o Lenovo XClarity Orchestrator para gerenciar vários tipos de servidores.

Antes de iniciar

Para executar esta tarefa, você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** ou **Administrador de Segurança** foi atribuída.

Reveja as considerações de gerenciamento antes de gerenciar um dispositivo (consulte Considerações sobre gerenciamento de dispositivos).

Revise as configurações globais de descoberta antes de gerenciar um dispositivo (consulte Definindo configurações de descoberta globais).

Para descobrir e gerenciar dispositivos de borda que não respondem ao protocolo de descoberta de serviço, consulte Gerenciando dispositivos ThinkEdge Client.

A opção de gerenciamento em massa está disponível apenas para servidores. Ela não comporta outros tipos de dispositivo.

Sobre esta tarefa

O XClarity Orchestrator monitora e gerencia dispositivos por meio de gerenciadores de recursos. Ao conectar um gerenciador de recursos, o XClarity Orchestrator gerencia todos os dispositivos gerenciados por esse gerenciador de recursos.

Também é possível trazer dispositivos para o gerenciamento usando o XClarity Orchestrator. O XClarity Orchestrator lista dispositivos que já foram descobertos (mas não gerenciados) pelos gerenciadores de recursos. Ao gerenciar dispositivos descobertos a partir do XClarity Orchestrator, os dispositivos são gerenciados pelo gerenciador de recursos que o descobriu. Ao descobrir e gerenciar dispositivos manualmente usando endereços IP, nomes de host ou sub-redes, escolha qual gerenciador de recursos deseja usar para gerenciar os dispositivos. O XClarity Management Hub pode ser usado para gerenciar dispositivos ThinkEdge Client. O XClarity Management Hub 2.0 pode ser usado para gerenciar dispositivos ThinkServer. O Lenovo XClarity Administrator pode ser usado para gerenciar servidores, armazenamento, comutadores e chassi.

Notas:

- Se você tentar gerenciar um dispositivo por meio do XClarity Management Hub 2.0 e esse dispositivo já for gerenciado por outro XClarity Management Hub 2.0, o XClarity Orchestrator removerá a conta do usuário de gerenciamento e as assinaturas do dispositivo sem o reconhecimento de gerenciamento antigo e, em seguida, gerenciará o dispositivo novamente por meio do novo hub de gerenciamento. Após esse processo, o dispositivo ainda é gerenciado, mas fica offline no hub de gerenciamento antigo. No entanto, o dispositivo não envia mais dados a ele. Esteja ciente de que você deve cancelar manualmente o gerenciamento dos dispositivos do primeiro hub de gerenciamento pelo portal conectado.
- Se você tentar gerenciar um dispositivo por meio do XClarity Management Hub 2.0 e esse dispositivo já for gerenciado por meio de outro XClarity Administrator, o XClarity Orchestrator removerá a conta do usuário de gerenciamento, as assinaturas e as informações de LDAP e de SSO que estão registradas no XCC pelo XClarity Administrator do dispositivo sem o reconhecimento do XClarity Administrator e, em seguida, gerenciará o dispositivo novamente por meio do novo XClarity Management Hub 2.0. Após esse processo, o dispositivo ainda é gerenciado, mas fica offline no hub XClarity Administrator. No entanto, o dispositivo não envia mais dados a ele. Esteja ciente de que você deve cancelar manualmente o gerenciamento dos dispositivos do XClarity Administrator pelo portal conectado.

Os dispositivos a seguir podem ser descobertos automaticamente pelos gerenciadores de recursos usando um protocolo de descoberta de serviço.
- Servidores e dispositivos ThinkSystem e ThinkAgile
- Servidores ThinkEdge SE
- Chassi do Flex System e dispositivos ThinkSystem e Flex System em um chassi do Flex System
- Servidores em rack e em torre ThinkServer
- Servidores e dispositivos System x, Converged HX e NeXtScale
- Dispositivos de armazenamento

Procedimento

Para gerenciar seus servidores, conclua um dos procedimentos a seguir.
- Descobrir manualmente servidores
- Gerenciar servidores descobertos
- Gerenciar um *grande número* de servidores

Descobrir manualmente servidores

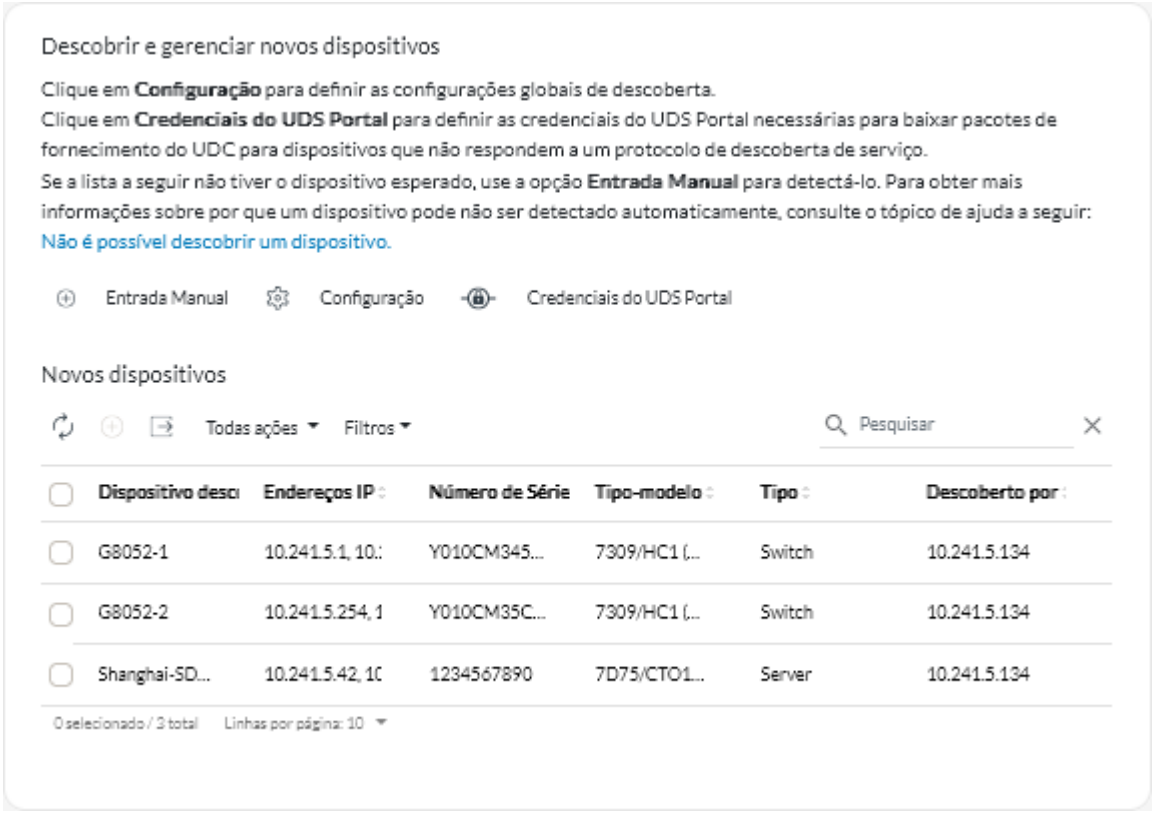
Para descobrir manualmente e gerenciar servidores específicos que não estão na mesma sub-rede que o servidor do orquestrador, conclua as etapas a seguir.

1. Na barra de menus do XClarity Orchestrator, clique em **Recursos ( ) → Novos dispositivos** para exibir o cartão Descobrir e gerenciar novos dispositivos.
2. Clique em **Entrada Manual** para exibir a caixa de diálogo Descobrir Novos dispositivos.
3. Selecione **Dispositivos que respondem ao protocolo de descoberta de serviço** e, em seguida, clique em **Avançar**.
4. Selecione **Manual** e clique em **Avançar**.
5. Escolha como deseja descobrir os dispositivos e, em seguida, especifique os valores apropriados.
   - **Endereços IP/Nomes de host**. Insira o endereço IP IPV4 ou IPv6 ou o nome de domínio totalmente qualificado para cada dispositivo que você deseja gerenciar (por exemplo, 192.0.2.0 ou d1.acme.com).
   - **Intervalos de IP**. Insira os endereços IP inicial e final para o conjunto de dispositivos que você deseja gerenciar.
   - **Sub-redes**. Insira o endereço IP e a máscara para a sub-rede. O XClarity Orchestrator verifica a sub-rede para dispositivos gerenciáveis.
6. Selecione o Gerenciador de Recursos que você deseja usar para gerenciar os dispositivos.
7. Clique em **Descobrir dispositivos**.Quando o processo de descoberta é concluído, os dispositivos descobertos são listados na tabela Novos dispositivos.

Gerenciar servidores descobertos

Para gerenciar dispositivos já descobertos, conclua as etapas a seguir.

1. Na barra de menus do XClarity Orchestrator, clique em **Recursos ( ) → Novos dispositivos** para exibir o cartão Descobrir e gerenciar novos dispositivos.



2. Clique em **Todas as Ações → Atualizar** para descobrir todos os dispositivos gerenciáveis no domínio XClarity Orchestrator. A descoberta pode levar vários minutos.
3. Selecione um ou mais servidores que você deseja gerenciar.
4. Clique no ícone **Gerenciar dispositivos selecionados** (⊕) para exibir a caixa de diálogo Gerenciar dispositivos descobertos.
5. Revise a lista de dispositivos selecionados para gerenciar e clique em **Avançar**.
6. Especifique o nome do usuário e a senha para autenticação no servidor.

   Dica: considere usar uma conta de supervisor ou administrador para gerenciar o dispositivo. Se uma conta com autoridade de nível inferior for usada, poderá ocorrer uma falha no gerenciamento ou poderá ser realizado êxito, mas alguns recursos poderão falhar.
7. **Opcional:** selecione **Criar uma conta de recuperação e desabilitar todos os usuários locais** e, em seguida, especifique a senha de recuperação.Quando desativadas, as contas do usuário locais são usadas para autenticação.

   Quando ativado, o Gerenciador de Recursos atribuído cria uma conta do usuário de autenticação gerenciada e uma conta de recuperação (RECOVERY_ID) no servidor, e todas as outras contas do usuário locais estão desabilitadas. A conta do usuário de autenticação gerenciada é usada pelo XClarity Orchestrator e pelo gerenciador de recursos para autenticação. Se houver um problema com o XClarity Orchestrator ou o Gerenciador de Recursos e ele parar de funcionar por alguma razão, *não* será possível fazer login no Baseboard Management Controller usando contas do usuário normais. No entanto, é possível fazer login usando a conta RECOVERY_ID.

   Importante: Certifique-se de gravar a senha de recuperação para uso futuro.

   Nota: Não há suporte para a conta de recuperação para servidores ThinkServer e System x M4.
8. **Opcional:** habilite **Definir nova senha se as credenciais estiverem expiradas** e, em seguida, especifique a nova senha do servidor.Se a senha atual do servidor tiver expirado, ocorrerá uma falha na

descoberta até que a senha seja alterada. Se você especificar uma nova senha, as credenciais serão alteradas e o processo de gerenciamento poderá continuar. A senha será alterada apenas se a senha atual expirou.

9. Selecione **Gerenciar**.Um trabalho é criado para concluir o processo de gerenciamento em segundo plano. É possível monitorar o status do processo de gerenciamento na caixa de diálogo ou no log de trabalhos clicando em **Monitoramento ( ) → Trabalhos** (consulte Monitorando trabalhos).

   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.

   - O Gerenciador de Recursos falhou e não pode ser recuperado.

     Nota: Se a instância do Gerenciador de Recursos de Substituição usar o mesmo endereço IP do Gerenciador de Recursos com falha, você poderá gerenciar o dispositivo novamente usando a conta `RECOVERY_ID` e a senha (se aplicável) e a opção **Forçar gerenciamento**.
   - O Gerenciador de Recursos foi desligado antes do cancelamento do gerenciamento dos dispositivos.
   - O cancelamento do gerenciamento de dispositivos não foi bem-sucedido.
   - O XClarity Orchestrator mostra um dispositivo gerenciado como offline depois que o endereço IP do dispositivo foi alterado.

Gerenciar um *grande número* de servidores

Para gerenciar um grande número de servidores, conclua as etapas a seguir.

1. Na barra de menus do XClarity Orchestrator, clique em **Recursos ( ) → Novos dispositivos** para exibir o cartão Descobrir e gerenciar novos dispositivos.
2. Clique no botão **Gerenciar em massa** para exibir a caixa de diálogo Gerenciar em massa.
3. Selecione o Gerenciador de Recursos que você deseja usar para gerenciar os dispositivos.
4. Insira o endereço IP ou o nome de domínio totalmente qualificado para cada servidor que você deseja gerenciar, separado por uma vírgula (por exemplo, `192.0.2.0`, `d1.acme.com`).

   Importante:

   - Todos esses servidores especificados devem usar as mesmas credenciais.
   - FQDNs podem conter apenas caracteres alfanuméricos, pontos e traços.
5. Clique em **Avançar**.
6. Especifique o nome do usuário e a senha para autenticação no servidor.

   Dica: considere usar uma conta de supervisor ou administrador para gerenciar o dispositivo. Se uma conta com autoridade de nível inferior for usada, poderá ocorrer uma falha no gerenciamento ou poderá ser realizado êxito, mas alguns recursos poderão falhar.
7. **Opcional:** selecione **Criar uma conta de recuperação e desabilitar todos os usuários locais** e, em seguida, especifique a senha de recuperação.Quando desativadas, as contas do usuário locais são usadas para autenticação.

   Quando ativado, o Gerenciador de Recursos atribuído cria uma conta do usuário de autenticação gerenciada e uma conta de recuperação (RECOVERY_ID) no servidor, e todas as outras contas do usuário locais estão desabilitadas. A conta do usuário de autenticação gerenciada é usada pelo XClarity Orchestrator e pelo gerenciador de recursos para autenticação. Se houver um problema com o XClarity Orchestrator ou o Gerenciador de Recursos e ele parar de funcionar por alguma razão, *não* será possível fazer login no Baseboard Management Controller usando contas do usuário normais. No entanto, é possível fazer login usando a conta RECOVERY_ID.

   Importante: Certifique-se de gravar a senha de recuperação para uso futuro.

Nota: Não há suporte para a conta de recuperação para servidores ThinkServer e System x M4.

8. **Opcional:** habilite **Definir nova senha se as credenciais estiverem expiradas** e, em seguida, especifique a nova senha do servidor.Se a senha atual do servidor tiver expirado, ocorrerá uma falha na descoberta até que a senha seja alterada. Se você especificar uma nova senha, as credenciais serão alteradas e o processo de gerenciamento poderá continuar. A senha será alterada apenas se a senha atual expirou.
9. Selecione **Gerenciar**.Um trabalho é criado para concluir o processo de gerenciamento em segundo plano. É possível monitorar o status do processo de gerenciamento na caixa de diálogo ou no log de trabalhos clicando em **Monitoramento (** **) → Trabalhos** (consulte Monitorando trabalhos).

   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.

   - O Gerenciador de Recursos falhou e não pode ser recuperado.

     Nota: Se a instância do Gerenciador de Recursos de Substituição usar o mesmo endereço IP do Gerenciador de Recursos com falha, você poderá gerenciar o dispositivo novamente usando a conta `RECOVERY_ID` e a senha (se aplicável) e a opção **Forçar gerenciamento**.
   - O Gerenciador de Recursos foi desligado antes do cancelamento do gerenciamento dos dispositivos.
   - O cancelamento do gerenciamento de dispositivos não foi bem-sucedido.
   - O XClarity Orchestrator mostra um dispositivo gerenciado como offline depois que o endereço IP do dispositivo foi alterado.

Depois de concluir

É possível realizar as ações a seguir no dispositivo gerenciado.

- Monitore o status e os detalhes do dispositivo (consulte Exibindo o status dos dispositivos e Visualizando detalhes de dispositivos).
- Cancele o gerenciamento e remova um dispositivo selecionando clicando em **Recursos** ( ) e, em seguida, clique no tipo de dispositivo na navegação à esquerda para exibir uma placa com uma exibição tabular de todos os dispositivos gerenciados desse tipo, selecione os dispositivos cujo gerenciamento deseja cancelar e, em seguida, clique no ícone **Cancelar gerenciamento** ( ).

  Notas:

  – É possível cancelar o gerenciamento de, no máximo, **50** dispositivos ao mesmo tempo.
  – Nenhum trabalho ativo deve estar em execução no dispositivo.
  – Se o XClarity Orchestrator não puder se conectar ao Gerenciador de Recursos (por exemplo, se as credenciais estiverem expiradas ou se houver problemas de rede), selecione **Forçar cancelamento de gerenciamento mesmo se o dispositivo não estiver acessível**.
  – Por padrão, o gerenciamento dos dispositivos gerenciados pelo XClarity Administrator e que permanecem offline por 24 horas ou mais é cancelado automaticamente (consulte Definindo configurações de descoberta globais).
  – Para a maioria dos dispositivos, determinadas informações sobre o dispositivo ficam retidas após o gerenciamento do dispositivo ser cancelado. Quando o gerenciamento dos dispositivos é cancelado:
    – A conta do usuário de gerenciamento e as assinaturas de evento e de métricas são removidas do dispositivo.
    – Para dispositivos gerenciados pelo XClarity Administrator, se o Call Home estiver habilitado no momento no XClarity Administrator, o Call Home será desabilitado no dispositivo.
    – Para dispositivos gerenciados pelo XClarity Administrator, se o encapsulamento estiver habilitado no dispositivo, as regras de firewall do dispositivo serão alteradas para as configurações antes de o dispositivo ser gerenciado.

  - Informações sensíveis, inventário e eventos e alertas que foram gerados pelo dispositivo são descartados no hub de gerenciamento.
  - Eventos e alertas que foram gerados pelo hub de gerenciamento do dispositivo ficam retidos no hub de gerenciamento.

Gerenciando dispositivos ThinkEdge Client

Os dispositivos ThinkEdge Client não têm Baseboard Management Controllers e, portanto, não são descobertos usando protocolos de descoberta de serviço. Você deve instalar um agente Universal Device Client (UDC) em dispositivos ThinkEdge Client para que os dispositivos possam ser descobertos e gerenciados com segurança pelo Lenovo XClarity Management HubGerenciador de Recursos atribuído. Somente os Gerenciadores de Recursos Lenovo XClarity Management Hub podem descobrir e gerenciar esses dispositivos.

Antes de iniciar

Reveja as considerações de gerenciamento antes de gerenciar um dispositivo (consulte Considerações sobre gerenciamento de dispositivos).

Verifique se, pelo menos, um Lenovo XClarity Management HubGerenciador de Recursos está conectado ao XClarity Orchestrator (consulte Conectando gerenciadores de recursos).

Para executar esta tarefa, você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** ou **Administrador de Segurança** foi atribuída.

Verifique se as credenciais do UDS Portal estão configuradas com o ID do cliente e o segredo. As credenciais são usadas para assinar a política usada no pacote de fornecimento do cliente. O UDS Portal é a fonte confiável para assinar essa política para que o agente UDC funcione corretamente. Para configurar as credenciais, clique em **Recursos** ( ) → **Novos dispositivos** na barra de menus, clique em **Credenciais do UDS Portal** e, em seguida, insira o ID do cliente e o segredo. Você deve solicitar o ID do cliente e o segredo da Lenovo enviando um e-mail para uedmcredreq@lenovo.com, usando "Credenciais do UDS Portal" na descrição de e-mail e inclua o nome da sua empresa, informações de contato (e-mail ou número de telefone) e o Número de Cliente da Lenovo de 10 dígitos.

Verifique se um agente UDC *não está* instalado atualmente no dispositivo ThinkEdge Client. Se um agente UDC estiver instalado, você deverá desinstalá-lo executando os comandos a seguir. Você deve ter privilégios elevados para instalar o agente UDC.

- **Linux**
  ```
  sudo apt purge udc-release
  ```
- **Windows**
  ```
  PUSHD %windir%\System32\drivers\Lenovo\udc\Data\InfBackup\.\UDCInfInstaller.exe -uninstall

  POPD
  ```

Verifique se o servidor DNS está configurado para incluir os domínios a seguir, em que *(hub-domain}* é o nome de domínio totalmente qualificado do Gerenciador de Recursos XClarity Management Hub que você deseja usar para gerenciar os dispositivos ThinkEdge Client.
- api.*(hub-domain}*
- api-mtls.*(hub-domain}*
- auth.*(hub-domain}*
- mqtt.*(hub-domain}*
- mqtt-mtls.*(hub-domain}*
- s3.*(hub-domain}*
- s3console.*(hub-domain}*

Sobre esta tarefa

O XClarity Orchestrator monitora e gerencia dispositivos por meio de gerenciadores de recursos. Ao conectar um gerenciador de recursos, o XClarity Orchestrator gerencia todos os dispositivos gerenciados por esse gerenciador de recursos.

Também é possível trazer dispositivos para o gerenciamento usando o XClarity Orchestrator. O XClarity Orchestrator lista dispositivos que já foram descobertos (mas não gerenciados) pelos gerenciadores de recursos. Ao gerenciar dispositivos descobertos a partir do XClarity Orchestrator, os dispositivos são gerenciados pelo gerenciador de recursos que o descobriu. Ao descobrir e gerenciar dispositivos manualmente usando endereços IP, nomes de host ou sub-redes, escolha qual gerenciador de recursos deseja usar para gerenciar os dispositivos. O XClarity Management Hub pode ser usado para gerenciar dispositivos ThinkEdge Client. O XClarity Management Hub 2.0 pode ser usado para gerenciar dispositivos ThinkServer. O Lenovo XClarity Administrator pode ser usado para gerenciar servidores, armazenamento, comutadores e chassi.

É possível localizar uma lista completa de dispositivos ThinkEdge Client compatíveis no Site de suporte do Lenovo XClarity clicando na guia **Compatibilidade** e, em seguida, clicando no link para os tipos de dispositivo apropriados.

Nota: Os servidores ThinkEdge (como SE350, SE360 e SE450) têm Baseboard Management Controllers e podem ser descobertos usando um protocolo de descoberta de serviço. Para gerenciar esses dispositivos, consulte Gerenciando servidores.

Procedimento

Para descobrir e gerenciar dispositivos ThinkEdge Client, conclua as etapas a seguir.

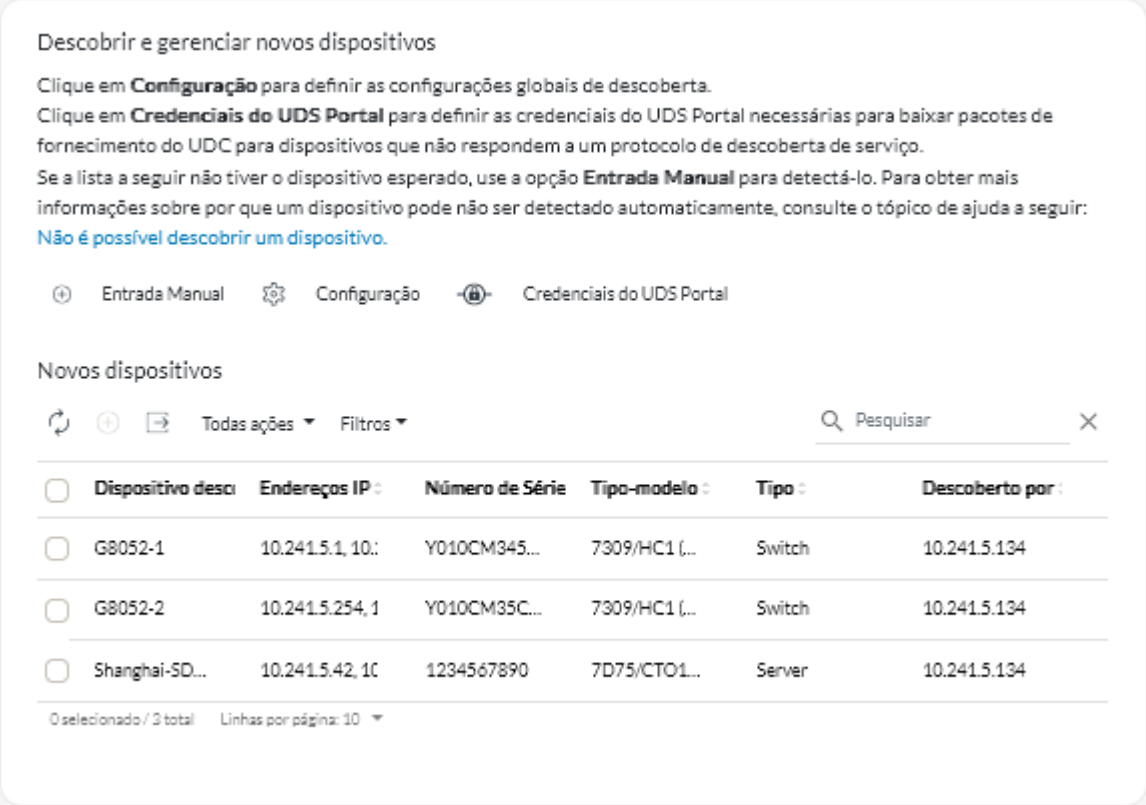
1. Instale o agente UDC em cada dispositivo ThinkEdge Client.
   a. Na barra de menus do XClarity Orchestrator, clique em **Recursos** ( ) → **Novos dispositivos** para exibir o cartão Descobrir e gerenciar novos dispositivos.
   b. Clique em **Entrada Manual** para exibir a caixa de diálogo Descobrir Novos dispositivos.
   c. Selecione **Dispositivos que não respondem ao protocolo de descoberta de serviço** e, em seguida, clique em **Avançar**.
   d. Selecione o endereço IP do Gerenciador de Recursos XClarity Management Hub que você deseja usar para gerenciar os dispositivos ThinkEdge Client.Apenas Gerenciadores de Recursos XClarity Management Hub em estado funcional podem ser selecionados.
   e. Selecione o tipo de sistema operacional instalado no servidor.
      - **Linux ARM**
      - **Linux x86**
      - **Windows**
   f. Selecione o número de dias antes que o instalador do agente UDC se torne inutilizável depois de ser baixado. O valor padrão é **30** dias.
   g. Selecione o número de vezes que você planeja instalar o agente UDC em um servidor. Geralmente, esse é o número de dispositivos nos quais você precisa instalar o agente UDC. É possível especificar até **1.000.000** usos; o padrão é **10** usos.
   h. Clique em **Baixar o agente UDC** para baixar o instalador do agente UDC para seu sistema local.Um trabalho é criado para concluir o processo de download em segundo plano. É possível monitorar o status do processo de download na caixa de diálogo ou no log de trabalhos clicando em **Monitoramento** ( ) → **Trabalhos** (consulte Monitorando trabalhos).
   i. Clique em **Fechar** para fechar a caixa de diálogo.

j. Copie o instalador do agente UDC para cada dispositivo ThinkEdge Client apropriado, descompacte o pacote e, em seguida, instale o agente UDC nesses dispositivos usando o comando a seguir. Você deve ter privilégios de **administrador** para instalar o agente UDC.
   - **Linux** `install.sh`
   - **Windows** `setup.cmd`

   Após o agente UDC ser instalado com êxito em cada dispositivo ThinkEdge Client, os dispositivos podem ser descobertos automaticamente pelo Gerenciador de Recursos XClarity Management Hub selecionado.

2. Gerencie os dispositivos ThinkEdge Client.
   a. Na barra de menus do XClarity Orchestrator, clique em **Recursos** ( ) → **Novos dispositivos** para exibir o cartão Descobrir e gerenciar novos dispositivos.

      Nota: Pode levar um tempo para que endereços IP apareçam na tabela.



   b. Clique em **Todas as Ações** → **Atualizar** para descobrir todos os dispositivos gerenciáveis no domínio XClarity Orchestrator. A descoberta pode levar vários minutos.
   c. Selecione um ou mais dispositivos ThinkEdge Client que você deseja gerenciar.
   d. Clique no ícone **Gerenciar** ( ) para exibir a caixa de diálogo Gerenciar dispositivos.
   e. Revise a lista de dispositivos selecionados para gerenciar.
   f. Selecione **Gerenciar**.Um trabalho é criado para concluir o processo de gerenciamento em segundo plano. É possível monitorar o status do processo de gerenciamento na caixa de diálogo ou no log de trabalhos clicando em **Monitoramento** ( ) → **Trabalhos** (consulte Monitorando trabalhos).

      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.

      - O Gerenciador de Recursos falhou e não pode ser recuperado.

Nota: Se a instância do Gerenciador de Recursos de Substituição usar o mesmo endereço IP do Gerenciador de Recursos com falha, você poderá gerenciar o dispositivo novamente usando a conta `RECOVERY_ID` e a senha (se aplicável) e a opção **Forçar gerenciamento**.

- O Gerenciador de Recursos foi desligado antes do cancelamento do gerenciamento dos dispositivos.
- O cancelamento do gerenciamento de dispositivos não foi bem-sucedido.
- O XClarity Orchestrator mostra um dispositivo gerenciado como offline depois que o endereço IP do dispositivo foi alterado.

Depois de concluir

É possível realizar as ações a seguir no dispositivo gerenciado.

- Monitore o status e os detalhes do dispositivo (consulte Exibindo o status dos dispositivos e Visualizando detalhes de dispositivos).
- Cancele o gerenciamento e remova um dispositivo selecionando clicando em **Recursos** (⚙) e, em seguida, clique no tipo de dispositivo na navegação à esquerda para exibir uma placa com uma exibição tabular de todos os dispositivos gerenciados desse tipo, selecione os dispositivos cujo gerenciamento deseja cancelar e, em seguida, clique no ícone **Cancelar gerenciamento** (🗑).

  Notas:

  – É possível cancelar o gerenciamento de, no máximo, **50** dispositivos ao mesmo tempo.
  – Nenhum trabalho ativo deve estar em execução no dispositivo.
  – Se o XClarity Orchestrator não puder se conectar ao Gerenciador de Recursos (por exemplo, se as credenciais estiverem expiradas ou se houver problemas de rede), selecione **Forçar cancelamento de gerenciamento mesmo se o dispositivo não estiver acessível**.
  – Por padrão, o gerenciamento dos dispositivos gerenciados pelo XClarity Administrator e que permanecem offline por 24 horas ou mais é cancelado automaticamente (consulte Definindo configurações de descoberta globais).
  – Para a maioria dos dispositivos, determinadas informações sobre o dispositivo ficam retidas após o gerenciamento do dispositivo ser cancelado. Quando o gerenciamento dos dispositivos é cancelado:
    – A conta do usuário de gerenciamento e as assinaturas de evento e de métricas são removidas do dispositivo.
    – Para dispositivos gerenciados pelo XClarity Administrator, se o Call Home estiver habilitado no momento no XClarity Administrator, o Call Home será desabilitado no dispositivo.
    – Para dispositivos gerenciados pelo XClarity Administrator, se o encapsulamento estiver habilitado no dispositivo, as regras de firewall do dispositivo serão alteradas para as configurações antes de o dispositivo ser gerenciado.
    – Informações sensíveis, inventário e eventos e alertas que foram gerados pelo dispositivo são descartados no hub de gerenciamento.
    – Eventos e alertas que foram gerados pelo hub de gerenciamento do dispositivo ficam retidos no hub de gerenciamento.

Gerenciando dispositivos de armazenamento

O Lenovo XClarity Orchestrator pode gerenciar diversos tipos de dispositivos de armazenamento, dispositivos e bibliotecas de fita da Lenovo.

Antes de iniciar

Para executar esta tarefa, você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** ou **Administrador de Segurança** foi atribuída.

Reveja as considerações de gerenciamento antes de gerenciar um dispositivo (consulte Considerações sobre gerenciamento de dispositivos).

Para descobrir e gerenciar dispositivos de borda que não respondem ao protocolo de descoberta de serviço, consulte Gerenciando dispositivos ThinkEdge Client.

A opção de gerenciamento em massa está disponível apenas para servidores. Ela não comporta outros tipos de dispositivo.

Sobre esta tarefa

O XClarity Orchestrator monitora e gerencia dispositivos por meio de gerenciadores de recursos. Ao conectar um gerenciador de recursos, o XClarity Orchestrator gerencia todos os dispositivos gerenciados por esse gerenciador de recursos.

Também é possível trazer dispositivos para o gerenciamento usando o XClarity Orchestrator. O XClarity Orchestrator lista dispositivos que já foram descobertos (mas não gerenciados) pelos gerenciadores de recursos. Ao gerenciar dispositivos descobertos a partir do XClarity Orchestrator, os dispositivos são gerenciados pelo gerenciador de recursos que o descobriu. Ao descobrir e gerenciar dispositivos manualmente usando endereços IP, nomes de host ou sub-redes, escolha qual gerenciador de recursos deseja usar para gerenciar os dispositivos. O XClarity Management Hub pode ser usado para gerenciar dispositivos ThinkEdge Client. O XClarity Management Hub 2.0 pode ser usado para gerenciar dispositivos ThinkServer. O Lenovo XClarity Administrator pode ser usado para gerenciar servidores, armazenamento, comutadores e chassi.

Procedimento

Para gerenciar seus dispositivos de armazenamento, execute um dos procedimentos a seguir.
- Descobrir dispositivos de armazenamento manualmente
- Gerenciar dispositivos de armazenamento descobertos

Descobrir dispositivos de armazenamento manualmente

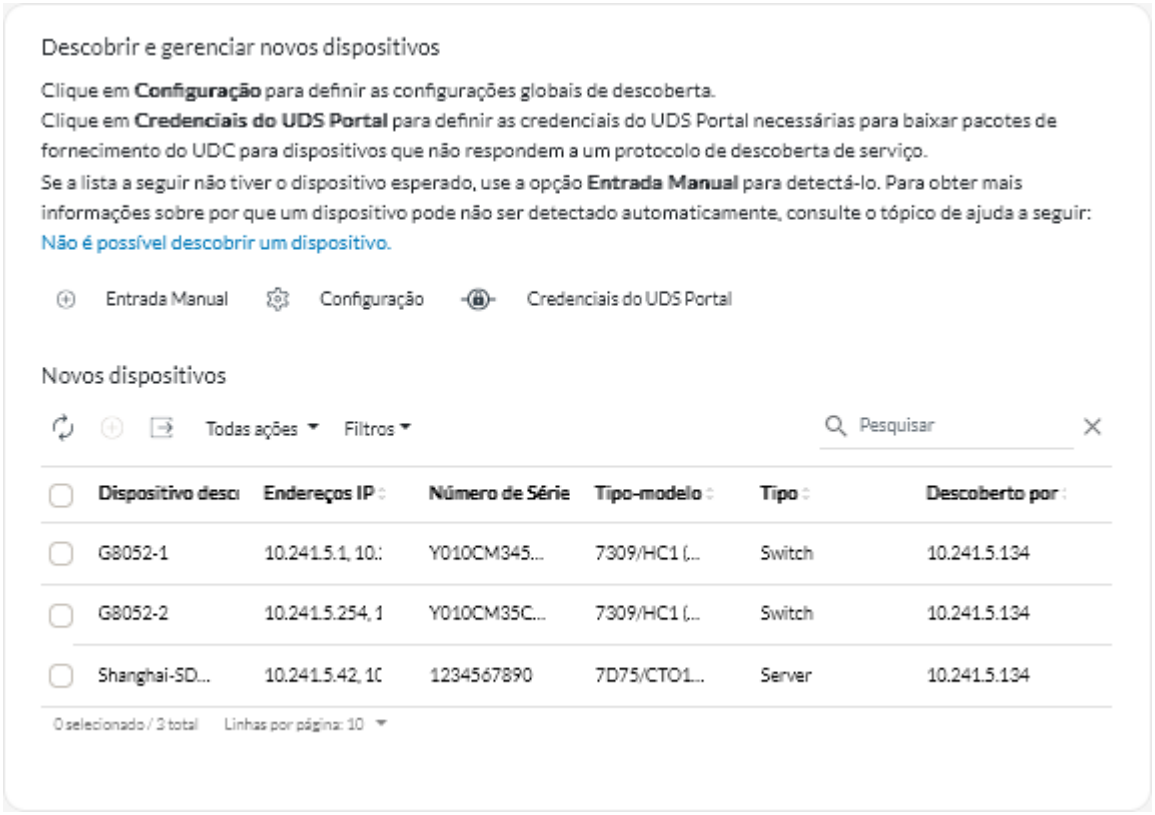
Para descobrir manualmente e, em seguida, gerenciar dispositivos de gerenciamento específicos que não estão na mesma sub-rede que o servidor do orquestrador, conclua as etapas a seguir.

1. Na barra de menus do XClarity Orchestrator, clique em **Recursos** (⚙) → **Novos dispositivos** para exibir o cartão Descobrir e gerenciar novos dispositivos.
2. Clique em **Entrada Manual** para exibir a caixa de diálogo Descobrir Novos dispositivos.
3. Selecione **Dispositivos que respondem ao protocolo de descoberta de serviço** e, em seguida, clique em **Avançar**.
4. Selecione **Manual** e clique em **Avançar**.
5. Escolha como deseja descobrir os dispositivos e, em seguida, especifique os valores apropriados.
   - **Endereços IP/Nomes de host**. Insira o endereço IP IPV4 ou IPv6 ou o nome de domínio totalmente qualificado para cada dispositivo que você deseja gerenciar (por exemplo, 192.0.2.0 ou d1.acme.com).
   - **Intervalos de IP**. Insira os endereços IP inicial e final para o conjunto de dispositivos que você deseja gerenciar.
   - **Sub-redes**. Insira o endereço IP e a máscara para a sub-rede. O XClarity Orchestrator verifica a sub-rede para dispositivos gerenciáveis.
6. Selecione o Gerenciador de Recursos que você deseja usar para gerenciar os dispositivos.
7. Clique em **Descobrir dispositivos**.Quando o processo de descoberta é concluído, os dispositivos descobertos são listados na tabela Novos dispositivos.

Gerenciar dispositivos de armazenamento descobertos

Para gerenciar dispositivos já descobertos, conclua as etapas a seguir.

1. Na barra de menus do XClarity Orchestrator, clique em **Recursos** (⚙) → **Novos dispositivos** para exibir o cartão Descobrir e gerenciar novos dispositivos.



2. Clique em **Todas as Ações** → **Atualizar** para descobrir todos os dispositivos gerenciáveis no domínio XClarity Orchestrator. A descoberta pode levar vários minutos.
3. Selecione um ou mais dispositivos de armazenamento que você deseja gerenciar.
4. Clique no ícone **Gerenciar dispositivos selecionados** (⊕) para exibir a caixa de diálogo Gerenciar dispositivos descobertos.
5. Revise a lista de dispositivos selecionados para gerenciar e clique em **Avançar**.
6. Especifique o nome do usuário e a senha para autenticação no servidor.

   Dica: considere usar uma conta de supervisor ou administrador para gerenciar o dispositivo. Se uma conta com autoridade de nível inferior for usada, poderá ocorrer uma falha no gerenciamento ou poderá ser realizado êxito, mas alguns recursos poderão falhar.
7. Selecione **Gerenciar**.Um trabalho é criado para concluir o processo de gerenciamento em segundo plano. É possível monitorar o status do processo de gerenciamento na caixa de diálogo ou no log de trabalhos clicando em **Monitoramento** (📈) → **Trabalhos** (consulte Monitorando trabalhos).

   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.

   - O Gerenciador de Recursos falhou e não pode ser recuperado.

Nota: Se a instância do Gerenciador de Recursos de Substituição usar o mesmo endereço IP do Gerenciador de Recursos com falha, você poderá gerenciar o dispositivo novamente usando a conta `RECOVERY_ID` e a senha (se aplicável) e a opção **Forçar gerenciamento**.

- O Gerenciador de Recursos foi desligado antes do cancelamento do gerenciamento dos dispositivos.
- O cancelamento do gerenciamento de dispositivos não foi bem-sucedido.
- O XClarity Orchestrator mostra um dispositivo gerenciado como offline depois que o endereço IP do dispositivo foi alterado.

Depois de concluir

É possível realizar as ações a seguir no dispositivo gerenciado.

- Monitore o status e os detalhes do dispositivo (consulte Exibindo o status dos dispositivos e Visualizando detalhes de dispositivos).
- Cancele o gerenciamento e remova um dispositivo selecionando clicando em **Recursos** (⚙) e, em seguida, clique no tipo de dispositivo na navegação à esquerda para exibir uma placa com uma exibição tabular de todos os dispositivos gerenciados desse tipo, selecione os dispositivos cujo gerenciamento deseja cancelar e, em seguida, clique no ícone **Cancelar gerenciamento** (🗑).

  Notas:

  – É possível cancelar o gerenciamento de, no máximo, **50** dispositivos ao mesmo tempo.
  – Nenhum trabalho ativo deve estar em execução no dispositivo.
  – Se o XClarity Orchestrator não puder se conectar ao Gerenciador de Recursos (por exemplo, se as credenciais estiverem expiradas ou se houver problemas de rede), selecione **Forçar cancelamento de gerenciamento mesmo se o dispositivo não estiver acessível**.
  – Por padrão, o gerenciamento dos dispositivos gerenciados pelo XClarity Administrator e que permanecem offline por 24 horas ou mais é cancelado automaticamente (consulte Definindo configurações de descoberta globais).
  – Para a maioria dos dispositivos, determinadas informações sobre o dispositivo ficam retidas após o gerenciamento do dispositivo ser cancelado. Quando o gerenciamento dos dispositivos é cancelado:
    – A conta do usuário de gerenciamento e as assinaturas de evento e de métricas são removidas do dispositivo.
    – Para dispositivos gerenciados pelo XClarity Administrator, se o Call Home estiver habilitado no momento no XClarity Administrator, o Call Home será desabilitado no dispositivo.
    – Para dispositivos gerenciados pelo XClarity Administrator, se o encapsulamento estiver habilitado no dispositivo, as regras de firewall do dispositivo serão alteradas para as configurações antes de o dispositivo ser gerenciado.
    – Informações sensíveis, inventário e eventos e alertas que foram gerados pelo dispositivo são descartados no hub de gerenciamento.
    – Eventos e alertas que foram gerados pelo hub de gerenciamento do dispositivo ficam retidos no hub de gerenciamento.

Gerenciando chassi

O Lenovo XClarity Orchestrator pode gerenciar diversos tipos de chassi e componentes do chassi.

Antes de iniciar

Para executar esta tarefa, você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** ou **Administrador de Segurança** foi atribuída.

Reveja as considerações de gerenciamento antes de gerenciar um dispositivo (consulte Considerações sobre gerenciamento de dispositivos).

Para descobrir e gerenciar dispositivos de borda que não respondem ao protocolo de descoberta de serviço, consulte Gerenciando dispositivos ThinkEdge Client.

A opção de gerenciamento em massa está disponível apenas para servidores. Ela não comporta outros tipos de dispositivo.

Sobre esta tarefa

O XClarity Orchestrator monitora e gerencia dispositivos por meio de gerenciadores de recursos. Ao conectar um gerenciador de recursos, o XClarity Orchestrator gerencia todos os dispositivos gerenciados por esse gerenciador de recursos.

Também é possível trazer dispositivos para o gerenciamento usando o XClarity Orchestrator. O XClarity Orchestrator lista dispositivos que já foram descobertos (mas não gerenciados) pelos gerenciadores de recursos. Ao gerenciar dispositivos descobertos a partir do XClarity Orchestrator, os dispositivos são gerenciados pelo gerenciador de recursos que o descobriu. Ao descobrir e gerenciar dispositivos manualmente usando endereços IP, nomes de host ou sub-redes, escolha qual gerenciador de recursos deseja usar para gerenciar os dispositivos. O XClarity Management Hub pode ser usado para gerenciar dispositivos ThinkEdge Client. O XClarity Management Hub 2.0 pode ser usado para gerenciar dispositivos ThinkServer. O Lenovo XClarity Administrator pode ser usado para gerenciar servidores, armazenamento, comutadores e chassi.

Procedimento

Para gerenciar seu chassi, conclua um dos procedimentos a seguir.
- Descobrir manualmente o chassi
- Gerenciar chassi descoberto

Descobrir manualmente o chassi

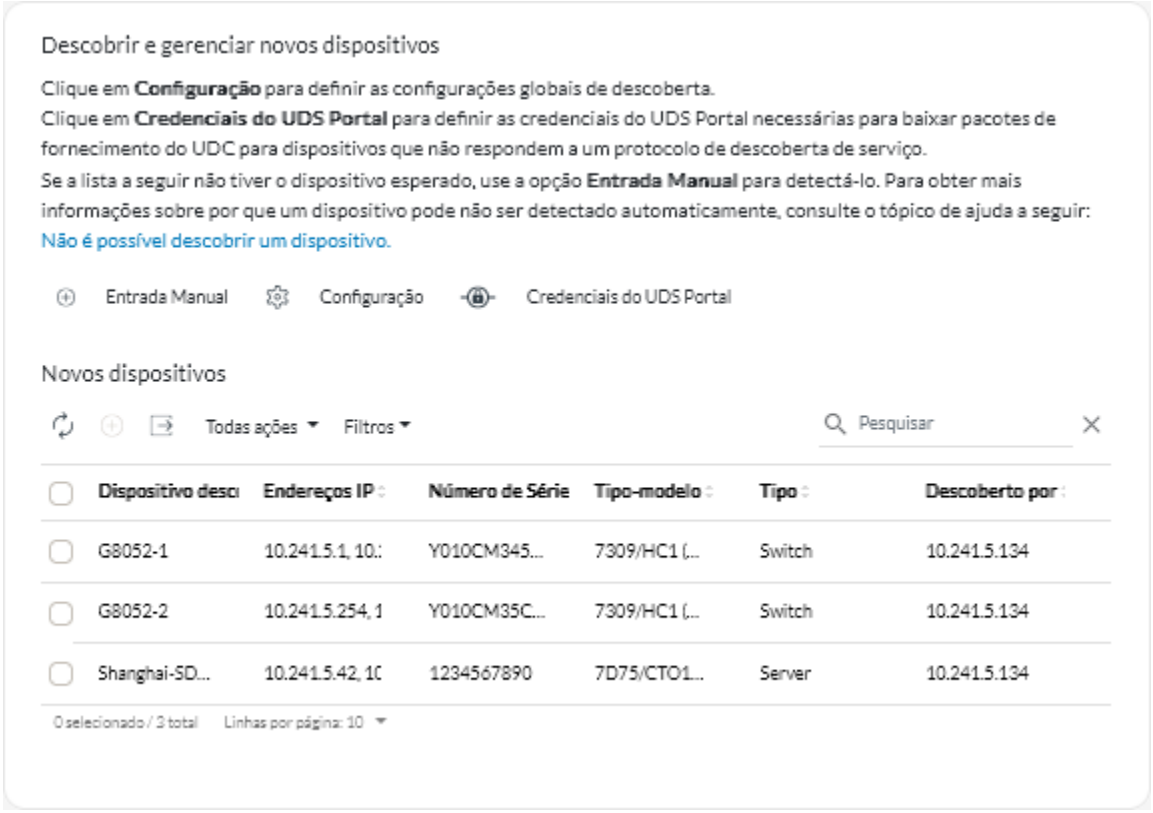
Para descobrir manualmente e, em seguida, gerenciar chassi específico que não está na mesma sub-rede que o servidor do orquestrador, conclua as etapas a seguir.

1. Na barra de menus do XClarity Orchestrator, clique em **Recursos** ( ) → **Novos dispositivos** para exibir o cartão Descobrir e gerenciar novos dispositivos.
2. Clique em **Entrada Manual** para exibir a caixa de diálogo Descobrir Novos dispositivos.
3. Selecione **Dispositivos que respondem ao protocolo de descoberta de serviço** e, em seguida, clique em **Avançar**.
4. Selecione **Manual** e clique em **Avançar**.
5. Escolha como deseja descobrir os dispositivos e, em seguida, especifique os valores apropriados.
   - **Endereços IP/Nomes de host**. Insira o endereço IP IPV4 ou IPv6 ou o nome de domínio totalmente qualificado para cada dispositivo que você deseja gerenciar (por exemplo, 192.0.2.0 ou d1.acme.com).
   - **Intervalos de IP**. Insira os endereços IP inicial e final para o conjunto de dispositivos que você deseja gerenciar.
   - **Sub-redes**. Insira o endereço IP e a máscara para a sub-rede. O XClarity Orchestrator verifica a sub-rede para dispositivos gerenciáveis.
6. Selecione o Gerenciador de Recursos que você deseja usar para gerenciar os dispositivos.
7. Clique em **Descobrir dispositivos**.Quando o processo de descoberta é concluído, os dispositivos descobertos são listados na tabela Novos dispositivos.

Gerenciar chassi descoberto

Para gerenciar dispositivos já descobertos, conclua as etapas a seguir.

1. Na barra de menus do XClarity Orchestrator, clique em **Recursos (⚙) → Novos dispositivos** para exibir o cartão Descobrir e gerenciar novos dispositivos.



2. Clique em **Todas as Ações → Atualizar** para descobrir todos os dispositivos gerenciáveis no domínio XClarity Orchestrator. A descoberta pode levar vários minutos.
3. Selecione um ou mais chassis que você deseja gerenciar.
4. Clique no ícone **Gerenciar dispositivos selecionados** (⊕) para exibir a caixa de diálogo Gerenciar dispositivos descobertos.
5. Revise a lista de dispositivos selecionados para gerenciar e clique em **Avançar**.
6. Especifique o nome do usuário e a senha para autenticação no servidor.

   Dica: considere usar uma conta de supervisor ou administrador para gerenciar o dispositivo. Se uma conta com autoridade de nível inferior for usada, poderá ocorrer uma falha no gerenciamento ou poderá ser realizado êxito, mas alguns recursos poderão falhar.
7. **Opcional:** selecione **Criar uma conta de recuperação e desabilitar todos os usuários locais** e, em seguida, especifique a senha de recuperação.Quando desativadas, as contas do usuário locais são usadas para autenticação.

   Quando ativado, o Gerenciador de Recursos atribuído cria uma conta do usuário de autenticação gerenciada e uma conta de recuperação (RECOVERY_ID) no servidor, e todas as outras contas do usuário locais estão desabilitadas. A conta do usuário de autenticação gerenciada é usada pelo XClarity Orchestrator e pelo gerenciador de recursos para autenticação. Se houver um problema com o XClarity Orchestrator ou o Gerenciador de Recursos e ele parar de funcionar por alguma razão, *não* será

possível fazer login no Baseboard Management Controller usando contas do usuário normais. No entanto, é possível fazer login usando a conta RECOVERY_ID.

Importante: Certifique-se de gravar a senha de recuperação para uso futuro.

Nota: Não há suporte para a conta de recuperação para servidores ThinkServer e System x M4.

8. **Opcional:** habilite **Definir nova senha se as credenciais estiverem expiradas** e, em seguida, especifique a nova senha do servidor.Se a senha atual do servidor tiver expirado, ocorrerá uma falha na descoberta até que a senha seja alterada. Se você especificar uma nova senha, as credenciais serão alteradas e o processo de gerenciamento poderá continuar. A senha será alterada apenas se a senha atual expirou.
9. Selecione **Gerenciar**.Um trabalho é criado para concluir o processo de gerenciamento em segundo plano. É possível monitorar o status do processo de gerenciamento na caixa de diálogo ou no log de trabalhos clicando em **Monitoramento ( ) → Trabalhos** (consulte Monitorando trabalhos).

   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.

   - O Gerenciador de Recursos falhou e não pode ser recuperado.

     Nota: Se a instância do Gerenciador de Recursos de Substituição usar o mesmo endereço IP do Gerenciador de Recursos com falha, você poderá gerenciar o dispositivo novamente usando a conta `RECOVERY_ID` e a senha (se aplicável) e a opção **Forçar gerenciamento**.
   - O Gerenciador de Recursos foi desligado antes do cancelamento do gerenciamento dos dispositivos.
   - O cancelamento do gerenciamento de dispositivos não foi bem-sucedido.
   - O XClarity Orchestrator mostra um dispositivo gerenciado como offline depois que o endereço IP do dispositivo foi alterado.

Depois de concluir

É possível realizar as ações a seguir no dispositivo gerenciado.

- Monitore o status e os detalhes do dispositivo (consulte Exibindo o status dos dispositivos e Visualizando detalhes de dispositivos).
- Cancele o gerenciamento e remova um dispositivo selecionando clicando em **Recursos** ( ) e, em seguida, clique no tipo de dispositivo na navegação à esquerda para exibir uma placa com uma exibição tabular de todos os dispositivos gerenciados desse tipo, selecione os dispositivos cujo gerenciamento deseja cancelar e, em seguida, clique no ícone **Cancelar gerenciamento** ( ).

  Notas:

  – É possível cancelar o gerenciamento de, no máximo, **50** dispositivos ao mesmo tempo.
  – Nenhum trabalho ativo deve estar em execução no dispositivo.
  – Se o XClarity Orchestrator não puder se conectar ao Gerenciador de Recursos (por exemplo, se as credenciais estiverem expiradas ou se houver problemas de rede), selecione **Forçar cancelamento de gerenciamento mesmo se o dispositivo não estiver acessível**.
  – Por padrão, o gerenciamento dos dispositivos gerenciados pelo XClarity Administrator e que permanecem offline por 24 horas ou mais é cancelado automaticamente (consulte Definindo configurações de descoberta globais).
  – Para a maioria dos dispositivos, determinadas informações sobre o dispositivo ficam retidas após o gerenciamento do dispositivo ser cancelado. Quando o gerenciamento dos dispositivos é cancelado:
    – A conta do usuário de gerenciamento e as assinaturas de evento e de métricas são removidas do dispositivo.

- Para dispositivos gerenciados pelo XClarity Administrator, se o Call Home estiver habilitado no momento no XClarity Administrator, o Call Home será desabilitado no dispositivo.
- Para dispositivos gerenciados pelo XClarity Administrator, se o encapsulamento estiver habilitado no dispositivo, as regras de firewall do dispositivo serão alteradas para as configurações antes de o dispositivo ser gerenciado.
- Informações sensíveis, inventário e eventos e alertas que foram gerados pelo dispositivo são descartados no hub de gerenciamento.
- Eventos e alertas que foram gerados pelo hub de gerenciamento do dispositivo ficam retidos no hub de gerenciamento.

Cancelando o gerenciando de dispositivos

É possível usar o Lenovo XClarity Orchestrator para remover dispositivos do gerenciamento pelo respectivo Gerenciador de Recursos. Esse processo é chamado de *cancelamento de gerenciamento*.

Antes de iniciar

Para executar esta tarefa, você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** ou **Administrador de Segurança** foi atribuída.

Nenhum trabalho ativo deve estar em execução no dispositivo.

Sobre esta tarefa

O XClarity Orchestrator cancela automaticamente os dispositivos que permanecem offline por 24 horas ou mais por padrão (consulte Definindo configurações de descoberta globais).

Para a maioria dos dispositivos, o XClarity Orchestrator e o Gerenciador de Recursos retêm determinadas informações sobre o dispositivo após o gerenciamento ser cancelado. Essa informação é reaplicada ao gerenciar o mesmo dispositivo novamente.

Procedimento

Para cancelar o gerenciamento de dispositivos, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Recursos ( )** e, em seguida, clique no tipo de dispositivo para exibir uma placa com uma exibição tabular de todos os dispositivos gerenciados do tipo em questão.

Etapa 2. Selecione um ou mais dispositivos cujo gerenciamento deve ser cancelado.

Etapa 3. Clique o ícone **Cancelar gerenciamento** ( ) para exibir a caixa de diálogo Cancelamento de gerenciamento.

Etapa 4. Selecione **Forçar cancelamento de gerenciamento mesmo se o dispositivo não estiver acessível**.

Etapa 5. Clique em **Cancelar Gerenciamento**.

A caixa de diálogo Cancelar gerenciamento mostra o progresso de cada etapa no processo de cancelamento de gerenciamento.

Usando o VMware Tools

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

Para obter informações sobre como usar o VMware Tools, consulte Usando o utilitário de configuração do VMware Tools no site do Centro de documentação do VMware vSphere.

Definindo configurações de rede

É possível configurar uma única interface de rede (usando configurações de IPv4 e IPv6), configurações de roteamento da Internet e configurações de proxy.

Antes de iniciar

Saiba mais: Como configurar redes e servidores NTP

Você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** é atribuída.

Revise as seguintes considerações ao escolher a interface.

- A interface deve ser configurada para oferecer suporte à descoberta e ao gerenciamento. Ela deve ser capaz de comunicar os gerenciadores de recursos e os dispositivos gerenciados por eles.
- Se você pretende enviar manualmente os dados de serviço coletados para o suporte da Lenovo ou usar a notificação automática de problemas (Call Home), as interfaces de rede devem estar conectadas à Internet, de preferência, por meio de um firewall.

Atenção:

- Se você alterar o endereço IP do dispositivo virtual do XClarity Orchestrator depois de conectar gerenciadores de recursos, o XClarity Orchestrator perderá a comunicação com os gerenciadores, e estes serão exibidos offline. Se você precisar alterar o endereço IP do dispositivo virtual após a inicialização do XClarity Orchestrator, certifique-se de que todos os gerenciadores de recursos estejam desconectados (excluídos) antes de alterar o endereço IP.
- Se a interface de rede estiver configurada para usar DHCP, o endereço IP poderá ser alterado quando o arrendamento do DHCP expirar. Se o endereço IP for alterado, você deverá desconectar (excluir) os gerenciadores de recursos e, em seguida, reconectá-los. Para evitar esse problema, altere a interface de rede para um endereço IP estático ou certifique-se de que o servidor DHCP esteja configurado para que o endereço do DHCP seja baseado em um endereço MAC ou que o arrendamento do DHCP não expire.
- A conversão de endereço de rede (NAT), que remapeia um espaço de endereço IP em outro, não é suportada.

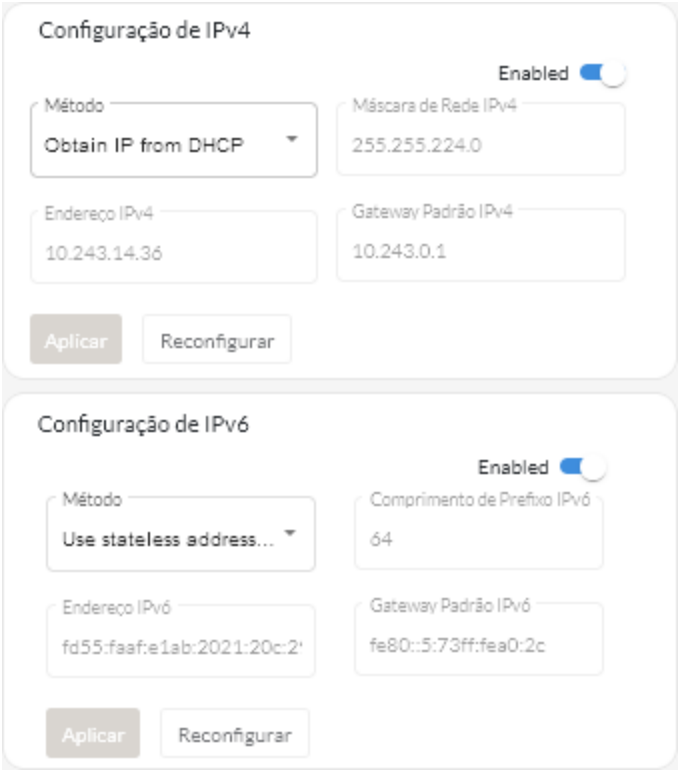
Procedimento

Para definir as configurações de rede, clique em **Administração** (⚙) → **Rede** na barra de menus do XClarity Orchestrator e, em seguida, complete uma ou mais das etapas a seguir.

- **Configurar definições de IP**É possível optar por usar as configurações de rede IPv4 e IPv6 das placas Configuração de IPv4 e Configuração de IPv6. Habilite e modifique as definições de configuração de IP aplicáveis e, em seguida, clique em **Aplicar**.
  - **Configurações de IPv4**. É possível configurar o método de atribuição de IP, o endereço IPv4, a máscara de rede e o gateway padrão. Para o método de atribuição de IP, é possível optar por usar um endereço IP atribuído estaticamente ou obter um endereço IP do servidor DHCP. Ao usar um endereço IP estático, você deve fornecer um endereço IP, uma máscara de rede e um gateway padrão. O gateway padrão deve ser um endereço IP válido e deve estar na mesma sub-rede que a interface de rede.

    Se DHCP for usado para obter um endereço IP, o gateway padrão também usará DHCP.

– **Configurações de IPv6.** É possível configurar o método de atribuição de IP, o endereço IPv6, o tamanho do prefixo e o gateway padrão.Para o método de atribuição de IP, é possível optar por usar um endereço IP atribuído estaticamente, a configuração de endereço stateful (DHCPv6) ou uma configuração automática de endereço sem estado. Ao usar um endereço IP estático, você deve fornecer um endereço IPv6, o tamanho do prefixo e um gateway. O gateway deve ser um endereço IP válido e deve estar na mesma sub-rede que a interface de rede.



- **Definir as configurações de roteamento da Internet**Opcionalmente, configure o sistema de nomes de domínio (DNS) no cartão Configuração de DNS. Em seguida, clique em **Aplicar**.

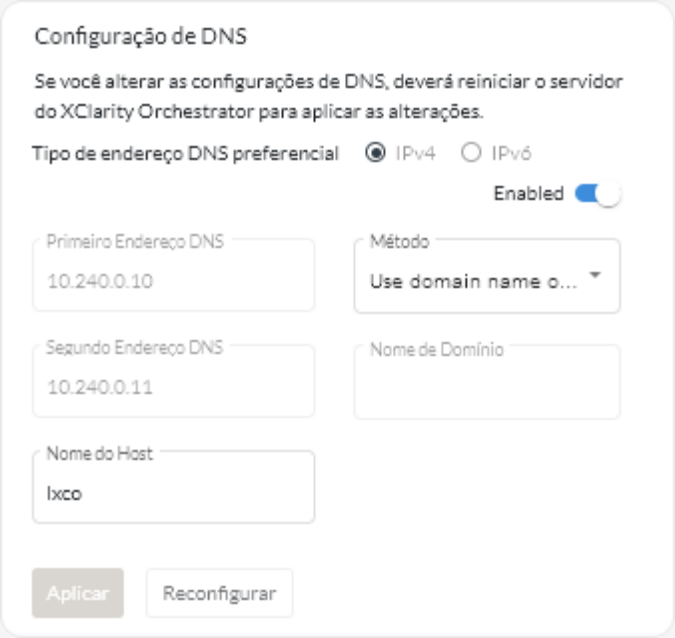
  Atualmente, apenas endereços IPv4 são suportados.

  Escolha se o DHCP deve ser usado para obter os endereços IP ou para especificar endereços IP estáticos ativando ou desativando o **DNS do DHCP**. Se você optar por usar endereços IP estáticos, especifique o endereço IP para pelo menos um e até dois servidores DNS.

  Especifique o nome do host DNS e o nome de domínio. É possível optar por recuperar o nome de domínio de um servidor DHCP ou especificar um nome de domínio personalizado.

  Notas:

  – 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 Orchestrator renovar o arrendamento do DHCP.
  – Ao alterar as configurações de DNS, você deve reiniciar manualmente a máquina virtual para aplicar as alterações.
  – Se você alterar a configuração DNS de DHCP para um endereço IP estático, altere também o endereço IP do servidor DNS.



- **Configurar definições de proxy HTTP**Opcionalmente, habilite e especifique o nome do host do servidor proxy, a porta e as credenciais opcionais da placa Configuração de proxy. Em seguida, clique em **Aplicar**.

  Notas:
  - 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.

Configurando data e hora

É necessário configurar pelo menos um (e até quatro) servidor Network Time Protocol (NTP) para sincronizar os registros de data e hora do Lenovo XClarity Orchestrator com todos os eventos recebidos dos gerenciadores de recursos.

Antes de iniciar

Você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** é atribuída.

Cada servidor NTP deve ser acessível na rede. Considere a possibilidade de configurar um servidor NTP no sistema local em que XClarity Orchestrator está em execução.

Se você alterar a hora no servidor NTP, poderá levar alguns minutos para o XClarity Orchestrator ser sincronizado com a nova hora.

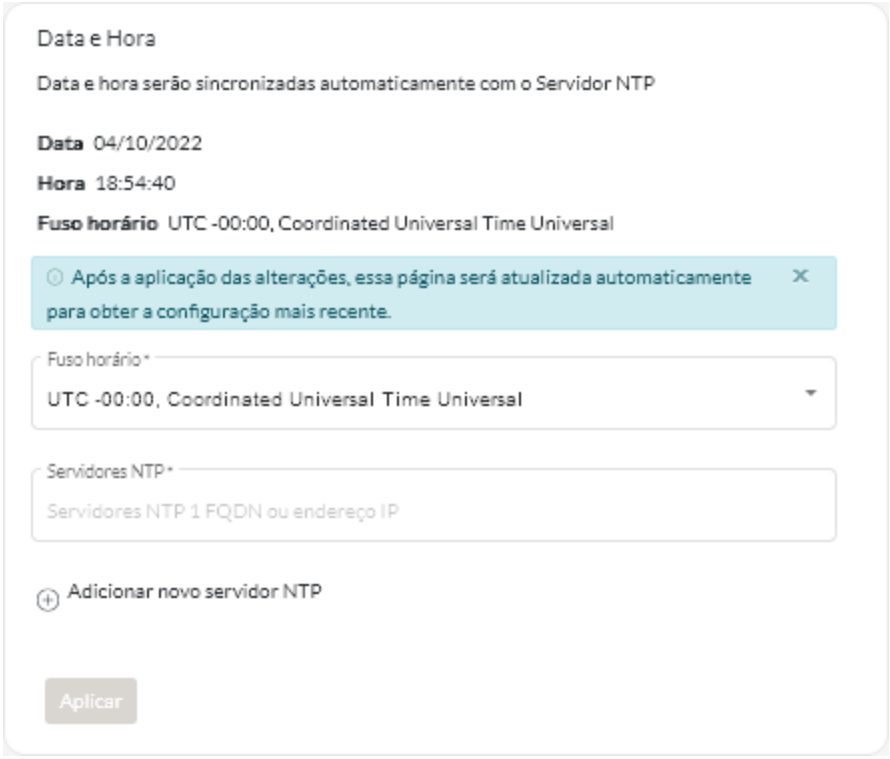
Atenção: O dispositivo virtual do XClarity Orchestrator e seu host devem ser configurados para sincronização com a mesma origem de horário para evitar a falta de sincronização de horário acidental entre o XClarity Orchestrator e seu host. Normalmente, o host é configurado para que seus dispositivos virtuais tenham o horário sincronizado com ele. Se o XClarity Orchestrator estiver definido para sincronizar-se com uma origem diferente de seu host, você deverá desativar a sincronização de horário entre o dispositivo virtual XClarity Orchestrator e seu host.

- **ESXi**Siga as instruções no VMware – Página Desabilitar Sincronização de Tempo.
- **Hyper-V**No Gerenciador Hyper-V, clique com o botão direito na máquina virtual XClarity Orchestrator e clique em **Configurações**. Na caixa de diálogo, clique em **Gerenciamento → Serviços de integração** no painel de navegação e, em seguida, desmarque **Sincronização de horário**.

Procedimento

Para definir data e hora para XClarity Orchestrator, conclua as seguintes etapas.

Etapa 1. Na barra de menu do XClarity Orchestrator, clique em **Administração (⚙) → Data e Hora** para exibir o cartão Data e Hora.



Etapa 2. Escolha o fuso horário onde o host para XClarity Orchestrator está localizado.

Se o fuso horário selecionado estiver em horário de verão (DST), a hora será ajustada automaticamente para DST.

Etapa 3. Especifique o nome do host ou o endereço IP para cada servidor NTP na rede. Você pode definir até quatro servidores NTP.

Etapa 4. Clique em **Aplicar**.

Trabalhando com certificados de segurança

O Lenovo XClarity Orchestrator usa certificados SSL para estabelecer uma comunicação segura e confiável entre o XClarity Orchestrator e seus gerenciadores de recursos gerenciados (como o Lenovo XClarity Administrator ou Schneider Electric EcoStruxure IT Expert), bem como a comunicação com o XClarity Orchestrator por usuários ou com serviços diferentes. Por padrão, o XClarity Orchestrator e o Lenovo XClarity Administrator usam certificados gerados pelo XClarity Orchestrator que são autoassinados e emitidos por uma autoridade de certificação interna.

Antes de iniciar

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

Sobre esta tarefa

O certificado de servidor padrão, produzido exclusivamente em cada instância do XClarity Orchestrator, fornece segurança adequada para muitos ambientes. É possível escolher se você quer deixar o XClarity Orchestrator gerenciar certificados, ou se você pode ter uma função mais ativa personalizando e substituindo os certificados de servidor. O XClarity Orchestrator 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 Orchestrator a ser usado como o certificado de servidor final para todos os seus serviços hospedados.
- Baixe o certificado de servidor para seu sistema local para poder importá-lo na lista do navegador da Web de certificados confiáveis.

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

O XClarity Orchestrator age como um cliente ao se comunicar com os gerenciadores de recursos e serviços externos. Quando isso ocorre, o gerenciador de recursos ou o serviço externo fornece seu certificado de servidor a ser verificado pelo XClarity Orchestrator. O XClarity Orchestrator mantém uma lista de certificados em que ele confia. Se o *certificado confiável* fornecido pelo gerenciador de recursos ou serviço externo não estiver listado, o XClarity Orchestrator se desconectará do dispositivo gerenciado ou do serviço externo para evitar a troca de qualquer informação confidencial de segurança com uma origem não confiável.

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

- **Certificado do Servidor**. Durante a primeira inicialização, uma chave exclusiva e o certificado autoassinado são gerados. Eles são usados como autoridade de certificação raiz padrão, que pode ser gerenciada na página Autoridade de Certificação nas configurações de segurança do XClarity Orchestrator. Não é necessário gerar novamente esse certificado raiz, a menos que a chave tenha sido comprometida ou se sua organização tiver uma política que obrigue a substituição periódica de todos os certificados (consulte Gerando novamente o certificado de servidor assinado internamente do XClarity Orchestrator).Também durante a configuração inicial, uma chave separada é gerada e um certificado do servidor é criado e assinado pela autoridade de certificação interna. Esse certificado é usado como o certificado do servidor padrão do XClarity Orchestrator. Ele é gerado de novo automaticamente sempre que o XClarity Orchestrator detecta que seus endereços de rede (endereços IP ou DNS) foram alterados para garantir que o certificado contenha os endereços corretos para o servidor. Ele pode ser personalizado e gerado sob demanda (consulte Gerando novamente o certificado de servidor assinado internamente do XClarity Orchestrator).

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

  Se você optar por usar o certificado de servidor autoassinado padrão, é recomendável importar o certificado de servidor no seu navegador da Web como uma autoridade raiz confiável para evitar mensagens de erro de certificado no seu navegador (consulte Importando o certificado do servidor em um navegador da Web).

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

- **Certificados confiáveis**Esse armazenamento confiável gerencia certificados usados para estabelecer uma conexão segura com os recursos locais quando o XClarity Orchestrator age como cliente. Exemplos de recursos locais são gerenciadores de recursos gerenciados, software local ao encaminhar um evento etc.
- **Certificados de serviço externos**. Esse armazenamento confiável gerencia certificados usados para estabelecer uma conexão segura com serviços externos quando o XClarity Orchestrator age como cliente. Exemplos de serviços externos são serviços online do Suporte Lenovo que são usados para recuperar informações de garantia ou criar tíquetes de serviço, software externo (como Splunk) para o qual eventos podem ser encaminhados. Ele contém certificados confiáveis pré-configurados das Autoridades de Certificação Raiz de determinados provedores de autoridade de certificação geralmente confiáveis e conhecidos mundialmente, como o Digicert e o Globalsign).Ao configurar o XClarity Orchestrator para usar um recurso que exija uma conexão com outro serviço externo, consulte a documentação para determinar se você precisa adicionar manualmente um certificado a esse armazenamento confiável.

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

Adicionando um certificado confiável para serviços externos

Esses certificados são usados para estabelecer relações de confiança com serviços externos. Por exemplo, os certificados neste armazenamento confiável são usados ao recuperar informações de garantia da Lenovo, criar tíquetes, encaminhar eventos para um aplicativo externo (como Splunk) e usar servidores LDAP externos.

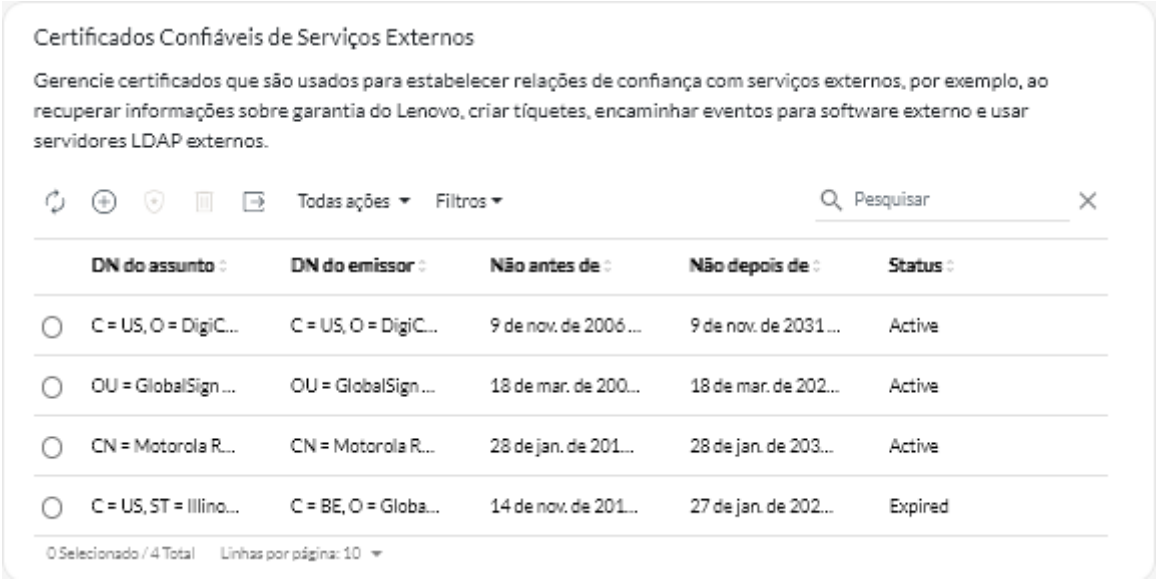
Antes de iniciar

Os certificados neste armazenamento confiável não são confiáveis ao estabelecer conexões para outros serviços, a menos que você os adicione ao armazenamento confiável principal de certificados confiáveis. Remover certificados desse armazenamento confiável impede o funcionamento desses serviços.

Procedimento

Para adicionar um certificado confiável, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Administração (⚙) → Segurança** e, em seguida, clique em **Certificados de Serviços Externos** na navegação esquerda para exibir a placa Certificados Confiáveis de Serviços Externos.



Etapa 2. Clique no ícone **Adicionar** (⊕) para adicionar um certificado. A caixa de diálogo Adicionar Certificado é exibida.

Etapa 3. Copie e cole os dados do certificado no formato PEM.

Etapa 4. Clique em **Adicionar**.

Depois de concluir

É possível executar as seguintes ações na placa Certificados Confiáveis para Serviços Externos.

- Exiba os detalhes de um certificado confiável selecionado clicando no ícone **Exibir** (🛡).
- Salve um certificado confiável selecionado no sistema local clicando no ícone **Exibir** (🛡) e, em seguida, em **salvar como pem**.
- Exclua um certificado confiável selecionado clicando no ícone **Excluir** (🗑).

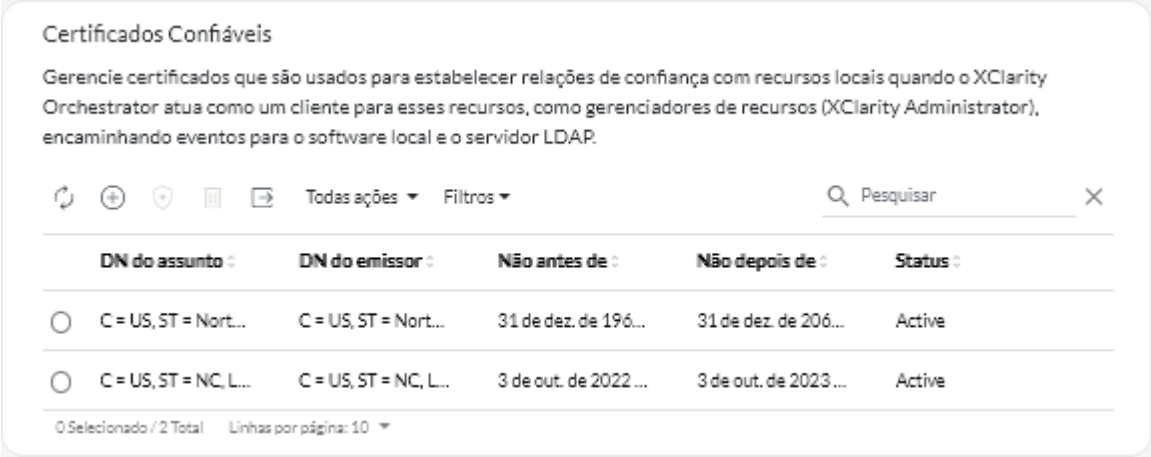
Adicionando um certificado confiável para serviços internos

Esses certificados são usados para estabelecer relações de confiança com recursos locais quando o Lenovo XClarity Orchestrator atua como um cliente para esses recursos, como gerenciadores de recursos, encaminhamento de eventos para software local e o servidor LDAP integrado. Além disso, o certificado da CA interno e o certificado da CA de um certificado de servidor assinado externamente personalizado (se estiver instalado) estão presentes nesse armazenamento confiável para dar suporte à comunicação interna do XClarity Orchestrator.

Procedimento

Para adicionar um certificado confiável, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Administração (⚙) → Segurança** e, em seguida, clique em **Certificados Confiáveis** na navegação esquerda para exibir a placa Certificados Confiáveis.



Etapa 2. Clique no ícone **Adicionar** (⊕) para adicionar um certificado. A caixa de diálogo Adicionar Certificado é exibida.

Etapa 3. Copie e cole os dados do certificado no formato PEM.

Etapa 4. Clique em **Adicionar**.

Depois de concluir

É possível executar as ações a seguir a partir da placa Certificado Confiável.

- Exiba os detalhes de um certificado confiável selecionado clicando no ícone **Exibir** (🛡).
- Salve um certificado confiável selecionado no sistema local clicando no ícone **Exibir** (🛡) e, em seguida, em **salvar como pem**.
- Exclua um certificado confiável selecionado clicando no ícone **Excluir** (🗑).

Instalando um certificado de servidor assinado externamente confiável XClarity Orchestrator

É possível usar um certificado do servidor assinado confiável por uma autoridade de certificação (CA) privada ou comercial. Para usar um certificado de servidor assinado externamente, gere uma solicitação de assinatura de certificado (CSR) e, em seguida, importe o certificado do servidor resultante para substituir o existente.

Sobre esta tarefa

Como prática recomendada, sempre use certificados assinados v3.

O certificado de servidor assinado externamente deve ser criado a partir da solicitação de assinatura de certificado que foi gerada mais recentemente usando o botão **Gerar Arquivo CSR**.

O conteúdo do certificado de servidor assinado externamente deve ser um pacote de certificados que contém a cadeia de assinatura de CA inteira, incluindo o certificado raiz da CA, os certificados intermediários e o certificado do servidor.

Se o novo certificado de servidor não tiver sido assinado por terceiros confiáveis, na próxima vez que você se conectar ao XClarity Orchestrator, o navegador da Web exibirá uma mensagem de segurança e uma caixa de diálogo solicitando a aceitação do novo certificado no navegador. Para evitar mensagens de segurança, é possível importar o certificado do servidor para a lista de certificados confiáveis do seu navegador da Web (consulte Importando o certificado do servidor em um navegador da Web).

O XClarity Orchestrator começa a usar o novo certificado do servidor sem encerrar a sessão atual. As novas sessões são estabelecidas usando o novo certificado. Para usar o novo certificado em uso, reinicie seu navegador da Web.

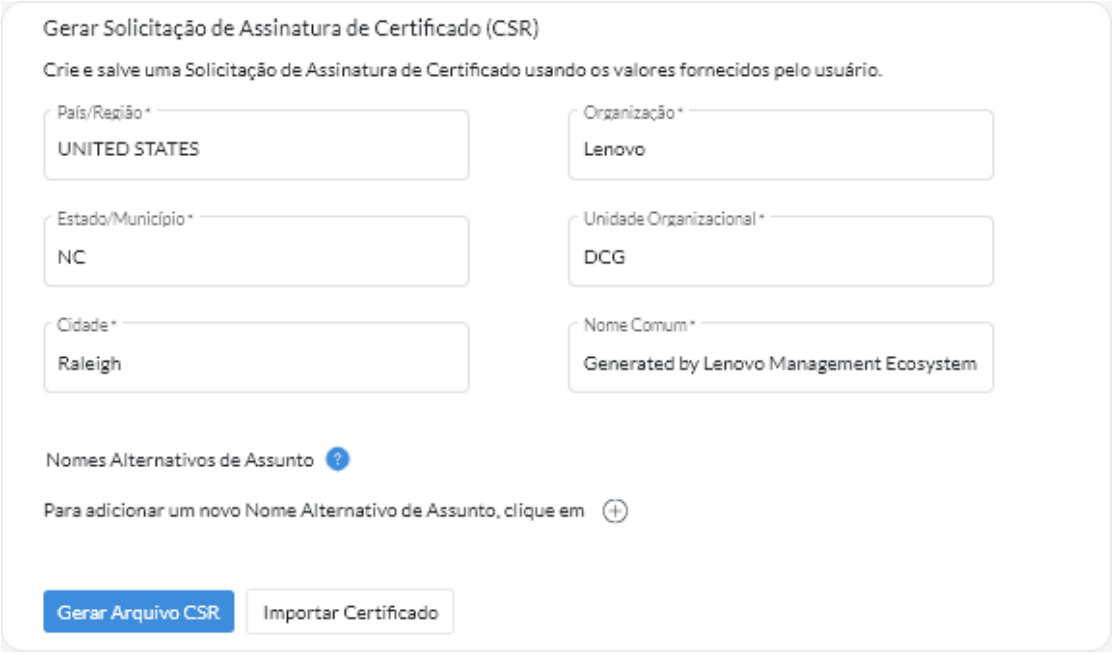
Importante: Quando o certificado do servidor for modificado, todas as sessões do usuário estabelecidas deverão aceitar o novo certificado clicando em CTRL + F5 para atualizar o navegador da Web e restabelecer a conexão com o XClarity Orchestrator.

Procedimento

Para gerar e instalar um certificado de servidor assinado externamente, conclua as seguintes etapas.

Etapa 1. Crie uma solicitação de assinatura de certificado e salve o arquivo no sistema local.

1. Na barra de menus do XClarity Orchestrator, clique em **Administração** (⚙) → **Segurança** e, em seguida, clique em **Certificado do Servidor** na navegação esquerda para exibir a placa Gerar solicitação de assinatura de certificado.



2. Na placa Gerar Solicitação de Assinatura de Certificado (CSR), preencha os campos da solicitação.
   - Código ISO 3166 de duas letras para o país ou a região de origem associado à organização do certificado (por exemplo, EUA para os Estados Unidos).
   - Nome completo do Estado ou da província a ser associado ao certificado (por exemplo, Califórnia ou New Brunswick).
   - Nome completo da cidade a ser associada ao certificado (por exemplo, San Jose). O tamanho do valor não pode exceder 50 caracteres.
   - Organização (empresa) que deve ser proprietária do certificado. Normalmente, esse é o nome da pessoa jurídica da empresa. Ele deve incluir todos os sufixos, como Ltd., Inc. ou

Corp (por exemplo, ACME International Ltd.). O tamanho desse valor não pode exceder 60 caracteres.

- (Opcional) Unidade organizacional que deve ser proprietária do certificado (por exemplo, Divisão ABC). O tamanho desse valor não pode exceder 60 caracteres.
- Nome comum do proprietário do certificado. Este deve ser o nome do host do servidor que está usando o certificado. O tamanho desse valor não pode exceder 63 caracteres.
- (Opcional) Sujeito a nomes alternativos de assunto que serão adicionados à extensão X.509 "subjectAltName" quando a CSR for gerada.Por padrão, XClarity Orchestrator define automaticamente os nomes alternativos de assunto para a CSR com base no endereço IP e no nome do host que são descobertos pelas interfaces de rede do sistema operacional convidado XClarity Orchestrator. Você pode personalizar, excluir ou adicionar esses valores de nome alternativo de assunto. Entretanto, os nomes alternativos de assunto devem ter o nome de domínio (FQDN) ou o endereço IP totalmente qualificado do servidor, e o nome do assunto deve ser definido como FQDN.

  O nome especificado deve ser válido para o tipo selecionado.
  – **DNS** (use o FQDN, por exemplo, hostname.labs.company.com)
  – **Endereço IP** (por exemplo, 192.0.2.0)
  – **email** (por exemplo, example@company.com)

  Nota: Todos os nomes alternativos de assunto listados na tabela serão validados, salvos e adicionados à CSR apenas depois que você gerar a CSR na próxima etapa.

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

Etapa 3. Importe o certificado de servidor assinado externamente e o certificado da CA XClarity Orchestrator e substitua o certificado do servidor atual.

1. Na placa Gerar Solicitação de Assinatura de Certificado (CSR), clique em **Importar Certificado** para exibir a caixa de diálogo Importar Certificado.
2. Copie e cole o certificado do servidor e o certificado da CA em formato PEM. Você deve fornecer a cadeia de certificados inteira, começando com o certificado do servidor e terminando no certificado da CA raiz.
3. Clique em **Importar** para armazenar o certificado do servidor no armazenamento confiável XClarity Orchestrator.

Etapa 4. Aceite o novo certificado pressionando CTRL + F5 para atualizar o navegador e, em seguida, restabeleça a conexão com a interface da Web. Isso deve ser feito por todas as sessões do usuário estabelecidas.

Gerando novamente o certificado de servidor assinado internamente do XClarity Orchestrator

É possível gerar um novo certificado do servidor para substituir o certificado assinado internamente atual do Lenovo XClarity Orchestrator ou para restabelecer um certificado gerado pelo XClarity Orchestrator se o XClarity Orchestrator usar um certificado de servidor assinado externamente personalizado. O novo certificado de servidor assinado internamente é usado pelo XClarity Orchestratorpara acesso HTTPS.

Sobre esta tarefa

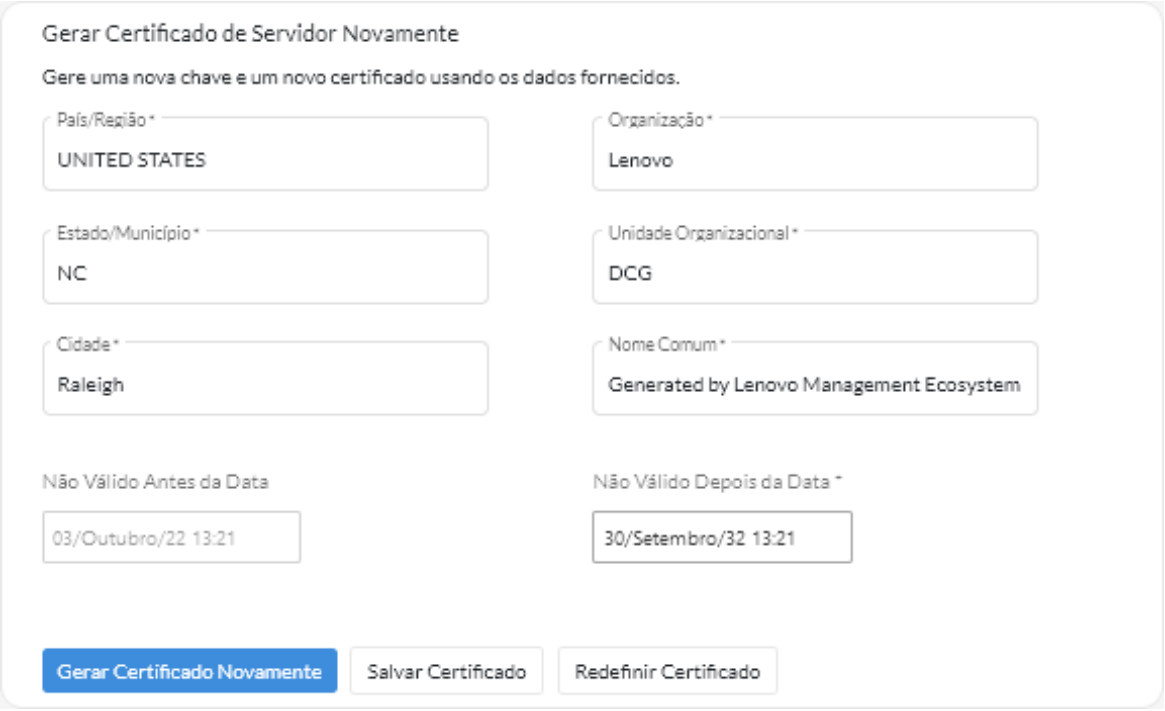
O certificado do servidor que está atualmente em uso no , assinado interna ou externamente, permanecerá em uso até que um novo certificado do servidor seja gerado novamente e assinado.

Importante: Quando o certificado do servidor for modificado, todas as sessões do usuário estabelecidas deverão aceitar o novo certificado clicando em CTRL + F5 para atualizar o navegador da Web e restabelecer a conexão com o XClarity Orchestrator.

Procedimento

Para gerar um certificado de servidor assinado internamente do XClarity Orchestrator, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Administração (⚙) → Segurança** e, em seguida, clique em **Certificado do Servidor** na navegação esquerda para exibir a placa Gerar Certificado de Servidor Novamente.



Etapa 2. Na placa Gerar Certificado de Servidor Novamente e preencha os campos da solicitação.

- Código ISO 3166 de duas letras para o país ou a região de origem a ser associado à organização do certificado (por exemplo, EUA para os Estados Unidos).
- Nome completo do Estado ou da província a ser associado ao certificado (por exemplo, Califórnia ou New Brunswick).
- Nome completo da cidade a ser associada ao certificado (por exemplo, San Jose). O tamanho do valor não pode exceder 50 caracteres.
- Organização (empresa) que deve ser proprietária do certificado. Normalmente, é o nome da pessoa jurídica da empresa. Ele deve incluir todos os sufixos, como Ltd., Inc. ou Corp (por exemplo, ACME International Ltd.). O tamanho desse valor não pode exceder 60 caracteres.
- (Opcional) Unidade organizacional que deve ser proprietária do certificado (por exemplo, Divisão ABC). O tamanho desse valor não pode exceder 60 caracteres.
- Nome comum do proprietário do certificado. Geralmente, esse é o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do servidor que usa o certificado (por exemplo, `www.domainname.com` ou `192.0.2.0`). O tamanho desse valor não pode exceder 63 caracteres.
- Data e hora em que o certificado do servidor não será mais válido.

Nota: Não é possível alterar os nomes alternativos de assunto ao gerar novamente o certificado do servidor.

Etapa 3. Clique em **Gerar Certificado Novamente** para gerar novamente o certificado assinado internamente e, em seguida, clique em **Gerar Certificado Novamente** para confirmar.

Etapa 4. Aceite o novo certificado pressionando CTRL + F5 para atualizar o navegador e, em seguida, restabeleça a conexão com a interface da Web. Isso deve ser feito por todas as sessões do usuário estabelecidas.

Depois de concluir

É possível executar as ações a seguir a partir da placa Gerar Certificado de Servidor Novamente.

- Salve o certificado de servidor atual no sistema local em formato PEM clicando em **Salvar Certificado**.
- Gere novamente o certificado do servidor usando a configuração padrão **Redefinir Certificado**. Quando solicitado, pressione CTRL + F5 para atualizar o navegador e, em seguida, restabeleça a conexão com a interface da Web.

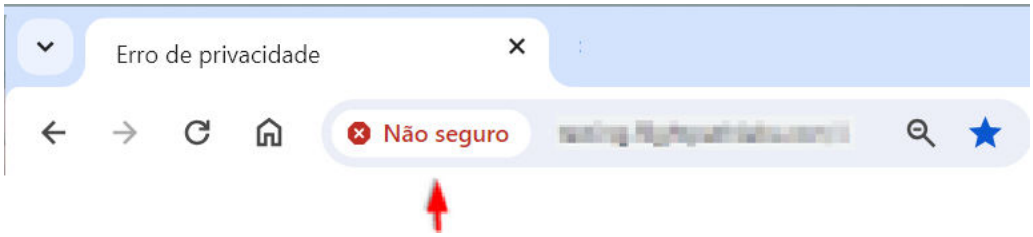
Importando o certificado do servidor em um navegador da Web

É possível salvar uma cópia do certificado do servidor atual, em formato PEM, para seu sistema local. Em seguida, você pode importar o certificado para a lista de certificados confiáveis do seu navegador da Web ou para outros aplicativos (como Lenovo XClarity Mobile ou Lenovo XClarity Integrator) a fim de evitar mensagens de aviso de segurança do navegador da Web ao acessar o Lenovo XClarity Orchestrator.

Procedimento

Para importar o certificado de servidor em um navegador da Web, conclua as etapas a seguir.

- **Chrome**
  1. Exporte o certificado do servidor XClarity Orchestrator.
     a. Clique no ícone de aviso "Não seguro" na barra de endereços superior, por exemplo:



     b. Clique em **Certificado (inválido)** para exibir a caixa de diálogo Certificado.
     c. Clique na guia **Detalhes**.
     d. Clique em **Copiar em Arquivo** para exibir o Assistente de Exportação de Certificados.
     e. Selecione **Padrão de sintaxe da mensagem criptográfica** e clique em **Avançar**.
     f. Especifique o nome e o local do arquivo de certificado e clique em **Concluir** para exportar o certificado.
     g. Clique em **OK** para fechar a caixa de diálogo Certificado.
  2. Importe o certificado de servidor XClarity Orchestrator para a lista de certificados confiáveis de autoridade raiz de seu navegador.
     a. No navegador Chrome, clique nos três pontos no canto superior direito da janela e, em seguida, clique em **Configurações**.

b. Role até a seção **Privacidade e Segurança** e clique em **Gerenciar certificados** para exibir a caixa de diálogo Certificados.

c. Clique em **Importar**, selecione o arquivo de certificado que você exportou anteriormente e clique em **Avançar**.

d. Clique em **Procurar** ao lado do **Armazenamento de certificados** e selecione **Autoridades de Certificação Raiz Confiáveis**. Em seguida, clique em **OK**.

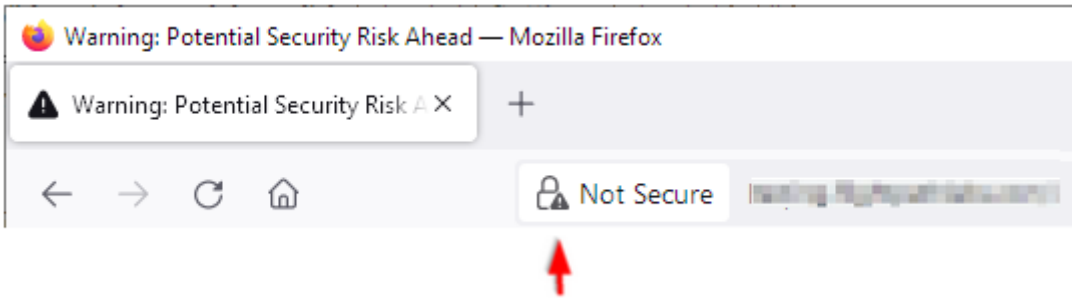
e. Clique em **Concluir**.

f. Feche e abra novamente o navegador Chrome e, em seguida, abra o XClarity Orchestrator.

- **Firefox**

1. Exporte o certificado do servidor XClarity Orchestrator.

a. Clique no ícone de aviso "Não seguro" na barra de endereços superior, por exemplo:



b. Expanda Conexão não Protegida e clique em Mais Informações para exibir uma caixa de diálogo.

c. Clique em **Exibir certificados**.

d. Role para baixo até a seção Download e clique no link **PEM (cert)**.

e. Selecione **Salvar Arquivo** e clique em **OK**.

2. Importe o certificado de servidor XClarity Orchestrator para a lista de certificados confiáveis de autoridade raiz de seu navegador.
   a. Abra o navegador e clique em **Ferramentas → Opções → Avançado**.
   b. Clique na guia **Certificados**.
   c. Clique em **Exibir certificados**.
   d. Clique em **Importar** e vá até o local onde o certificado foi baixado.
   e. Selecione o certificado e clique em **Abrir**.

Gerenciando autenticação

É possível optar por usar o servidorLightweight Directory Access Protocol (LDAP) ou outro servidor LDAP externo como servidor de autenticação.

O *servidor de autenticação* é um registro do usuário utilizado para autenticar as credenciais do usuário. O Lenovo XClarity Orchestrator oferece suporte a três tipos de servidores de autenticação:

- **Servidor de autenticação local**. Por padrão, o XClarity Orchestrator é configurado para usar o servidor LDAP local (integrado) que reside no servidor do orquestrador.
- **Servidor LDAP externo**. O Microsoft Active Directory é suportado como um servidor LDAP externo. Este servidor deve residir em um servidor do Microsoft Windows externo conectado à rede de gerenciamento.

Configurando um servidor de autenticação LDAP externo

Lenovo XClarity Orchestrator inclui um servidor de autenticação local (incorporado). Você também pode optar por usar seu próprio servidor LDAP do Active Directory externo.

Antes de iniciar

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

Somente o Microsoft Active Directory é suportado como um servidor LDAP externo.

O XClarity Orchestrator não clona automaticamente grupos de usuários definidos no servidor LDAP externo. Entretanto, é possível clonar manualmente o grupo de usuários LDAP (consulte Criando grupos de usuários).

Para que um usuário LDAP externo possa fazer login no XClarity Orchestrator, o usuário deve ser um membro direto de um grupo de usuários LDAP que foi clonado no XClarity Orchestrator. O XClarity Orchestrator não reconhece usuários membros de grupos aninhados no grupo de usuários LDAP clonado definido no servidor LDAP externo.

Sobre esta tarefa

Se um servidor LDAP externo não estiver configurado, o XClarity Orchestrator sempre autenticará um usuário utilizando o servidor de autenticação local.

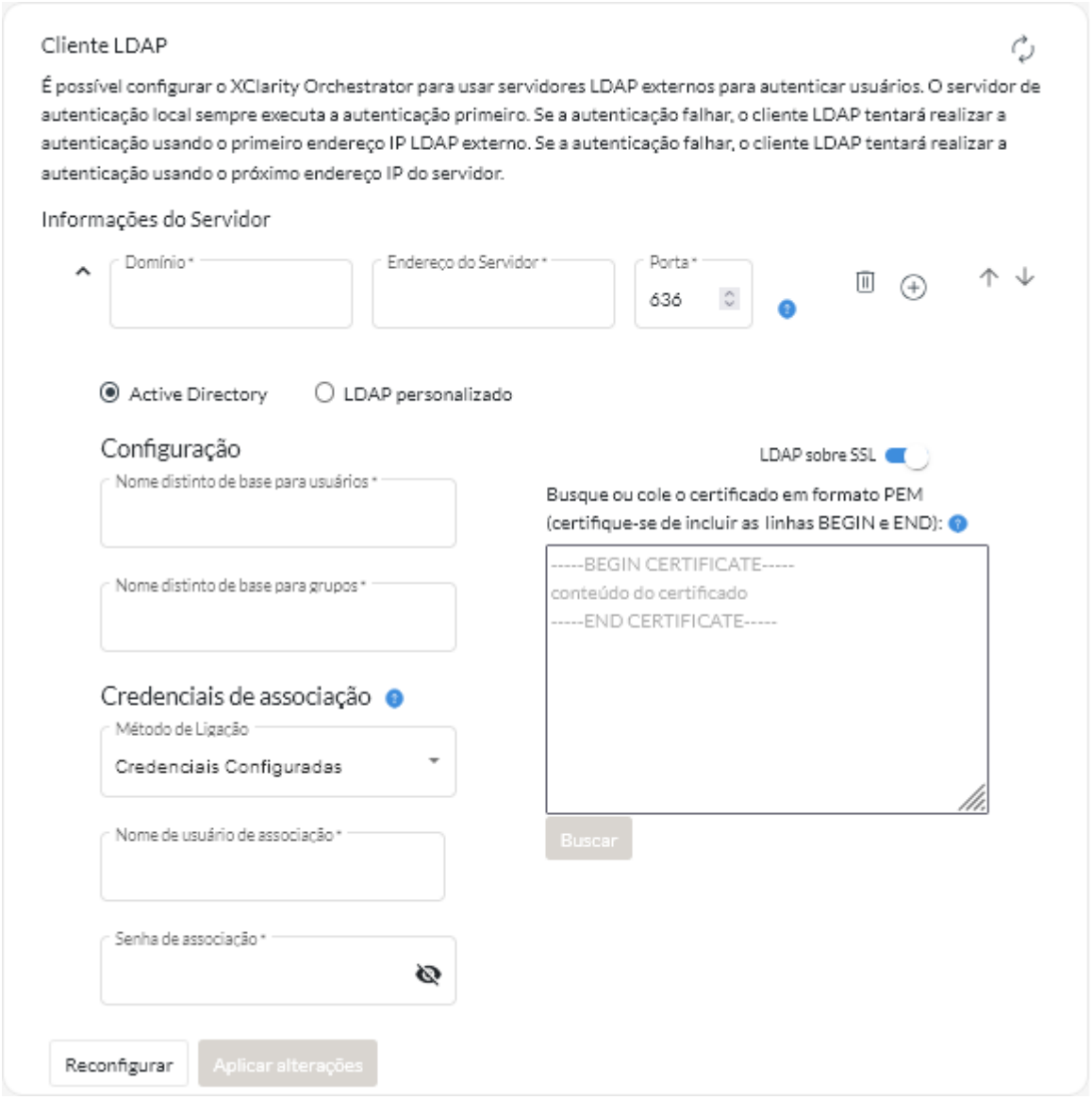
Se um servidor LDAP externo não estiver configurado, o XClarity Orchestrator primeiro tentará autenticar um usuário utilizando o servidor de autenticação local. Se a autenticação falhar, o XClarity Orchestrator tentará autenticar usando o endereço IP do primeiro servidor LDAP. Se a autenticação falhar, o cliente LDAP tentará autenticar usando o endereço IP do próximo servidor LDAP.

Quando um usuário LDAP externo faz login no XClarity Orchestrator pela primeira vez, uma conta de usuário com o nome <username>@<domain> é clonada automaticamente no XClarity Orchestrator. É possível adicionar usuários LDAP externos clonados a grupos de usuários ou usar grupos LDAP para controle de acesso. Também é possível adicionar privilégios de supervisor a um usuário LDAP externo.

Procedimento

Para configurar o XClarity Orchestrator para usar um servidor de autenticação LDAP externo, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Administração (⚙) → Segurança** e, em seguida, clique em **Cliente LDAP** na navegação esquerda para exibir a placa Cliente LDAP.



Etapa 2. Configure cada servidor LDAP externo usando as etapas a seguir.

1. Clique no ícone **Adicionar** (⊕) para adicionar um servidor LDAP.
2. Especifique o nome do domínio, o endereço IP e a porta para o servidor LDAP externo.

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

   Quando o número da porta estiver definido como 3268 ou 3269, o sistema assumirá que a entrada identifica um catálogo global. O cliente LDAP tenta autenticar usando o controlador de domínio para o primeiro endereço IP do servidor configurado. Se isso falhar, o cliente LDAP tentará autenticar usando o controlador de domínio para o próximo endereço IP do servidor.
3. Você também pode optar por ativar a personalização de configurações avançadas.Quando você optar por usar uma configuração personalizada, poderá especificar o filtro de pesquisa do usuário. Se você não especificar um filtro de pesquisa do usuário, o `(&(objectClass=user)(|(userPrincipalName={0})(sAMAccountName={0})))` será usado por padrão.

Se a configuração avançada estiver desativada, a configuração padrão do Active Directory será usada.

4. Especifique o nome distinto da base de LDAP totalmente qualificado a partir do qual o cliente LDAP inicia a pesquisa pela autenticação do usuário.
5. Especifique o nome distinto da base de LDAP totalmente qualificado a partir do qual o cliente LDAP inicia a pesquisa por grupos de usuários (por exemplo, `dc=company,dc=com`).
6. Opcionalmente, especifique credenciais para vincular o XClarity Orchestrator ao servidor de autenticação externo. É possível usar um dos dois métodos de vinculação.

   - **Credenciais Configuradas** Use esse método de vinculação para usar o nome do cliente e a senha específicos para vincular o XClarity Orchestrator ao servidor de autenticação externo. Se essa vinculação falhar, o processo de autenticação também falhará. Especifique o nome distinto LDAP totalmente qualificado (por exemplo, `cn=somebody,dc=company,dc=com`) ou o endereço de e-mail (por exemplo, `somebody@company.com`) da conta do usuário e a senha a ser usada para autenticação LDAP para vincular o XClarity Orchestrator ao servidor LDAP. Se essa vinculação falhar, o processo de autenticação também falhará.

     O nome distinto deve ser uma conta de usuário no domínio que tem pelo menos privilégios somente leitura.

     Se o servidor LDAP não tiver subdomínios, será possível especificar o nome do usuário sem o domínio (por exemplo, `user1`). No entanto, se o servidor LDAP tiver subdomínios (por exemplo, subdomínio `new.company.com` no domínio `company.com`), você deverá especificar o nome de usuário e o domínio (por exemplo, `user1@company.com`).

     Atenção: Se você alterar a senha do cliente no servidor LDAP externo, também atualize a nova senha no XClarity Orchestrator (consulte Não é possível fazer login no XClarity Orchestrator na documentação online do XClarity Orchestrator).

   - **Credenciais de Login**. Use esse método de vinculação para usar o nome de usuário XClarity Orchestrator LDAP e a senha para vincular o XClarity Orchestrator ao servidor de autenticação externo.Especifique o nome distinto LDAP totalmente qualificado de uma conta de usuário de *teste* e a senha a ser usada para autenticação LDAP para validar a conexão com o servidor de autenticação.

     Essas credenciais do usuário não são salvas. Se a operação for bem-sucedida, todas as vinculações futuras usarão o nome do usuário e a senha que você usou para fazer login no XClarity Orchestrator. Se essa vinculação falhar, o processo de autenticação também falhará.

     Nota: Você deve estar conectado ao XClarity Orchestrator usando um ID de usuário totalmente qualificado (por exemplo, administrator@domain.com).
7. Como opção, opte por usar LDAP seguro selecionando o botão de alternância **LDAP sobre SSL** e, em seguida, clicando em **Buscar** para recuperar e importar o certificado SSL confiável. Quando a caixa de diálogo Buscar certificado de servidor for exibida, clique em **Aceitar** para usar o certificado.Se você optar por usar LDAP sobre SSL, o XClarity Orchestrator usa o protocolo LDAPS para se conectar com segurança ao servidor de autenticação externo. Quando essa opção é selecionada, os certificados confiáveis são usados para habilitar o suporte a LDAP seguro.

   Atenção: Se você optar por desabilitar LDAP sobre SSL, o XClarity Orchestrator usa um protocolo não seguro para se conectar ao servidor de autenticação externo. Se você escolher essa configuração, o hardware poderá ficar vulnerável a ataques à segurança.
8. Também é possível reordenar os servidores LDAP usando os ícones **Mover para Cima** (↑) e **Mover para Baixo** (↓). O cliente LDAP tenta autenticar usando o primeiro endereço IP do

servidor. Se a autenticação falhar, o cliente LDAP tentará autenticar usando o próximo endereço IP do servidor.

Importante: Para autenticação LDAP segura, use o certificado para a autoridade de certificado raiz (CA) do servidor LDAP ou um dos certificados intermediários do servidor. É possível recuperar o certificado da CA raiz ou intermediário de um prompt de comandos executando o comando a seguir, em que *{FullyQualifiedHostNameOrIpAddress}* é o nome totalmente qualificado do servidor LDAP externo. O certificado CA raiz ou intermediário é normalmente o último certificado na saída, a última seção `BEGIN--END`.

```
openssl s_client -showcerts -connect {FullyQualifiedHostNameOrIpAddress}:636
```

9. Clique em **Aplicar alterações**. O XClarity Orchestrator tenta testar o endereço IP, a porta, os certificados SSL e as credenciais de vinculação e valida a conexão do servidor LDAP para detectar erros comuns. Se a validação passar, a autenticação do usuário ocorrerá no servidor de autenticação externo quando um usuário fizer login no XClarity Orchestrator. Se a validação falhar, mensagens de erro serão exibidas indicando a origem de erros.

   Nota: Se a validação for bem-sucedida e as conexões com o servidor LDAP forem concluídas com êxito, a autenticação do usuário poderá falhar se o nome distinto raiz estiver incorreto.

Depois de concluir

É possível remover uma configuração do servidor LDAP clicando no ícone **Excluir** (🗑) ao lado da configuração. Quando você exclui uma configuração do servidor LDAP, se não houver outras configurações do servidor LDAP no mesmo domínio, os usuários de clone e os grupos de usuários de clone nesse domínio também serão removidos.

Gerenciando usuários e sessões de usuários

As *contas do usuário* são usadas para fazer login e gerenciar o Lenovo XClarity Orchestrator.

Criando usuários

É possível criar manualmente contas de usuário no servidor de autenticação local (integrado). *Contas de usuário local* são usadas para fazer login no Lenovo XClarity Orchestrator e autorizar o acesso aos recursos.

Sobre esta tarefa

Os usuários em um servidor LDAP externo são clonados automaticamente no servidor de autenticação local com o nome *{username}@{domain}* na primeira vez que os usuários fazem login. Essa conta de usuário clonada pode ser usada apenas para autorizar o acesso aos recursos. A autenticação ainda ocorre por meio do servidor de autenticação LDAP para esses usuários, e as alterações na conta do usuário (que não sejam descrição e funções) devem ser feitas por meio de LDAP

O XClarity Orchestrator controla o acesso a funções (ações) usando funções. É possível atribuir uma função diferente aos usuários locais e clonados adicionando esses usuários a um ou mais grupos de usuários associados às funções desejadas. Por padrão, todos os usuários são membros do grupo de usuários **OperatorGroup** (consulte Criando grupos de usuários).

Pelo menos um usuário deve ser membro de um grupo de usuários *local* ao qual a função predefinida de **Supervisor** é atribuída (consulte Controlando o acesso a funções).

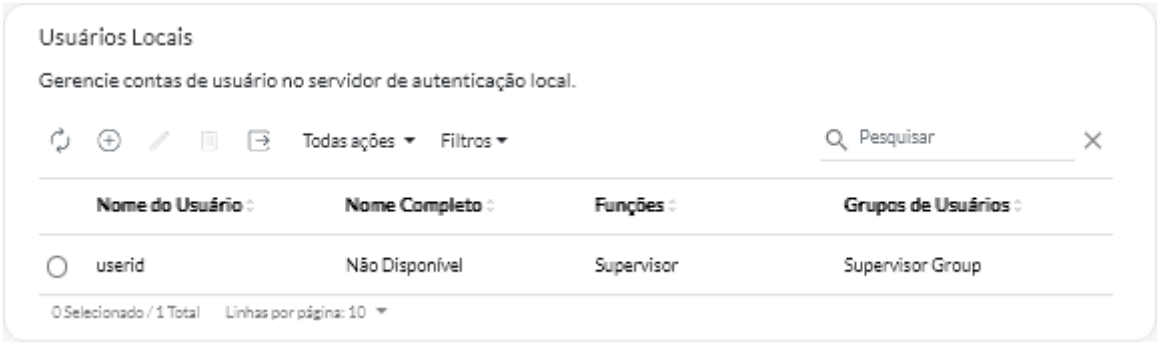
Atenção: Para que um usuário LDAP externo possa fazer login no XClarity Orchestrator, o usuário deve ser um membro direto de um grupo de usuários LDAP que foi clonado no XClarity Orchestrator. O XClarity

Orchestrator não reconhece usuários membros de grupos aninhados no grupo de usuários LDAP clonado definido no servidor LDAP externo.

Procedimento

Para criar um usuário local, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Administração (⚙) → Segurança** e, em seguida, clique em **Usuários Locais** na navegação esquerda para exibir a placa Usuários Locais.



Etapa 2. Clique no ícone **Criar** (⊕) para criar um usuário. A caixa de diálogo Criar Novo Usuário é exibida.

Etapa 3. Preencha as informações a seguir na caixa de diálogo.

- Insira um nome de usuário exclusivo. É possível especificar até 32 caracteres, incluindo alfanuméricos, ponto (.), traço (-) e sublinhado (_).

  Nota: Os nomes de usuário não fazem distinção entre maiúsculas e minúsculas.

- Insira as senhas nova e de confirmação. Por padrão, as senhas devem conter **8** – **256** caracteres e devem atender aos critérios a seguir.

  Importante: É recomendável usar senhas fortes de 16 ou mais caracteres.

  – Deve conter pelo menos um caractere alfabético e não deve ter mais de dois caracteres sequenciais, incluindo sequências de caracteres alfabéticos, dígitos e teclas de teclado QWERTY (por exemplo, "abc", "123" e "asd" não são permitidos)
  – Deve conter pelo menos um número
  – Deve conter pelo menos dois dos caracteres a seguir.
    – Caracteres alfabéticos maiúsculos (A – Z)
    – Caracteres alfabéticos minúsculos (a – z)
    – Caracteres especiais ; @ _ ! ' $ & +

    Caracteres de espaço em branco não são permitidos.
  – Não deve repetir nem reverter o nome do usuário.
  – Não deve conter mais de dois caracteres consecutivos (por exemplo, "aaa", "111" e "..." não são permitidos).

- (Opcional) Especifique informações de contato para a conta do usuário, incluindo o nome completo, o endereço de e-mail e o número de telefone.

  Dica: para o nome completo, especifique até 128 caracteres, incluindo letras, números, espaços, pontos, hifens, apóstrofos e vírgulas.

Etapa 4. Clique na guia **Grupos de Usuários** e selecione os grupos de usuários aos quais esse usuário deve ser membro.

Dica: se um grupo de usuários não estiver selecionado, o **OperatorGroup** será atribuído por padrão

Etapa 5. Clique em **Criar**.

A conta do usuário é adicionada à tabela.

Depois de concluir

É possível executar as ações a seguir na placa Usuários Locais.

- Exibir propriedades do usuário clicando na linha na tabela para um usuário exibir a caixa de diálogo Detalhes do Usuário.
- Modifique as propriedades de um usuário selecionado, incluindo a senha e os grupos de usuários, clicando no ícone **Editar** ( ).
- Exclua um usuário selecionado clicando no ícone **Excluir** ( ).Não é possível excluir o grupo de usuários LDAP existente de usuários LDAP
- Exporte detalhes do usuário, como nome do usuário, nome e sobrenome, clicando no ícone **Exportar** ( ).

Criando grupos de usuários

Os grupos de usuários são usados para autorizar o acesso aos recursos.

Antes de iniciar

Saiba mais: Como criar um grupo de usuários

É possível criar manualmente grupos de usuários no repositório local. Grupos de usuários locais contêm usuários locais e clonados.

É possível clonar qualquer grupo de usuários definido em um servidor LDAP externo. O grupo de usuários LDAP clonado é nomeado *{domain}\{groupName}* no repositório local. Esse grupo de usuários clonado pode ser usado apenas para autorizar o acesso aos recursos. As alterações no nome do grupo, na descrição e na associação devem ser feitas por meio do LDAP.

Para que um usuário LDAP externo possa fazer login no XClarity Orchestrator, o usuário deve ser um membro direto de um grupo de usuários LDAP que foi clonado no XClarity Orchestrator.

Se a configuração do servidor LDAP estiver configurada para usar credenciais de login no XClarity Orchestrator usando um ID do usuário local do XClarity Orchestrator, será solicitado que você forneça credenciais de usuário LDAP ao clonar um grupo de usuários LDAP. Em todos os outros casos, as credenciais não são necessárias.

Sobre esta tarefa

O XClarity Orchestrator fornece os seguintes grupos de usuários predefinidos, um para cada função predefinida. Para obter mais informações sobre funções, consulte Controlando o acesso a funções.

- **Grupo de supervisores**. Os usuários neste grupo de usuários são atribuídos à função de **Supervisor**.
- **Grupo de administradores de hardware**. Os usuários neste grupo de usuários recebem a função **Administrador de Hardware**.
- **Grupo de administradores de segurança**. Os usuários neste grupo de usuários são atribuídos à função **Administrador de Segurança**.
- **Grupo de relatores.** Os usuários neste grupo de usuários recebem a função de **Relator**.
- **Grupo de administradores de atualizações**. Os usuários neste grupo de usuários são atribuídos à função **Administrador de Atualizações**.

- **Grupo de operadores**. Os usuários neste grupo de usuários são atribuídos à função de **Operador**.
- **Grupo de legado do operador**. Os usuários neste grupo de usuários são atribuídos à função **Legado do Operador**. Observe que este grupo de usuário será substituído em uma versão futura.

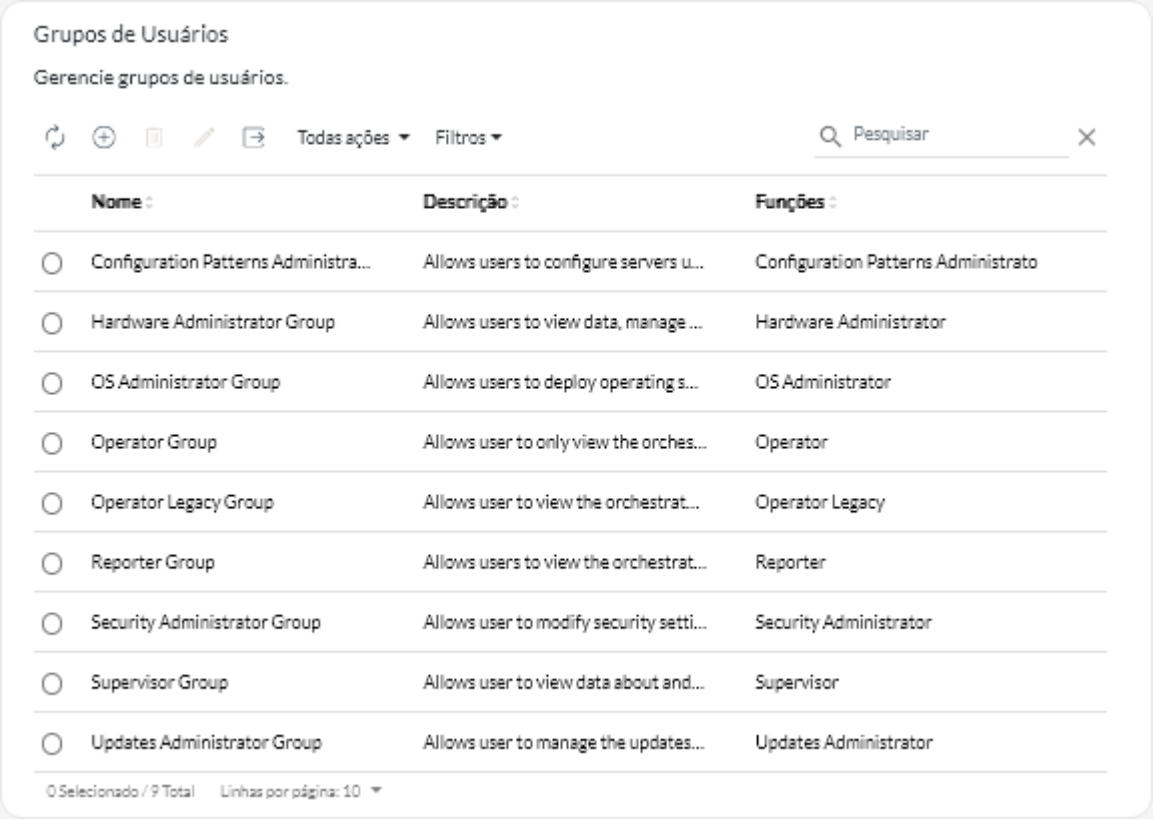
Pelo menos um usuário deve ser membro de um grupo de usuários *local* ao qual a função predefinida de **Supervisor** é atribuída (consulte Controlando o acesso a funções).

Para que um usuário LDAP externo possa fazer login no XClarity Orchestrator, o usuário deve ser um membro direto de um grupo de usuários LDAP que foi clonado no XClarity Orchestrator. O XClarity Orchestrator não reconhece usuários membros de grupos aninhados no grupo de usuários LDAP clonado definido no servidor LDAP externo.

Procedimento

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

- **Criar um grupo de usuários locais**
  1. Na barra de menu do XClarity Orchestrator, clique em **Administração** (⚙) → **Segurança** e clique em **Grupos de Usuários** na navegação esquerda para exibir o cartão Grupos de Usuários.



  2. Clique no ícone **Criar** (⊕) para exibir a caixa de diálogo Criar grupo.
  3. Selecione **Grupo de usuários local** como o tipo de grupo.
  4. Especifique o nome e a descrição opcional deste grupo de usuários.
  5. Clique na guia **Usuários Disponíveis** e selecione os usuários que deseja incluir neste grupo de usuários.
  6. Clique na guia **Funções** e selecione as funções que deseja atribuir neste grupo de usuários.Se uma função não estiver selecionada, a função **Operador** será atribuída por padrão.

7. Clique em **Criar**.

- **Clonar um grupo de usuários a partir de um servidor LDAP externo**
  1. Na barra de menu do XClarity Orchestrator, clique em **Administração (⚙) → Segurança** e clique em **Grupos de Usuários** na navegação esquerda para exibir o cartão Grupos de Usuários.
  2. Clique no ícone **Criar** (⊕) para exibir a caixa de diálogo Criar grupo.
  3. Selecione **Grupo de Usuários LDAP** como o tipo de grupo.
  4. Como opção, especifique uma descrição para o grupo.
  5. Selecione a configuração LDAP para o servidor LDAP externo que contém o grupo de usuários que você deseja adicionar.

     Dica: Comece a digitar para encontrar todos os nomes de grupo que contêm a palavra-chave especificada
  6. Se o servidor LDAP externo estiver configurado usando credenciais de login, especifique o nome de usuário e a senha para fazer login no servidor LDAP externo.
  7. Especifique uma sequência de pesquisa (com pelo menos três caracteres) no campo **Pesquisar Grupo** e clique em **Pesquisar** para localizar grupos de usuários no servidor LDAP externo que correspondam à sequência de pesquisa. Em seguida, selecione o grupo que você deseja adicionar.
  8. Clique na guia **Funções** e selecione as funções que deseja atribuir neste grupo de usuários.Se uma função não estiver selecionada, a função **Operador** será atribuída por padrão.
  9. Clique em **Criar**.

Depois de concluir

É possível executar as ações a seguir na placa Grupos de Usuários.

- Modifique as propriedades, a associação local e as funções de um grupo de usuários selecionado clicando no ícone **Editar** (✎).
  - Quando você adiciona ou remove um usuário de um grupo, o usuário é desconectado automaticamente das funções (permissões) alteradas após a atribuição de novos grupos. Quando o usuário fizer login novamente, ele poderá executar ações com base nas funções agregadas dos grupos de usuários atribuídos.
  - Cada usuário deve ser membro de pelo menos um grupo de usuários. Se você configurar esse atributo como uma matriz vazia ou Null, **OperatorGroup** será atribuído por padrão.
  - Para grupos de usuários predefinidos, é possível modificar apenas a associação de grupo.
  - Para o grupo de usuários LDAP, é possível modificar apenas a descrição e as funções. Use o servidor LDAP externo para alterar outras propriedades e associação.
- Exclua um grupo de usuários selecionado clicando no ícone **Excluir** (🗑).

  Nota: Não é possível excluir os grupos de usuários predefinidos.
- Exiba os membros de um grupo de usuários clicando no nome do grupo para exibir a caixa de diálogo Exibir grupo e, em seguida, clicando na guia **Resumo de membros**.

Alterando detalhes da conta do usuário

Você pode alterar a senha, o nome completo, o endereço de e-mail e o número de telefone de sua conta de usuário.

Sobre esta tarefa

As senhas de usuário expiram após **0** dias, por padrão.

Procedimento

Para alterar a senha e outros atributos, conclua as etapas a seguir.

Etapa 1. Na barra de título do XClarity Orchestrator, clique no menu **Conta do usuário** ( ) no canto superior direito e, em seguida, clique em **Alterar senha**. A caixa de diálogo Alterar senha é exibida.

Etapa 2. Insira a senha atual.

Etapa 3. Insira as senhas nova e de confirmação. Por padrão, as senhas devem conter **8** – **256** caracteres e devem atender aos critérios a seguir.

- Deve conter pelo menos um caractere alfabético e não deve ter mais de dois caracteres sequenciais, incluindo sequências de caracteres alfabéticos, dígitos e teclas de teclado QWERTY (por exemplo, "abc", "123" e "asd" não são permitidos)
- Deve conter pelo menos um número
- Deve conter pelo menos dois dos caracteres a seguir.
  - Caracteres alfabéticos maiúsculos (A – Z)
  - Caracteres alfabéticos minúsculos (a – z)
  - Caracteres especiais ; @ _ ! ' $ & +

  Caracteres de espaço em branco não são permitidos.
- Não deve repetir nem reverter o nome do usuário.
- Não deve conter mais de dois caracteres consecutivos (por exemplo, "aaa", "111" e "..." não são permitidos).

Etapa 4. Altere o nome completo, o endereço de e-mail e o número de telefone se apropriado.

Etapa 5. Clique em **Alterar**.

Alterando detalhes para outro usuário

Os usuários supervisores podem alterar os detalhes, como a senha, de outro usuário.

Sobre esta tarefa

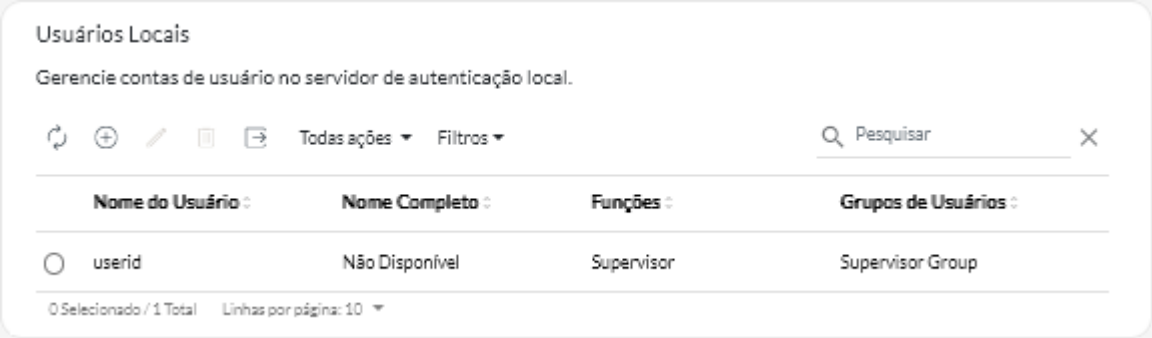
As senhas de usuário expiram após **0** dias, por padrão.

É possível configurar o tempo de expiração da senha e também as regras de complexidade de senha (consulte Definindo configurações de segurança do usuário).

Procedimento

Para criar um usuário local, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Administração ( ) → Segurança** e, em seguida, clique em **Usuários Locais** na navegação esquerda para exibir a placa Usuários Locais.



Etapa 2. Selecione a conta do usuário.

Etapa 3. Clique no ícone **Editar** (✎) para modificar as propriedades do usuário. A caixa de diálogo Editar Usuário é exibida.

Etapa 4. Insira as senhas nova e de confirmação. Por padrão, as senhas devem conter **8** – **256** caracteres e devem atender aos critérios a seguir.

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

Etapa 5. Clique em **Editar**.

Definindo configurações de segurança do usuário

As configurações de segurança da conta do usuário definem as configurações de senha, login e sessão do usuário para usuários locais.

Saiba mais: Como definir configurações de segurança do usuário

Procedimento

Para definir configurações de segurança para usuários locais, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Administração (⚙) → Segurança** e, em seguida, clique em **Configurações de Segurança de Conta** na navegação esquerda para exibir a placa Configurações de Segurança de Conta.

Etapa 2. Defina as configurações de segurança a seguir.

Configuração de segurança	Descrição	Valores permitidos	Valores padrão
Período de Expiração da Senha	Período de tempo, em dias, durante o qual um usuário pode usar uma senha antes de precisar alterá-la Com valores menores, os invasores têm menos tempo para adivinhar senhas. Se for definido como 0, as senhas nunca expirarão.	**0 – 365**	**0**
Período de aviso de expiração da senha	O período de tempo, em dias, anterior à data de expiração da senha em que os usuários começam a receber avisos sobre a proximidade de uma expiração da senha. Se for definido como 0, os usuários não serão avisados.	**0 – 30**	**0**
Ciclo mínimo de reutilização de senha	O número mínimo de vezes que uma senha exclusiva deve ser especificada ao alterar a senha antes de poder começar a repetir senhas Se definido como 0, os usuários poderão reutilizar as senhas imediatamente.	**0 – 10**	**5**
Intervalo mínimo de mudança de senha	O período de tempo mínimo, em horas, que deve decorrer antes que um usuário possa alterar uma senha novamente após já tê-la alterado O valor especificado para essa configuração não pode ultrapassar o valor especificado para a configuração **Período de expiração da senha**. Se definido como 0, os usuários poderão alterar as senhas imediatamente.	**0 – 240**	**1**
Número máximo de falhas de login	O número máximo de vezes que o usuário pode tentar fazer login com uma senha incorreta antes que a conta do usuário seja bloqueada **Nota:** Tentativas de login consecutivas usando o mesmo nome de usuário e a mesma contagem de senha como um único login com falha. Se for definido como 0, as contas nunca serão bloqueadas.	**0 – 10**	**5**

Configuração de segurança	Descrição	Valores permitidos	Valores padrão
Falha ao redefinir contador de login	Quantidade de tempo desde a última tentativa de login com falha antes de o **Número máximo de falhas de login** ser redefinido como 0. Se for definido como 0, o contador nunca será redefinido. Por exemplo, se o número máximo de falhas de login for 2, e você falhar ao fazer login uma vez, depois de falhar uma segunda vez 24 horas depois, o sistema registrará que você não falhou no login duas vezes e sua conta será bloqueada. **Nota:** Essa configuração é aplicada apenas quando a configuração **Número máximo de falhas de login** é definida como 1 ou superior.	**0 – 60**	**15**
Período de bloqueio após número máximo de falhas de login	O período de tempo mínimo, em minutos, depois do qual um usuário bloqueado pode tentar fazer login novamente Uma conta de usuário bloqueada não pode ser usada para obter acesso ao XClarity Orchestrator, mesmo se uma senha válida for fornecida. Se for definido como 0, as contas de usuário nunca serão bloqueadas. **Nota:** Essa configuração é aplicada apenas quando a configuração **Número máximo de falhas de login** é definida como 1 ou superior.	**0 – 2880**	**60**

Configuração de segurança	Descrição	Valores permitidos	Valores padrão
Tempo limite da sessão de inatividade da web	A quantidade de tempo, em minutos, que uma sessão do usuário estabelecida com o servidor do orquestrador pode ficar inativa antes que a sessão do usuário expire e o usuário seja automaticamente desconectado. Esse tempo-limite se aplica a todas as ações (como abrir uma página, atualizar a página atual ou modificar dados). Esse é o tempo-limite principal para a sessão do usuário. Quando uma sessão está ativa, o cronômetro é redefinido sempre que o usuário executa qualquer ação. Depois que o valor de tempo-limite for excedido, a página de login será exibida na próxima vez em que o usuário tentar executar uma ação. Se for definido como 0, esse tempo-limite será desativado. **Nota:** Alterar essa configuração afeta imediatamente todas as sessões do usuário, independentemente do tipo de autenticação. As sessões existentes inativas por mais tempo do que o novo valor de tempo-limite estão expiradas.	**0**, **60 – 1440**	**1440**
Tempo-limite de inatividade da Web para operações completas	Período, em minutos, que uma sessão do usuário estabelecida com o servidor do orquestrador pode ficar inativa antes que as ações que modificam dados (como criação, atualização ou exclusão de um recurso) estejam desativadas Este é um tempo-limite secundário opcional e é menor do que o valor principal do **Tempo-limite da sessão de inatividade da web**. Quando uma sessão está ativa, o cronômetro é redefinido sempre que o usuário executa qualquer ação. Se esse valor de tempo-limite for excedido, mas o valor principal de **Tempo-limite da sessão de inatividade da web** *não for* excedido, o usuário estará restrito a ações somente leitura (como abrir ou atualizar uma página) até que o valor principal de **Tempo-limite da sessão de inatividade da web** seja excedido; entretanto, se o usuário tentar executar uma ação que modifique os dados, a sessão do usuário expirará e a página de login será exibida. Se for definido como 0, esse tempo-limite será desativado. **Nota:** Alterar essa configuração afeta imediatamente todas as sessões do	**0**, **15 – 60**	**30**

Configuração de segurança	Descrição	Valores permitidos	Valores padrão
	usuário, independentemente do tipo de autenticação. As sessões existentes inativas por mais tempo do que o novo valor de tempo-limite estão expiradas.		
Tempo de expiração obrigatório de uma sessão baseada na Web	A quantidade de tempo, em horas, que uma sessão do usuário estabelecida com o servidor do orquestrador pode ficar aberta antes que o usuário seja desconectado automaticamente, seja qual for a atividade do usuário **Nota:** Alterar essa configuração afeta imediatamente todas as sessões do usuário, independentemente do tipo de autenticação. As sessões existentes inativas por mais tempo do que o novo valor de tempo-limite estão expiradas.	**24 – 240**	**24**
Tamanho mínimo de senha	O número mínimo de caracteres que podem ser usados para especificar uma senha válida	**8 – 256**	**256**
Tamanho máximo de senha	O número máximo de caracteres que podem ser usados para especificar uma senha válida	**8 – 128**	**128**
Máximo de sessões ativas para um usuário específico	O número máximo de sessões ativas para um usuário específico que tem permissão a qualquer momento. Quando o número máximo é atingido, a sessão ativa mais antiga para um usuário (com base no carimbo de data e hora de criação) é removida antes da criação de uma nova sessão para esse usuário. Se definido como 0, um número ilimitado de sessões ativas é permitido para um usuário específico. **Nota:** Apenas as sessões do usuário que começam após a alteração da configuração são afetadas.	**0 – 20**	**20**

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

Etapa 3. Clique em **Aplicar**.

Depois que as alterações forem aplicadas, as novas configurações terão efeito imediatamente. Se você alterar políticas de senha, essas políticas serão impostas na próxima vez que um usuário fizer login ou alterar a senha.

Depois de concluir

É possível executar a seguinte ação na placa Configurações de Segurança de Conta.

- Para redefinir essas configurações para os valores padrão, clique em **Restaurar padrões**.

Monitorando sessões ativas do usuário

É possível determinar quem fez login na interface da Web do XClarity Orchestrator.

Antes de iniciar

Por padrão, as sessões do usuário sem atividade por mais de 24 horas são desconectadas automaticamente. É possível configurar o tempo limite da sessão de inatividade da Web (consulte Definindo configurações de segurança do usuário)

Procedimento

Para exibir uma lista de todas as sessões do usuário ativas (incluindo a sessão atual), clique em **Administração (⚙) → Segurança** na barra de menus do XClarity Orchestrator e, em seguida, clique em **Sessões Ativas** na navegação esquerda para exibir a placa Sessões Ativas.

Depois de concluir

É possível executar a ação a seguir na placa Sessões Ativas.

- Desconecte uma sessão de usuário selecionada clicando no ícone **Excluir** (🗑).

  Nota: Não é possível desconectar a sessão atual.

Controlando o acesso a funções

O Lenovo XClarity Orchestrator usa *funções* e *grupos de usuários* para determinar quais funções (ações) um usuário pode executar.

Sobre esta tarefa

Uma *função* é um conjunto de funções. Quando uma função é atribuída a um grupo de usuários, todos os usuários desse grupo podem executar as funções que estão incluídas nessa função.

O XClarity Orchestrator fornece as seguintes funções predefinidas.

- **Supervisor**. Permite que os usuários exibam dados e executem todas as ações disponíveis no servidor do Orchestrator e todos os recursos gerenciados (Gerenciadores de Recursos e dispositivos).Os usuários atribuídos a essa função sempre têm acesso a todos os recursos (dispositivos e gerenciadores de recursos) e todas as funções. Não é possível restringir o acesso a recursos ou funções para essa função.

Você deve ter privilégios de supervisor para realizar as ações a seguir.
- Reiniciar o servidor do orquestrador
- Realizar tarefas de manutenção, como instalar licenças e atualizar para uma versão mais recente
- Conectar e desconectar gerenciadores de recursos
- Modificar configurações do sistema, como preferências de rede e data e hora
- Concordar em enviar dados periódicos para a Lenovo

Deve haver pelo menos um usuário com privilégios de supervisor.

Importante: Ao fazer upgrade do XClarity Orchestrator v1.0 para uma versão posterior, todos os usuários criados no XClarity Orchestrator v1.0 recebem privilégios de supervisor por padrão. Um usuário do supervisor pode remover os privilégios de supervisor para usuários que não deveriam ter esses privilégios.

- **Administrador de hardware**. Permite que os usuários exibam dados, gerenciem e implantem padrões de configuração, gerenciem e implantem sistemas operacionais usando perfis de SO, exibam e personalizem a análise e realizem ações em recursos acessíveis. Essa função proíbe os usuários de atualizar software ou firmware em recursos gerenciados e gerenciar grupos de recursos.
- **Administrador de Configuração do Servidor**. Permite que os usuários configurem servidores usando padrões de configuração, exibam análises predefinidas e exibam recursos acessíveis. Essa função impede que os usuários acessem os dispositivos remotamente e liguem e desliguem dispositivos.
- **Administrador do SO**. Permite que os usuários implantem sistemas operacionais usando perfis de SO, exibam análises predefinidas e exibam dados de recursos acessíveis. Essa função impede que os usuários acessem os dispositivos remotamente e liguem e desliguem dispositivos.
- **Administrador de Atualizações**. Permite que os usuários atualizem o firmware em dispositivos e software em Gerenciadores de Recursos, exibam dados para recursos acessíveis e exibam a análise predefinida.
- **Administrador de Segurança**. Permite que os usuários modifiquem configurações de segurança e executem ações relacionadas à segurança no servidor do Orchestrator, exibam dados para todos os recursos gerenciados, gerenciem o grupo de recursos e exibam a análise predefinida.Os usuários que recebem essa função sempre têm acesso a todos os recursos (dispositivos e gerenciadores de recursos). Você não pode restringir o acesso aos recursos para essa função.
- **Relator**. Permite que os usuários exibam a configuração do servidor do Orchestrator, exibam dados sobre recursos acessíveis, criem consultas para gerar relatórios personalizados e criem encaminhadores de dados para agendar e enviar relatórios por e-mail. Essa função impede os usuários de provisionar recursos e de ligar e desligar dispositivos.
- **Operador**. Permite que os usuários exibam apenas a configuração do servidor do Orchestrator e os dados para recursos acessíveis. Essa função proíbe os usuários de executar ações ou modificar configurações no servidor do orquestrador e nos recursos gerenciados, criar e exibir relatórios de análise e criar alertas personalizados.
- **Legado do Operador**. Permite que os usuários exibam dados e executem determinadas ações em recursos acessíveis, como gerenciamento de estoque, alertas e tíquetes de serviço. Essa função proíbe os usuários de atualizar o software ou o firmware em recursos gerenciados, criar grupos de recursos, criar e exibir relatórios de análise e criar alertas personalizados.

  Atenção: Ao fazer upgrade do XClarity Orchestrator v1.2 para uma versão posterior, os usuários atribuídos à função **Operador** são alterados automaticamente para a função **Legado do Operador** e adicionados ao grupo de usuários **OperatorLegacyGroup**. A função **Legado do Operador** e o grupo de usuários **OperatorLegacyGroup** serão substituídos em uma versão futura.

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

Nota: A exibição de dados relacionados a recursos não é restrita com base em funções. Todos os usuários podem visualizar dados relacionados a recursos (como inventário, alertas, trabalhos e tíquetes de serviço) para recursos que podem ser acessadas.

Procedimento

Para exibir informações sobre as funções predefinidas, clique em **Administração (⚙) → Segurança** na barra de menu do XClarity Orchestrator e clique em **Funções** na navegação esquerda.

Clique na linha para qualquer função para exibir a caixa de diálogo Funções com informações sobre as propriedades de função, a lista de funções na função e uma lista de grupos de usuários aos quais a função é atribuída.

Atribuindo funções aos usuários

O Lenovo XClarity Orchestrator usa *funções* e *grupos de usuários* para determinar quais funções (ações) um usuário pode executar.

Antes de iniciar

Quando as funções são alteradas para um usuário que está conectado atualmente a uma sessão ativa, a sessão do usuário é encerrada automaticamente, e o usuário é desconectado da interface do usuário. Quando o usuário faz login novamente, ele pode executar as funções com base nas novas atribuições de função.

Sobre esta tarefa

Quando você atribui várias funções a um grupo de usuários, as funções em cada função são agregadas.

Todos os usuários que são membros de um grupo de usuários têm permissão para executar as funções que são incluídas nas funções atribuídas a esse grupo de usuários.

É possível modificar as funções de um usuário das seguintes maneiras:
- Adicionando ou removendo o usuário de um grupo de usuários
- Adicionando ou removendo funções de um grupo de usuários do qual o usuário é membro
- Excluindo um grupo de usuários do qual o usuário é membro

Notas:

- Quando os usuários LDAP são adicionados ou removidos dos grupos de usuários LDAP no servidor LDAP, as alterações nas associações entre o usuário LDAP e o grupo de usuários LDAP são atualizadas automaticamente no XClarity Orchestrator com base em grupos de usuários LDAP clonados existentes.
- Quando as funções atribuídas a um grupo de usuários mudam, o usuário deve fazer login novamente para que as alterações nas funções tenham efeito.

Controlando o acesso a recursos

Lenovo XClarity Orchestrator usa *listas de controle de acesso* (ACLs) para determinar quais recursos (dispositivos, gerenciadores de recursos e XClarity Orchestrator) os usuários podem acessar. Quando um usuário tem acesso a um conjunto específico de recursos, esse usuário pode ver dados (como inventário, eventos, alertas e análises) que são relacionados a apenas esses recursos

Sobre esta tarefa

Uma ACL é uma união de grupos de usuários e grupos de recursos.

- Os *grupos de usuários* identificam os usuários afetados por essa ACL. A ACL deve conter um único grupo de usuários. Usuários que são membros de um grupo ao qual a função de **Supervisor** predefinida é atribuída sempre têm acesso a todos os recursos. Não é possível limitar o acesso de recurso para usuários supervisores.

  Quando o acesso baseado em recursos é ativado, usuários que *não são* membros de um grupo ao qual a função de **Supervisor** predefinida é atribuída não têm acesso a nenhum recurso (dispositivos e gerenciadores de recursos) por padrão. Você deve adicionar usuários não supervisores a um grupo de usuários que faça parte de uma lista de controle de acesso para permitir que esses usuários acessem um conjunto específico de recursos.

  Quando o acesso baseado em recursos é desabilitado, todos os usuários têm acesso a todos os recursos (dispositivos e gerenciadores de recursos) por padrão.
- Os *grupos de recursos* identificam os recursos (dispositivos, gerenciadores de recursos e XClarity Orchestrator) que podem ser acessados. A ACL deve conter pelo menos um grupo de recursos.

  Nota: Um usuário que tem acesso a um grupo de gerenciadores não obtém automaticamente acesso a todos os dispositivos que são gerenciados por esse gerenciador de recursos. Você deve fornecer acesso explícito aos dispositivos usando grupos de dispositivos.

Procedimento

Para controlar o acesso a recursos, conclua as etapas a seguir.

Etapa 1. Crie um grupo de usuários que possa acessar os recursos.

Etapa 2. Crie um ou mais grupos de recursos aos quais você deseja controlar o acesso.

Etapa 3. Crie uma lista de controle de acesso que contém o grupo de usuários e um ou mais grupos de recursos.

Etapa 4. Habilite o controle de acesso baseado em recursos.

Habilitando o acesso baseado em recursos

Se você deseja limitar os recursos que os usuários podem acessar, ative o acesso baseado em recursos.

Sobre esta tarefa

Usuários que são membros de um grupo ao qual a função de **Supervisor** predefinida é atribuída sempre têm acesso a todos os recursos. Não é possível limitar o acesso de recurso para usuários supervisores.

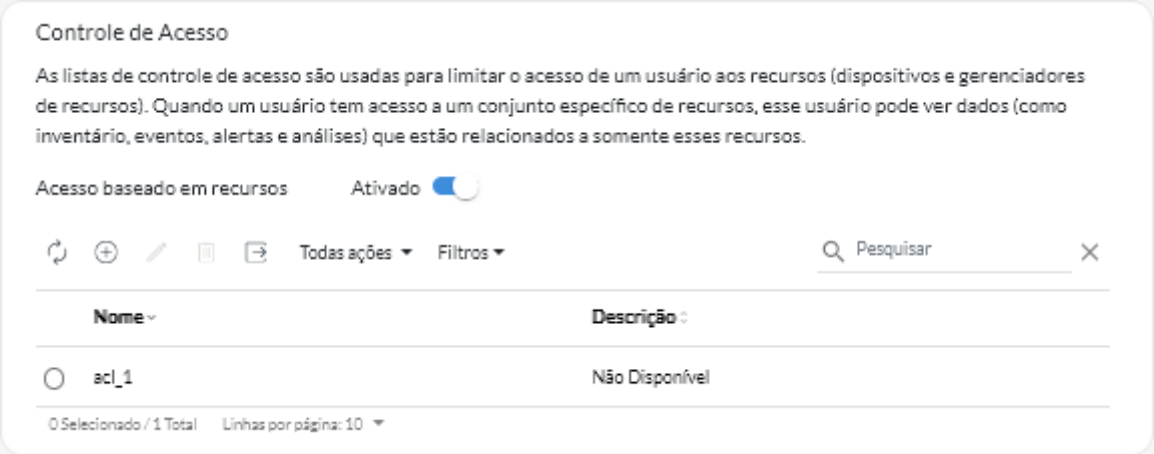
Quando o acesso baseado em recursos é ativado, usuários que *não são* membros de um grupo ao qual a função de **Supervisor** predefinida é atribuída não têm acesso a nenhum recurso (dispositivos e gerenciadores de recursos) por padrão. Você deve adicionar usuários não supervisores a um grupo de usuários que faça parte de uma lista de controle de acesso para permitir que esses usuários acessem um conjunto específico de recursos.

Quando o acesso baseado em recursos é desabilitado, todos os usuários têm acesso a todos os recursos (dispositivos e gerenciadores de recursos) por padrão.

Procedimento

Para ativar os controles de acesso baseados em recursos, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Orchestrator, clique em **Administração (⚙) → Segurança** e clique em **Controles de Acesso** na navegação esquerda para exibir o cartão Controle de Acesso.



Etapa 2. Clique no botão de alternância **Acesso Baseado em Recursos** para ativar o controle de acesso de recursos usando listas de controle de acesso.

Criando listas de controle de acesso

O Lenovo XClarity Orchestrator usa *listas de controle de acesso* (ACLs) para determinar quais recursos (dispositivos, gerenciadores de recursos e XClarity Orchestrator) os usuários podem acessar. Quando um usuário tem acesso a um conjunto específico de recursos, esse usuário pode ver dados (como inventário, eventos, alertas e análises) que são relacionados a apenas esses recursos

Antes de iniciar

Saiba mais: Como criar listas de controle de acesso

Certifique-se de que os grupos de usuários que você deseja associar à ACL estejam definidos (consulte Criando grupos de usuários).

Certifique-se de que todos os grupos de usuários que você deseja associar a esta ACL estejam definidos (consulte Criando grupos de recursos).

Sobre esta tarefa

Uma ACL é uma união de grupos de usuários e grupos de recursos.

- Os *grupos de usuários* identificam os usuários afetados por essa ACL. A ACL deve conter um único grupo de usuários. Usuários que são membros de um grupo ao qual a função de **Supervisor** predefinida é atribuída sempre têm acesso a todos os recursos. Não é possível limitar o acesso de recurso para usuários supervisores.

  Quando o acesso baseado em recursos é ativado, usuários que *não são* membros de um grupo ao qual a função de **Supervisor** predefinida é atribuída não têm acesso a nenhum recurso (dispositivos e gerenciadores de recursos) por padrão. Você deve adicionar usuários não supervisores a um grupo de usuários que faça parte de uma lista de controle de acesso para permitir que esses usuários acessem um conjunto específico de recursos.

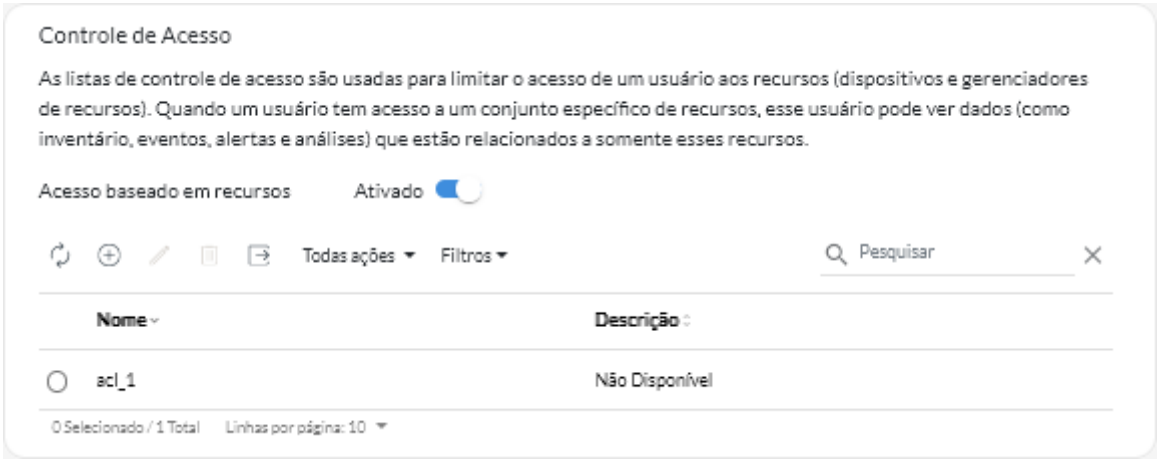
  Quando o acesso baseado em recursos é desabilitado, todos os usuários têm acesso a todos os recursos (dispositivos e gerenciadores de recursos) por padrão.
- Os *grupos de recursos* identificam os recursos (dispositivos, gerenciadores de recursos e XClarity Orchestrator) que podem ser acessados. A ACL deve conter pelo menos um grupo de recursos.

Nota: Um usuário que tem acesso a um grupo de gerenciadores não obtém automaticamente acesso a todos os dispositivos que são gerenciados por esse gerenciador de recursos. Você deve fornecer acesso explícito aos dispositivos usando grupos de dispositivos.

Procedimento

Para criar uma lista de controle de acesso, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Orchestrator, clique em **Administração (⚙) → Segurança** e clique em **Controles de Acesso** na navegação esquerda para exibir o cartão Controle de Acesso.



Etapa 2. Clique no ícone **Adicionar** (⊕) para adicionar uma ACL. A caixa de diálogo Criar Controle de Acesso é exibida

Etapa 3. Especifique o nome e a descrição opcional para a ACL.

Etapa 4. Clique em **Grupo de Usuários** e selecione o grupo de usuários que você deseja incluir nesta ACL.

Etapa 5. Clique em **Grupos de Recursos** e selecione os grupos de recursos que você deseja incluir nesta ACL.

Etapa 6. Clique em **Criar**.

A lista de controle de acesso é adicionada à tabela

Depois de concluir

É possível executar as ações a seguir nesta página.

- Visualize o grupo de usuários e os grupos de recursos em uma ACL específica clicando em qualquer lugar na linha dessa ACL.
- Modifique as propriedades e a associação de uma ACL selecionada clicando no ícone **Editar** (✎).
- Exclua uma ACL selecionada clicando no ícone **Excluir** (🗑).
- Se um usuário não puder acessar dados de um recurso específico ou se um usuário puder acessar dados de um recurso específico que não deveria ser acessado, identifique as listas de controle de acesso que estão associadas ao usuário e, em seguida, exiba a associação de cada grupo de recursos que também está associado a essas listas de controle de acesso. Certifique-se de que o recurso em questão esteja ou não incluído nesses grupos de recursos.

Gerenciando espaço em disco

É possível gerenciar a quantidade de espaço em disco usado pelo Lenovo XClarity Orchestrator excluindo arquivos que não são mais necessários

Sobre esta tarefa

Procedimento

Para excluir arquivos desnecessários, conclua um ou mais dos seguintes procedimentos.

Arquivos de dados de serviço do dispositivo

1. No Lenovo XClarity Orchestrator, clique em **Administração** ( ) → **Serviço e Suporte** e clique na guia **Dados do serviço** para exibir o cartão Dados de Serviço do Dispositivo.
2. Selecione um ou mais arquivos de dados de serviço a serem excluídos e clique no ícone **Excluir** ( ).

Imagens do sistema operacional

1. Na barra de menus do Lenovo XClarity Orchestrator, clique em **Administração** ( ) → **Implantação do SO** e, em seguida, clique na guia **Gerenciamento de SO** para exibir o cartão Imagens do SO.
2. Selecione uma ou mais imagens do SO a serem excluídas e clique no ícone **Excluir** ( ).

Atualizar arquivos de carga útil

Certifique-se de que as atualizações não sejam usadas em uma política de conformidade de atualizações. É possível remover uma atualização de uma política do cartão Aplicar e Ativar (consulte Criando e atribuindo políticas de conformidade de atualização).

1. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento** ( ) → **Atualizações** e, em seguida, clique na guia **Gerenciamento do Repositório** para exibir o cartão de Gerenciamento do Repositório.
2. Selecione um ou mais pacotes de atualização ou arquivos a serem excluídos.
3. Clique no ícone **Excluir somente arquivos de carga útil** ( ) para excluir apenas o arquivo de imagem (carga útil) para cada atualização selecionada. As informações sobre a atualização (o arquivo de metadados XML) permanecem no repositório e o status de download muda para "Não baixado".

Atualizações do XClarity Orchestrator

É possível excluir atualizações do servidor do orquestrador que estão no estado Baixado. A coluna **Status Aplicado** na tabela indica o status da atualização.

1. Na barra de menus do XClarity Orchestrator, clique em **Manutenção** ( ) e clique na guia **Atualização do Servidor do Orchestrator** para exibir o cartão Atualização do Servidor do Orchestrator.
2. Selecione uma ou mais atualizações a serem excluídas e clique no ícone **Excluir** ( ).A coluna **Status adquirido** das atualizações excluídas é alterada para "Não baixado".

Reiniciando o XClarity Orchestrator

Há determinadas situações em que você pode precisar reiniciar o Lenovo XClarity Orchestrator, por exemplo, ao gerar novamente ou fazer upload de um certificado do servidor. É possível reiniciar o Lenovo XClarity Orchestrator na interface da Web.

Antes de iniciar

Você deve ter autoridade de **Supervisor** para reiniciar o XClarity Orchestrator.

Considere fazer o backup do servidor do orquestrador antes de reiniciar (consulte Backup e restauração de dados do servidor do orquestrador).

Certifique-se de que não haja nenhum trabalho em execução no momento. Os trabalhos em execução são cancelados durante o processo de reinicialização. Para exibir o log de trabalhos, consulte Monitorando trabalhos.

Durante o processo de reinicialização, os trabalhos são interrompidos, todos os usuários são desconectados e a conectividade com o servidor do orquestrador é perdida. Aguarde 15 minutos ou mais (dependendo do número de dispositivos gerenciados) para que o servidor do orquestrador seja reiniciado antes de fazer login novamente (Efetuando login no XClarity Orchestrator).

Depois que o XClarity Orchestrator for reiniciado, ele coletará novamente o inventário de cada dispositivo gerenciado. Aguarde cerca de 30 a 45 minutos, dependendo do número de dispositivos gerenciados, antes de tentar atualizações de firmware, implantações de padrão de configuração ou implantações do sistema operacional.

Procedimento

Para iniciar o XClarity Orchestrator, conclua um dos procedimentos a seguir.

Na interface do usuário

1. Na barra de menu do XClarity Orchestrator, clique em **Manutenção → Reinicialização do dispositivo**.
2. Clique em **Reiniciar**.
3. Clique em **Sim**.
4. Atualize o navegador.

No hipervisor

Microsoft Hyper-V

1. No painel do Server Manager, clique em **Hyper-V**.
2. Clique com o botão direito no servidor e clique em **Gerenciador Hyper-V**.
3. Clique com o botão direito na máquina virtual e clique em **Redefinir**.

VMware ESXi

1. Conectar-se ao host pelo VMware vSphere Client.
2. Clique com o botão direito na máquina virtual e clique em **Energia → Redefinir**.
3. Clique na guia **Console**.

Quando o dispositivo virtual é iniciado, os endereços IPv4 e IPv6 atribuídos pelo DHCP são listados para cada interface, conforme mostrado no exemplo a seguir.

```
Lenovo XClarity Orchestrator  Version x.x.x
------------------------------------------

eth0      Link encap:Ethernet  HWaddr 2001:db8:65:12:34:56
          inet addr: 192.0.2.10  Bcast 192.0.2.55  Mask 255.255.255.0
          inet6 addr: 2001:db8:56ff:fe80:bea3/64 Scope:Link
```

```
================================================================================
================================================================================

You have 118 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
  3. To select subnet for Lenovo XClarity virtual appliance internal network
  x. To continue without changing IP settings
  … …
```

É possível definir as configurações de IP do dispositivo virtual no console. Se você não fizer uma seleção no período especificado ou se inserir `x`, a inicialização inicial continuará usando as configurações de IP atribuídas por padrão.

- **Atribua endereços IP estáticos para a porta eth0**. Digite `1` e siga os prompts para alterar as configurações.
- **Atribua novos endereços IP para a porta eth0 usando DHCP**. Digite `2` e siga os prompts para alterar as configurações.
- **Selecione a sub-rede para a rede interna do dispositivo virtual**. Digite `3` e siga os prompts para alterar as configurações.Por padrão, o XClarity Orchestrator usa a sub-rede **192.168.252.0/24** para a rede interna. Caso essa sub-rede se sobreponha à rede do host, altere a sub-rede para uma das outras opções disponíveis para evitar problemas de rede.
  - 192.168.252.0/24
  - 172.31.252.0/24
  - 10.255.252.0/24

Importante: Se você especificar valores inválidos, um erro será retornado. Você tem até quatro tentativas de inserir valores válidos.

Backup e restauração de dados do servidor do orquestrador

O Lenovo XClarity Orchestrator não inclui funções de backup e restauração internas. Em vez disso, use as funções de backup disponíveis no sistema operacional do host virtual em que XClarity Orchestrator está instalado.

Sobre esta tarefa

Sempre faça backup do XClarity Orchestrator após o processo de configuração inicial e depois de fazer alterações significativas de configuração, incluindo:
- Antes de atualizar XClarity Orchestrator
- Depois de fazer mudanças na rede
- Depois de adicionar usuários ao XClarity Orchestrator servidor de autenticação local
- Depois de gerenciar novos gerenciadores de recursos

Se você tem procedimentos de backup e restauração para hosts virtuais, verifique se eles incluem o XClarity Orchestrator.

Importante:

- Verifique se todos os trabalhos em execução foram concluídos e se o XClarity Orchestrator foi desligado antes de criar um backup.
- Faça backup do XClarity Orchestrator regularmente. Se o sistema operacional do host desligar inesperadamente, não será possível autenticar com XClarity Orchestrator após o sistema operacional do host ser reiniciado. Para resolver esse problema, restaure XClarity Orchestrator do backup mais recente.

Backup e restauração de dados do servidor do orquestrador em um host VMware ESXi

Às vezes, você pode precisar restaurar os dados do servidor do orquestrador de um backup. Várias alternativas estão disponíveis para fazer backup e restaurar um dispositivo virtual de um XClarity Orchestrator em execução em um host do VMware ESXi. O processo específico a usar para restaurar de um backup geralmente é baseado no processo que foi utilizado para criar o backup. Este tópico discute como fazer backup e restaurar usando o VMware vSphere Client.

Sobre esta tarefa

Se o VMware vCenter Server estiver instalado, você poderá usar o recurso de backup fornecido com o VMware vCenter para fazer backup do XClarity Orchestrator.

Se você não tiver o VMware vCenter Server instalado, é possível usar o VMware vSphere Client para criar um backup da máquina virtual copiando os arquivos da pasta XClarity Orchestrator para outra pasta no mesmo repositório de dados. Também é possível copiar arquivos para um repositório de dados diferente ou mesmo para um host diferente para proteção de backup adicional.

Nota: O VMware vCenter Server não precisa executar um backup usando esse procedimento.

Procedimento

- **Fazendo backup do XClarity Orchestrator** Para criar um backup do XClarity Orchestrator usando o VMware vSphere Client, execute as etapas a seguir.
  1. Desligamento do XClarity Orchestrator.
  2. Inicie o VMware vSphere Client e conecte-se ao host do ESXi em que XClarity Orchestrator está localizado.
  3. Crie uma nova pasta no mesmo repositório de dados usado por XClarity Orchestrator.
     a. Selecione o host do ESXi na árvore de navegação e clique na guia **Configurar** na janela direita.
     b. Clique em **Hardware → Armazenamento**.
     c. Clique com o botão direito no repositório de dados para XClarity Orchestrator, e clique em **Procurar Armazenamento de dados**.
     d. Selecione a pasta raiz e, em seguida, crie uma nova pasta para conter uma cópia dos arquivos do XClarity Orchestrator.
  4. Clique na pasta XClarity Orchestrator.
  5. Selecione todos os arquivos na pasta e copie os arquivos para a pasta de backup que você acabou de criar.
  6. Reinicie o XClarity Orchestrator.
- **Restaurando o XClarity Orchestrator**Para restaurar o XClarity Orchestrator usando o backup criado no procedimento anterior, execute as etapas a seguir.
  1. Inicie o VMware vSphere Client e conecte-se ao host do ESXi em que XClarity Orchestrator está instalado.
  2. Clique com o botão direito em XClarity Orchestrator na árvore de navegação esquerda e, em seguida, clique em **Energia → Desligar**.
  3. Clique com o botão direito em XClarity Orchestrator na árvore de navegação esquerda novamente e, em seguida, clique em **Remover do Inventário**.
  4. Exclua os arquivos da pasta XClarity Orchestrator no armazenamento de dados usado pelo XClarity Orchestrator.
     a. Selecione o host do ESXi na árvore de navegação e clique na guia **Configurar** na janela direita.

b. Clique em **Hardware → Armazenamento**.

c. Clique com o botão direito no repositório de dados para XClarity Orchestrator, e clique em **Procurar Armazenamento de dados**.

d. Selecione a pasta XClarity Orchestrator.

e. Selecione todos os arquivos na pasta, clique com o botão direito nos arquivos e clique em **Excluir itens selecionados**.

5. Selecione a pasta em que os arquivos de backup são armazenados.
6. Selecione todos os arquivos na pasta e copie-os para a pasta XClarity Orchestrator.
7. Na pasta XClarity Orchestrator, clique com o botão direito no arquivo VMX e clique em **Adicionar a inventário**.
8. Conclua o assistente para adicionar dados do XClarity Orchestrator.
9. Reinicie o XClarity Orchestrator do VMware vSphere Client.
10. Quando solicitado a escolher se a VM foi movida ou copiada, selecione **movido**.

    Importante: Se você selecionar **copiado**, a VM receberá um UUID diferente do UUID da VM original, o que faz a VM agir como uma nova instância e não é possível ver os dispositivos gerenciados anteriormente.

Backup e restauração de dados do servidor do orquestrador em um host Microsoft Hyper-V

Às vezes, você pode precisar restaurar os dados do servidor do orquestrador Lenovo XClarity Orchestrator de um backup. Várias alternativas estão disponíveis para fazer backup e restaurar um dispositivo virtual do XClarity Orchestrator em execução em um host do Microsoft Hyper-V. O processo específico a usar para restaurar de um backup geralmente é baseado no processo que foi utilizado para criar o backup. Este tópico discute como fazer backup e restaurar usando o Windows Server Backup.

Antes de iniciar

Certifique-se de que o Windows Server Backup esteja configurado corretamente concluindo as etapas a seguir.

1. Inicie o Windows Server Manager.
2. Clique em **Gerenciar → Adicionar Funções e Recursos**.
3. Ignore as etapas do assistente até atingir a página **Selecionar Recursos**.
4. Marque a caixa de seleção **Backup do Windows Server**.
5. Conclua o assistente.

Procedimento

- **Fazendo backup do XClarity Orchestrator**Para criar um backup do XClarity Orchestrator usando o Windows Server Backup, execute as etapas a seguir.
  1. Inicie o backup do Windows Server e vá até **Backup Local**.
  2. No painel Ação, clique em **Backup Único** para iniciar após o Assistente de Backup Único.
  3. Na página Opções de Backup, clique em **Opções Diferentes** e em **Avançar**.
  4. Na página Selecionar Configuração de Backup, clique em **Personalizar** e em **Avançar**.
  5. Na página Selecionar Itens para Backup, clique em **Adicionar Itens** para exibir a janela Selecionar Itens.
  6. Expanda o item Hyper-V, clique na máquina virtual do XClarity Orchestrator e clique em **OK**.
  7. Clique em **Avançar** para continuar.

8. Na página Especificar Tipo de Destino, escolha o tipo de armazenamento do backup (uma unidade local ou uma pasta compartilhada remota) e, em seguida, clique em **Avançar**.
9. Na página Selecionar Destino de Backup ou Especificar Pasta Remota, especifique o local desejado para armazenar o backup e clique em **Avançar**.
10. Clique em **Backup** para iniciar o processo de backup.

- **Restaurando o XClarity Orchestrator**Para restaurar o XClarity Orchestrator usando o backup criado no procedimento anterior, execute as etapas a seguir.
  1. Inicie o backup do Windows Server e vá até **Backup Local**.
  2. No painel Ação, clique em **Recuperação** para iniciar após o Assistente de Recuperação.
  3. Na página Introdução, especifique o local em que o backup foi armazenado e clique em **Avançar**.
  4. Na página Selecionar Data de Backup, escolha o backup que você deseja restaurar e clique em **Avançar**.
  5. Na página Selecionar Tipo de Recuperação, selecione a opção **Hyper-V** e clique em **Avançar**.
  6. Na página Selecionar Itens a Recuperar, expanda Hyper-V e selecione a máquina virtual do XClarity Orchestrator. Em seguida, clique em **Avançar**.
  7. Na página Especificar Opções de Recuperação, opte por recuperar a VM para seu local original e clique em **Avançar**.
  8. Na página Confirmação, clique em **Recuperar**. A máquina virtual é restaurada e registrada no Hyper-V.
  9. Reinicie o XClarity Orchestrator a partir do Gerenciador Hyper-V.

Capítulo 3. Monitorando recursos e atividades

É possível usar o Lenovo XClarity Orchestrator para monitorar inventários de ativos, conformidade de firmware e configuração, status de funcionamento e histórico de eventos de dispositivos gerenciados.

Exibindo um resumo do ambiente

O painel é o hub do Lenovo XClarity Orchestrator que fornece acesso às informações que são importantes para você. Ele contém cartões de relatório que resumem o status de recursos e atividades em seu ambiente, incluindo integridade, conformidade e alertas de dispositivos.

Para acessar o painel, clique em **Painel ( )** na barra de menu do XClarity Orchestrator.

É possível alterar o escopo do resumo somente para os dispositivos gerenciados por um gerenciador de recursos específico ou em um grupo de recursos específico usando o menu suspenso **Selecionar gerenciador**.

É possível clicar em qualquer uma das estatísticas vinculadas no painel para exibir uma lista filtrada de dados que atendam aos critérios.

Garantia

A placa Garantia resume o período de garantia para dispositivos gerenciados, incluindo os dados a seguir.
- Número de dispositivos para os quais a garantia está expirada
- Número de dispositivos para os quais a garantia está ativa
- Número de dispositivos para os quais dados de garantia não estão disponíveis

Tíquetes de serviço

A placa Tíquetes resume o gerenciado, incluindo os dados a seguir.
- Número total de tíquetes de serviço ativos
- Número de tíquetes de serviço que estão abertos
- Número de tíquetes de serviço que estão em andamento
- Número de tíquetes de serviço que estão em espera
- Número de tíquetes de serviço que estão fechados
- Número de tíquetes de serviço em outros estados

Conformidade do firmware

O cartão Conformidade do firmware resume a conformidade com a política de conformidade de firmware atribuída a dispositivos gerenciados no XClarity Orchestrator, incluindo os dados a seguir.
- Número de dispositivos que *não estão* em conformidade
- Número de dispositivos em conformidade
- Número de dispositivos que *não* têm uma política de conformidade de firmware atribuída
- Número de dispositivos para os quais a conformidade não é suportada
- Número de dispositivos para os quais a conformidade está sendo verificada em relação à política atribuída

Nota: Esses dados representam a conformidade de firmware com base em políticas atribuídas pelo XClarity Orchestrator. Eles não representam políticas atribuídas por gerenciadores de recursos gerenciados do Lenovo XClarity Administrator.

Conformidade de configuração

A placa Conformidade de configuração resume a conformidade com os padrões de configuração do servidor em dispositivos gerenciados, incluindo os dados a seguir.

- Número de dispositivos que *não estão* em conformidade com o padrão atribuído
- Número de dispositivos que estão em conformidade com o padrão atribuído
- Número de dispositivos que *não* têm um padrão atribuído
- O número de dispositivos para os quais uma verificação de conformidade de configuração está em andamento
- Número de dispositivos para os quais uma reinicialização manual é necessária para concluir a implantação do padrão (reinicialização pendente)
- O número de dispositivos para os quais a última implantação de padrão falhou

Nota: Esses dados representam a conformidade com a configuração do servidor para todos os dispositivos com base em padrões atribuídos por XClarity Orchestrator. Eles não representam padrões atribuídos por gerenciadores de recursos gerenciados do XClarity Administrator.

Correções de segurança

O cartão Correções de segurança resume o número de dispositivos gerenciados que têm vulnerabilidades e exposições comuns (CVEs) para as quais uma correção de segurança está disponível, pela gravidade de CVE mais alta.

- Número de dispositivos que têm pelo menos vulnerabilidades críticas
- Número de dispositivos que têm pelo menos uma ou mais vulnerabilidades altas, médias ou baixas, mas não críticas
- Número de dispositivos que não têm vulnerabilidades conhecidas e são protegidos

Idade do firmware

O cartão Idade do firmware resume a idade do firmware por tipo de componente.

- Número de firmware com mais de 2 anos para cada tipo de componente
- Número de firmware entre 1 e 2 anos para cada tipo de componente
- Número de firmware entre 6 meses e 1 ano para cada tipo de componente
- Número de firmware com menos de 6 meses para cada tipo de componente

Status de funcionamento geral

A placa Estados de Funcionamento Geral resume os dispositivos gerenciados que estão atualmente íntegros e não íntegros em seu ambiente.

Essa placa inclui os dados a seguir.

- Um gráfico circular representando a porcentagem de dispositivos gerenciados que estão em um estado íntegro (normal) e estado não íntegro (crítico, aviso e desconhecido)

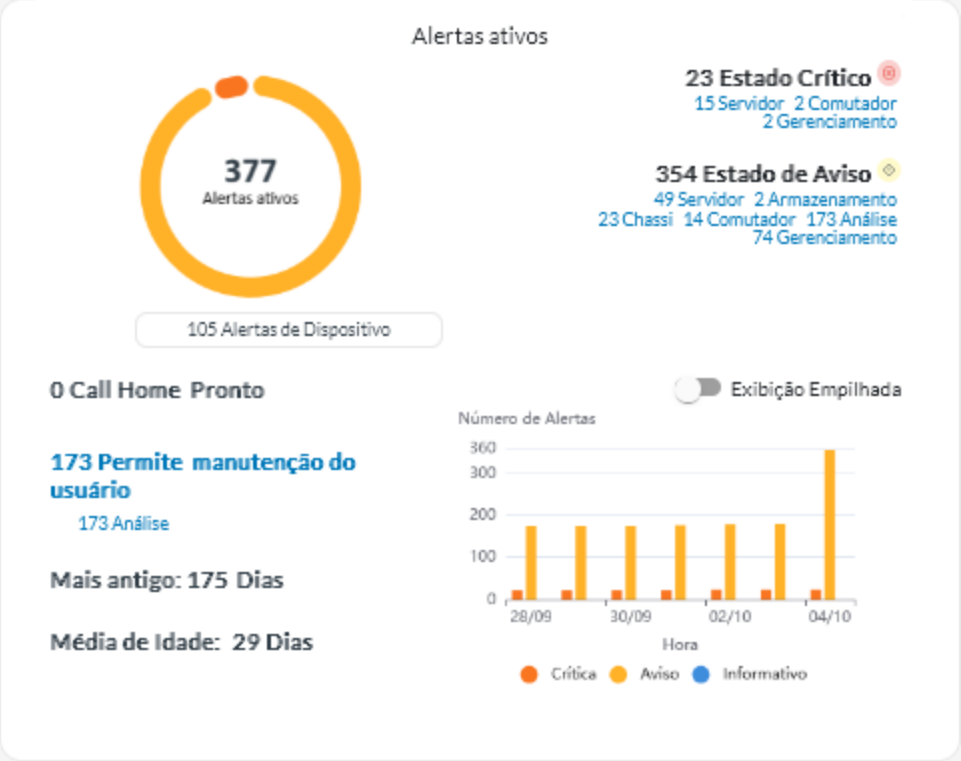
  Dica: cada barra colorida nos gráficos circulares indica o número de dispositivos em um estado específico. É possível passar o mouse sobre cada barra colorida para obter mais informações sobre o estado.
- Número total e porcentagem de dispositivos que estão íntegros e não estão íntegros
- Número de dispositivos de cada tipo que estão atualmente em estados crítico, de aviso, normal e desconhecido

  Dica: é possível clicar no número de dispositivos em um estado específico para abrir uma página com uma lista filtrada de dispositivos que corresponderem aos critérios.
- Um gráfico de linhas que representa o número de dispositivos em estados não íntegros, com o tempo

  Dica: cada barra colorida no gráfico de barras indica o número de dispositivos em um estado específico. É possível passar o mouse sobre cada barra colorida para obter mais informações sobre o estado.

Alertas ativos

A placa Alertas Ativos de Dispositivos resume os alertas ativos gerados pelos dispositivos gerenciados.



Essa placa inclui os dados a seguir.

- Um gráfico circular que representa a porcentagem de alertas ativos para cada gravidade (crítico, aviso, informativo e desconhecido)

  Dica: cada barra colorida nos gráficos circulares indica o número de alertas com uma gravidade específica. É possível passar o mouse sobre cada barra colorida para obter mais informações sobre a gravidade.
- Número total de alertas ativos
- Número de dispositivos que têm alertas ativos
- Número total de alertas ativos para cada severidade e o número de dispositivos de cada tipo que têm alertas ativos para cada severidade

  Dica: é possível clicar no número de dispositivos em um estado específico para abrir uma página com uma lista filtrada de dispositivos que corresponderem aos critérios.
- Um gráfico de linhas que representa o número de dispositivos em estados não íntegros, com o tempo

  Dica: cada barra colorida no gráfico de barras indica o número de alertas com uma gravidade específica. É possível passar o mouse sobre cada barra colorida para obter mais informações sobre a gravidade.
- Número de alertas ativos que abriram um tíquete de serviço com o Centro de Suporte Lenovo (call home)
- Número total de alertas ativos que requerem ação do usuário (podem ser reparados pelo usuário) e o número dispositivos de cada tipo que têm alertas ativos que podem ser reparados pelo usuário
- Duração do alerta ativo mais antigo
- Duração média de todos os alertas ativos

Exibindo o status e os detalhes do gerenciador de recursos

É possível exibir o tipo, a versão, o status e a conectividade de cada gerenciador de recursos.

Sobre esta tarefa

A coluna **Status de Integridade** identifica a integridade geral de um gerenciador de recursos. Os estados de funcionamento a seguir são usados.

- (Normal)
- (Aviso)
- (Crítico)

Procedimento

Para exibir os detalhes dos gerenciadores de recursos, clique em **Recursos (⚙) → Gerenciador de Recursos** na barra de menus do XClarity Orchestrator para exibir a placa Gerenciadores de Recursos.

Depois de concluir

É possível executar as ações a seguir a partir da placa Gerenciadores de Recursos.

- Conecte um gerenciador de recursos clicando no ícone **Conectar** (⊕) (consulte Conectando gerenciadores de recursos).
- Desconecte e remova o gerenciador de recursos selecionado clicando no ícone **Excluir** (🗑).

  Nota: Se o XClarity Orchestrator não puder se conectar ao gerenciador de recursos (por exemplo, se as credenciais estiverem expiradas ou se houver problemas de rede), selecione **Forçar desconexão**.

  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 .)

  Quando o gerenciador de recursos é removido, todos os dispositivos que são gerenciados por esse gerenciador de recursos também são removidos. Isso inclui inventário de dispositivo, logs, dados de métricas e relatórios analíticos.
- Exiba um resumo de status de todos os gerenciadores de recursos ou para um gerenciador de recursos selecionado clicando em **Painel (⊞)** na barra de menus do XClarity Orchestrator. É possível restringir o

escopo a um único gerenciador de recursos ou grupo de recursos usando o menu suspenso **Selecionar gerenciador**.

Exibindo o status dos dispositivos

É possível exibir o status de todos os dispositivos gerenciados em todos os gerenciadores de recursos.

Procedimento

Para exibir o status dos dispositivos gerenciados, conclua as etapas a seguir.

- **Resumo de status de todos os dispositivos**Na barra de menus do XClarity Orchestrator, clique em **Painel ( )** para exibir as placas de painel com uma visão geral e o status de todos os dispositivos gerenciados e outros recursos (consulte Exibindo um resumo do ambiente).

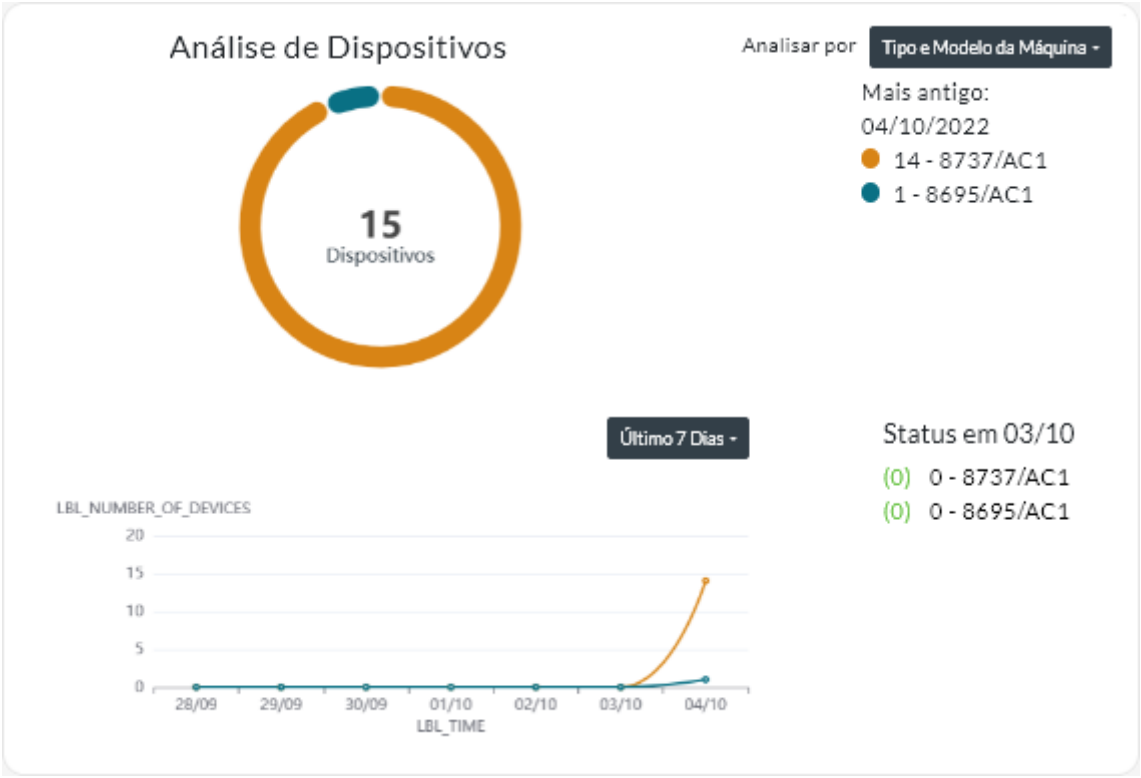
  É possível alterar o escopo do resumo somente para os dispositivos gerenciados por um gerenciador de recursos específico ou em um grupo de recursos específico usando o menu suspenso **Selecionar gerenciador**.

  Cada barra colorida nos gráficos circulares e de barras indica o número de dispositivos em um estado específico. É possível passar o mouse sobre cada barra colorida para obter mais informações sobre o estado. Também é possível clicar no número de dispositivos em cada estado para exibir uma lista de todos os dispositivos que correspondem ao critério.

- **Status de todos os dispositivos de um tipo específico**Para exibir os resumos de alertas ativos, clique em **Recursos** ( ) na barra de menus do XClarity Orchestrator e, em seguida, clique no tipo de dispositivo para exibir uma placa com uma exibição tabular de todos os dispositivos do tipo em questão. Por exemplo, se você selecionar **Servidores**, uma lista de todos os servidores em rack, em torre e densos e todos os servidores Flex System e ThinkSystem em um chassi será exibida.

  É possível alterar o escopo do resumo com base na propriedade do dispositivo na lista suspensa **Analisar por**.
  - **Tipo e Modelo da Máquina**. (padrão) Esse relatório resume a integridade do dispositivo por modelo e tipo de máquina (MTM).

- **Tipo de Máquina**. Esse relatório resume a integridade do dispositivo por tipo de máquina.
- **Nome do Produto**. Esse relatório resume a integridade do dispositivo por produto.



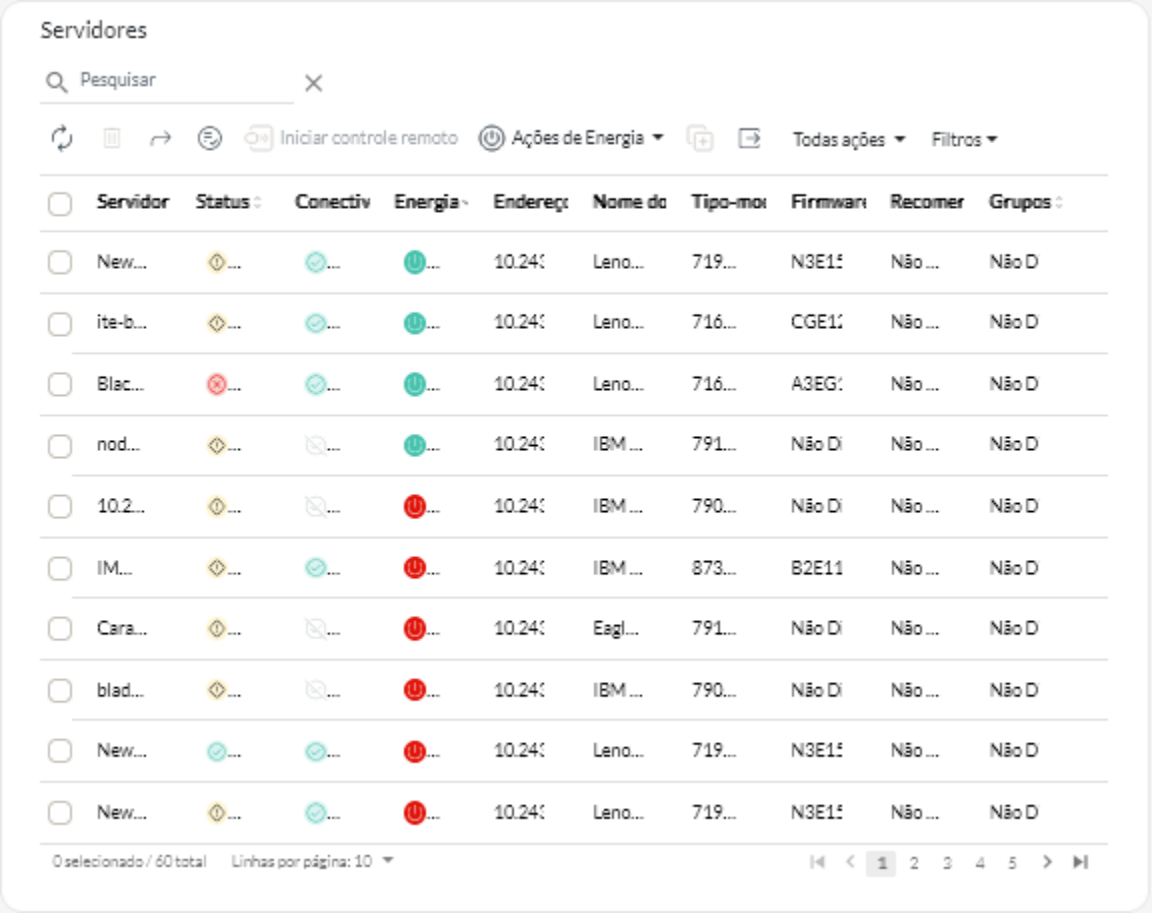
O XClarity Orchestrator resume a integridade do dispositivo com base em critérios específicos. Cada resumo inclui as seguintes informações.

- Um gráfico circular que mostra o número total de dispositivos que não estão íntegros e a porcentagem de dispositivos em cada estado não íntegro (crítico, aviso e desconhecido).

  Cada barra colorida nos gráficos circulares indica o número de dispositivos em um estado específico. É possível passar o mouse sobre cada barra colorida para obter mais informações sobre o estado.
- Um gráfico de linhas que mostra o número de dispositivos em cada estado de integridade por dia ao longo do número especificado de dias.

  Cada barra colorida no gráfico de linhas indica o número de dispositivos em um estado específico. É possível passar o mouse sobre cada barra colorida para obter mais informações sobre o estado.
- O número de dispositivos de cada tipo que não estão íntegros em um dia específico. O dia atual é mostrado por padrão. É possível alterar o dia passando o mouse sobre cada dia no gráfico de linhas.

- **Status de um dispositivo específico**Na barra de menus do XClarity Orchestrator, clique em **Recursos (**) e, em seguida, clique no tipo de dispositivo para exibir uma placa com uma exibição tabular de todos os dispositivos do tipo. Por exemplo, se você selecionar **Servidores**, uma lista de todos os servidores em rack, em torre e densos e todos os servidores Flex System e ThinkSystem em um chassi será exibida.



A coluna **Status** identifica a integridade geral de um dispositivo. Os estados de funcionamento a seguir são usados. Se um dispositivo estiver em um estado não íntegro, use o registro de alertas para identificar e resolver os problemas (consulte Monitorando alertas ativos).

- ( ) Normal
- ( ) Aviso
- ( ) Crítico

A coluna **Conectividade** identifica o status de conexão entre o dispositivo e o XClarity Orchestrator. Os estados de conectividade a seguir são usados.

- ( ) Offline
- ( ) gerenciado Offline
- ( ) Online
- ( ) Parcial
- ( ) Pendente

A coluna **Energia** identifica o status de energia. Os estados de energia a seguir são usados.

- ( ) Ligado
- ( ) Desligado

A coluna **Recomendação** identifica o número de recomendações para o cliente (dicas técnicas) online relacionadas a cada servidor. Clique no número para exibir o cartão Recomendação na página detalhes do dispositivo para exibir uma lista de recomendações para cliente online, incluindo o resumo e o link

para cada recomendação. Clique em um link para abrir uma página da Web com detalhes da recomendação em questão.

Depois de concluir

É possível executar a ação a seguir dos cartões do dispositivo.

- Adicione um dispositivo selecionado a um grupo clicando em **Todas as Ações → Adicionar itens ao Grupo**.
- Encaminhe relatórios sobre tipos de dispositivo específicos de forma recorrente em um ou mais endereços de e-mail clicando no ícone **Criar encaminhador de relatórios** (⊕). O relatório é enviado usando os filtros de dados que estão aplicados atualmente à tabela. Todas as colunas da tabela mostradas e ocultas são incluídas no relatório. Para obter mais informações, consulte Encaminhando relatórios.
- Adicione um relatório sobre um tipo de dispositivo específico a determinado encaminhador de relatório usando os filtros de dados que estão aplicados atualmente à tabela clicando no ícone **Adicionar ao encaminhador de relatórios** (↱). Se o encaminhador de relatórios já incluir um relatório desse tipo de dispositivo, o relatório será atualizado para usar os filtros de dados atuais.

Visualizando detalhes de dispositivos

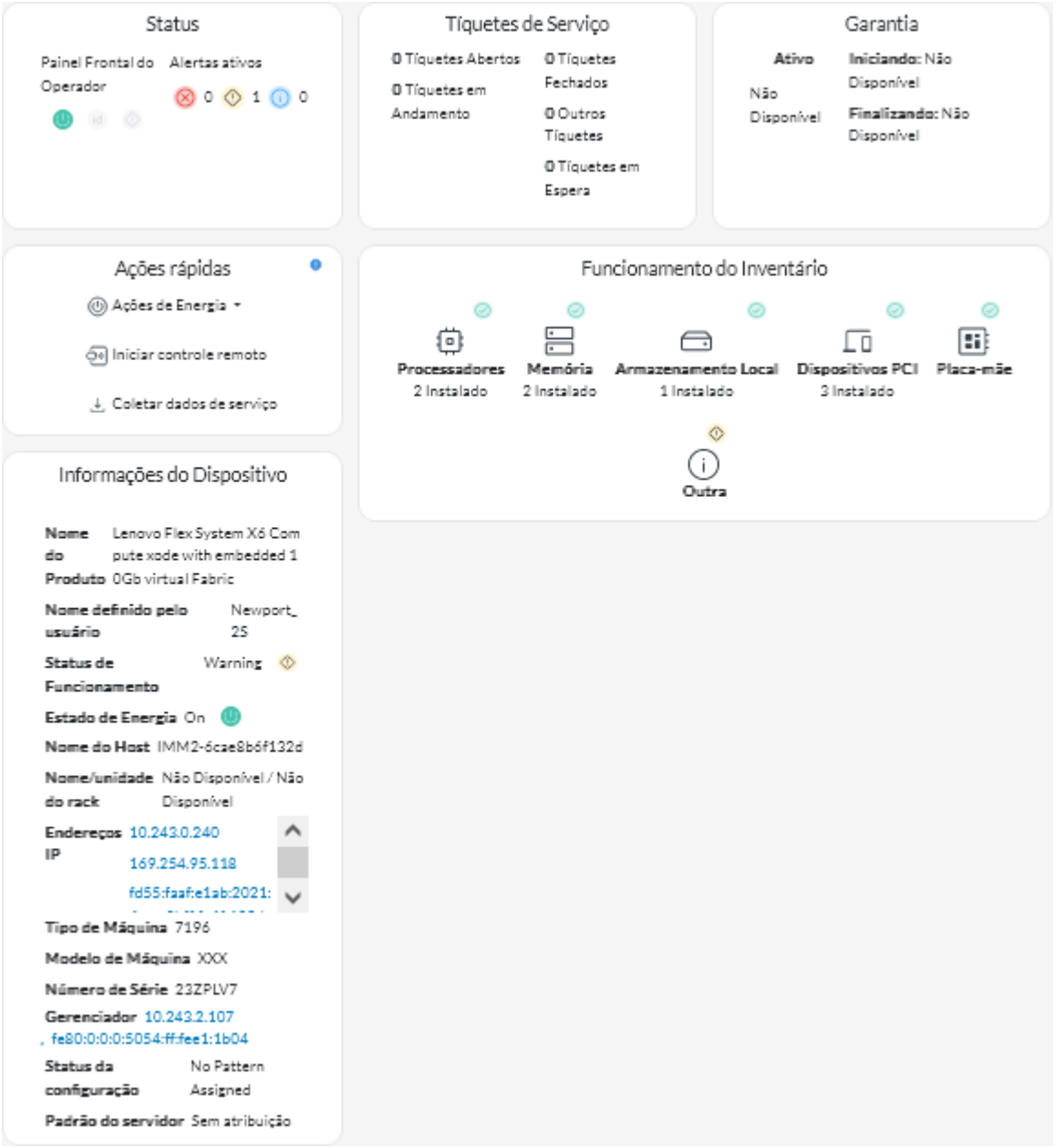
É possível exibir informações detalhadas sobre cada dispositivo, incluindo o resumo geral de integridade e status do dispositivo, recomendação, alertas e eventos, métricas do sistema e firmware.

Procedimento

Para exibir os detalhes de um dispositivo, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Recursos (⚙)** e, em seguida, clique no tipo de dispositivo para exibir uma placa com uma exibição tabular de todos os dispositivos gerenciados do tipo em questão.

Etapa 2. Clique na linha do dispositivo para exibir as placas de resumo desse dispositivo.



Etapa 3. Conclua uma ou mais das seguintes ações.

Os detalhes em cada cartão podem variar dependendo do tipo de dispositivo.

- Clique em **Resumo** para exibir um resumo geral do dispositivo, incluindo informações do dispositivo, inventário, integridade, Informações do SO, métricas do sistema, tíquetes de serviço e garantia. Esta página também inclui o cartão **Ações rápidas** que lista ações que podem ser realizadas no dispositivo (como executar ações de energia, coletar dados de serviço e iniciar uma sessão de controle remoto).Esta página exibe o estado de cada LED no painel do operador frontal.
  - **LED de Energia**
    - **Aceso** ( ). O dispositivo está ligado.
    - **Apagado** ( ). O dispositivo está desligado.

  - **LED de Local**
    - **Aceso** (). O LED de Local no painel de controle está aceso.
    - **Piscando** (). O LED de Local no painel de controle está aceso ou piscando.
    - **Apagado** (). O LED de Local no painel de controle não está aceso.
  - **LED de falha**
    - **Aceso** (). O LED de falha no painel de controle está aceso.
    - **Apagado** (). O LED de Falha no painel de controle não está aceso.
- Clique em **Inventário** para exibir detalhes sobre os componentes de hardware no dispositivo (como processadores, módulos de memória, unidades, fontes de alimentação, ventiladores, dispositivos PCI e placa-mãe).

  Notas:

  - O inventário *não é* suportado para estes dispositivos de armazenamento: ThinkSystem DS2200, Lenovo Storage S2200 e S3200 e Nó de Armazenamento do Flex System V7000.
  - Os detalhes de firmware *não estão* disponíveis para estes dispositivos de armazenamento: ThinkSystem DS4200 e DS6200 e Lenovo Storage DX8200C, DX8200D e DX8200N.
- Clique em **Log de Alertas** para exibir a lista de alertas ativos e estatísticas de alerta do dispositivo (consulte Monitorando alertas ativos).
- Clique em **Log de Eventos** para exibir a lista de eventos do dispositivo (consulte Monitorando eventos).
- Clique em **Firmware** para exibir uma lista de níveis de firmware atuais do dispositivo e de componentes do dispositivo.
- Clique em **Serviço** para exibir informações sobre arquivos de dados de serviço e tíquetes de serviço para o dispositivo.
- Clique em **Utilização** para exibir métricas de utilização, temperatura e energia do sistema ao longo do tempo para dispositivos ThinkAgile e ThinkSystem.
- Clique em **Recomendação** para exibir uma lista de recomendações ao cliente online, incluindo o resumo e o link de cada recomendação. Clique em um link para abrir uma página da Web com detalhes da recomendação em questão.

Depois de concluir

Além de exibir o resumo e informações detalhadas sobre um dispositivo, você pode executar as seguintes ações em um dispositivo nesta página.

- Inicie a interface da Web do Baseboard Management Controller na guia **Resumo** clicando no endereço IP principal do dispositivo.
- Inicie a interface da Web do dispositivo na guia **Resumo** clicando no Endereço IP.
- Inicie a interface da Web do gerenciador de recursos que gerencia os dispositivos na guia **Resumo** clicando no nome ou endereço IP do gerenciador de recursos.

Exibindo o status e os detalhes dos recursos da infraestrutura

É possível exibir o status e informações detalhadas dos recursos de infraestrutura do datacenter (como PDUs e UPSs), que são gerenciados por meio de um gerenciador de recursos do Schneider Electric EcoStruxure IT Expert.

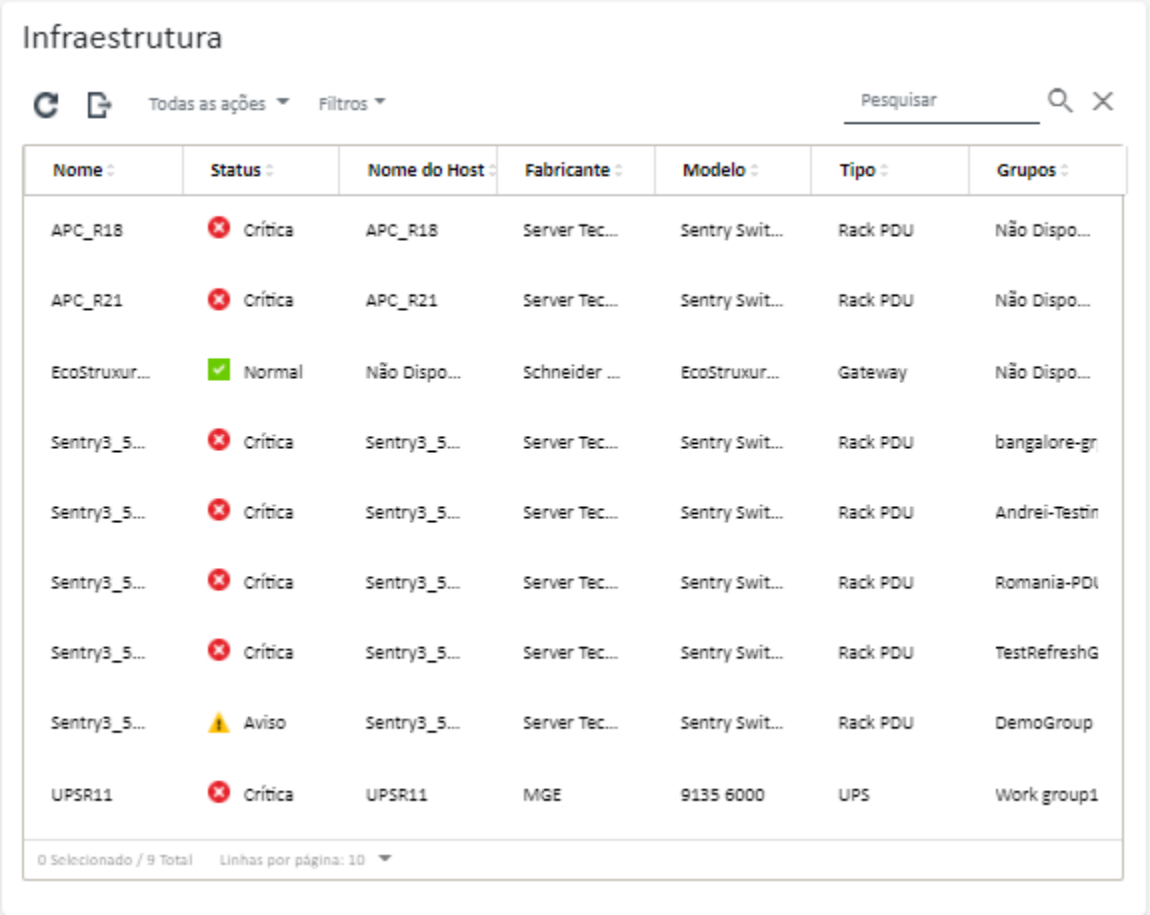
Antes de iniciar

A coluna **Status** identifica o funcionamento geral de um gerenciador de infraestrutura. Os estados de funcionamento a seguir são usados. Se um recurso da infraestrutura estiver em um estado não íntegro, use o log de alertas para identificar e resolver os problemas (consulte Monitorando alertas ativos).

- (🟢) Normal
- (⚠) Aviso
- (🔴) Crítico

Procedimento

- **Status de um recurso de infraestrutura específico**Para exibir o status dos recursos da infraestrutura, clique em **Recursos (⚙) → Infraestrutura** na barra de menus do XClarity Orchestrator para exibir o cartão Infraestrutura. Se um recurso da infraestrutura estiver em um estado não íntegro, use o log de alertas para identificar e resolver os problemas (consulte Monitorando alertas ativos).



- **Detalhes de um recurso de infraestrutura específico**
  1. Na barra de menus do XClarity Orchestrator, clique em **Recursos (⚙) → Infraestrutura** para exibir a placa de infraestrutura.
  2. Clique na linha do recurso da infraestrutura para exibir o cartão de resumo desse recurso.
  3. Conclua uma ou mais das seguintes ações.
     - Clique em **Resumo** para exibir um resumo geral do recurso, incluindo informações e o status do dispositivo.

- Clique em Log de **Alertas** para exibir a lista de alertas ativos e estatísticas de alerta do recurso (consulte Monitorando alertas ativos).
- Clique em Log de **Eventos** para exibir a lista de eventos do recurso (consulte Monitorando eventos).
- Clique em **Sensores** para exibir a lista de sensores no recurso. É possível determinar a medida mais recente do sensor na placa Sensores ou selecionar um ou mais sensores e, em seguida, clicar no ícone **Gráfico** ( ) para visualizar os gráficos de linha ao longo do tempo para cada sensor selecionado. Os sensores com a mesma unidade (como watts ou amps) são representados no mesmo gráfico.

  Nota: Schneider Electric EcoStruxure IT Expert coleta dados do sensor a cada 5 minutos e XClarity Orchestrator sincroniza esses dados a cada hora. Atualmente, o XClarity Orchestrator salva apenas os últimos 60 minutos de dados.

Depois de concluir

Além de exibir o resumo e informações detalhadas sobre um recurso da infraestrutura, você pode executar as seguintes ações nesta página.

- Iniciar a interface da Web de determinados recursos da infraestrutura da guia **Resumo** clicando no endereço IP do recurso.

Monitorando trabalhos

Trabalhos são tarefas demoradas executadas em segundo plano. É possível exibir um log de todos os trabalhos que são iniciados pelo Lenovo XClarity Orchestrator.

Sobre esta tarefa

Se uma tarefa demorada tiver como alvo vários recursos, um trabalho separado será criado para cada recurso.

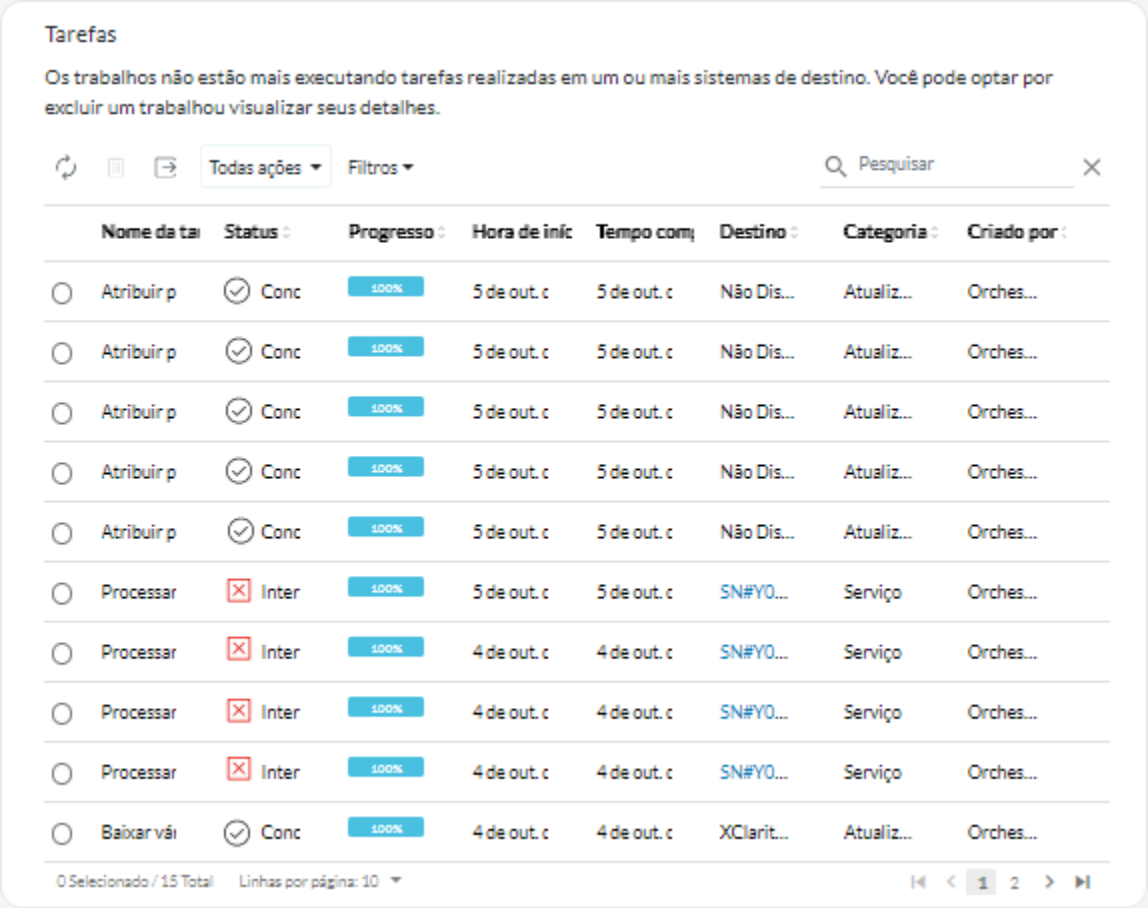
É possível ver o status e os detalhes sobre cada trabalho no log de trabalhos. O log de trabalhos pode conter no máximo 500 trabalhos ou 1 GB. Quando o tamanho máximo for atingido, os trabalhos mais antigos concluídos com êxito serão excluídos. Se não houver nenhum trabalho concluído com êxito no log, os trabalhos mais antigos concluídos com avisos serão excluídos. Se não houver nenhum trabalho concluído com êxito nem com avisos no log, os trabalhos mais antigos concluídos com erros serão excluídos.

Nota: Os trabalhos que estão em execução por mais de 24 horas são interrompidos e colocados no estado Expirado.

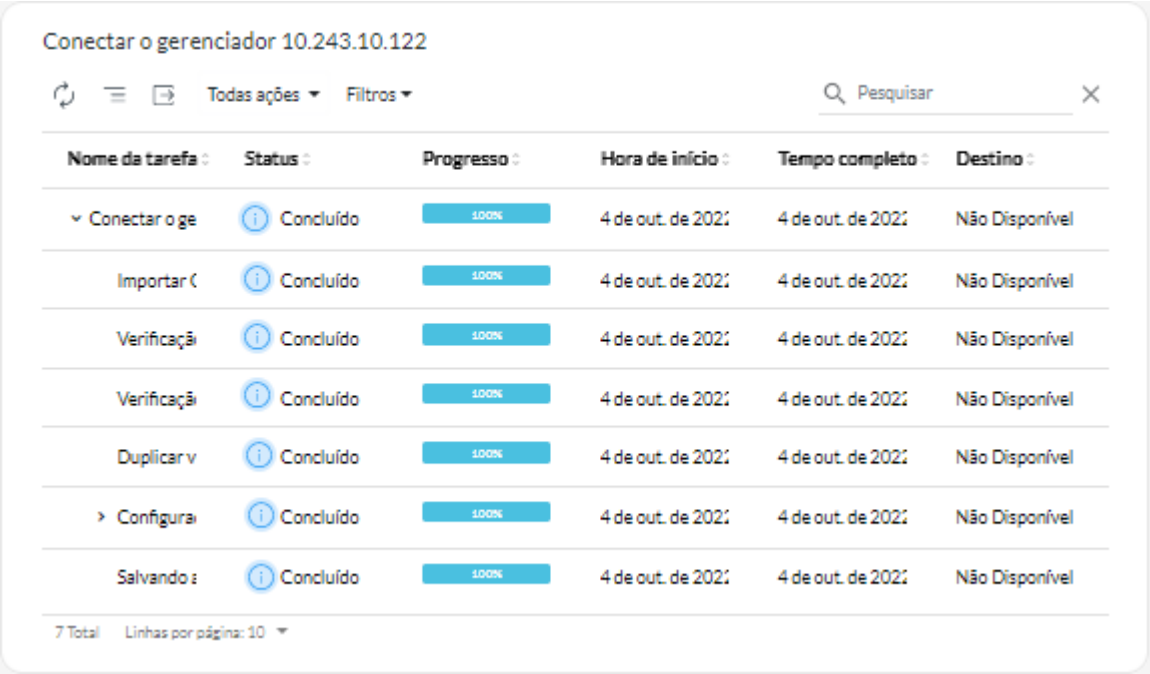
Procedimento

Para exibir trabalhos, conclua uma ou mais das etapas a seguir.

- **Exibir tarefas programadas**Clique em **Monitoramento ( ) → Trabalhos** na barra de menu do XClarity Orchestrator e, em seguida, clique na guia **Tarefas programadas** para exibir o cartão Tarefas programadas. Esta placa lista informações sobre cada tarefa programada, incluindo o status, o carimbo de data e hora em que o trabalho está programado para ser executado e o carimbo de data e hora em que o trabalho foi lançado.
- **Exibir trabalhos**Clique em **Monitoramento ( ) → Trabalhos** na barra de menus do XClarity Orchestrator para exibir o cartão Trabalhos. Este cartão lista informações sobre cada trabalho, incluindo status, progresso, carimbos de data/hora de início e término e recurso de destino.



Para exibir informações detalhadas sobre um trabalho, clique na linha desse trabalho na tabela. Os cartões são exibidos para listar informações sobre cada subtarefa no trabalho (incluindo o status, o progresso, os carimbos de data/hora de início e término, os dispositivos de destino e o log de trabalhos).



Depois de concluir

É possível executar as ações a seguir no cartão Trabalhos.

- Exclua um trabalho ou subtarefa *concluído* ou *expirado* do log de trabalhos selecionando o trabalho ou a tarefa e clicando no ícone **Excluir** (🗑).

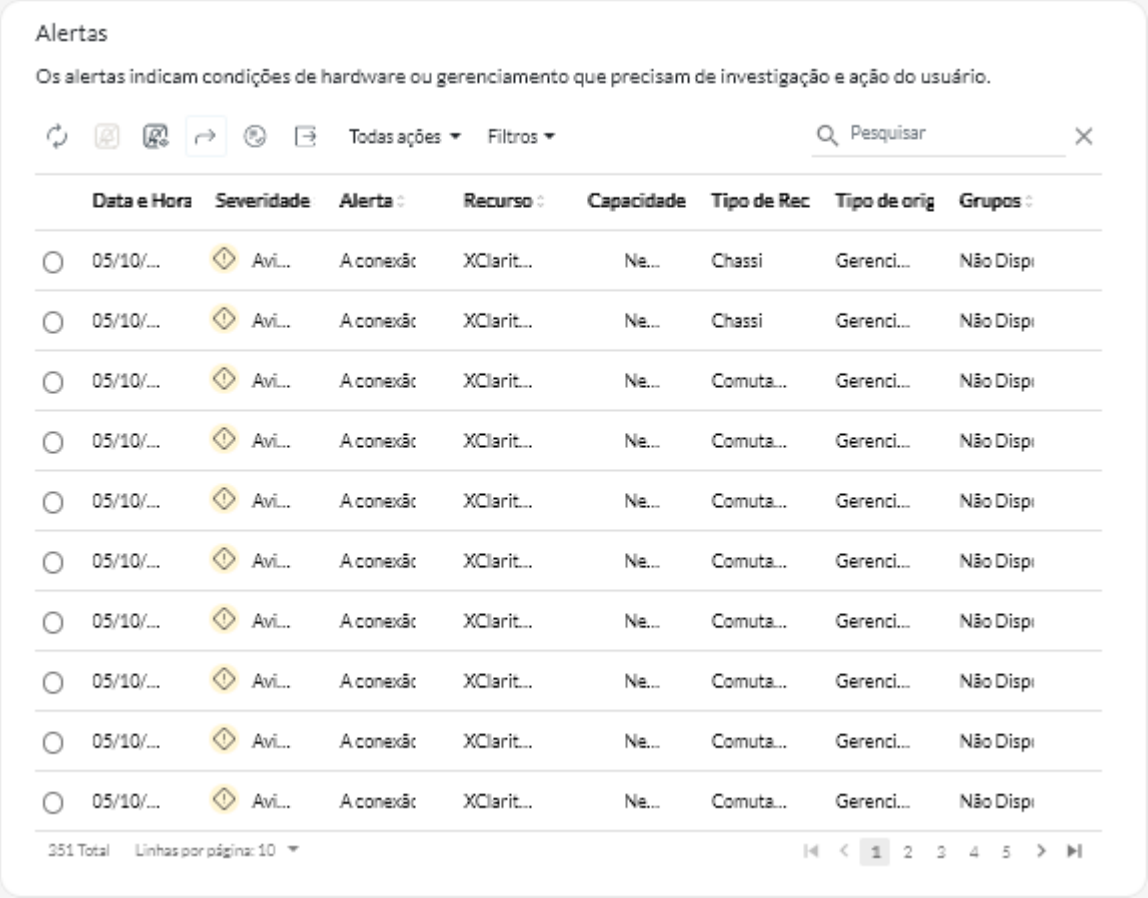
Monitorando alertas ativos

Alertas são eventos de hardware ou do Orchestrator que requerem investigação e ação do usuário. O Lenovo XClarity Orchestrator sonda os gerenciadores de recursos assincronamente e exibe os alertas que são recebidos desses gerenciadores.

Sobre esta tarefa

Não há limite para o número de alertas ativos armazenados no repositório local.

No cartão Alertas, é possível exibir uma lista de todos os alertas ativos.



A coluna **Gravidade** identifica a gravidade do alerta. As seguintes gravidades são usadas.

- (ⓘ) **Informativo**. Nenhuma ação é necessária.
- (⚠) **Aviso**. A ação pode ser adiada ou nenhuma ação é necessária.
- (⊗) **Crítico**. Uma ação imediata é necessária.

A coluna **Capacidade de Manutenção** identifica se o dispositivo requer o serviço e quem normalmente realiza esse serviço. Os tipos de capacidade de manutenção a seguir são usados.

- **Nenhum**. O alerta é informativo e não requer o serviço.
- ( ) **Usuário**. Toma ação de recuperação apropriada para resolver o problema.
- ( ) **Suporte**. Se o Call Home estiver ativado para o XClarity Orchestrator ou para o gerenciador de recursos que gerencia o dispositivo associado, o alerta normalmente será enviado ao Centro de Suporte Lenovo, a menos que um tíquete de serviço aberto para o mesmo ID do alerta já exista para o dispositivo (consulte Abrindo automaticamente tíquetes de serviço usando Call Home na documentação online do XClarity Orchestrator). Se o Call Home não estiver ativado, é recomendável abrir manualmente um tíquete de serviço para resolver o problema (consulte Abrindo manualmente um tíquete de serviço no centro de suporte da Lenovo na documentação online do XClarity Orchestrator).

Se houver alertas ativos, as estatísticas de alerta serão exibidas na placa Análise de Alertas. É possível exibir estatísticas de alerta por gravidade, origem, recurso e capacidade de manutenção para o dia atual e em um período específico (consulte Analisando alertas ativos).

Procedimento

Para exibir alertas ativos, conclua uma ou mais das etapas a seguir.

- **Exibir todos os alertas ativos**Clique em **Monitoramento ( ) → Alertas** na barra de menus do XClarity Orchestrator para exibir o cartão Alertas.

  Para exibir informações sobre um alerta específico, clique na descrição na coluna **Alerta**. Um pop-up é exibido com informações sobre a origem do alerta, explicações e ações de recuperação.
- **Exibir alertas ativos de um dispositivo específico**
  1. Na barra de menus do XClarity Orchestrator, clique em **Recursos ( )** e, em seguida, clique no tipo de dispositivo para exibir uma placa com uma exibição tabular de todos os dispositivos gerenciados do tipo em questão.
  2. Clique na linha de um dispositivo para exibir as placas de resumo desse dispositivo.

3. Clique em **Log de Alertas** para exibir a lista de alertas ativos do dispositivo na placa Análise de Alertas.Para exibir informações sobre um alerta específico, clique na descrição na coluna **Alerta**. Um pop-up é exibido com informações sobre a origem do alerta, explicações e ações de recuperação.

Monitorando eventos

No Lenovo XClarity Orchestrator, você tem acesso a uma lista histórica de todos os eventos de recurso e de auditoria.

Saiba mais:  Como monitorar eventos de um dispositivo específico

Sobre esta tarefa

Um *evento de recurso* identifica uma condição de hardware ou do orquestrador que ocorreu em um dispositivo gerenciado, gerenciador de recursos ou no XClarity Orchestrator. Você pode usar esses eventos para rastrear e analisar problemas relacionados ao hardware e ao servidor do orquestrador.

Um *evento de auditoria* é um registro das atividades do usuário que foram executadas a partir de um gerenciador de recursos ou no XClarity Orchestrator. É possível usar esses eventos de auditoria para rastrear e analisar problemas relacionados à autenticação.

O log de eventos contém eventos de recurso e de auditoria. Ele pode conter no máximo 100.000 eventos de todas as origens. No máximo 50.000 eventos podem ser de um único gerenciador de recursos e de seus dispositivos gerenciados. Um máximo de 1.000 eventos pode ser de um único dispositivo gerenciado. Quando o número máximo de eventos for atingido, o evento mais antigo será descartado quando o próximo evento for recebido.

A coluna **Gravidade** identifica a gravidade do evento. As seguintes gravidades são usadas.

- () **Informativo**. Nenhuma ação é necessária.
- () **Aviso**. A ação pode ser adiada ou nenhuma ação é necessária.
- () **Crítico**. Uma ação imediata é necessária.

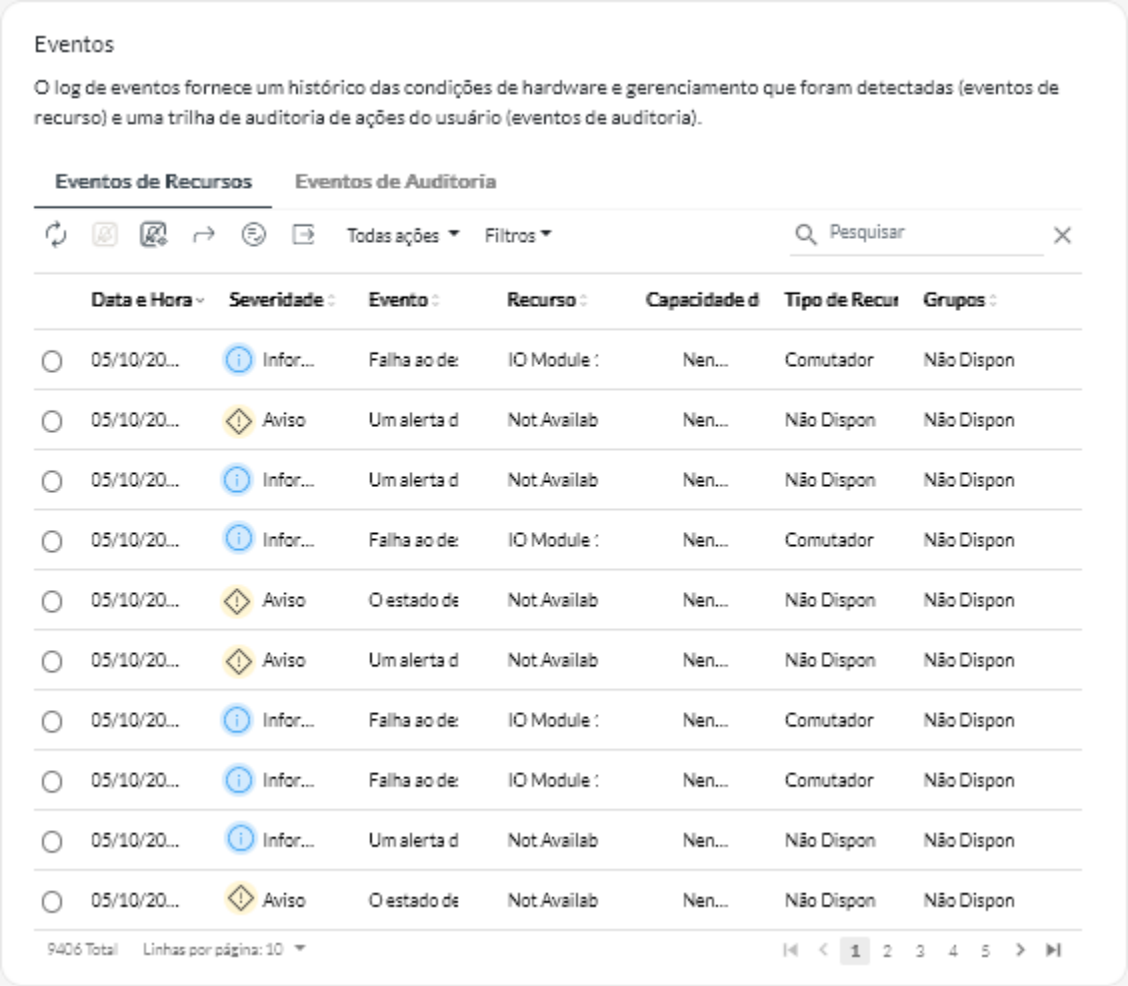
A coluna **Capacidade de Manutenção** identifica se o dispositivo requer o serviço e quem normalmente realiza esse serviço. Os tipos de capacidade de manutenção a seguir são usados.

- **Nenhum**. O alerta é informativo e não requer o serviço.
- () **Usuário**. Toma ação de recuperação apropriada para resolver o problema.
- () **Suporte**. Se o Call Home estiver ativado para o XClarity Orchestrator ou para o gerenciador de recursos que gerencia o dispositivo associado, o alerta normalmente será enviado ao Centro de Suporte Lenovo, a menos que um tíquete de serviço aberto para o mesmo ID do alerta já exista para o dispositivo (consulte Abrindo automaticamente tíquetes de serviço usando Call Home na documentação online do XClarity Orchestrator). Se o Call Home não estiver ativado, é recomendável abrir manualmente um tíquete de serviço para resolver o problema (consulte Abrindo manualmente um tíquete de serviço no centro de suporte da Lenovo na documentação online do XClarity Orchestrator).

Procedimento

Para exibir eventos, conclua uma ou mais das etapas a seguir.

- **Exibir todos os eventos de recurso ou auditoria**Clique em **Monitoramento () → Eventos** na barra de menus do XClarity Orchestrator para exibir a placa Eventos. Em seguida, clique na guia **Eventos de Recurso** ou **Eventos de Auditoria** para exibir as entradas de log.



- **Exibir os eventos de recurso ou de auditoria para um dispositivo específico**
  1. Clique em **Recursos ( )** na barra de menus do XClarity Orchestrator e, em seguida, clique no tipo de dispositivo para exibir uma placa com uma exibição tabular de todos os dispositivos gerenciados do tipo em questão.
  2. Clique na linha de um dispositivo para exibir as placas de resumo desse dispositivo.
  3. Clique na guia **Log de eventos** para exibir a página Eventos desse dispositivo.

Excluindo alertas e eventos

Se houver eventos específicos e alertas ativos que não sejam do seu interesse, você poderá excluir os eventos e os alertas ativos de todas as páginas e resumos em que os eventos e os alertas são exibidos. Os eventos e os alertas excluídos ainda estão no log, mas são ocultos em todas as páginas em que os eventos e os alertas são exibidos, incluindo visualizações de log e status do recurso.

Sobre esta tarefa

Os eventos excluídos são ocultos para todos os usuários, não apenas para o usuário que define a configuração.

Quando você exclui um evento que tem um alerta associado, esse alerta também é excluído.

Procedimento

Conclua as etapas a seguir para excluir alertas e eventos.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Monitoramento** ( ) → **Alertas** ou **Monitoramento** ( ) → **Eventos** para exibir o cartão Alertas ou Eventos.

Etapa 2. Selecione os alertas ou eventos a serem excluídos e clique no ícone **Excluir** ( ). A caixa de diálogo Excluir alertas ou Excluir eventos é exibida.

Etapa 3. Selecione uma das opções a seguir.

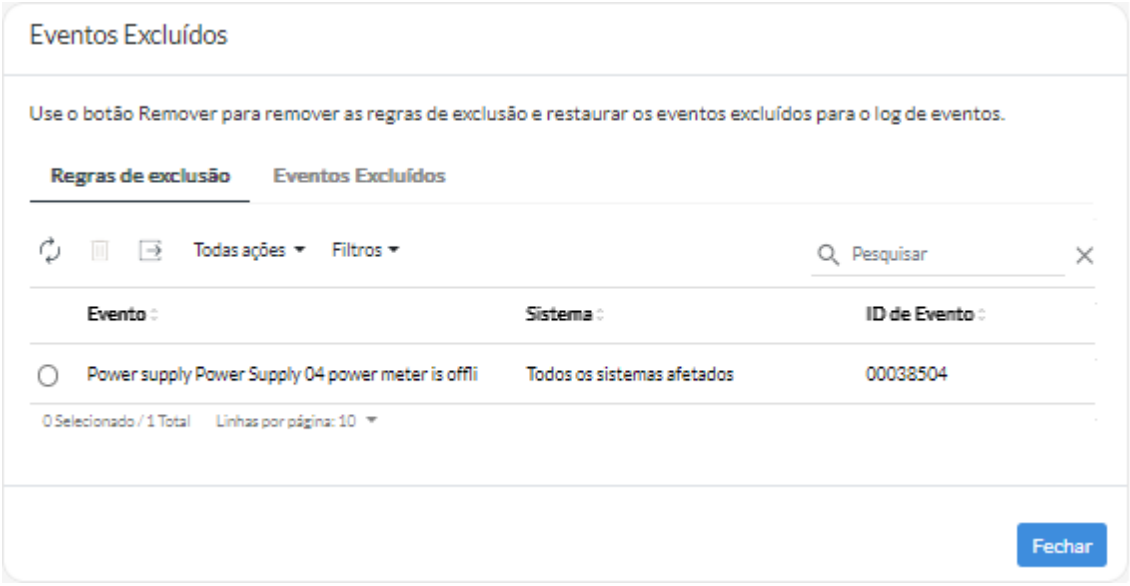
- **Excluir eventos selecionados de todos os dispositivos**. Exclui os eventos selecionados de todos os dispositivos gerenciados.
- **Excluir eventos somente de dispositivos no escopo da instância selecionada**. Exclui os eventos selecionados dos dispositivos gerenciados os quais eventos selecionados se aplicam.

Etapa 4. Clique em **Salvar**.

Depois de concluir

Quando você exclui eventos, o XClarity Orchestrator cria regras de exclusão baseadas em informações fornecidas.

- Exiba uma lista de regras de exclusão e eventos e alertas excluídos clicando no ícone **Exibir Exclusões** ( ) para exibir a caixa de diálogo Alertas excluídos ou Eventos excluídos. Clique na guia **Regras de Exclusão** para exibir as regras de exclusão ou clique na guia **Alertas Excluídos** ou **Eventos Excluídos** para exibir os alertas ou eventos excluídos.



- Restaure os eventos que foram excluídos nos logs removendo a regra de exclusão apropriada. Para remover uma regra de exclusão, clique no ícone **Exibir Exclusões** ( ) para exibir a caixa de diálogo Alertas excluídos ou Eventos excluídos, selecione as regras de exclusão a serem restauradas e clique no ícone **Excluir** ( ).

Encaminhamento de eventos, inventário e dados métricos

Você pode encaminhar dados de evento, inventário e métricas do Lenovo XClarity Orchestrator para aplicativos externos, que podem ser usados para monitorar e analisar dados.

Sobre esta tarefa

Dados de eventos

O XClarity Orchestrator pode encaminhar eventos que ocorrem em seu ambiente para ferramentas externas, com base em critérios (filtros) especificados. Cada evento gerado é monitorado para ver se ele corresponde aos critérios. Se corresponder, o evento será encaminhado para o local especificado usando o protocolo indicado.

O XClarity Orchestrator oferece suporte ao encaminhamento de dados de evento para as ferramentas externas a seguir.

- **E-mail**. O dados do evento são encaminhados para um ou mais endereços de e-mail usando SMTP.
- **Intelligent Insights**. Os dados do evento são encaminhados em um formato predefinido para o SAP Data Intelligence. É possível usar o SAP Data Intelligence para gerenciar e monitorar os dados do evento.
- **REST**. Os dados do evento são encaminhados pela rede para um serviço da Web REST.
- **Syslog**. Os dados do evento são encaminhados na rede para um servidor de log central onde ferramentas nativas podem ser usadas para monitorar o syslog.

O XClarity Orchestrator usa *filtros globais* para definir o escopo dos dados de evento a serem encaminhados. É possível criar filtros de evento para encaminhar somente eventos com propriedades específicas, incluindo códigos de eventos, classes de evento, gravidades de evento e tipos de serviço. Também é possível criar filtros de dispositivo apenas para encaminhar eventos gerados por dispositivos específicos.

Dados de inventário e eventos

O XClarity Orchestrator pode encaminhar todos os dados de inventário e evento para todos os aplicativos externos, que podem ser usados para monitorar e analisar dados.

- **Splunk**. Os dados de eventos são encaminhados em um formato predefinido para um aplicativo Splunk. Em seguida, é possível usar o Splunk para criar diagramas e gráficos baseados nos dados de eventos.É possível definir várias configurações Splunk; no entanto, o XClarity Orchestrator pode encaminhar eventos para apenas uma configuração Splunk. Portanto, apenas uma configuração Splunk pode ser habilitada por vez.

Dados de métricas

O XClarity Orchestrator pode encaminhar dados de métricas que ele coleta sobre dispositivos gerenciados para a ferramenta externa a seguir.

- **TruScale Infrastructure Services**. Os dados de métricas são encaminhados em um formato predefinido para o Lenovo TruScale Infrastructure Services. É possível usar o TruScale Infrastructure Services para gerenciar e monitorar os dados de métricas.

  Atenção: As informações sobre o encaminhador TruScale Infrastructure Services são destinadas apenas a representantes do Serviço Lenovo.

  É possível definir vários encaminhadores TruScale Infrastructure Services; no entanto, o XClarity Orchestrator pode encaminhar dados de métricas para apenas um encaminhador TruScale Infrastructure Services. Portanto, apenas um encaminhador TruScale Infrastructure Services pode ser ativado por vez.

  Saiba mais: Conheça o Lenovo TruScale Infrastructure Services

Procedimento

Conclua as seguintes etapas para encaminhar os dados.

Etapa 1. **Crie um destino do encaminhador.**

Destinos de encaminhador são configurações comuns que podem ser usadas por vários encaminhadores de dados. O destino do encaminhador identifica onde os dados devem ser enviados para um tipo específico de encaminhador.

Etapa 2. **Crie filtros de evento e recursos (apenas para encaminhadores de evento).**

É possível atribuir *filtros comuns de encaminhamento de dados* a vários encaminhadores de dados. Esses filtros são usados para definir critérios específicos para determinar quais eventos encaminhar para quais recursos.

Se você não atribuir filtros ao encaminhador de dados, todos os eventos para todos os recursos serão encaminhados para o destino do encaminhador selecionado.

Etapa 3. **Crie e ative um encaminhador de dados.**

É possível criar e ativar encaminhadores de dados para encaminhar dados de evento para um aplicativo externo específico. Você deve escolher um destino de encaminhador que seja aplicável ao tipo de encaminhador que você está criando.

Criando filtros de encaminhamento de dados

Você pode definir *filtros de encaminhamento de dados* comuns que podem ser usados por vários encaminhadores para acionar o encaminhamento de dados que corresponda a critérios específicos.

Sobre esta tarefa

É possível criar os tipos de filtro a seguir.

- *Filtros de eventos* encaminham eventos que correspondem a códigos de evento específicos ou propriedades (como classes de evento, gravidades de evento e tipos de serviço)
  - Todos os códigos e propriedades se aplicam a todas as fontes de eventos.
  - Se nenhuma propriedade de classe estiver selecionada, será feita a correspondência com todas as propriedades.
  - Se nenhuma propriedade que permite manutenção estiver selecionada, será feita a correspondência com todas as propriedades que permitem manutenção.
  - Se nenhuma propriedade de gravidade estiver selecionada, será feita a correspondência com todas as propriedades de gravidade.
  - Se nenhum código de evento estiver especificado, será feita a correspondência com todos os códigos de evento.
- Os *filtros de recursos* encaminham dados gerados por recursos específicos (XClarity Orchestrator, gerenciadores de recursos e dispositivos). É possível escolher um subconjunto de recursos selecionando um ou mais grupos de recursos.
  - Se um tipo de recurso estiver desabilitado, nenhum dado desse tipo de recurso será encaminhado.
  - Se um tipo de recurso estiver habilitado e nenhum grupo estiver selecionado, todos os dados desse tipo de recurso serão encaminhados.
  - Se um tipo de recurso estiver habilitado e um ou mais grupos estiverem selecionados, somente os dados gerados pelos recursos nos grupos selecionados serão encaminhados.

Você pode reutilizar os filtros de recursos e de eventos em vários encaminhadores; no entanto, você pode adicionar no máximo um filtro de eventos e um filtro de recursos a cada encaminhador.

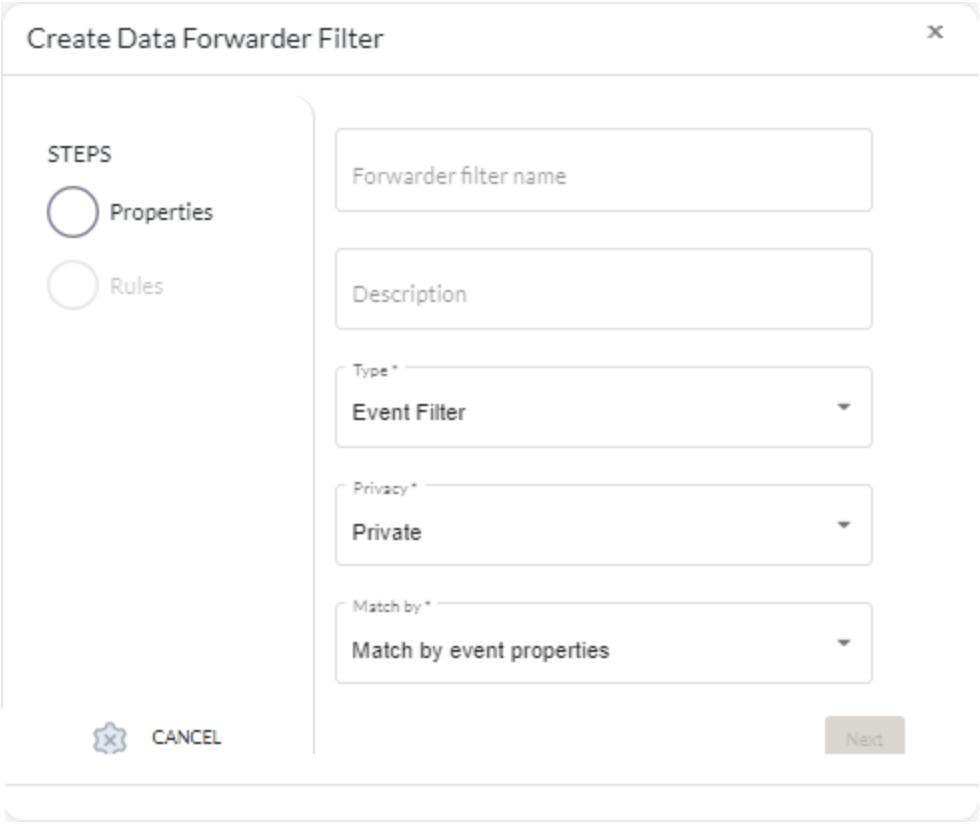
Procedimento

Para criar um filtro de encaminhamento de dados, conclua uma das etapas a seguir dependendo do tipo de filtro que você deseja criar.

- **Filtros de eventos**

1. Na barra de menus do XClarity Orchestrator, clique em **Monitoramento ( ) → Encaminhamento** e clique em **Filtros do Encaminhador de Dados** na navegação esquerda para exibir o cartão Filtros de encaminhador de dados.

2. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Criar filtro de encaminhador de dados.



3. Especifique o nome do filtro e a descrição opcional.
4. Selecione **Filtro de eventos** como o tipo de filtro.
5. Selecione o tipo do privacidade.
   - **Privado**. Somente o usuário que criou o filtro pode usá-lo.

– **Público**. Qualquer usuário pode usar o filtro.

6. Escolha Propriedades de evento ou códigos de eventos como critérios para esse filtro.
7. Clique em **Regras** e selecione os critérios para esse filtro com base no tipo de critério selecionado na etapa anterior.
   – **Corresponder eventos por propriedades**. Selecione uma ou mais gravidade, capacidade de manutenção e propriedades de classe. Somente eventos que correspondem às propriedades selecionadas são encaminhados.Por exemplo, se você escolher aviso e gravidades críticas, classes de adaptador e memória, os dados de evento serão encaminhados apenas para eventos de memória de aviso, eventos de memória críticos, eventos do adaptador de aviso e eventos críticos do adaptador, independentemente da capacidade de manutenção do evento. Se você selecionar somente a capacidade de manutenção do usuário, os dados do evento serão encaminhados apenas para os eventos com capacidade de manutenção, independentemente da gravidade ou da classe.

     Notas:
     – Se você não selecionar uma propriedade de classe, será feita a correspondência com todas as propriedades de classe.
     – Se você não selecionar uma propriedade com capacidade de manutenção, será feita a correspondência com todas as propriedades com capacidade de manutenção
     – Se você não selecionar uma propriedade de gravidade, será feita a correspondência com todas as propriedades de gravidade.

   – **Faça a correspondência dos eventos por código**. Insira um código de evento que você deseja filtrar e, em seguida, clique no ícone **Adicionar** (⊕) para adicionar o código de evento à lista. Repita o procedimento para cada código de evento que você deseja adicionar. É possível excluir um código de evento clicando no ícone **Excluir** (🗑) ao lado do código específico.Somente eventos que correspondam a um dos códigos de evento listados são encaminhados.

     É possível especificar um código de evento completo ou parcial. Por exemplo, FQXXOCO0001I corresponde ao evento específico, FQXXOSE corresponde a todos os eventos de segurança do XClarity Orchestrator e CO001 corresponde a todos os eventos que contêm esses caracteres.

     Se você não especificar um código de evento, será feita a correspondência com todos os códigos de evento.

     Para encontrar uma lista de códigos de eventos disponíveis, consulte na documentação online do XClarity Orchestrator.
8. Clique em **Criar** para criar o filtro.O filtro é adicionado à tabela.

- **Filtros de recursos**
  1. Na barra de menus do XClarity Orchestrator, clique em **Monitoramento (📈) → Encaminhamento** e clique em **Filtros do Encaminhador de Dados** na navegação esquerda para exibir o cartão Filtros de encaminhador de dados.
  2. Clique no ícone **Criar** (⊕) para exibir a caixa de diálogo Criar filtro de encaminhador de dados.
  3. Especifique o nome do filtro e a descrição opcional.
  4. Selecione **Filtro de recursos** como o tipo de filtro.
  5. Selecione o tipo do privacidade.
     – **Privado**. Somente o usuário que criou o filtro pode usá-lo.
     – **Público**. Qualquer usuário pode usar o filtro.
  6. Clique em **Recursos** e selecione a origem de eventos para esse filtro.
     – **Faça a correspondência com todos os eventos do XClarity Orchestrator**. Encaminha eventos gerados por este XClarity Orchestrator. Essa opção é desativada por padrão.

- **Faça a correspondência com todos os eventos de gerenciador de recursos**. Encaminha eventos que são gerados por um gerenciador de recursos. Essa opção é desativada por padrão.
  - Se você desabilitar essa opção, os eventos não serão encaminhados de nenhum gerenciador de recursos.
  - Se você habilitar essa opção, mas não selecionar nenhum grupo de gerentes, os eventos gerados por todos os gerenciadores de recursos serão encaminhados.
  - Se você habilitar essa opção e selecionar ou mais grupos de gerenciadores, os eventos gerados apenas por gerenciadores de recursos nos grupos selecionados serão encaminhados.

  Dica: é possível criar grupos de gerenciadores a partir dessa placa clicando no ícone **Criar** (⊕).
- **Faça a correspondência com todos os eventos de dispositivo**. Encaminha eventos gerados por um dispositivo. Essa opção é ativada por padrão.
  - Se você desabilitar essa opção, os eventos não serão encaminhados de nenhum dispositivo.
  - Se você habilitar essa opção, mas não selecionar nenhum grupo de dispositivos, os eventos gerados por todos os dispositivos serão encaminhados.
  - Se você habilitar essa opção e selecionar ou mais grupos de dispositivos, os eventos gerados apenas por dispositivos nos grupos selecionados serão encaminhados.

  Dica: é possível criar grupos de dispositivos a partir dessa placa clicando no ícone **Criar** (⊕).

7. Clique em **Criar** para criar o filtro.O filtro é adicionado à tabela.

Depois de concluir

Você pode executar a seguinte ação no cartão Filtros do Encaminhador de Dados.

- Remova um filtro selecionado clicando no ícone **Excluir** (🗑).Não é possível excluir um filtro atribuído a um encaminhador.

Encaminhando eventos para o SAP Data Intelligence

É possível configurar o Lenovo XClarity Orchestrator para encaminhar eventos para o SAP Data Intelligence (Intelligent Insights).

Antes de iniciar

Atenção: A conexão entre o XClarity Orchestratore o SAP Data Intelligence usa o transporte criptografado, mas não verifica o certificado TLS do sistema remoto.

Sobre esta tarefa

Se o controle de acesso baseado em recursos estiver ativado, os dados serão encaminhados apenas para os recursos que você pode acessar usando listas de controle de acesso. Se você não for um membro de um grupo ao qual a função predefinida de **Supervisor** é atribuída, deverá atribuir uma ou mais listas de controle de acesso aos encaminhadores que você criar. Se desejar enviar dados para todos os recursos que você pode acessar, selecione todas as listas de controle de acesso associadas que estão disponíveis para você. Se você for um membro de um grupo ao qual a função predefinida de **Supervisor** é atribuída, poderá optar por enviar dados para todos os recursos ou por atribuir listas de controle de acesso para limitar os recursos.

Não é possível filtrar dados encaminhados para o SAP Data Intelligence.

O exemplo a seguir mostra o formato padrão dos dados encaminhados para o SAP Data Intelligence. Palavras entre colchetes duplos são atributos substituídos por valores reais quando os dados são encaminhados.

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
```

```
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

Procedimento

Para encaminhar dados de eventos para o SAP Data Intelligence, conclua as seguintes etapas.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Monitoramento** (📈) → **Encaminhamento** e clique em **Encaminhadores de Dados** na navegação esquerda para exibir o cartão Encaminhadores de Dados.

Etapa 2. Clique no ícone **Criar** (⊕) para exibir a caixa de diálogo Criar Encaminhador de Dados.

Etapa 3. Especifique o nome do encaminhador e a descrição opcional.

Etapa 4. Escolha para habilitar ou desabilitar o encaminhador clicando no botão de alternância **Estado**.

Etapa 5. Selecione **Intelligent Insights** como o tipo de encaminhador.

Etapa 6. Clique em **Configuração** e preencha as informações específicas do protocolo.

- Insira o nome do host ou endereço IP do SAP Data Intelligence.
- Insira a porta a ser usada para o encaminhamento de eventos. O padrão é `443`.
- Insira o caminho do recurso em que o encaminhador deve publicar os eventos (por exemplo, /rest/test).
- Selecione o método REST. Este pode ser um dos valores a seguir.
  - **PUT**
  - **POST**
- Selecione o protocolo a ser usado para o encaminhamento de eventos. Este pode ser um dos valores a seguir.
  - **HTTP**
  - **HTTPS**
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é `30` segundos.
- Se a autenticação for necessária, selecione um dos tipos de autenticação a seguir.
  - **Básico**. Autentica para o servidor especificado usando o tenant, a ID do usuário e a senha especificados.
  - **Token**. Autentica para o servidor especificado usando o nome de cabeçalho e valor do token especificado

Etapa 7. Clique em **Listas de Controle de Acesso** e selecione uma ou mais listas de controle de acesso que você deseja associar a esse encaminhador.

Se o acesso baseado em recursos estiver habilitado, você deverá selecionar pelo menos uma lista de controle de acesso.

Dica: como opção, os usuários que são membros de um grupo ao qual a função predefinida de **Supervisor** é atribuída podem selecionar **Associar tudo** em vez de selecionar listas de controle de acesso para que os dados encaminhados não sejam restritos.

Etapa 8. Clique em **Criar** para criar o encaminhador.

Depois de concluir

Você pode executar as seguintes ações no cartão Encaminhadores de Dados.

- Ative ou desative um encaminhador selecionado clicando no botão de alternância na coluna **Estado**
- Modifique um encaminhador selecionado clicando no ícone **Editar** ( ).
- Remova um encaminhador selecionado clicando no ícone **Excluir** ( ).

Encaminhando eventos para um serviço Web REST

É possível configurar o Lenovo XClarity Orchestrator para encaminhar eventos específicos a um serviço da Web REST.

Antes de iniciar

Atenção: Uma conexão segura não é estabelecida ao encaminhar dados para esse serviço. Os dados são enviados por um protocolo de texto claro.

Sobre esta tarefa

Se o controle de acesso baseado em recursos estiver ativado, os dados serão encaminhados apenas para os recursos que você pode acessar usando listas de controle de acesso. Se você não for um membro de um grupo ao qual a função predefinida de **Supervisor** é atribuída, deverá atribuir uma ou mais listas de controle de acesso aos encaminhadores que você criar. Se desejar enviar dados para todos os recursos que você pode acessar, selecione todas as listas de controle de acesso associadas que estão disponíveis para você. Se você for um membro de um grupo ao qual a função predefinida de **Supervisor** é atribuída, poderá optar por enviar dados para todos os recursos ou por atribuir listas de controle de acesso para limitar os recursos.

Os *filtros de encaminhamento de dados* são usados para definir o escopo de eventos que você deseja encaminhar, com base em códigos de evento, classes de evento, severidades de evento, tipos de serviço e no recurso que gerou o evento. Certifique-se de que os filtros de eventos e de recursos que você deseja usar para este encaminhador já estejam criados (consulte Criando filtros de encaminhamento de dados).

O exemplo a seguir mostra o formato padrão dos dados encaminhados para um serviço da Web REST. Palavras entre colchetes duplos são atributos substituídos por valores reais quando os dados são encaminhados.

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

Procedimento

Para encaminhar dados a um serviço Web REST, conclua as seguintes etapas.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Monitoramento** ( ) → **Encaminhamento** e clique em **Encaminhadores de Dados** na navegação esquerda para exibir o cartão Encaminhadores de Dados.

Etapa 2. Clique no ícone **Criar** (⊕) para exibir a caixa de diálogo Criar Encaminhador de Dados.

Etapa 3. Especifique o nome do encaminhador e a descrição opcional.

Etapa 4. Escolha para habilitar ou desabilitar o encaminhador clicando no botão de alternância **Estado**.

Etapa 5. Selecione **REST** como o tipo de encaminhador.

Etapa 6. Clique em **Configuração** e preencha as informações específicas do protocolo.

- Inclua o nome do host ou o endereço IP do servidor REST.
- Insira a porta a ser usada para o encaminhamento de eventos. O padrão é `80`.
- Insira o caminho do recurso em que o encaminhador deve publicar os eventos (por exemplo, /rest/test).
- Selecione o método REST. Este pode ser um dos valores a seguir.
  - **PUT**
  - **POST**
- Selecione o protocolo a ser usado para o encaminhamento de eventos. Este pode ser um dos valores a seguir.
  - **HTTP**
  - **HTTPS**
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.
- Se a autenticação for necessária, selecione um dos tipos de autenticação a seguir.
  - **Básico**. Autentica ao servidor especificado usando o ID do usuário e senha especificados.
  - **Token**. Autentica para o servidor especificado usando o nome de cabeçalho e valor do token especificado.

Etapa 7. Clique em **Filtros** e, como opção, selecione os filtros que você deseja usar para este encaminhador.

É possível selecionar no máximo um filtro de eventos e um filtro de recursos.

Se você não selecionar um filtro, os dados serão encaminhados para todos os eventos gerados por todos os recursos (dispositivos, gerenciadores de recursos e o XClarity Orchestrator).

Nessa guia, também é possível optar por encaminhar o evento excluído definindo o botão de alternância **Eventos Excluídos** como **Sim**.

Etapa 8. Clique em **Listas de Controle de Acesso** e selecione uma ou mais listas de controle de acesso que você deseja associar a esse encaminhador.

Se o acesso baseado em recursos estiver habilitado, você deverá selecionar pelo menos uma lista de controle de acesso.

Dica: como opção, os usuários que são membros de um grupo ao qual a função predefinida de **Supervisor** é atribuída podem selecionar **Associar tudo** em vez de selecionar listas de controle de acesso para que os dados encaminhados não sejam restritos.

Etapa 9. Clique em **Criar** para criar o encaminhador.

Depois de concluir

Você pode executar as seguintes ações no cartão Encaminhadores de Dados.

- Ative ou desative um encaminhador selecionado clicando no botão de alternância na coluna **Estado**
- Modifique um encaminhador selecionado clicando no ícone **Editar** (✎).
- Remova um encaminhador selecionado clicando no ícone **Excluir** (🗑).

Encaminhando eventos para um serviço de email usando SMTP

É possível configurar o Lenovo XClarity Orchestrator para encaminhar eventos específicos para um ou mais endereços de e-mail usando SMTP.

Antes de iniciar

Atenção: Uma conexão segura não é estabelecida ao encaminhar dados para esse serviço. Os dados são enviados por um protocolo de texto claro.

Para encaminhar o e-mail para um serviço e-mail baseado na Web (como Gmail, Hotmail ou Yahoo), o servidor SMTP deve dar suporte ao encaminhamento do e-mail da Web.

Antes de configurar um encaminhador de eventos para um serviço Web do Gmail, revise as informações no Encaminhando eventos para um serviço SMTP Gmail.

Sobre esta tarefa

Se o controle de acesso baseado em recursos estiver ativado, os dados serão encaminhados apenas para os recursos que você pode acessar usando listas de controle de acesso. Se você não for um membro de um grupo ao qual a função predefinida de **Supervisor** é atribuída, deverá atribuir uma ou mais listas de controle de acesso aos encaminhadores que você criar. Se desejar enviar dados para todos os recursos que você pode acessar, selecione todas as listas de controle de acesso associadas que estão disponíveis para você. Se você for um membro de um grupo ao qual a função predefinida de **Supervisor** é atribuída, poderá optar por enviar dados para todos os recursos ou por atribuir listas de controle de acesso para limitar os recursos.

Os *filtros de encaminhamento de dados* são usados para definir o escopo de eventos que você deseja encaminhar, com base em códigos de evento, classes de evento, severidades de evento, tipos de serviço e no recurso que gerou o evento. Certifique-se de que os filtros de eventos e de recursos que você deseja usar para este encaminhador já estejam criados (consulte Criando filtros de encaminhamento de dados).

O exemplo a seguir mostra o formato padrão dos dados encaminhados para um serviço de e-mail. Palavras entre colchetes duplos são atributos substituídos por valores reais quando os dados são encaminhados.

Assunto do e-mail

```
Event Forwarding
```

Corpo do e-mail

```
{
   "groups": [],
   "acls": [],
   "local": null,
   "eventID": "FQXHMEM0216I",
   "severity": "Warning",
   "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
   "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
   "msg": "The event forwarder destination cannot be reached. Therefore new events are not being
          forwarded.",
   "description": "The event forwarder destination cannot be reached. Therefore new events are not
                   being forwarded.",
   "userAction": "Look in the online documentation to determinate more information about this event
                  based on the eventID. At the moment the orchestrator server can not offer more
                  information.",
   "recoveryURL": null,
   "flags": [],
   "userid": null,
   "action": "None",
   "eventClass": "System",
```

```
    "args": [],
    "service": "None",
    "lxcaUUID": "23C87F0A2CB6491097489193447A655C",
    "managerID": "23C87F0A2CB6491097489193447A655C",
    "failFRUNumbers": null,
    "failFRUSNs": null,
    "failFRUUUIDs": "[FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF]",
    "msgID": null,
    "timeStamp": "2021-03-12T18:32:14.000Z",
    "eventDate": "2021-03-12T18:32:14Z",
    "commonEventID": "FQXHMEM0216I",
    "sequenceNumber": "17934247",
    "details": null,
    "device": {
       "name": "xhmc194.labs.lenovo.com",
       "mtm": null,
       "serialNumber": null
    },
    "resourceType": "XClarity Administrator",
    "componentType": "XClarity Administrator",
    "sourceType": "Management",
    "resourceName": "xhmc194.labs.lenovo.com",
    "fruType": "other",
    "ipAddress": "10.243.2.107",
    "_id": 252349
}
```


Procedimento

Para encaminhar dados a um serviço de e-mail usando SMTP, conclua as seguintes etapas.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Monitoramento (📈) → Encaminhamento** e clique em **Encaminhadores de Dados** na navegação esquerda para exibir o cartão Encaminhadores de Dados.

Etapa 2. Clique no ícone **Criar** (⊕) para exibir a caixa de diálogo Criar Encaminhador de Dados.

Etapa 3. Especifique o nome do encaminhador e a descrição opcional.

Etapa 4. Escolha para habilitar ou desabilitar o encaminhador clicando no botão de alternância **Estado**.

Etapa 5. Selecione **E-mail** como o tipo de encaminhador.

Etapa 6. Clique em **Configuração** e preencha as informações específicas do protocolo.

- Inclua o nome do host ou o endereço IP do servidor SMTP.
- Insira a porta a ser usada para o encaminhamento de eventos. O padrão é `25`.
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é `30` segundos.
- Insira o endereço de e-mail para cada destinatário. Separe diversos endereços de e-mail usando uma vírgula.
- **Opcional:** insira o endereço de e-mail do remetente (por exemplo, john@company.com) e o domínio do remetente. Se você não especificar um endereço de e-mail, o endereço do remetente será LXCO.<*source_identifier*>@<*smtp_host*> por padrão.

  Se você especificar apenas o domínio do remetente, o formato do endereço do remetente será <*LXCO_host_name*>@<*sender_domain*> (por exemplo, XClarity1@company.com).

  Notas:

  – Se você configurou o servidor SMTP para requerer um nome do host para encaminhar e-mail e não configurou um nome do host para XClarity Orchestrator, é possível que o servidor

SMTP descarte os eventos encaminhados. Se o XClarity Orchestrator não tiver um nome do host, o evento será encaminhado com o endereço IP. Se o endereço IP não pode ser obtido, o "localhost" é enviado no seu lugar, o que pode fazer com que o servidor SMTP descarte o evento.

  - Se você especificar o domínio do remetente, a origem não identificará o endereço do remetente. Ao invés disso, as informações sobre a origem do evento serão incluídas no corpo do e-mail, incluindo o nome do sistema, endereço IP, tipo/modelo e o número de série.
  - Se o servidor SMTP só aceita e-mails que foram enviados por um usuário registrado, o endereço padrão do remetente (`LXCO.<source_identifier}@{smtp_host>`) é rejeitado. Nesse caso, você deve especificar pelo menos um nome de domínio no campo **Do Usuário**.

- Para estabelecer uma conexão segura com o servidor SMTP, selecione um dos tipos de conexão a seguir.
  - **SSL**. Usa o protocolo SSL para formar uma comunicação segura.
  - **STARTTLS**. Usa o protocolo TLS para formar uma comunicação segura em um canal não seguro.

  Se um destes tipos de conexão for selecionado, o XClarity Orchestrator tentará baixar e importar o certificado do servidor SMTP para seu armazenamento confiável do XClarity Orchestrator. Você será solicitado a aceitar esse certificado.
- Se a autenticação for necessária, selecione um dos tipos de autenticação a seguir.
  - **Regular**. Autentica ao servidor SMTP especificado usando o ID do usuário e senha especificados.
  - **OAUTH2**. Usa protocolo SASL (Simple Authentication and Security Layer) para autenticar o servidor SMTP especificado usando o nome de usuário e o token de segurança especificados. Normalmente, o nome do usuário é o seu endereço de e-mail.

    Atenção: O token de segurança expira após um curto período de tempo. É sua responsabilidade atualizar o token de segurança.
  - **Nenhum**. Nenhuma autenticação é usada.

Etapa 7. Clique em **Filtros** e, como opção, selecione os filtros que você deseja usar para este encaminhador.

É possível selecionar no máximo um filtro de eventos e um filtro de recursos.

Se você não selecionar um filtro, os dados serão encaminhados para todos os eventos gerados por todos os recursos (dispositivos, gerenciadores de recursos e o XClarity Orchestrator).

Nessa guia, também é possível optar por encaminhar o evento excluído definindo o botão de alternância **Eventos Excluídos** como **Sim**.

Etapa 8. Clique em **Listas de Controle de Acesso** e selecione uma ou mais listas de controle de acesso que você deseja associar a esse encaminhador.

Se o acesso baseado em recursos estiver habilitado, você deverá selecionar pelo menos uma lista de controle de acesso.

Dica: como opção, os usuários que são membros de um grupo ao qual a função predefinida de **Supervisor** é atribuída podem selecionar **Associar tudo** em vez de selecionar listas de controle de acesso para que os dados encaminhados não sejam restritos.

Etapa 9. Clique em **Criar** para criar o encaminhador.

Depois de concluir

Você pode executar as seguintes ações no cartão Encaminhadores de Dados.

- Ative ou desative um encaminhador selecionado clicando no botão de alternância na coluna **Estado**
- Modifique um encaminhador selecionado clicando no ícone **Editar** (✎).
- Remova um encaminhador selecionado clicando no ícone **Excluir** (🗑).

Encaminhando eventos para um serviço SMTP Gmail

É possível configurar o Lenovo XClarity Orchestrator para encaminhar eventos para um serviço de e-mail baseado na Web, como Gmail.

Use os seguintes exemplos de configuração para ajudá-lo a configurar seu encaminhador de evento para usar o serviço Gmail SMTP.

Nota: Gmail recomenda o usar o método de autenticação OAUTH2 para comunicação mais seguro. Se você optar por usar autenticação regular, você receberá um e-mail indicando que um aplicativo tentou usar sua conta sem usar os padrões de segurança mais recente. O e-mail inclui instruções para configurar sua conta de e-mail para aceitar esses tipos de aplicativos.

Para obter informações sobre como configurar um servidor SMTP Gmail, consulte https://support.google.com/a/answer/176600?hl=en.

Autenticação normal usando SSL na porta 465

Este exemplo comunica com o servidor SMTP do Gmail usando o protocolo SSL pela porta 465 e autentica usando uma conta de usuário e senha válidas do Gmail.

Parâmetro	Valor
Host	smtp.gmail.com
Porta	465
SSL	Selecionar
STARTTLS	Limpar
Autenticação	Regular
Usuário	Endereço de e-mail do Gmail válido
Senha	Senha de autenticação do Gmail
Do endereço	(opcional)

Autenticação normal usando TLS na porta 587

Este exemplo comunica com o servidor SMTP do Gmail usando o protocolo TLS pela porta 587 e autentica usando uma conta de usuário e senha válidas do Gmail.

Parâmetro	Valor
Host	smtp.gmail.com
Porta	587
SSL	Limpar
STARTTLS	Selecionar
Autenticação	Regular
Usuário	Endereço de e-mail do Gmail válido

Parâmetro	Valor
Senha	Senha de autenticação do Gmail
Do endereço	(opcional)

Autenticação OAUTH2 usando TLS na porta 587

Este exemplo comunica com o servidor SMTP do Gmail usando o protocolo TLS pela porta 587 e autentica usando uma conta de usuário e um token de segurança válidos do Gmail.

Use o seguinte procedimento de amostra para obter o token de segurança.

1. Crie um projeto no Console dos Desenvolvedores do Google e recupere o ID e o segredo do cliente. Para obter mais informações, consulte o website Página Google Sign-In for Websites.
   a. Em um navegador da Web, abra o Página Google APIs.
   b. Clique em **Selecione um projeto → Crie um projeto** no menu nesta página da Web. A caixa de diálogo Novo Projeto é exibida.
   c. Digite um nome, selecione **Sim** para concordar o contrato de licença e clique em **Criar**.
   d. Na guia **Visão geral**, use o campo de pesquisa para procurar por "gmail".Clique em **API DO GMAIL** nos resultados da pesquisa.
   e. Clique em **Habilitar**.
   f. Clique na guia **Credenciais**.
   g. Clique em **Tela do acordo de OAuth**.
   h. Digite um nome no campo **Nome do produto mostrado aos usuários** e clique em **Salvar**.
   i. Clique em **Criar credenciais → ID do cliente OAuth**.
   j. Selecione **Outro** e insira um nome.
   k. Clique em **Criar**. A caixa de diálogo OAuth client é exibida com seu ID do cliente e cliente em segredo.
   l. Registre o ID do e o segredo do cliente para uso posterior.
   m. Clique em **OK** para fechar a caixa de diálogo.
2. Use o script do Python oauth2.py para gerar e autorizar um token de segurança, inserindo o ID e o segredo do cliente que foi gerado quando você criou o projeto.

   Nota: O Python 2.7 é necessário para concluir esta etapa. É possível baixar e instalar o Python 2.7 a partir do Site do Python.
   a. Em um navegador da Web, abra o Página gmail-oauth2-tools.
   b. Clique em **Bruto** e, em seguida, salve o conteúdo como um nome de arquivo `oauth2.py` no sistema local.
   c. Execute o seguinte comando no terminal (Linux) ou uma linha de comandos (Windows).
   ```
   py oauth2.py --user={your_email> --client_id={client_id}
      --client_secret={client_secret} --generate_oauth2_token
   ```
   Exemplo
   ```
   py oauth2.py --user=jon@gmail.com
      --client_id=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
      --client_secret=3tnyXgEiBIbT2mOOzqnlTszk --generate_oauth2_token
   ```
   Esse comando retorna uma URL que você deve usar para autorizar o token e para recuperar um código de verificação do website do Google, por exemplo:
   ```
   To authorize token, visit this url and follow the directions:

   https://accounts.google.com/o/oauth2/auth?client_id=884243132302
   ```

```
-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&amp;redirect_uri=
urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&amp;response_type=code&amp;scope=https%3A%2F%2Fmail.
google.com%2F

Enter verification code:
```

d. Em um navegador da Web, abra a URL que foi retornada na etapa anterior.

e. Clique em **Permitir** para concordar com este serviço. Um código de verificação a ser retornado.

f. Insira o código de verificação no comando `oauth2.py`.O comando retorna o token de segurança e atualiza o token, por exemplo:

```
Refresh Token: 1/K8lPGx6UQQajj7tQGYKq8mVG8lVvGIVzHqzxFIMeYEQMEudVrK5jSpoR3OzcRFq6
Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
Access Token Expiration Seconds: 3600
```

Importante: O token de segurança expira após um período de tempo. Você pode usar o script do Python oauth2.py e o token atualizado para gerar um novo token de segurança. É sua responsabilidade gerar um novo token de segurança e o atualizar o encaminhador de evento no Lenovo XClarity Orchestrator com o novo token.

3. Na interface da Web Lenovo XClarity Orchestrator, configure o encaminhador de eventos por e-mail usando os atributos a seguir.

Parâmetro	Valor
Host	smtp.gmail.com
Porta	587
SSL	Limpar
STARTTLS	Selecionar
Autenticação	OAUTH2
Usuário	Endereço de e-mail do Gmail válido
Token	Token de segurança
Do endereço	(opcional)

Encaminhando inventário e eventos para o Splunk

Você pode configurar o Lenovo XClarity Orchestrator para encaminhar inventário e eventos em um formato predefinido para um aplicativo Splunk. Em seguida, você pode usar o Splunk para criar gráficos com base nos dados para ajudar a analisar condições e prever problemas no seu ambiente.

Antes de iniciar

Atenção: Uma conexão segura não é estabelecida ao encaminhar dados para esse serviço. Os dados são enviados por um protocolo de texto claro.

Sobre esta tarefa

O Splunk é uma ferramenta para operadores de data center para rastrear e analisar logs de eventos e outros dados. A Lenovo fornece um aplicativo XClarity Orchestrator para Splunk que analisa os eventos encaminhados pelo XClarity Orchestrator e apresenta a análise em um conjunto de painéis. É possível monitorar os painéis nesse aplicativo como um auxílio para localizar possíveis problemas em seu ambiente para que você possa reagir antes que ocorram problemas graves. Para obter mais informações, consulte Guia do Usuário do Aplicativo XClarity Orchestrator para Splunk na documentação online do XClarity Orchestrator.

É possível definir várias configurações Splunk; no entanto, o XClarity Orchestrator pode encaminhar eventos para apenas uma instância Splunk. Portanto, apenas uma configuração Splunk pode ser habilitada por vez.

Se o controle de acesso baseado em recursos estiver ativado, os dados serão encaminhados apenas para os recursos que você pode acessar usando listas de controle de acesso. Se você não for um membro de um grupo ao qual a função predefinida de **Supervisor** é atribuída, deverá atribuir uma ou mais listas de controle de acesso aos encaminhadores que você criar. Se desejar enviar dados para todos os recursos que você pode acessar, selecione todas as listas de controle de acesso associadas que estão disponíveis para você. Se você for um membro de um grupo ao qual a função predefinida de **Supervisor** é atribuída, poderá optar por enviar dados para todos os recursos ou por atribuir listas de controle de acesso para limitar os recursos.

Não é possível filtrar dados encaminhados para os aplicativos Splunk.

Procedimento

Para encaminhar inventário e dados de eventos para um aplicativo Splunk, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Monitoramento** () → **Encaminhamento** e clique em **Encaminhadores de Dados** na navegação esquerda para exibir o cartão Encaminhadores de Dados.

Etapa 2. Clique no ícone **Criar** () para exibir a caixa de diálogo Criar Encaminhador de Dados.

Etapa 3. Especifique o nome do encaminhador e a descrição opcional.

Etapa 4. Escolha para habilitar ou desabilitar o encaminhador clicando no botão de alternância **Estado**.

Etapa 5. Selecione **Splunk** como o tipo de encaminhador.

Etapa 6. Clique em **Configuração** e preencha as informações específicas do protocolo.

- Inclua o nome do host ou o endereço IP do aplicativo Splunk.
- Especifique a conta do usuário e a senha a serem usadas para fazer login no serviço Splunk.
- Especifique os números de porta de dados e API REST a serem usados para conectar-se ao serviço Splunk.
- Especifique um ou mais índices do coletor de eventos HTTP. O índice padrão é **Ixco**.
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é `30` segundos.

Etapa 7. Clique em **Listas de Controle de Acesso** e selecione uma ou mais listas de controle de acesso que você deseja associar a esse encaminhador.

Se o acesso baseado em recursos estiver habilitado, você deverá selecionar pelo menos uma lista de controle de acesso.

Dica: como opção, os usuários que são membros de um grupo ao qual a função predefinida de **Supervisor** é atribuída podem selecionar **Associar tudo** em vez de selecionar listas de controle de acesso para que os dados encaminhados não sejam restritos.

Etapa 8. Clique em **Criar** para criar o encaminhador.

Depois de concluir

Você pode executar as seguintes ações no cartão Encaminhadores de Dados.

- Ative ou desative um encaminhador selecionado clicando no botão de alternância na coluna **Estado**
- Modifique um encaminhador selecionado clicando no ícone **Editar** ().
- Remova um encaminhador selecionado clicando no ícone **Excluir** ().

Encaminhando eventos para um syslog

É possível configurar o Lenovo XClarity Orchestrator para encaminhar eventos específicos a um syslog.

Antes de iniciar

Atenção: Uma conexão segura não é estabelecida ao encaminhar dados para esse serviço. Os dados são enviados por um protocolo de texto claro.

Sobre esta tarefa

Se o controle de acesso baseado em recursos estiver ativado, os dados serão encaminhados apenas para os recursos que você pode acessar usando listas de controle de acesso. Se você não for um membro de um grupo ao qual a função predefinida de **Supervisor** é atribuída, deverá atribuir uma ou mais listas de controle de acesso aos encaminhadores que você criar. Se desejar enviar dados para todos os recursos que você pode acessar, selecione todas as listas de controle de acesso associadas que estão disponíveis para você. Se você for um membro de um grupo ao qual a função predefinida de **Supervisor** é atribuída, poderá optar por enviar dados para todos os recursos ou por atribuir listas de controle de acesso para limitar os recursos.

Os *filtros de encaminhamento de dados* são usados para definir o escopo de eventos que você deseja encaminhar, com base em códigos de evento, classes de evento, severidades de evento, tipos de serviço e no recurso que gerou o evento. Certifique-se de que os filtros de eventos e de recursos que você deseja usar para este encaminhador já estejam criados (consulte Criando filtros de encaminhamento de dados).

O exemplo a seguir mostra o formato padrão dos dados encaminhados para um syslog. Palavras entre colchetes duplos são atributos substituídos por valores reais quando os dados são encaminhados.

```
{
   "appl": "LXCO",
   "groups": [],
   "acls": [],
   "local": null,
   "eventID": "FQXHMEM0216I",
   "severity": "Warning",
   "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
   "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
   "msg": "The event forwarder destination cannot be reached. Therefore new events are not being
           forwarded.",
   "description": "The event forwarder destination cannot be reached. Therefore new events are not
                   being forwarded.",
   "userAction": "Look in the online documentation to determinate more information about this event
                  based on the eventID. At the moment the orchestrator server can not offer more
                  information.",
   "recoveryURL": null,
   "flags": [],
   "userid": null,
   "action": "None",
   "eventClass": "System",
   "args": [],
   "service": "None",
   "lxcaUUID": "23C87F0A2CB6491097489193447A655C",
   "managerID": "23C87F0A2CB6491097489193447A655C",
   "failFRUNumbers": null,
   "failFRUSNs": null,
   "failFRUUUIDs": "[FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF]",
   "msgID": null,
   "timeStamp": "2021-03-12T18:32:14.000Z",
   "eventDate": "2021-03-12T18:32:14Z",
   "commonEventID": "FQXHMEM0216I",
```

```
   "sequenceNumber": "17934247",
   "details": null,
   "device": {
      "name": "xhmc194.labs.lenovo.com",
      "mtm": null,
      "serialNumber": null
   },
   "resourceType": "XClarity Administrator",
   "componentType": "XClarity Administrator",
   "sourceType": "Management",
   "resourceName": "xhmc194.labs.lenovo.com",
   "fruType": "other",
   "ipAddress": "10.243.2.107",
   "_id": 252349
}
```


Procedimento

Para encaminhar dados a um syslog, conclua as seguintes etapas.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Monitoramento** ( ) → **Encaminhamento** e clique em **Encaminhadores de Dados** na navegação esquerda para exibir o cartão Encaminhadores de Dados.

Etapa 2. Clique no ícone **Criar** (⊕) para exibir a caixa de diálogo Criar Encaminhador de Dados.

Etapa 3. Especifique o nome do encaminhador e a descrição opcional.

Etapa 4. Escolha para habilitar ou desabilitar o encaminhador clicando no botão de alternância **Estado**.

Etapa 5. Selecione **Syslog** como o tipo de encaminhador.

Etapa 6. Clique em **Configuração** e preencha as informações específicas do protocolo.

- Inclua o nome do host ou o endereço IP do syslog.
- Insira a porta a ser usada para o encaminhamento de eventos. O padrão é 514.
- Selecione o protocolo a ser usado para o encaminhamento de eventos. Este pode ser um dos valores a seguir.
  - **UDP**
  - **TCP**
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é 30 segundos.
- **Opcional:** selecione o formato do carimbo de data/hora no syslog. Este pode ser um dos valores a seguir.
  - **Hora local**. O formato padrão, por exemplo, Fri Mar 31 05:57:18 EDT 2017.
  - **Horário GMT**. Padrão internacional (ISO8601) para data e hora, por exemplo, 2017-03-31T05:58:20-04:00.

Etapa 7. Clique em **Filtros** e, como opção, selecione os filtros que você deseja usar para este encaminhador.

É possível selecionar no máximo um filtro de eventos e um filtro de recursos.

Se você não selecionar um filtro, os dados serão encaminhados para todos os eventos gerados por todos os recursos (dispositivos, gerenciadores de recursos e o XClarity Orchestrator).

Nessa guia, também é possível optar por encaminhar o evento excluído definindo o botão de alternância **Eventos Excluídos** como **Sim**.

Etapa 8. Clique em **Listas de Controle de Acesso** e selecione uma ou mais listas de controle de acesso que você deseja associar a esse encaminhador.

Se o acesso baseado em recursos estiver habilitado, você deverá selecionar pelo menos uma lista de controle de acesso.

Dica: como opção, os usuários que são membros de um grupo ao qual a função predefinida de **Supervisor** é atribuída podem selecionar **Associar tudo** em vez de selecionar listas de controle de acesso para que os dados encaminhados não sejam restritos.

Etapa 9. Clique em **Criar** para criar o encaminhador.

Depois de concluir

Você pode executar as seguintes ações no cartão Encaminhadores de Dados.

- Ative ou desative um encaminhador selecionado clicando no botão de alternância na coluna **Estado**
- Modifique um encaminhador selecionado clicando no ícone **Editar** ( ).
- Remova um encaminhador selecionado clicando no ícone **Excluir** ( ).

Encaminhamento de dados de métricas para umLenovo TruScale Infrastructure Services

É possível configurar o Lenovo XClarity Orchestrator para encaminhar dados de métricas (telemetria) a um Lenovo TruScale Infrastructure Services.

Antes de iniciar

Saiba mais: Conheça o Lenovo TruScale Infrastructure Services

Atenção: Estas etapas de configuração são destinadas apenas a representantes do Serviço Lenovo.

Uma conexão segura é estabelecida ao encaminhar dados para TruScale Infrastructure Services.

Verifique se o XClarity Orchestrator está executando a versão v1.2.0 ou posterior.

Verifique se os gerenciadores de recursos do Lenovo XClarity Administrator que gerenciam os dispositivos para os quais você deseja encaminhar dados de métricas estão executando a v3.0.0 mais o pacote de correções ou posterior.

Verifique se os gerenciadores de recursos apropriados do XClarity Administrator estão conectados ao XClarity Orchestrator (consulte Conectando gerenciadores de recursos).

Verifique se os dispositivos para os quais você deseja encaminhar dados de métricas estão executando o firmware mais recente do Lenovo XClarity Controller (consulte Aplicando e ativando atualizações aos gerenciadores de recursos).

Verifique se as configurações de data e hora estão definidas corretamente nos recursos a seguir.
- XClarity Orchestrator (consulte Configurando data e hora)
- Gerenciador de recursos do XClarity Administrator (consulte Configurando data e hora na documentação online do XClarity Administrator)
- Baseboard Management Controllers em cada dispositivo (consulte Definindo a data e a hora do XClarity Controller na documentação online do Lenovo XClarity Controller)

Verifique se as configurações de rede no XClarity Orchestrator estão definidas corretamente.

Verifique se os dados de métricas estão sendo coletados para os dispositivos gerenciados visualizando os gráficos de utilização na página de resumo do dispositivo (consulte Visualizando detalhes de dispositivos). Se os dados de métricas não são exibidos, consulte Solução de problemas de encaminhamento de dados .

Para saber mais sobre o Lenovo TruScale Infrastructure Services, consulte o Site do TruScale Infrastructure Services.

Sobre esta tarefa

É possível definir várias configurações do Lenovo TruScale Infrastructure Services; no entanto, o XClarity Orchestrator pode encaminhar eventos para apenas uma instância do Lenovo TruScale Infrastructure Services. Portanto, apenas uma configuração do Lenovo TruScale Infrastructure Services pode ser habilitada por vez.

Se o controle de acesso baseado em recursos estiver ativado, os dados serão encaminhados apenas para os recursos que você pode acessar usando listas de controle de acesso. Se você não for um membro de um grupo ao qual a função predefinida de **Supervisor** é atribuída, deverá atribuir uma ou mais listas de controle de acesso aos encaminhadores que você criar. Se desejar enviar dados para todos os recursos que você pode acessar, selecione todas as listas de controle de acesso associadas que estão disponíveis para você. Se você for um membro de um grupo ao qual a função predefinida de **Supervisor** é atribuída, poderá optar por enviar dados para todos os recursos ou por atribuir listas de controle de acesso para limitar os recursos.

Não é possível filtrar dados encaminhados a um Lenovo TruScale Infrastructure Services.

O exemplo a seguir mostra o formato padrão dos dados encaminhados para um Lenovo TruScale Infrastructure Services. Palavras entre colchetes duplos são atributos substituídos por valores reais quando os dados são encaminhados.

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

Procedimento

Para encaminhar dados a um Lenovo TruScale Infrastructure Services, conclua as seguintes etapas.

Etapa 1. Adicione os certificados SSL confiáveis fornecidos pelo Lenovo TruScale Infrastructure Services.

1. Na barra de menus do XClarity Orchestrator, clique na barra de menus do XClarity Orchestrator, clique em **Administração (⚙) → Segurança** e clique em **Certificados Confiáveis** na navegação esquerda para exibir o cartão Certificados Confiáveis.
2. Clique no ícone **Adicionar** (⊕) para adicionar um certificado. A caixa de diálogo Adicionar Certificado é exibida.
3. Copie e cole os dados do certificado no formato PEM.
4. Clique em **Adicionar**.

Etapa 2. Na barra de menus do XClarity Orchestrator, clique em **Monitoramento (**) → **Encaminhamento** e clique em **Encaminhadores de Dados** na navegação esquerda para exibir o cartão Encaminhadores de Dados.

Etapa 3. Clique no ícone **Criar** (⊕) para exibir a caixa de diálogo Criar Encaminhador de Dados.

Etapa 4. Especifique o nome do encaminhador e a descrição opcional.

Etapa 5. Escolha para habilitar ou desabilitar o encaminhador clicando no botão de alternância **Estado**.

Etapa 6. Selecione **TruScale Infrastructure Services** como o tipo de encaminhador.

Etapa 7. Clique em **Configuração** e preencha as informações específicas do protocolo.

- Insira o nome do host ou o endereço IP do TruScale Infrastructure Service.
- Insira a porta a ser usada para o encaminhamento de eventos. O padrão é `9092`.
- Como opção, insira a frequência, em minutos, quando os dados são enviados. O padrão é `60` minutos.
- Insira o nome do tópico.
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é `300` segundos.

Etapa 8. Clique em **Validar conexão** para garantir que uma conexão possa ser estabelecida com base na configuração.

Atenção: A validação da conexão pode levar alguns minutos para ser concluído. É possível fechar a mensagem pop-up e continuar a criar o encaminhador sem interromper o processo de validação. Quando a validação é concluída, outra mensagem popup é exibida para notificar se a conexão foi bem-sucedida.

Etapa 9. Clique em **Listas de Controle de Acesso** e selecione uma ou mais listas de controle de acesso que você deseja associar a esse encaminhador.

Se o acesso baseado em recursos estiver habilitado, você deverá selecionar pelo menos uma lista de controle de acesso.

Dica: como opção, os usuários que são membros de um grupo ao qual a função predefinida de **Supervisor** é atribuída podem selecionar **Associar tudo** em vez de selecionar listas de controle de acesso para que os dados encaminhados não sejam restritos.

Etapa 10. Clique em **Criar** para criar o encaminhador.

Depois de concluir

Você pode executar as seguintes ações no cartão Encaminhadores de Dados.

- Ative ou desative um encaminhador selecionado clicando no botão de alternância na coluna **Estado**
- Modifique um encaminhador selecionado clicando no ícone **Editar** (✎).
- Remova um encaminhador selecionado clicando no ícone **Excluir** (🗑).

Encaminhando relatórios

É possível encaminhar relatórios de forma recorrente para um ou mais endereços de e-mail usando um serviço da Web SMTP.

Sobre esta tarefa

Um *relatório* é qualquer dado que é apresentado no formato em tabela na interface do usuário. Os relatórios a seguir são compatíveis atualmente.

- Alertas ativos

- Eventos de auditoria e de recursos
- Dispositivos gerenciados (servidores, armazenamento, comutadores e chassi)
- Conformidade do firmware do dispositivo
- Conformidade da configuração do servidor
- Status de garantia para servidores
- Tíquetes de serviço ativos

Criando configurações de destino do encaminhador

É possível definir configurações de destino comuns que podem ser usadas por vários encaminhadores de relatório. O destino identifica para onde os relatórios devem ser enviados.

Procedimento

Para criar uma configuração de destino para encaminhadores de relatório, conclua as seguintes etapas.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Monitoramento** () → **Encaminhamento** e clique em **Destinos do encaminhador** na navegação esquerda para exibir o cartão Destinos do encaminhador.

Etapa 2. Clique no ícone **Criar** () para exibir a caixa de diálogo Criar destinos do encaminhador.

Etapa 3. Especifique o nome do encaminhador de relatórios e a descrição opcional.

Etapa 4. Selecione **SMTP** como o tipo de destino.

Etapa 5. Clique em **Configuração** e preencha as informações específicas do protocolo.

- Insira o nome do host ou o endereço (de e-mail) do servidor SMTP.
- Insira a porta a ser usada para o destino. O padrão é `25`.
- Insira o período de tempo limite (em segundos) para a solicitação. O padrão é `30` segundos.
- Insira o endereço de e-mail para cada destinatário. Separe diversos endereços de e-mail usando uma vírgula.
- **Opcional:** insira o endereço de e-mail do remetente (por exemplo, john@company.com) e o domínio do remetente. Se você não especificar um endereço de e-mail, o endereço do remetente será LXCO.*{source_identifier}@{smtp_host}* por padrão.

  Se você especificar apenas o domínio do remetente, o formato do endereço do remetente será *{LXCO_host_name}@{sender_domain}* (por exemplo, `XClarity1@company.com`).

  Notas:

  – Se você configurou o servidor SMTP para requerer um nome do host para encaminhar e-mail e não configurou um nome do host para XClarity Orchestrator, é possível que o servidor SMTP descarte o e-mail. Se o XClarity Orchestrator não tiver um nome do host, o e-mail será encaminhado com o endereço IP. Se o endereço IP não pode ser obtido, o "localhost" é enviado no seu lugar, o que pode fazer com que o servidor SMTP descarte o e-mail.

  – Se você especificar o domínio do remetente, a origem não identificará o endereço do remetente. Em vez disso, as informações sobre a origem dos dados serão incluídas no corpo do e-mail, incluindo o nome do sistema, endereço IP, tipo/modelo de máquina e o número de série.

  – Se o servidor SMTP só aceita e-mails que forem enviados por um usuário registrado, o endereço padrão do remetente (`LXCO.`*<source_identifier>*`@{smtp_host>`) é rejeitado. Nesse caso, você deve especificar pelo menos um nome de domínio no campo **Do Usuário**.

- Para estabelecer uma conexão segura com o servidor SMTP, selecione um dos tipos de conexão a seguir.
  – **SSL**. Usa o protocolo SSL para formar uma comunicação segura.

– **STARTTLS**. Usa o protocolo TLS para formar uma comunicação segura em um canal não seguro.

Se um destes tipos de conexão for selecionado, o XClarity Orchestrator tentará baixar e importar o certificado do servidor SMTP para seu armazenamento confiável do XClarity Orchestrator. Você será solicitado a aceitar esse certificado.

- Se a autenticação for necessária, selecione um dos tipos de autenticação a seguir.
  - **Regular**. Autentica ao servidor SMTP especificado usando o ID do usuário e senha especificados.
  - **OAUTH2**. Usa protocolo SASL (Simple Authentication and Security Layer) para autenticar o servidor SMTP especificado usando o nome de usuário e o token de segurança especificados. Normalmente, o nome do usuário é o seu endereço de e-mail.

    Atenção: O token de segurança expira após um curto período de tempo. É sua responsabilidade atualizar o token de segurança.
  - **Nenhum**. Nenhuma autenticação é usada.

Etapa 6. Clique em **Criar** para criar a configuração do destino.

Depois de concluir

É possível executar as ações a seguir no cartão Destinos do encaminhador.

- Modifique um destino selecionado clicando no ícone **Editar** (✎).
- Remova um destino selecionado clicando no ícone **Excluir** (🗑).Não é possível excluir um destino atribuído a um encaminhador

Encaminhando relatórios usando e-mail

É possível encaminhar relatórios de forma recorrente para um ou mais endereços de e-mail usando um serviço da Web SMTP.

Sobre esta tarefa

Um *relatório* é qualquer dado que é apresentado no formato em tabela na interface do usuário. Os relatórios a seguir são compatíveis atualmente.

- Alertas ativos
- Eventos de auditoria e de recursos
- Dispositivos gerenciados (servidores, armazenamento, comutadores e chassi)
- Conformidade do firmware do dispositivo
- Conformidade da configuração do servidor
- Status de garantia para servidores
- Tíquetes de serviço ativos

Cada encaminhador de relatórios pode incluir apenas um relatório de cada tipo.

O relatório é criado como arquivo e salvo no host do servidor do Orchestrator. Se o arquivo tiver 10 MB ou menos, ele será encaminhado como um anexo de e-mail. Se o arquivo for maior que 10 MB, o e-mail incluirá o local dos arquivos. Também é possível baixar o arquivo clicando em **Histórico de relatórios** e em **Baixar** na linha para o relatório.

Lenovo XClarity Orchestrator armazena no máximo 100 relatórios. Se o número máximo de relatórios for atingido, o XClarity Orchestrator excluirá o relatório mais antigo antes de gerar um novo.

Procedimento

Para encaminhar um relatório por e-mail, conclua uma das etapas a seguir.

- **Enviar dados não filtrados**
  1. Na barra de menus do XClarity Orchestrator, clique em **Monitoramento (**) → **Encaminhamento** e clique em **Encaminhadores de relatórios** na navegação esquerda para exibir o cartão Relatórios.
  2. Clique no ícone **Criar** (⊕) para exibir a caixa de diálogo Criar relatório.
  3. Especifique o nome do encaminhador de relatórios e a descrição opcional.
  4. Opte por ativar ou desativar o encaminhador de relatórios clicando no botão de alternância **Estado**.
  5. Clique em **Lista de conteúdo** e selecione um ou mais relatórios que deseja encaminhar.
  6. Clique em **Destino do encaminhador** e selecione o destino (consulte Criando configurações de destino do encaminhador).
  7. Clique em **Programações** e especifique o dia da semana, a hora, a duração (data de início e final) quando você deseja que os relatórios sejam enviados. O relatório é enviado no mesmo dia e hora a todas as semanas durante a duração especificada.
  8. Clique em **Criar** para criar o encaminhador.
- **Enviar dados filtrados**
  1. Na barra de menus do XClarity Orchestrator, abra o cartão que contém o relatório a ser enviado. Os relatórios a seguir são compatíveis.
     - Dados do dispositivo (clique em **Recursos (**) → *{device_type}*)
     - Dados ativos de alerta (clique em **Monitoramento (**) → **Alertas**)
     - Dados de evento de recurso e auditoria (clique em **Monitoramento (**) → **Eventos**)
     - Conformidade de firmware (clique em **Provisionamento (**) → **Atualizações** → **Aplicar e Ativar** → **Dispositivos**)
     - Conformidade de configuração do servidor (clique em **Provisionamento (**) → **Configuração do servidor** → **Atribuir e implantar**)
     - Dados de garantia do dispositivo (clique em **Administração (**) → **Serviço e Suporte** → **Garantia**)
     - Tíquetes de serviço ativos (clique em **Administração (**) → **Serviço e Suporte** → **Tíquetes de Serviço**)
  2. Opcionalmente refine os dados definidos apenas para as informações de interesse, limitando o escopo dos dados apenas àqueles recursos que estão em gerenciadores e grupos de recursos específicos, e usando filtros e pesquisa para incluir dados que correspondam a critérios específicos (consulte Dicas e técnicas de interface do usuário).
  3. Clique em **Todas as Ações** → **Criar encaminhador de relatórios** para exibir a caixa de diálogo Criar encaminhador de relatórios.
  4. Especifique o nome do encaminhador de relatórios e a descrição opcional.
  5. Opte por ativar ou desativar o encaminhador de relatórios clicando no botão de alternância **Estado**.
  6. Clique em **Destino do encaminhador** e selecione o destino (consulte Criando configurações de destino do encaminhador).
  7. Clique em **Programações** e especifique o dia da semana, a hora, a duração (data de início e final) quando você deseja que os relatórios sejam enviados. O relatório é enviado no mesmo dia e hora a todas as semanas durante a duração especificada.
  8. Clique em **Criar** para criar o encaminhador.

Depois de concluir

É possível executar as ações a seguir no cartão Encaminhador de relatórios.

- Ativar ou desativar um encaminhador de relatórios selecionado clicando no botão de alternância na coluna **Estado**.
- Modifique um encaminhador de relatórios selecionado clicando no ícone **Editar** (✎).
- Remova um encaminhador de relatórios selecionado clicando no ícone **Excluir** (🗑).
- Salve os relatórios no sistema local clicando na guia **Histórico de relatórios** e, em seguida, clicando em **Baixar** na linha para cada relatório.

É possível adicionar um relatório a um encaminhador de relatórios existente em qualquer cartão de relatório compatível usando os filtros de dados atualmente aplicados à tabela clicando em **Todas as Ações → Adicionar conteúdo ao encaminhador de relatórios existente** a partir desse cartão. Se o encaminhador de relatórios já incluir um relatório desse tipo, ele será atualizado para usar os filtros de dados atuais.

Capítulo 4. Gerenciando recursos

É possível usar o Lenovo XClarity Orchestrator para gerenciar recursos, incluindo exibir detalhes de dispositivos offline.

Criando grupos de recursos

Um *grupo de recursos* é um conjunto estático de recursos que você pode visualizar e agir sobre ele coletivamente no Lenovo XClarity Orchestrator. Vários tipos de grupos de recursos são compatíveis.

Saiba mais: Como criar um grupo de recursos

Sobre esta tarefa

Vários tipos de grupos de recursos são compatíveis.

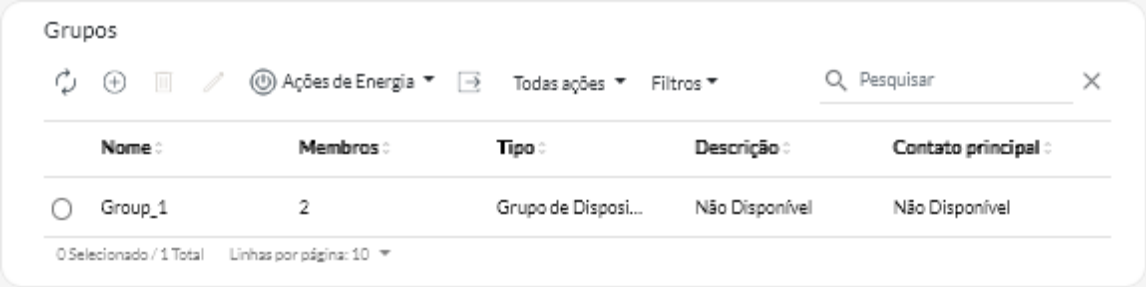
- Os *grupos de dispositivos dinâmicos* contêm um conjunto dinâmico de dispositivos com base em critérios específicos.
- *Grupos de dispositivos* contêm um conjunto de dispositivos específicos.
- *Grupos de gerenciadores* contêm um conjunto estático de gerenciadores de recursos específicos e o próprio XClarity Orchestrator.
- *Grupos de infraestrutura* contêm um conjunto de dispositivos de rede. Quando você gerencia um gerenciador de recursos Schneider Electric EcoStruxure IT Expert, o XClarity Orchestrator clona automaticamente coleções de "grupo" definidas em um EcoStruxure IT Expert gerenciado. O grupo clonado é nomeado *{domain}\{groupName}* no repositório local. Observe que as coleções do tipo local (site, edifício, sala, linha ou rack) não são clonadas.

Nota: Não é possível criar um grupo de recursos com uma combinação de dispositivos, gerenciadores de recursos e recursos de infraestrutura.

Procedimento

Para criar um grupo de recursos e gerenciar a associação, conclua as etapas a seguir.

- **Crie um grupo de dispositivos dinâmico e adicione dispositivos.**
  1. Na barra de menus do XClarity Orchestrator, clique em **Recursos** ( ) → **Grupos** para exibir o cartão Grupos.

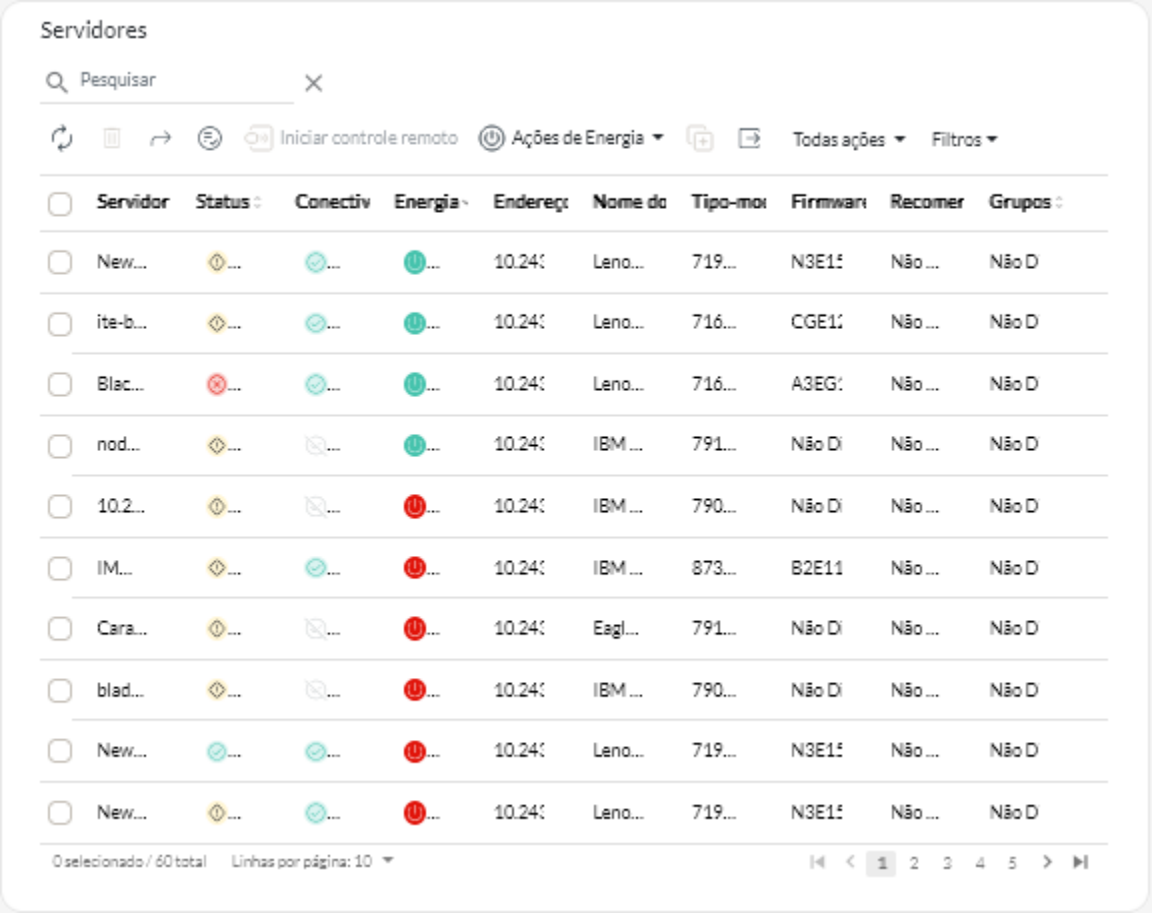


  2. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Criar grupo.
  3. Selecione o **Grupo dinâmico de dispositivos** como o tipo de grupo.
  4. Especifique o nome e a descrição opcional do grupo.

5. Clique em **Critérios do grupo** e selecione regras a serem usadas para associação ao grupo.

   - Decida se o dispositivo deve corresponder a **qualquer** (uma ou mais) ou **todas** as regras do menu suspenso de correspondências de **Critérios**.
   - Especifique o atributo, o operador e o valor de cada regra. Clique em **Adicionar critério** para adicionar outra regra.
6. Clique em **Informações de Contato**. É possível selecionar um contato de suporte primário (na coluna **Contatos primários**) e um ou mais contatos secundários (na coluna **Contatos secundários**) para atribuir a todos os dispositivos do grupo.
7. Clique em **Criar**O grupo é adicionado à tabela.

- **Crie um grupo de recursos estático e adicione recursos.**
  1. Na barra de menus do XClarity Orchestrator, clique em **Recursos (⚙) → Grupos** para exibir a placa Grupos.
  2. Clique no ícone **Criar** (⊕) para exibir a caixa de diálogo Criar grupo.
  3. Selecione **Grupo de Dispositivos** ou **Grupo de Gerenciadores** como tipo de grupo.
  4. Especifique o nome e a descrição opcional do grupo.
  5. Clique em **Dispositivos Disponíveis** ou **Gerenciadores de recursos disponíveis** dependendo do tipo de grupo e selecione os recursos que deseja incluir no grupo.
  6. Clique em **Informações de Contato**. É possível selecionar um contato de suporte primário (na coluna **Contatos primários**) e um ou mais contatos secundários (na coluna **Contatos secundários**) para atribuir a todos os dispositivos do grupo.
  7. Clique em **Criar**.O grupo é adicionado à tabela.
- **Adicione dispositivos a um grupo de dispositivos estáticos.**
  1. Na barra de menus do XClarity Orchestrator, clique em **Recursos (⚙)** e, em seguida, clique no tipo de dispositivo (como Servidores ou Comutadores) para exibir uma placa com todos os dispositivos do tipo em questão.



2. Selecione um ou mais dispositivos para adicionar a um grupo.
3. Clique no ícone **Adicionar item ao grupo** ( ).
4. Selecione um grupo existente ou especifique um nome e uma descrição opcional para criar um novo grupo e clique em **Aplicar**.

- **Adicione gerenciadores de dispositivos a um grupo de gerenciadores estático.**
  1. Na barra de menus do XClarity Orchestrator, clique em **Recursos ( ) → Gerenciadores de Recursos** para exibir o cartão Gerenciadores de Recursos.
  2. Selecione um ou mais gerenciadores de recursos para adicionar a um grupo.
  3. Clique no ícone **Adicionar item ao grupo** ( ).
  4. Selecione um grupo existente ou especifique um nome e uma descrição opcional para criar um novo grupo e clique em **Aplicar**.

Depois de concluir

É possível executar as ações a seguir na placa Grupos.

- Modifique as propriedades e associação de um grupo selecionado clicando no ícone **Editar** ( ).

  Nota: Para grupos de infraestrutura que foram clonados do Schneider Electric EcoStruxure IT Expert, use o Schneider Electric EcoStruxure IT Expert para alterar o nome do grupo, a descrição e a associação.
- Exclua um grupo selecionado clicando no ícone **Excluir** ( ).
- Exiba os membros de um grupo de recursos clicando no nome do grupo para exibir a caixa de diálogo Exibir grupo e, em seguida, clicando na guia **Resumo de membros**.

Gerenciando dispositivos offline

Se um dispositivo não for gerenciado atualmente por um gerenciador de recursos, você poderá usar o Lenovo XClarity Orchestrator para gerenciar os dispositivos no *modo offline* importando um arquivo de dados de serviço associado a esse dispositivo.

Sobre esta tarefa

Somente servidores com IMM2 ou XCC Baseboard Management Controllers podem ser gerenciados offline. Esses dispositivos são identificados na interface da Web usando o status de conectividade "Gerenciado offline".

É possível executar as ações a seguir nos dispositivos gerenciados offline. Todas as outras ações estão desabilitadas.

- Exibir inventário do dispositivo
- Excluir alertas e eventos
- Gerenciar dados de serviço
- Abrir tíquetes de serviço no Centro de Suporte Lenovo usando Call Home e gerenciar esses tíquetes de serviço
- Recuperar informações sobre garantia
- Funções de análise para prever e analisar problemas com esses dispositivos

Importante: O XClarity Orchestrator não se comunica com dispositivos offline para recuperar dados atualizados.

Procedimento

Para gerenciar dispositivos offline, conclua as etapas a seguir.

Etapa 1. Na barra de menus do Lenovo XClarity Orchestrator, clique em **Recursos** (⚙) → **Servidores**. A página Servidores é exibida.

Etapa 2. Clique no ícone **Importar** (⇄) para importar os arquivos de dados de serviço.

Etapa 3. Arraste e solte um ou mais arquivos de dados de serviço (no formato .gz, .tzz ou .tgz) na caixa de diálogo Importar ou clique em **Procurar** para localizar o arquivo.

Etapa 4. Opcionalmente, ative **Adicionar o servidor nos dados de serviço ao inventário apenas para exibição** para gerenciar o servidor aplicável no modo de gerenciamento offline (consulte Gerenciando dispositivos offline).

Etapa 5. Clique em **Importar** para importar e analisar o arquivo. Quando a análise for concluída, o **Status de análise** do arquivo importando mudará para "Analisado".

É possível monitorar o status do processo de importação e análise no log de trabalhos (Monitorando trabalhos).

Depois de concluir

É possível cancelar o gerenciamento de um dispositivo selecionado que é gerenciado offline clicando no ícone **Cancelar gerenciamento** (🗑).

Executando ações de energia em servidores gerenciados

É possível usar o Lenovo XClarity Orchestrator para ligar, desligar e reiniciar servidores gerenciados.

Antes de iniciar

Você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** ou **Hardware** é atribuída.

Os servidores ThinkSystem requerem um sistema operacional para executar operações de energia.

O sistema operacional no servidor deve ser compatível com a Advanced Configuration and Power Interface (ACPI) e configurado para permitir operações de encerramento.

Sobre esta tarefa

O XClarity Orchestrator é compatível com as ações de energia a seguir.

- **Ligar**. Liga os servidores selecionados que estão desligados atualmente.
- **Desligar normalmente**. Desliga o sistema operacional e desliga os servidores selecionados que estão ligados no momento.
- **Desligar imediatamente**. Desliga os servidores selecionados que estão ligados no momento.
- **Reiniciar normalmente**. Desliga o sistema operacional e reinicia os servidores selecionados que estão ligados no momento.
- **Reiniciar Imediatamente**. Reinicia os servidores selecionados que estão ligados no momento.
- **Reiniciar para Configuração do Sistema**. Reinicia a configuração BIOS/UEFI (F1) para servidores selecionados.
- **Reiniciar controlador de gerenciamento**. Reinicia o Baseboard Management Controller de servidores selecionados.

Notas:

- Para dispositivos ThinkEdge Client, somente o recurso **Reiniciar normalmente** é compatível.
- O status de conectividade do servidor deve ser online. Não é possível executar ações de energia em dispositivos que estão offline, incluindo dispositivos gerenciados offline.

É possível executar ações de energia em no máximo 25 dispositivos ao mesmo tempo.

- **Procedimento**

  Para ligar, desligar ou reiniciar servidores, execute as etapas a seguir

Para um único servidor

a. No menu XClarity Orchestrator, clique em **Recursos (→ Servidores**. O cartão Servidores é exibido com uma exibição tabular de todos os servidores gerenciados.
b. Clique na linha do servidor para exibir as placas de resumo desse servidor.
c. Na placa Ações rápidas, clique em **Ações de Energia** e, em seguida, clique na ação de energia desejada.
d. Clique em **Confirmar**.

Para vários servidores

a. No menu XClarity Orchestrator, clique em **Recursos (→ Servidores**. O cartão Servidores é exibido com uma exibição tabular de todos os servidores gerenciados.
b. Selecione um ou mais servidores. É possível selecionar no máximo 25 servidores.
c. Clique em **Ações de Energia** e, em seguida, clique na ação de energia desejada.

   Uma caixa de diálogo é exibida com uma lista de dispositivos selecionados. Os dispositivos que não são aplicáveis (não compatíveis com ações de energia) ficam esmaecidos.

d. Clique em **Confirmar**.

Para todos os servidores em um grupo

a. Na barra de menu do XClarity Orchestrator, clique em **Recursos** ( ) → **Grupos**. O cartão Grupos é exibido com uma exibição tabular de todos os grupos.
b. Selecione um grupo de servidores.
c. Na placa Ações rápidas, clique em **Ações de Energia** e, em seguida, clique na ação de energia desejada.

   Uma caixa de diálogo é exibida com uma lista de dispositivos selecionados. Os dispositivos que não são aplicáveis (não compatíveis com ações de energia) ficam esmaecidos.
d. Selecione os servidores específicos no grupo no qual atuar. É possível selecionar no máximo 25 servidores.
e. Clique em **Confirmar**.

   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 .)

Abrindo uma sessão de controle remoto para servidores gerenciados

É possível abrir uma sessão de controle remoto de um servidor gerenciado como se estivesse em um console local. Em seguida, você pode usar a sessão de controle remoto para executar operações, como ligar ou desligar o servidor, e montar logicamente uma unidade local ou remota.

Abrindo uma sessão de controle remoto para servidores ThinkSystem ou ThinkAgile

É possível abrir uma sessão de controle remoto de um servidor ThinkSystem gerenciado ou ThinkAgile como se estivesse em um console local. É possível então usar a sessão de controle remoto para executar operações de gerenciamento.

Antes de iniciar

Você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** ou **Hardware** é atribuída.

O servidor gerenciado deve ter um estado de funcionamento normal e estado de conectividade online. Para obter mais informações sobre como exibir o status do servidor, consulte Visualizando detalhes de dispositivos.

Leia as considerações a seguir para servidores ThinkSystem SR635 e SR655.
- É necessário ter o firmware do Baseboard Management Controller v2.94 ou posterior.
- Apenas o modo de vários usuários é suportado; o modo de usuário único não tem suporte.
- O Internet Explorer11 não é suportado.
- Não é possível ligar nem desligar um servidor a partir de uma sessão de controle remoto.

Sobre esta tarefa

Você pode iniciar uma sessão de controle remoto para um único servidor ThinkSystem ou ThinkAgile.

Para obter mais informações sobre como usar os recursos do console remoto e mídia, consulte a documentação do servidor ThinkSystem ou ThinkAgile.

Nota: Para servidores ThinkSystem e ThinkAgile, não é necessário um Java Runtime Environment (JRE) com suporte a Java WebStart.

Procedimento

Para abrir uma sessão do controle remoto para um servidor ThinkSystem ou ThinkAgile, conclua as etapas a seguir.

Etapa 1. No menu XClarity Orchestrator, clique em **Recursos (⚙) → Servidores**. O cartão Servidores é exibido com uma exibição tabular de todos os servidores gerenciados.

Etapa 2. Selecione o servidor para controlar remotamente.

Etapa 3. Clique no ícone **Iniciar controle remoto** (🖵).

Etapa 4. Aceite todos os avisos de segurança do navegador da Web.

Depois de concluir

Se a sessão de controle remoto não for aberta com êxito, consulte Problemas de controle remoto na documentação online do XClarity Orchestrator.

Abrindo uma sessão de controle remoto para servidores ThinkServer

É possível abrir uma sessão de controle remoto de servidores ThinkServer gerenciados como se estivesse em um console local. Em seguida, você pode usar a sessão de controle remoto para executar operações de energia e redefinição, montar logicamente uma unidade de rede ou local no servidor, fazer capturas de tela e gravar vídeos.

Antes de iniciar

Você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** ou **Hardware** é atribuída.

O servidor gerenciado deve ter um estado de funcionamento normal e estado de conectividade online. Para obter mais informações sobre como exibir o status do servidor, consulte Visualizando detalhes de dispositivos.

A chave do Features on Demand para o ThinkServer System Manager Premium Upgrade deve ser instalada no servidor gerenciado. Para obter mais informações sobre chaves FoD instaladas nos seus servidores, consulte Visualizando chaves do Feature on Demand na documentação online do Lenovo XClarity Administrator.

Um Java Runtime Environment (JRE) com suporte ao Java WebStart (como Adopt OpenJDK 8 com o plug-in IcedTea-Web v1.8) deve ser instalado no servidor local.

Sobre esta tarefa

Você pode abrir uma sessão de controle remoto para um único servidor ThinkServer.

Para obter mais informações sobre como usar os recursos do console remoto e mídia do ThinkServer, consulte a documentação do servidor ThinkServer.

Procedimento

Para abrir uma sessão do controle remoto para um servidor ThinkSystem ou ThinkAgile, conclua as etapas a seguir.

Etapa 1. No menu XClarity Orchestrator, clique em **Recursos (**) → **Servidores**. O cartão Servidores é exibido com uma exibição tabular de todos os servidores gerenciados.

Etapa 2. Selecione o servidor para controlar remotamente.

Etapa 3. Clique no ícone **Iniciar controle remoto** ( ).

Etapa 4. Aceite todos os avisos de segurança do navegador da Web.

Depois de concluir

Se a sessão de controle remoto não for aberta com êxito, consulte Problemas de controle remoto na documentação online do XClarity Orchestrator.

Abrindo uma sessão de controle remoto para servidores System x

É possível abrir uma sessão de controle remoto de servidores System x gerenciados como se estivesse em um console local. Em seguida, você pode usar a sessão de controle remoto para executar operações de energia e redefinição, montar logicamente uma unidade de rede ou local no servidor, fazer capturas de tela e gravar vídeos.

Antes de iniciar

Revise as considerações sobre segurança, desempenho e teclado antes de abrir uma sessão de controle remoto. Para obter mais informações sobre essas considerações, consulte Considerações sobre controle remoto.

Você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** ou **Hardware** é atribuída.

O servidor gerenciado deve ter um estado de funcionamento normal e estado de conectividade online. Para obter mais informações sobre como exibir o status do servidor, consulte Visualizando detalhes de dispositivos.

Use sua conta de usuário do Lenovo XClarity Orchestrator para fazer login na sessão de controle remoto. A conta do usuário deve ter autoridade de usuário suficiente para acessar e gerenciar um servidor.

Um Java Runtime Environment (JRE) com suporte ao Java WebStart (como Adopt OpenJDK 8 com o plug-in IcedTea-Web v1.8) deve ser instalado no servidor local.

A chave do Features on Demand para presença remota deve ser instalada e habilitada no servidor gerenciado. Você pode determinar se a presença remota está habilitada ou desabilitada na página Servidores e clicando em **Filtros → Presença Remota**. Se estiver desabilitado:

- Verifique se o servidor está em um status de funcionamento normal e estado de conectividade online.
- Verifique se o nível XClarity Controller Enterprise ou o upgrade avançado de MM está ativado para servidores que não são fornecidos com esses recursos já ativados por padrão.

A sessão de controle remoto usa as configurações de idioma definidas para o sistema operacional no sistema local.

Sobre esta tarefa

É possível iniciar várias sessões de controle remoto. Cada sessão pode gerenciar diversos servidores.

Nota: Para servidor Flex System x280, x480 e x880, é possível iniciar uma sessão de controle remoto só para o nó primário. Se você tentar iniciar uma sessão de controle remoto para um nó não primário em um sistema de vários nós, a caixa de diálogo do controle remoto é iniciada, mas nenhum vídeo é exibido.

Procedimento

Para abrir uma sessão do controle remoto para um servidor System x, conclua as etapas a seguir.

Etapa 1. No menu XClarity Orchestrator, clique em **Recursos ( ) → Servidores**. O cartão Servidores é exibido com uma exibição tabular de todos os servidores gerenciados.

Etapa 2. Selecione o servidor para controlar remotamente.

Se você não selecionar um servidor, uma sessão de controle remoto não selecionada será aberta.

Etapa 3. Clique no ícone **Iniciar controle remoto** ( ).

Etapa 4. Aceite todos os avisos de segurança do navegador da Web.

Etapa 5. Quando solicitado, selecione um dos seguintes modos de conexão:

- **Modo de usuário único**. Estabelece uma sessão de controle remoto exclusiva com o servidor. Todas as outras sessões de controle remoto para esse servidor são bloqueadas até que você se desconecte do servidor. Essa opção só estará disponível se não houver outras sessões de controle remoto estabelecidas com o servidor.
- **Modo multiusuário**. Permite que diversas sessões de controle remoto sejam estabelecidas com o mesmo servidor. O XClarity Orchestrator suporta até seis sessões de controle remoto simultâneas com o mesmo servidor.

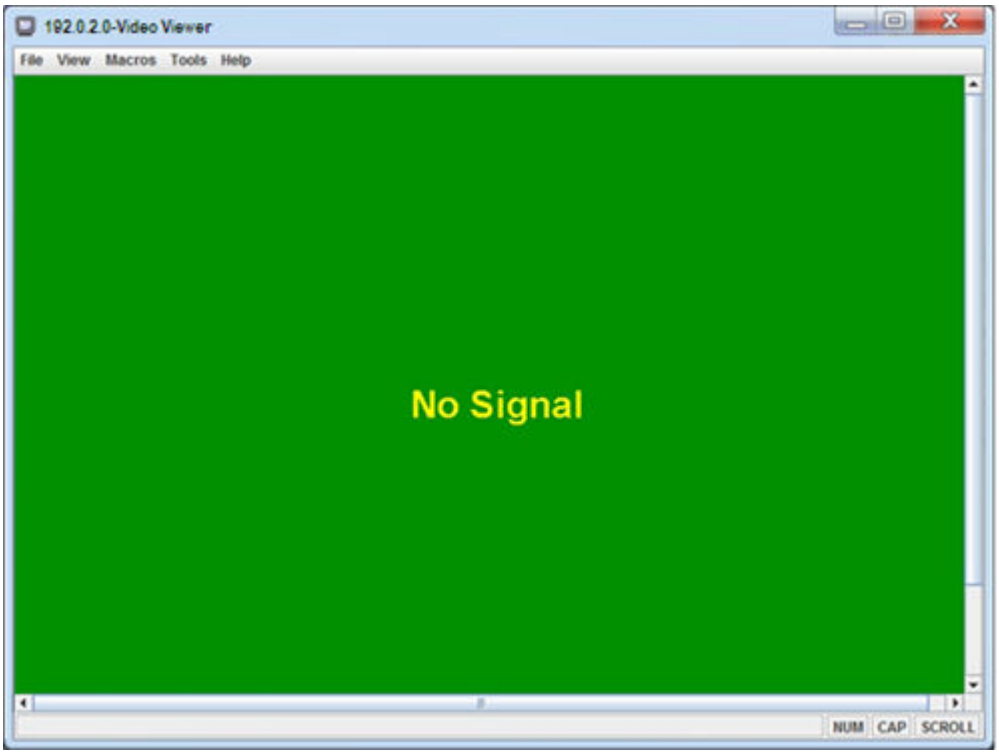
Etapa 6. Clique em **Iniciar controle remoto**.

Etapa 7. Quando solicitado, escolha se deseja salvar um atalho para a sessão de controle remoto no sistema local. É possível usar esse atalho para iniciar uma sessão de controle remoto sem fazer login na interface da Web do XClarity Orchestrator. O atalho contém um link que abre uma sessão de controle remoto a qual pode ser usada para adicionar servidores manualmente.

Nota: Seu sistema local deve ter acesso ao XClarity Orchestrator para validar a conta de usuário com o servidor de autenticação XClarity Orchestrator.

Depois de concluir

A sessão de controle remoto tem uma miniatura (ícone) para cada servidor que é gerenciado atualmente por meio da sessão.



Se a sessão de controle remoto não for aberta com êxito, consulte Problemas de controle remoto na documentação online do XClarity Orchestrator.

É possível executar as ações a seguir na sessão de controle remoto.

- Exibir vários consoles de servidor e mover-se entre os consoles do servidor clicando em uma miniatura. O console do servidor é exibido na área de sessão de vídeo. Se você estiver acessando mais servidores do que a quantidade permitida na área de ícones, clique no ícone **Rolar para a direita** ( ) e **Rolar para a esquerda** ( ) para rolar as miniaturas adicionais do servidor. Clique no ícone **Todas as sessões** ( ) para ver uma lista de todas as sessões do servidor abertas.
- Adicionar um console do servidor à sessão atual de controle remoto clicando no ícone **Adicionar servidor** ( ).
- Ocultar ou mostrar a área de miniatura clicando no ícone **Alternar Miniaturas** ( ).
- Exibir a sessão de controle remoto como uma janela ou uma tela cheia clicando no ícone **Tela** ( ) e em **Entrar em tela cheia** ou **Sair da tela cheia**.
- Usar os botões de tecla de aderência Ctrl, Alt e Shift para enviar pressionamentos de tecla diretamente para o servidor. Ao clicar em uma tecla de aderência, a tecla permanecerá ativa até que você pressione uma tecla do teclado ou clique no botão novamente.Para enviar uma combinação de tecla Ctrl ou Alt, clique em Ctrl ou Alt na barra de ferramentas, coloque o cursor na área de sessão de vídeo e pressione uma tecla no teclado.

  Nota: Se o modo de captura de mouse estiver ativado, pressione a tecla Alt esquerda para mover o cursor para fora da área da sessão de vídeo. Mesmo que o modo de captura do mouse esteja desabilitado por padrão, é possível habilitá-lo na página Barra de ferramentas (consulte Configurando preferências de controle remoto).
- Definir sequências de teclas personalizadas, conhecidas como teclas de acesso, clicando no ícone **Teclado** ( ).As definições de tecla de função são armazenadas no sistema a partir do qual você iniciou

a sessão de controle remoto. Portanto, se você iniciar a sessão de controle remoto a partir de outro sistema, terá que definir as teclas de função novamente. É possível exportar configurações do usuário, incluindo teclas de acesso, clicando no ícone **Preferência** (), clicando na guia **Configurações do usuário** e, em seguida, clicando em **Importar**.

- Fazer uma captura de tela da sessão do servidor selecionado atualmente e salvá-la em vários formatos clicando no ícone **Tela** () e, em seguida, em **Captura de tela**.
- Montar a mídia remota (como um CD, DVD, dispositivo USB, imagem de disco ou uma imagem de CD [ISO]) no servidor selecionado ou mover um dispositivo montado para outro servidor clicando no ícone **Mídia Remota** ().
- Fazer upload de imagens para um servidor de mídia remota clicando no ícone **Mídia Remota** (), clicando em **Montar mídia remota** e, em seguida, clicando em **Fazer upload da imagem para o IMM**.
- Ligar ou desligar o servidor a partir de um console remoto clicando no ícone **Energia** ().
- Alterar as preferências de controle remoto, incluindo a frequência com que o ícone de servidor é atualizado (consulte Configurando preferências de controle remoto).

Considerações sobre controle remoto

Esteja atento a segurança, desempenho e as considerações sobre o teclado relacionadas ao acesso aos servidores gerenciados usando uma sessão de controle remoto.

Considerações sobre segurança

A conta do usuário usada para iniciar a sessão de controle remoto deve ser um ID de usuário válido que foi definido no servidor de autenticação Lenovo XClarity Orchestrator. A conta do usuário também deve ter autoridade de usuário suficiente para acessar e gerenciar um servidor.

Por padrão, diversas sessões de controle remoto podem ser estabelecidas para um servidor. Entretanto, quando você inicia uma sessão de controle remoto, tem a opção de iniciá-la no modo de usuário único, que estabelece uma sessão exclusiva com o servidor. Todas as outras sessões de controle remoto para esse servidor são bloqueadas até que você se desconecte do servidor.

Nota: Essa opção só estará disponível se não houver outras sessões de controle remoto estabelecidas atualmente com o servidor.

Para usar o FIPS (Federal Information Processing Standard) 140, você deverá habilitá-lo manualmente concluindo as seguintes etapas no sistema local:

1. Localize o nome do provedor de criptografia certificada FIPS 140 instalada no seu sistema local.
2. Edite o arquivo `$(java.home)/lib/security/java.security`.
3. Altere a linha que inclui o `com.sun.net.ssl.internal.ssl.Provider` criando o nome do provedor do seu provedor criptográfico certificado FIPS 140. Por exemplo, altere:
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider`
   para:
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11-NSS`

Considerações de desempenho

Se uma sessão de controle remoto se tornar lenta ou não responder, feche todas as sessões de vídeo e mídia remota que você tenha estabelecido com o servidor selecionado para reduzir o número de conexões de servidor abertas. Além disso, você pode aumentar o desempenho alterando as preferências a seguir. Para obter mais informações, consulte Configurando preferências de controle remoto.

- **KVM**

  - Diminua a porcentagem da largura de banda de vídeo usada pelo aplicativo. A qualidade da imagem da sessão de controle remoto será reduzida.
  - Diminua a porcentagem de quadros atualizados pelo aplicativo. A taxa de atualização da sessão de controle remoto será reduzida.
- **Miniaturas**
  - Aumente a taxa do intervalo de atualização de miniatura. O aplicativo atualizará as miniaturas em uma taxa mais lenta.
  - Desative a exibição de miniaturas completamente.

O tamanho da janela da sessão de controle remoto e o número de sessões ativas podem afetar os recursos da estação de trabalho, como memória e largura de banda da rede, que podem influenciar o desempenho. A sessão de controle remoto usa um limite de 32 sessões abertas. Se mais de 32 sessões estiverem abertas, o desempenho pode ser reduzido severamente e a sessão de controle remoto pode ficar sem resposta. Você poderá consultar a degradação de desempenho com menos de 32 sessões abertas se os recursos, incluindo a largura de banda da rede e a memória local não forem suficientes.

Considerações de teclado

A sessão de controle remoto suporta os seguintes tipos de teclado:
- Belga com 105 teclas
- Português do Brasil
- Chinês
- Francês com 105 teclas
- Alemão com 105 teclas
- Italiano com 105 teclas
- Japonês com 109 teclas
- Koreano
- Português
- Russo
- Espanhol com 105 teclas
- Suíço com 105 teclas
- Britânico com 105 teclas
- Americano com 104 teclas

Para obter informações sobre as preferências do teclado, consulte Configurando preferências de controle remoto.

Configurando preferências de controle remoto

É possível alterar as configurações de preferências para a sessão atual de controle remoto.

Procedimento

Conclua as seguintes etapas para modificar as preferências do controle remoto.

Etapa 1. Para modificar as preferências do controle remoto, clique no ícone **Preferências** (). Todas as alterações têm efeito imediatamente.

- **KVM**
  - **Porcentagem de Largura de Banda de Vídeo**. O aumento da largura de banda melhora a qualidade na aparência da sessão de controle remoto, mas pode afetar o desempenho da sessão de controle remoto.
  - **Porcentagem de Quadros Atualizados**. O aumento da porcentagem de atualização de quadro aumenta a frequência com que a sessão de controle remoto é atualizada, mas pode afetar o desempenho da sessão de controle remoto.

- **Tipo de teclado**. Selecione o tipo de teclado que você está usando para a sessão de controle remoto. O tipo de teclado que você seleciona deve corresponder configurações do teclado no sistema local e corresponde as configurações do teclado no host remoto.

  Nota: Se você selecionar um teclado internacional e precisar inserir combinações de teclas que requerem a chave Gráficos Alternativos (AltGr), certifique-se de que o sistema operacional na estação de trabalho que você usa para chamar a sessão de controle remoto seja do mesmo tipo de sistema operacional do servidor que você deseja acessar remotamente. Por exemplo, se o servidor estiver executando Linux, certifique-se de chamar o aplicativo de controle remoto a partir de uma estação de trabalho que execute o Linux.
- **Dimensionar imagem na janela**. Selecione essa opção para dimensionar a imagem de vídeo recebida do servidor para o tamanho da área da sessão de vídeo.

- **Segurança**
  - **Preferir conexões no modelo de usuário único**. Especifique se as conexões no modo de usuário único é a opção padrão ao conectar-se a um servidor. Quando uma conexão é feita no modo de usuário único, apenas um usuário pode ser conectado a um servidor por vez. Se essa caixa não estiver selecionada, a função padrão será conectar-se ao servidor no modo multiusuário.
  - **Requerer (assegurar) conexões de tunelamento**. Selecione essa opção para acessar um servidor por meio do nó de gerenciamento. É possível usar essa opção para acessar um servidor de um cliente que não está na mesma rede que o servidor.

    Nota: O aplicativo de controle remoto sempre tentará se conectar diretamente ao servidor do sistema local onde o controle remoto foi iniciado. Se você selecionar essa opção, o aplicativo de controle remoto acessará o servidor por meio do Lenovo XClarity Orchestrator se a estação de trabalho do cliente não puder acessar o servidor diretamente.
- **Barra de ferramentas**

  Nota: Clique em **Restaurar Padrões** para restaurar todas as configurações nesta página para as definições padrões
  - **Fixar a barra de ferramentas na janela**. Por padrão, a barra de ferramentas fica oculta acima da janela da sessão de controle remoto e exibe apenas quando você move o ponteiro do mouse sobre ela. Se você selecionar esta opção, a barra de ferramentas é fixada à janela e é sempre exibida entre o painel miniatura e a janela da sessão do controle remoto.
  - **Mostrar botões do teclado**. Especifique onde mostrar os ícones de botões do teclado (CapsLock, NumLock e ScrollLock) na barra de ferramentas.
  - **Mostrar controle de energia**. Especifique se as opções de controle de energia devem ser exibidos na barra de ferramentas.
  - **Mostrar botões de tecla fixa**. Especifique se os ícones de botão de tecla fixa (Ctrl, Alt e Delete) devem ser exibidos na barra de ferramentas.
  - **Ocultar ponteiro do mouse local**. Especifique se você deseja exibir o ponteiro do mouse local quando posicionar o cursor na sessão do servidor exibida atualmente na área de sessão de vídeo.
  - **Ativar modo de captura de mouse**. Por padrão, o modo de captura de mouse fica desativado. Isso significa que você pode mover livremente o cursor para dentro e para fora da área da sessão de vídeo. Se você ativar o modo de captura de mouse, deverá pressionar a tecla Alt esquerda para poder mover o cursor para fora da área da sessão de vídeo. Se o modo de captura de mouse estiver ativado, será possível especificar o uso ou não das teclas Ctrl+Alt para sair do modo de captura de mouse. O padrão é usar a tecla Alt esquerda.

  - **Especificar opacidade do plano de fundo da barra de ferramentas**. A redução da porcentagem de opacidade permite exibir mais da área de sessão de vídeo através do plano de fundo da barra de ferramentas.

    Nota: Essa opção está disponível apenas quando a barra de ferramentas não está fixada na janela.

- **Miniaturas**
  - **Mostrar miniaturas**. Selecione essa opção para mostrar a área de miniatura na sessão de controle remoto.
  - **Especificar intervalo de atualização de miniatura**. A diminuição do intervalo para atualizar miniaturas aumenta a frequência com que as miniaturas do servidor são atualizadas.
- **Geral**
  - **Modo de depuração**. Especifica se o modo de depuração deve ser configurado para o aplicativo de controle remoto. As configurações determinam a granularidade de eventos que são registrados nos arquivos de log. Por padrão, apenas eventos graves são registrados.
  - **Herdar configurações de aparência do sistema**. Essa configuração altera a aparência para corresponder aos esquemas de cores configurados para o servidor local (executando o Windows). Você deve reiniciar o aplicativo de controle remoto para que essas configurações tenham efeito.
  - **Criar ícone do desktop**. Essa configuração cria um ícone de desktop em seu sistema local para que você possa iniciar o aplicativo de controle remoto diretamente do seu sistema. Você deve ainda ter acesso ao software de gerenciamento do seu sistema.
  - **Sincronizar com servidor de gerenciamento**. Essa definição assegura que os dados do servidor que são exibidos no aplicativo de controle remoto correspondam aos dados do servidor que são exibidos pelo software de gerenciamento.

Capítulo 5. Fornecimento de recursos

É possível usar o Lenovo XClarity Orchestrator para fornecer seus recursos gerenciados, como implantar atualizações nos gerenciadores de recursos do Lenovo XClarity Administrator e servidores gerenciados e configurar servidores gerenciados.

Fornecimento das configurações do servidor

Os padrões de configuração do servidor são usados para configurar rapidamente vários servidores a partir de um único conjunto de configurações definidas. Cada padrão define as características de configuração para um tipo de servidor específico. É possível criar um padrão de servidor aprendendo as configurações de servidor existente.

Antes de iniciar

Verifique se os servidores que você deseja configurar estão atualizados com o firmware mais recente.

Sobre esta tarefa

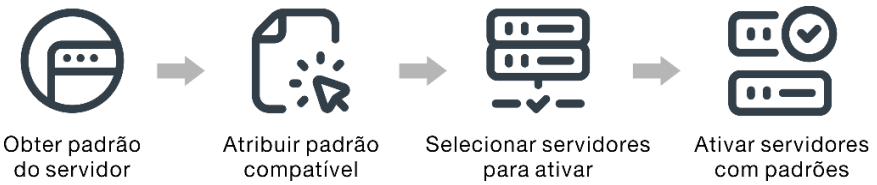
A configuração de servidores usando padrões é compatível apenas com servidores ThinkSystem (excluindo SR635 e SR655).

É possível usar padrões de configuração do servidor para definir as configurações e definições do Baseboard Management Controller e da Unified Extensible Firmware Interface (UEFI) nos servidores gerenciados. Os padrões integram suporte para virtualizar endereços de E/S. Assim, é possível virtualizar conexões de malha do servidor ou redefinir servidores sem interromper a malha.

Não é possível definir as configurações a seguir.
- Ordem de inicialização
- Armazenamento local e zoneamento de SAN
- Adaptadores de E/S
- Contas de usuários locais
- Servidores LDAP

Procedimento

A figura a seguir ilustra o fluxo de trabalho para configurar servidores gerenciados.



Etapa 1. **Criar um padrão de servidor**

É possível criar padrões para representar diferentes configurações usadas em seu data center, aprendendo as configurações e definições dos servidores existentes.

Importante: Considere criar um padrão para cada tipo de servidor em seu data center. Por exemplo, crie um padrão de servidor para todos os servidores ThinkSystem SR650 e outro padrão

de servidor para todos os servidores ThinkSystem SR850. Não implante um padrão de configuração criado para um tipo do servidor em outro tipo de servidor.

Para obter mais informações sobre como criar padrões de servidor, consulte Aprendendo um padrão de configuração de servidor de um servidor existente.

Etapa 2. **Atribuir o padrão a um ou mais servidores gerenciados**

É possível atribuir um padrão a vários servidores; entretanto, cada servidor pode ter apenas um padrão atribuídoXClarity Orchestrator.

Considere criar um padrão para cada tipo de servidor em seu data center. Por exemplo, crie um padrão de servidor para todos os servidores ThinkSystem SR650 e outro padrão de servidor para todos os servidores ThinkSystem SR850.

Não atribua nem implante um padrão de servidor criado para um tipo do servidor em outro tipo de servidor.

Depois de atribuir um padrão aplicável a um ou mais servidores de destino, o XClarity Orchestrator executa uma verificação de conformidade nos servidores para determinar se a configuração do servidor corresponde ao padrão. Os servidores que estão fora de conformidade com seu padrão atribuído são sinalizados.

Para obter mais informações sobre como criar padrões de servidor, consulte Aplicando e ativando atualizações aos gerenciadores de recursos.

Etapa 3. **Implantar o padrão atribuído nos servidores de destino**

Você pode implantar padrões atribuídos a um ou mais servidores específicos ou a grupos de servidores. Quando você implanta um padrão, as configurações e as definições desse padrão são gravados na memória compartilhada e, em seguida, ativados. Algumas configurações requerem uma reinicialização do sistema antes de serem ativadas.

Os servidores devem ser atualizados para ativar determinadas alterações de configuração, como configurações do Baseboard Management Controller e Unified Extensible Firmware Interface (UEFI). É possível escolher quando ativar as alterações:

- A **Ativação adiada** ativa todas as alterações de configuração após a próxima reinicialização do servidor. É necessário reiniciar o servidor manualmente para prosseguir com o processo de implantação.

  Importante: Use **Reiniciar normalmente** para reiniciar o servidor para continuar o processo de atualização. *Não* use **Reiniciar Imediatamente**.

Nota: As configurações em um servidor poderão ficar fora de conformidade com seu padrão se as configurações forem alteradas diretamente no servidor em vez de nos padrões atribuídos ou se ocorrer um problema quando o padrão atribuído for implantado, como um problema de firmware ou uma configuração inválida. É possível determinar o status de conformidade de cada servidor na guia **Atribuir e implantar**.

Atenção: O XClarity Orchestrator não atribui endereços IP e E/S a servidores individuais quando os padrões de servidor são implantados.

Para obter mais informações sobre como criar políticas de conformidade de atualização, consulte Atribuindo e implantando um padrão de configuração do servidor.

Etapa 4. **Modificar e reimplantar um padrão**É possível fazer alterações de configuração subsequentes em um padrão existente. Ao salvar o padrão, o XClarity Orchestrator executa uma verificação de

conformidade nos servidores que são atribuídos a esse padrão para determinar se a configuração do servidor corresponde ao padrão. É possível, então, reimplantar o padrão alterado para todos ou um subconjunto de servidores que são atribuídos a esse padrão.

Considerações sobre configuração do servidor

Antes de iniciar a configuração dos servidores usando Lenovo XClarity Orchestrator, revise as seguintes considerações importantes.

Considerações sobre servidor

- A configuração de servidores usando padrões é compatível apenas com servidores ThinkSystem (excluindo SR635 e SR655).
- Verifique se os servidores que você deseja configurar estão atualizados com o firmware mais recente.

Considerações sobre padrão de configuração

- É possível atribuir um padrão a vários servidores; entretanto, cada servidor pode ter apenas um padrão atribuídoXClarity Orchestrator.

  Nota: O XClarity Orchestrator não impede que você atribua ou implante um padrão de configuração do servidor em um servidor que tenha um padrão ou perfil de servidor atribuído em Lenovo XClarity Administrator. A implantação de um padrão usando XClarity Orchestrator pode afetar a conformidade do padrão em XClarity Administrator.
- É possível usar padrões de configuração do servidor para definir as configurações e definições do Baseboard Management Controller e da Unified Extensible Firmware Interface (UEFI) nos servidores gerenciados. Os padrões integram suporte para virtualizar endereços de E/S. Assim, é possível virtualizar conexões de malha do servidor ou redefinir servidores sem interromper a malha.

  Não é possível definir as configurações a seguir.
  - Ordem de inicialização
  - Armazenamento local e zoneamento de SAN
  - Adaptadores de E/S
  - Contas de usuários locais
  - Servidores LDAP
- Considere criar um padrão para cada tipo de servidor em seu data center. Por exemplo, crie um padrão de servidor para todos os servidores ThinkSystem SR650 e outro padrão de servidor para todos os servidores ThinkSystem SR850.
- Não atribua nem implante um padrão de servidor criado para um tipo do servidor em outro tipo de servidor.
- As configurações em um servidor podem ficar fora de conformidade com o padrão atribuído nas instâncias a seguir. É possível determinar o status de conformidade de cada servidor na guia **Atribuir e implantar**.
  - As configurações foram alteradas diretamente no servidor em vez de nos padrões atribuídos.
  - Ocorreu um problema durante a implantação do padrão, um problema de firmware ou uma configuração inválida.
  - O firmware foi atualizado, o que alterou as configurações e as definições.

    Nota: A implantação poderá falhar se o padrão atribuído for baseado em níveis de firmware anteriores. Nesse caso, é recomendável escolher aprender um novo padrão com base no firmware instalado atualmente ou modificar um padrão existente para excluir a configuração de itens específicos antes de implantar o padrão.

Considerações sobre o processo de configuração

- Enquanto a configuração estiver em andamento, o servidor de destino ficará bloqueado. Não é possível iniciar outras tarefas de gerenciamento no servidor de destino até o processo de configuração ser concluído.
- Depois que um padrão de configuração é implantado em um servidor, uma ou mais reinicializações podem ser necessárias para ativar totalmente as alterações. É possível optar por ativar todas as alterações reiniciando imediatamente o servidor. Se você optar por reiniciar o servidor imediatamente, minimizará o número de reinicializações necessárias do XClarity Orchestrator. Se optar por adiar a ativação, todas as alterações serão ativadas na próxima vez que o servidor for reiniciado. Se você escolher a ativação parcial, as alterações que não requerem uma reinicialização do servidor serão ativadas imediatamente e todas as outras alterações serão ativadas na próxima vez que o servidor for reiniciado.
- Certifique-se de que nenhum trabalho esteja em execução atualmente no servidor de destino. Se houver trabalhos em execução, o trabalho de configuração será colocado na fila até que todos os outros trabalhos sejam concluídos.
- Algumas funções avançadas do servidor são ativadas usando chaves do 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 do Features on Demand correspondente seja instalada.

Aprendendo um padrão de configuração de servidor de um servidor existente

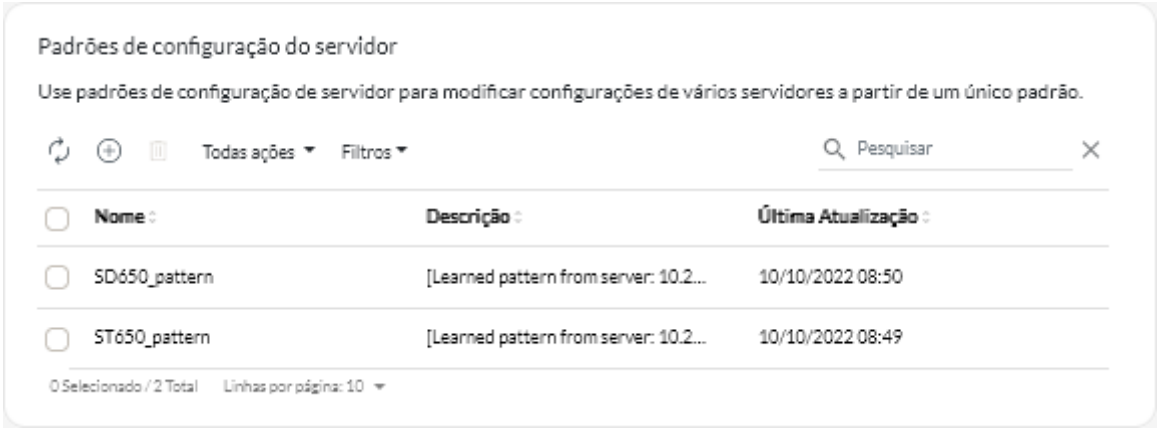
Padrões de configuração do servidor definem as característica de configuração para um tipo de servidor específico. É possível criar um padrão de servidor aprendendo as configurações de servidor existente

Antes de iniciar

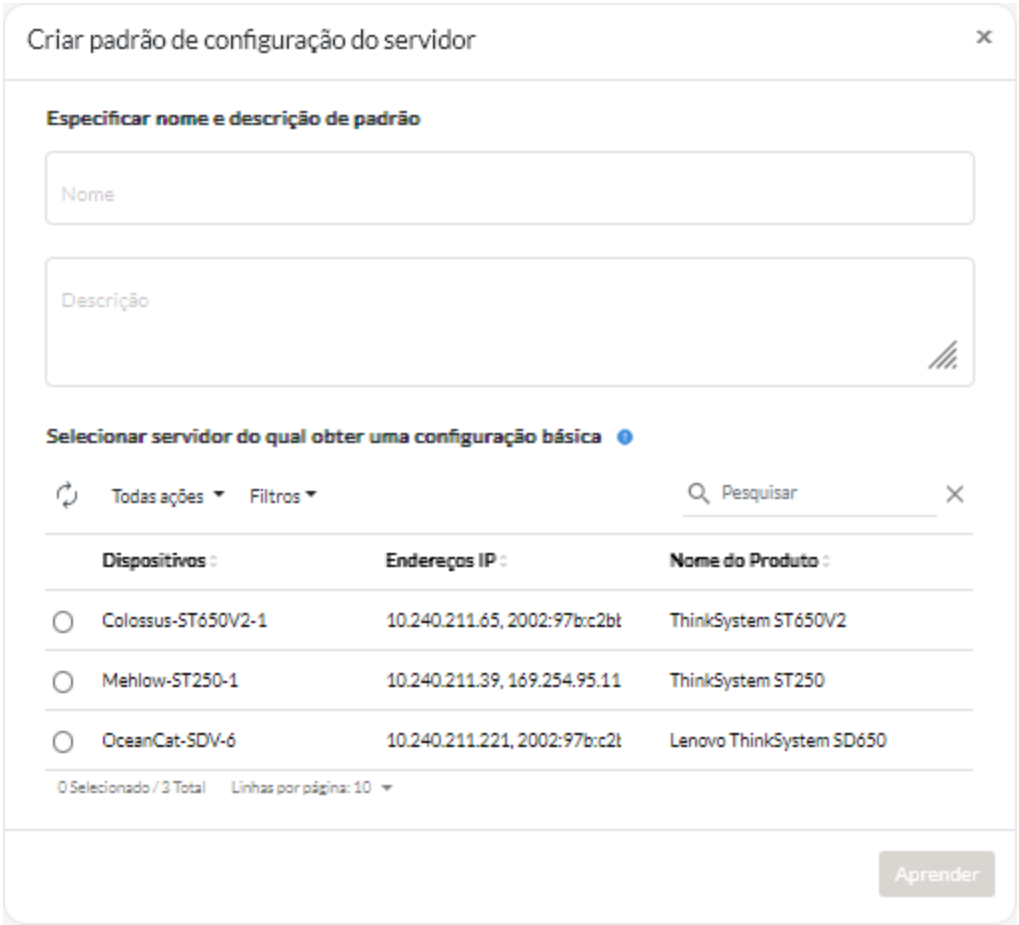
- Leia as considerações de configuração do servidor antes de tentar criar um padrão de configuração de servidor (consulte Atualizar considerações de implantação).
- Verifique se o servidor que você deseja usar para criar o padrão está online.
- Identifique os grupos de servidores que têm as mesmas opções de hardware e que você deseja que configurem da mesma maneira. É possível usar um padrão de servidor para implantar as mesmas definições de configuração em diversos servidores, com isso, controlando uma configuração comum de um local.

Para criar um padrão aprendendo a configuração de um servidor existente, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Orchestrator, clique em **Fornecimento ( ) → Configuração do servidor** e, em seguida, clique na guia **Padrões** para exibir o cartão Padrões de configuração do servidor.



Etapa 2. Clique no ícone **Criar** (⊕) para exibir a caixa de diálogo Criar padrão de configurações do servidor.



Etapa 3. Especifique o nome e a descrição opcional do padrão.

Etapa 4. Selecione o servidor que você deseja usar como base para esse padrão.

Nota: Os modelos de dispositivo incompatíveis são exibidos em texto cinza e não podem ser selecionados.

Etapa 5. Clique em **Aprender**.

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 .)

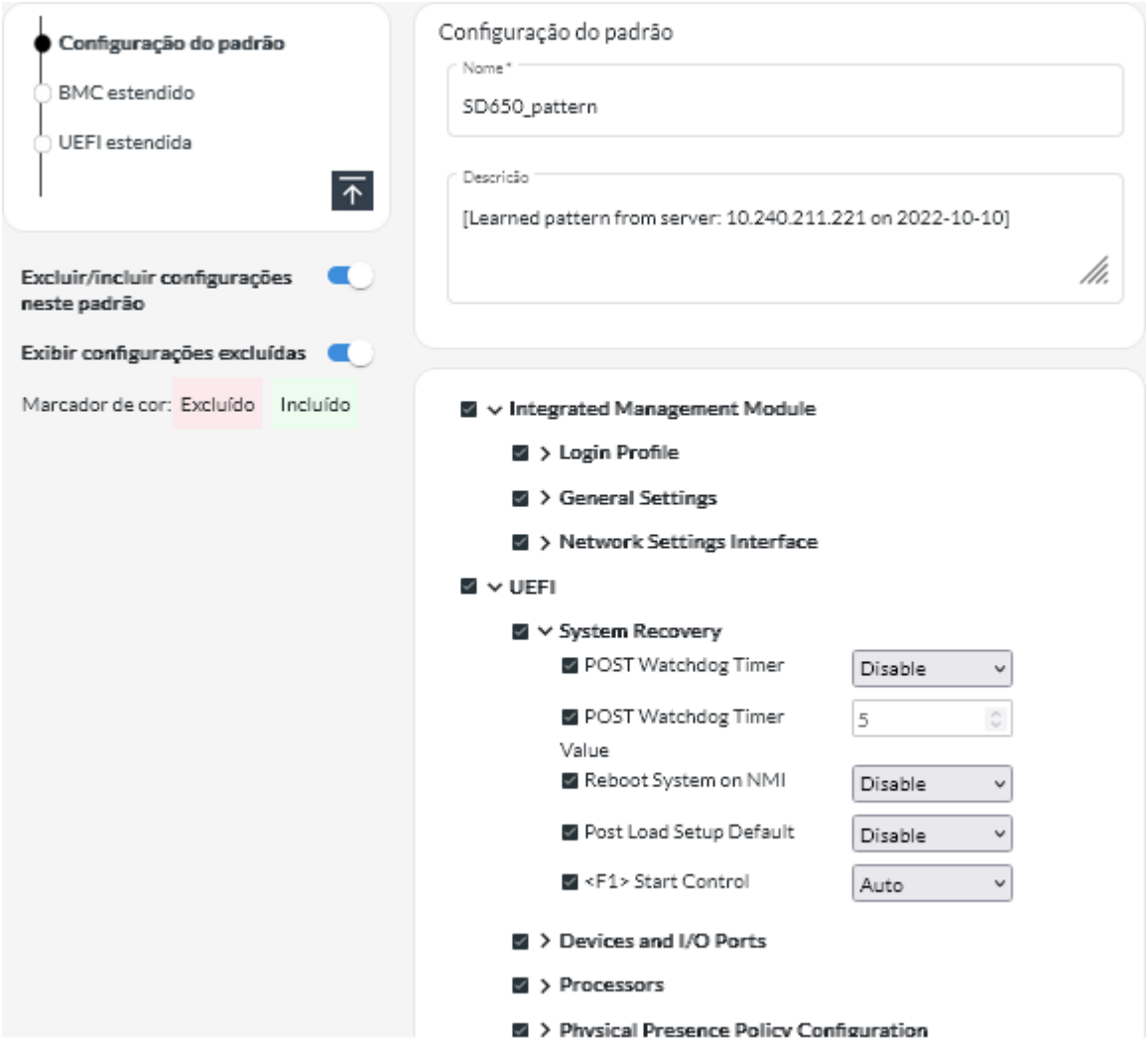
Depois de concluir

É possível executar as ações a seguir na placa Padrões.

- Exiba detalhes do padrão clicando na linha do padrão.
- Copie um padrão selecionado clicando no ícone **Copiar** ( ).
- Modifique as configurações em um padrão clicando na linha para o padrão para exibir seus detalhes, fazendo alterações necessárias e, em seguida, clicando em **Salvar**.Por padrão, todas as configurações aprendidas são incluídas no padrão. É possível excluir as configurações do padrão selecionando **Excluir/incluir configurações no padrão** e, em seguida, limpando as configurações que você não deseja no padrão. As configurações que são limpas (marcadas para exclusão) são realçadas em amarelo. Quando você clica em **Salvar**, apenas as configurações incluídas no padrão são listadas. Se você excluiu as configurações, poderá incluí-las novamente clicando em **Excluir/incluir configurações no padrão**, clicando em **Exibir configurações excluídas** e, em seguida, selecionando as configurações que deseja incluir. As configurações selecionadas (marcadas para inclusão) são realçadas em verde.

  Nota: A verificação de conformidade é baseada apenas em configurações incluídas. As configurações excluídas não são marcadas.

  Ao salvar o padrão modificado, o XClarity Orchestrator executa uma verificação de conformidade nos servidores que são atribuídos a esse padrão para determinar se a configuração do servidor corresponde ao padrão. Em seguida, é possível implantar o padrão alterado nos servidores que não são compatíveis (consulte Atribuindo e implantando um padrão de configuração do servidor).



- Copie um padrão de configuração clicando na linha para o padrão para exibir os detalhes do padrão e, em seguida, clicando em **Salvar como**.
- Exclua um padrão selecionado clicando no ícone **Excluir** ( ).Se o padrão for atribuído a um ou mais servidores, uma caixa de diálogo será exibida com uma lista de servidores aplicáveis. Quando você confirma a solicitação de exclusão, a atribuição do padrão é cancelada nesses servidores.

  Nota: Não é possível excluir um padrão que está sendo implantado ativamente em servidores.
- Atribua e implante um padrão em um ou mais servidores de destino (consulte Atribuindo e implantando um padrão de configuração do servidor).

Atribuindo e implantando um padrão de configuração do servidor

É possível atribuir e implantar um padrão de configuração do servidor em um ou mais servidores gerenciados.

Antes de iniciar

- Leia as considerações de configuração do servidor antes de tentar atribuir ou implantar um padrão em um servidor (consulte Atualizar considerações de implantação).
- Verifique se os servidores que você deseja configurar estão atualizados com o firmware mais recente.

- Não atribua nem implante um padrão de servidor criado para um tipo do servidor em outro tipo de servidor.
- XClarity Orchestrator não impede que você atribua ou implante um padrão de configuração do servidor em um servidor que tenha um padrão ou perfil de servidor atribuído em Lenovo XClarity Administrator. A implantação de um padrão usando XClarity Orchestrator pode afetar a conformidade do padrão em XClarity Administrator.
- XClarity Orchestrator não atribui endereços IP e E/S a servidores individuais quando os padrões de servidor são implantados.

Sobre esta tarefa

Quando um padrão é atribuído a um servidor, o XClarity Orchestrator executa uma verificação de conformidade para comparar as configurações atuais no servidor com as configurações no padrão de configuração e atualiza a coluna **Status de conformidade** com base nos resultados. O status de conformidade pode ser um dos valores a seguir.

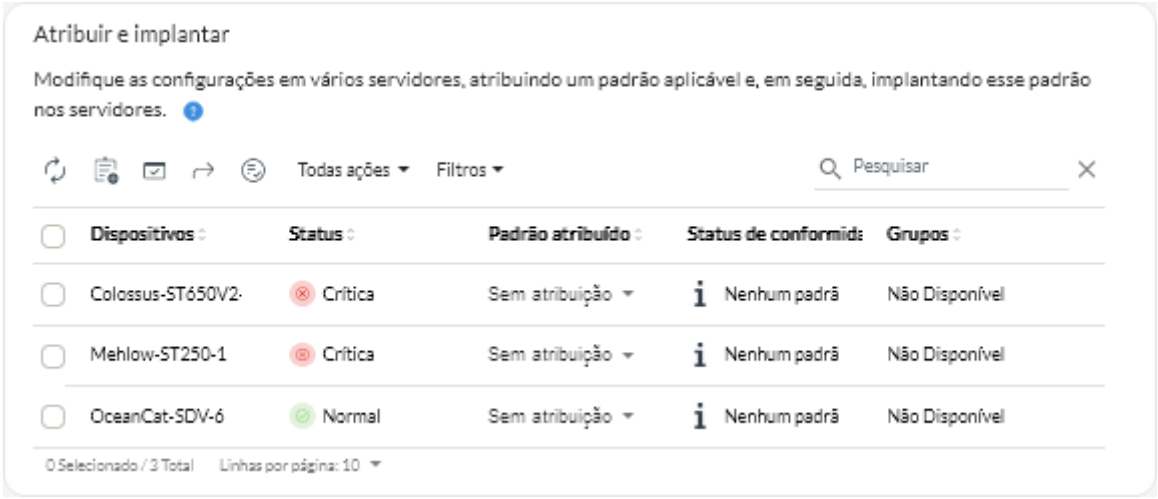
- **Compatível**. Todas as configurações no padrão atribuído corresponderão às configurações no servidor.
- **Não conforme**. Uma ou mais configurações no padrão atribuído *não* correspondem às configurações no servidor. Passe o mouse sobre a célula da tabela para exibir um pop-up que lista as configurações e valores não correspondentes.
- **Pendente**. Uma implantação de padrão ou uma verificação de conformidade está em andamento.
- **Reinicialização pendente**. O servidor precisa ser reiniciado para ativar as alterações de configuração após a implantação do padrão.
- **Não Disponível**. O padrão não é atribuído ao servidor.

Ao implantar um padrão em um servidor, o XClarity Orchestrator modifica as configurações do servidor para corresponder ao padrão de configuração do servidor atribuído. Quando a implantação for concluída, o XClarity Orchestrator executará a verificação de conformidade para verificar se as configurações no padrão atribuído correspondem à configuração no servidor e, em seguida, atualizará o status de conformidade para o servidor.

Procedimento

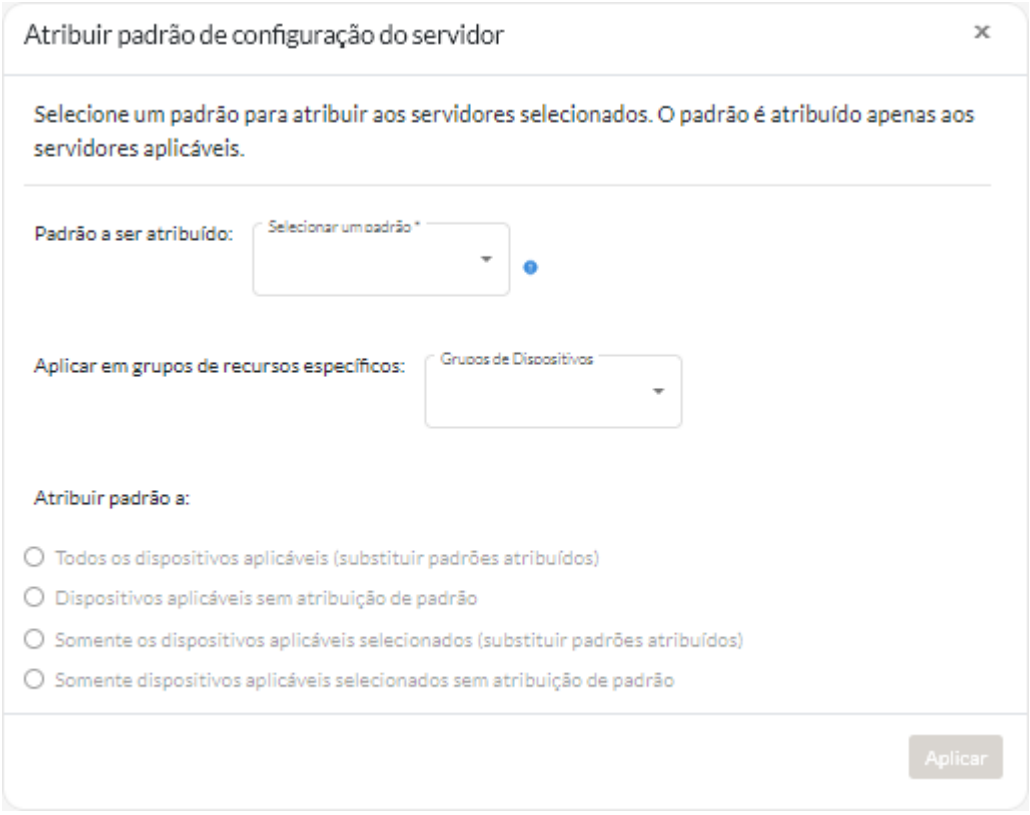
Para atribuir e implantar um padrão de configuração de servidor em um ou mais servidores, execute as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento ( ) → Configuração do servidor** e, em seguida, clique na guia **Atribuir e implantar** para exibir a placa Atribuir e Implantar Padrões de Configuração do Servidor.



Etapa 2. Atribua um padrão a um ou mais servidores.

1. Selecione um ou mais servidores.
2. Clique no ícone **Atribuir** ( ) para exibir a caixa de diálogo Atribuir padrão de configurações do servidor.



3. Selecione o padrão que você deseja atribuir.

Notas:

- Esta lista mostra todos os padrões aplicáveis para os servidores específicos. A lista poderá estar incompleta se o servidor do Orchestrator ainda estiver calculando os padrões aplicáveis. Nesse caso, feche a caixa de diálogo, aguarde algum tempo e abra a caixa de diálogo novamente.

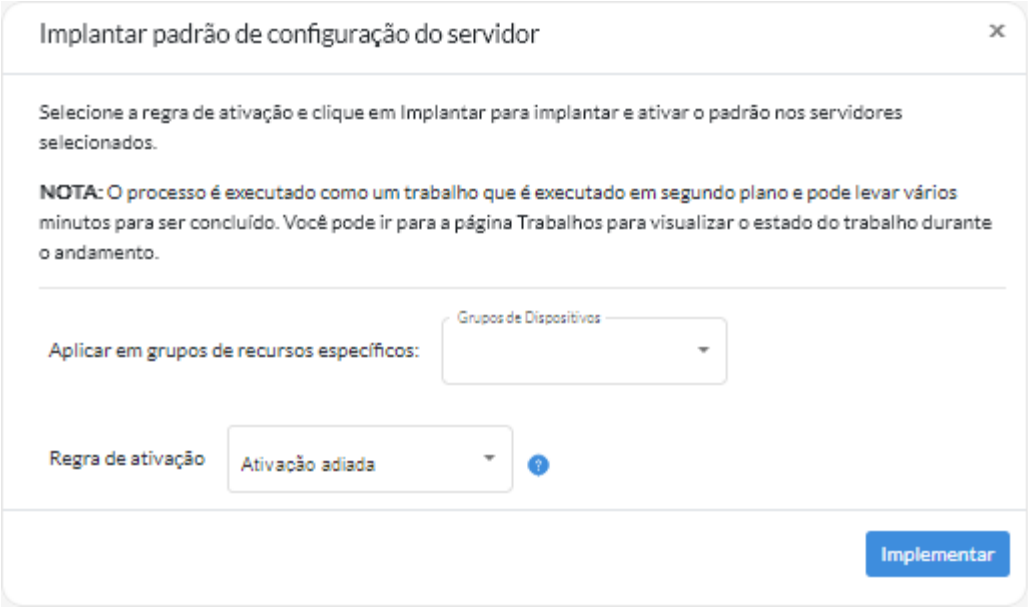
- Selecione o padrão **Sem atribuição** para cancelar a atribuição de um padrão na lista selecionada de dispositivos.

4. Selecione a regra de atribuição. Este pode ser um dos valores a seguir.
   - **Todos os dispositivos aplicáveis (substituir padrões atribuídos)**
   - **Dispositivos aplicáveis sem atribuição de padrão**
   - **Somente os dispositivos aplicáveis selecionados (substituir padrões atribuídos)**
   - **Somente dispositivos aplicáveis selecionados sem atribuição de padrão**
5. Clique em **Atribuir**.

Etapa 3. Implante o padrão atribuído nos servidores específicos.

1. Selecione um ou mais servidores.

   Nota: Os modelos de dispositivo incompatíveis são exibidos em texto cinza e não podem ser selecionados.
2. Clique no ícone **Implantar** ( ) para exibir a caixa de diálogo Implantar padrão de configurações do servidor.



3. Escolha quando ativar as atualizações.
   - A **Ativação adiada** ativa todas as alterações de configuração após a próxima reinicialização do servidor. É necessário reiniciar o servidor manualmente para prosseguir com o processo de implantação.

     Importante: Use **Reiniciar normalmente** para reiniciar o servidor para continuar o processo de atualização. *Não* use **Reiniciar Imediatamente**.
4. Clique em **Implantar**.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 .)

Depois de concluir

É possível executar as ações a seguir na placa Padrões.

- Execute manualmente uma verificação de conformidade de configuração em servidores selecionados clicando em **Todas as Ações → Verificação da conformidade**.

- Cancelamento da atribuição de um padrão de um ou mais servidores de destino atribuindo o padrão **Sem atribuição**.
- Encaminhe relatórios sobre conformidade de configuração de forma recorrente em um ou mais endereços de e-mail clicando no ícone **Criar encaminhador de relatórios** (⊕). O relatório é enviado usando os filtros de dados que estão aplicados atualmente à tabela. Todas as colunas da tabela mostradas e ocultas são incluídas no relatório. Para obter mais informações, consulte Encaminhando relatórios.
- Adicione um relatório de conformidade de configuração a um encaminhador de relatórios específico usando os filtros de dados que estão aplicados atualmente à tabela clicando no ícone **Adicionar ao encaminhador de relatórios** (↱). Se o encaminhador de relatórios já incluir um relatório de conformidade de configuração, ele será atualizado para usar os filtros de dados atuais.

Mantendo a conformidade da configuração do servidor

As configurações em um servidor poderão ficar fora de conformidade com as configurações do servidor alteradas sem usar padrões de configuração, se ocorrer um problema ao aplicar um padrão de configuração (por exemplo, se o padrão for criado a partir de um nível de firmware anterior ao que está no servidor) ou ao aplicar uma atualização de firmware que altere a configuração do servidor (por exemplo, as configurações podem ser adicionadas ou excluídas, os comportamentos de configuração podem mudar, novas opções podem ser adicionadas ou intervalos de valor podem mudar).

Sobre esta tarefa

É possível determinar o status de conformidade de cada servidor na coluna **Status de conformidade** na página Configuração do servidor: Atribuir e Implantar. Se um servidor não for compatível, passe o cursor sobre o status para determinar o motivo.

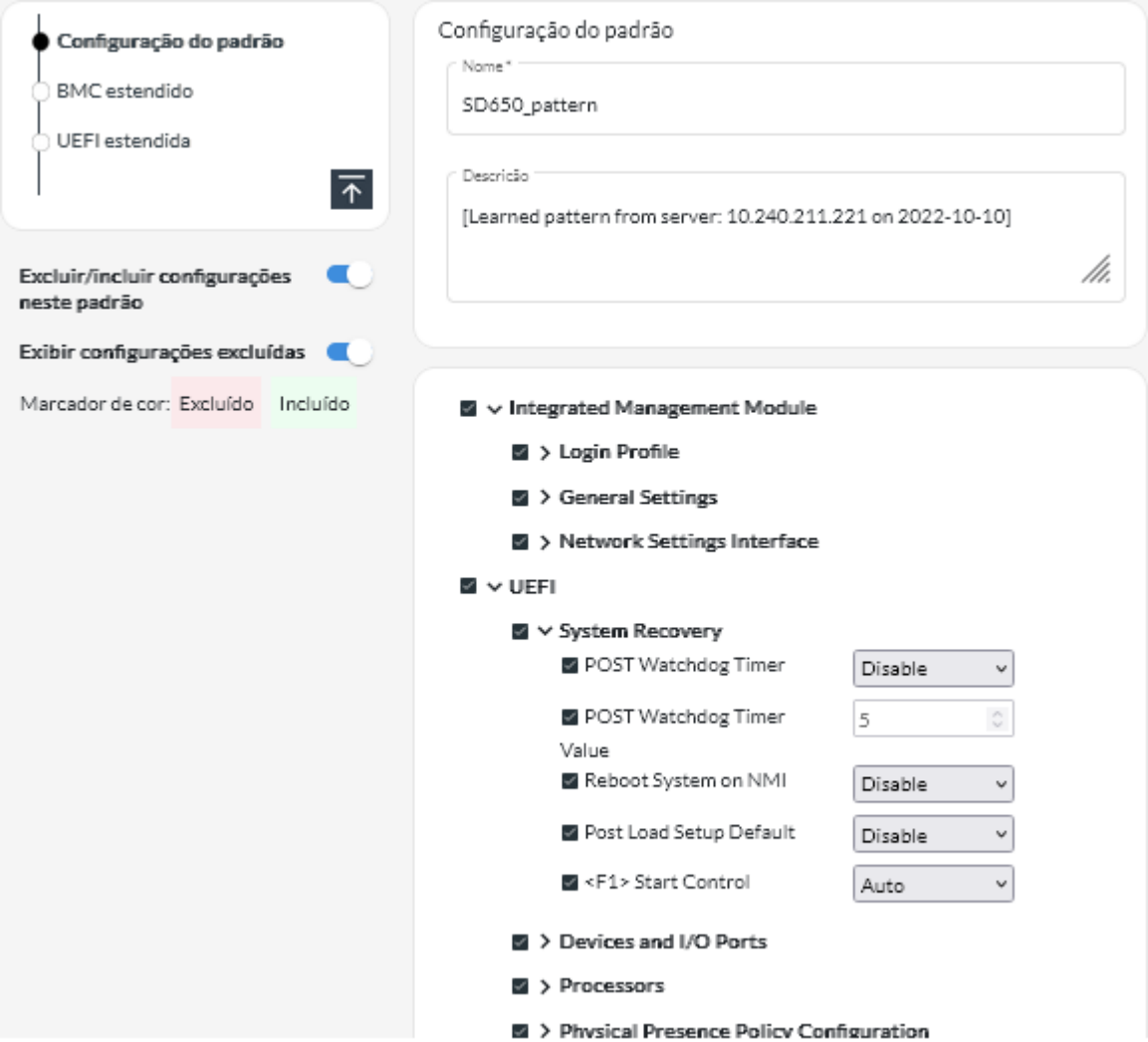
Procedimento

Para resolver problemas de conformidade de configuração do servidor, execute uma das etapas a seguir.

- Aprenda um novo padrão de configuração com base no nível de firmware atual (consulte Aprendendo um padrão de configuração de servidor de um servidor existente). Em seguida, atribua e aplique esse padrão ao servidor (consulte Atribuindo e implantando um padrão de configuração do servidor).
- Modifique o padrão de configuração aplicável para corrigir configurações fora da conformidade clicando na linha para o padrão para exibir seus detalhes, fazendo alterações necessárias e, em seguida, clicando em **Salvar**.Por padrão, todas as configurações aprendidas são incluídas no padrão. É possível excluir as configurações do padrão selecionando **Excluir/incluir configurações no padrão** e, em seguida, limpando as configurações que você não deseja no padrão. As configurações que são limpas (marcadas para exclusão) são realçadas em amarelo. Quando você clica em **Salvar**, apenas as configurações incluídas no padrão são listadas. Se você excluiu as configurações, poderá incluí-las novamente clicando em **Excluir/incluir configurações no padrão**, clicando em **Exibir configurações excluídas** e, em seguida, selecionando as configurações que deseja incluir. As configurações selecionadas (marcadas para inclusão) são realçadas em verde.

  Nota: A verificação de conformidade é baseada apenas em configurações incluídas. As configurações excluídas não são marcadas.

  Ao salvar o padrão modificado, o XClarity Orchestrator executa uma verificação de conformidade nos servidores que são atribuídos a esse padrão para determinar se a configuração do servidor corresponde ao padrão. Em seguida, é possível implantar o padrão alterado nos servidores que não são compatíveis (consulte Atribuindo e implantando um padrão de configuração do servidor).



- Crie uma cópia modificada do padrão de configuração clicando na linha para o padrão para exibir seus detalhes, fazendo alterações necessárias e, em seguida, clicando em **Salvar como**. Em seguida, atribua e aplique esse padrão ao servidor fora da conformidade (consulte Atribuindo e implantando um padrão de configuração do servidor).

Fornecendo sistemas operacionais

É possível usar o Lenovo XClarity Orchestrator para gerenciar o repositório de imagens do SO e implantar imagens do sistema operacional.

Antes de iniciar

O XClarity Orchestrator não implanta sistemas operacionais diretamente em dispositivos. Em vez disso, ele envia solicitações ao gerenciador de recursos aplicável para executar a implantação. O gerenciador de recursos deve ter as licenças necessárias para executar funções de implantação do SO.

Revise as considerações de implantação antes de tentar implantar sistemas operacionais em dispositivos gerenciados (consulte Considerações sobre implantação do sistema operacional).

Verifique se todo o firmware no servidor gerenciado está nos níveis mais recentes (consulte Fornecimento de atualizações para recursos gerenciados).

Verifique se a configuração no servidor gerenciado está atualizada (consulte Fornecimento das configurações do servidor).

Atenção: É recomendado *não* usar o XClarity Orchestrator para executar uma implantação do sistema operacional bare-metal em dispositivos Converged e ThinkAgile.

Nota: Verifique se os servidores são gerenciados usando o XClarity Administratorv4.0 ou posterior.

Sobre esta tarefa

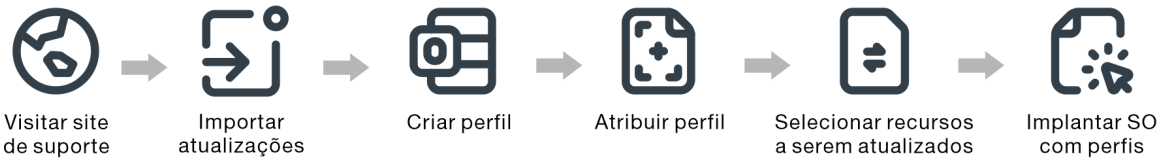
O XClarity Orchestrator fornece uma maneira simples de implantar imagens de sistema operacional em servidores *bare-metal*, que normalmente não têm um sistema operacional instalado. Se você implantar um sistema operacional em um servidor que possui um sistema operacional, o XClarity Orchestrator executará uma instalação nova que substitui as partições nos discos de destino.

Vários fatores determinam a quantidade de tempo necessária para implantar um sistema operacional em um servidor.

- A quantia de RAM instalada no servidor, o que afeta quanto tempo o servidor leva para iniciar.
- O número e os tipos de adaptadores de E/S instalados no servidor, o que afeta o tempo gasto para coletar dados do inventário. Isso também afeta o tempo gasto para o firmware UEFI ser iniciado quando o servidor é iniciado. Durante a implantação do sistema operacional, o servidor é reiniciado várias vezes.
- A quantidade de tráfego de rede. A imagem do sistema operacional é baixada no servidor pela rede de dados ou pela rede de implantação do sistema operacional.
- A quantidade de RAM, processadores e armazenamento de unidade de disco rígido que está disponível para o servidor do Orchestrator e gerenciadores de recursos.

Procedimento

A figura a seguir ilustra o fluxo de trabalho para implantar uma imagem do SO em um servidor.



Etapa 1. **Importe imagens do SO.**

Antes de implantar um sistema operacional em um servidor, você deve primeiro importar a imagem do sistema operacional para o repositório de imagens do SO no gerenciador de recursos do XClarity Orchestrator. Quando você importa uma imagem do SO:

- Verifica se há espaço suficiente no repositório de imagens do SO antes de importar o sistema operacional. Se você não tiver espaço suficiente para importar uma imagem, exclua uma imagem existente do repositório de imagens do SO e tente importar novamente a nova imagem.
- Cria um ou mais perfis dessa imagem e armazena o perfil no repositório de imagens do SO. Cada *perfil* inclui a imagem do SO e opções de instalação. Para obter informações adicionais sobre perfis predefinidos de imagem do SO, consulte Perfis de imagem do sistema operacional.

Um *sistema operacional de base* é a imagem do SO completa que foi importada para o repositório de imagens do SO. A imagem de base importada contém perfis predefinidos que descrevem as configurações de instalação para essa imagem. Você pode criar perfis personalizados com base

em perfis predefinidos na imagem do SO que pode ser implantada para configurações específicas.

Para obter uma lista de sistemas operacionais de base e personalizados suportados, consulte Sistemas operacionais suportados.

Etapa 2. **Personalizar e atribuir o perfil do SO**

Os perfis do sistema operacional são criados automaticamente ao importar um sistema operacional. Os perfis criados são baseados no tipo e na versão do sistema operacional. É possível modificar o perfil, incluindo credenciais do SO, nome do host, configurações de rede e armazenamento, chaves de licença e local de armazenamento.

Etapa 3. **Atribuir e implantar o perfil do SO**

É possível atribuir um perfil do SO a um ou mais servidores de destino e, em seguida, implantar o perfil nesses servidores. . Lembre-se de que para implantar um sistema operacional, o servidor deve ter um status de implantação de **Pronto**.

O XClarity Orchestrator não implanta sistemas operacionais diretamente em dispositivos. Em vez disso, ele envia uma solicitação ao gerenciador de recursos aplicável para executar a implantação e rastreia o progresso da solicitação. O XClarity Orchestrator identifica as dependências, garante que os recursos de destino sejam provisionados na ordem, transfere os arquivos aplicáveis ao gerenciador de recursos e cria uma solicitação para iniciar um trabalho no gerenciador de recursos para executar a implantação.

Antes de tentar implantar uma imagem do sistema operacional, revise Considerações sobre implantação do sistema operacional.

Para obter mais informações sobre como atribuir e implantar um perfil de SO, consulte Implantando uma imagem do sistema operacional.

Considerações sobre implantação do sistema operacional

Antes de tentar implantar uma imagem do sistema operacional, revise as seguintes considerações.

Considerações do gerenciador de recursos

- Para dispositivos que são gerenciados usando o Lenovo XClarity Administrator, garanta que a instância do XClarity Administrator tenha as licenças ou período de avaliação necessários para executar funções de implantação do SO.
- A implantação do SO não é aceita em dispositivos gerenciados pelo Lenovo XClarity Management Hub.

Considerações sobre dispositivo gerenciado

- Verifique se a função de implantação do SO é compatível com os dispositivos de destino..
- Certifique-se de que nenhum trabalho esteja em execução atualmente no servidor de destino. Para ver uma lista de trabalhos ativos, clique em **Monitoramento → Trabalhos**.
- Verifique se todo o firmware no servidor gerenciado está nos níveis mais recentes (consulte Fornecimento de atualizações para recursos gerenciados).
- Verifique se a configuração no servidor gerenciado está atualizada (consulte Fornecimento das configurações do servidor).Além disso, garanta que o dispositivo de destino não tenha um padrão de servidor adiado ou ativado parcialmente. Se um padrão de servidor foi adiado ou ativado parcialmente no servidor gerenciado, você deve reiniciar o servidor para aplicar todas as definições de configuração. Não tente implantar um sistema operacional em um servidor com um padrão de servidor ativado parcialmente.

Para determinar o status de configuração do servidor, consulte o campo **Status da configuração** na página Resumo do servidor gerenciado (consulte Visualizando detalhes de dispositivos).

- Garanta que uma senha da conta raiz que deve ser usada para implantar o sistema operacional seja definida. Para obter mais informações sobre como configurar a senha, consulte Configurando perfis do sistema operacional.
- Certifique-se de que não há nenhuma mídia montada (como ISOs) no servidor de destino. Além disso, certifique-se de que não haja nenhuma sessão de mídia remota ativa abertas para o controlador de gerenciamento.
- Certifique-se de que o carimbo de data/hora no BIOS esteja definido para a data e a hora atuais.
- Para servidores ThinkSystem
  - Verifique se a opção BIOS Legado está desabilitada. No utilitário de configuração BIOS/UEFI (F1), clique em **Configuração UEFI → Configurações do Sistema** e verifique se BIOS legado está definido como Desabilitado.
  - O recurso XClarity Controller Enterprise é necessário para a implantação do sistema operacional.
- Para servidores do System x
  - Verifique se a opção BIOS Legado está desabilitada. No utilitário de configuração BIOS/UEFI (F1), clique em **Configuração UEFI → Configurações do Sistema** e verifique se BIOS legado está definido como Desabilitado.
  - Verifique se uma chave FoD (Feature on Demand) para presença remota está instalada. Você pode determinar se a presença remota está ativada, desativada ou não está instalada em um servidor na página Servidores (consulte Visualizando detalhes de dispositivos).
- Para servidores Flex System, certifique-se de que o chassi esteja ligado.
- Para servidores NeXtScale, verifique se uma chave FoD (Feature on Demand) para presença remota está instalada. Você pode determinar se a presença remota está ativada, desativada ou não está instalada em um servidor na página Servidores (consulte Visualizando detalhes de dispositivos).
- Para dispositivos Converged e ThinkAgile, é recomendado *não* usar o XClarity Orchestrator para executar uma implantação do sistema operacional bare-metal.

Considerações sobre o sistema operacional

- Certifique-se de ter todas as licenças do sistema operacional aplicáveis para ativar os sistemas operacionais instalados. Você é responsável por obter licenças diretamente do fabricante do sistema operacional.
- Assegure-se de que a imagem do sistema operacional que você pretende implantar já esteja carregada no Repositório de imagens do SO. Para obter informações sobre como importar imagens, consulte Importando imagens do sistema operacional.
- Imagens do sistema operacional no repositório de imagens do SO podem não ser compatíveis apenas em certas plataformas de hardware. É possível determinar se um sistema operacional é compatível com um servidor específico no Site do guia de interoperabilidade do SO da Lenovo.
- Sempre instale o sistema operacional mais recente para garantir que possui os drivers de dispositivo do adaptador de E/S de caixa de entrada mais recentes necessários. Para o VMware, use a última Imagem Personalizada da Lenovo para ESXi, que inclui suporte para os adaptadores mais recentes. Para informações sobre como obter essa imagem, consulte Suporte VMware – Página da Web de downloads.

Para obter mais informações sobre limitações para sistemas operacionais específicos, consulte Sistemas operacionais suportados.

Considerações de rede

- Certifique-se de que todas as portas necessárias estejam abertas (consulte Disponibilidade da porta para sistemas operacionais implantados).

- Verifique se o gerenciador de recursos está configurado para usar redes de gerenciamento e de dados.
- Garanta que o gerenciador de recursos possa se comunicar com o servidor de destino (o Baseboard Management Controller e a rede de dados dos servidores) nas interfaces de rede de gerenciamento e de dados.Para especificar uma interface a ser usada para implantação do sistema operacional, consulte Configurando o acesso à rede na documentação online do XClarity Administrator.

  Para obter mais informações sobre a rede de implantação do sistema operacional e interfaces, consulte Considerações de rede na documentação online do XClarity Administrator.
- Se a rede estiver lenta ou instável, você poderá ter resultados imprevisíveis ao implantar sistemas operacionais.
- Você deve usar endereços IP atribuídos dinamicamente usando DHCP. Endereços IP estáticos não têm suporte.

Para obter mais informações sobre a rede de implantação do sistema operacional e interfaces, consulte Configurando o acesso à rede e Considerações de rede na documentação online do XClarity Administrator.

Considerações de armazenamento e opções de inicialização

- É possível instalar o sistema operacional em apenas uma unidade de disco local. Hipervisor incorporado, unidades M.2 e armazenamento SAN não são compatíveis.
- Cada servidor deve ter um adaptador RAID de hardware ou SAS/SATA HBA instalado e configurado. O RAID do software que geralmente está presente no adaptador de armazenamento Intel SATA integrado ou que é configurado como JBOD não é suportado. No entanto, se um adaptador RAID de hardware não estiver presente, configurar o adaptador SATA no Modo AHCI SATA habilitado para implantação do sistema operacional ou configurar discos bons não configurados como JBOD poderá funcionar em alguns casos. Para obter mais informações, consulte O instalador do SO não pode localizar a unidade de disco em que você deseja instalar na documentação online do XClarity Orchestrator.
- Certifique-se de que a opção de inicialização UEFI no servidor de destino esteja configurada como "Apenas inicialização UEFI" antes de implantar um sistema operacional. As opções de inicialização "Apenas legado" e "UEFI primeiro, depois legado" não são suportadas para implantação do sistema operacional.
- Cada servidor deve ter um adaptador RAID de hardware instalado e configurado.

  Atenção:

  – Somente o armazenamento configurado com RAID de hardware é suportado.

  – O RAID do software que geralmente está presente no adaptador de armazenamento Intel SATA integrado ou que é configurado como JBOD não é suportado. No entanto, se um adaptador RAID de hardware não estiver presente, configurar o adaptador SATA no **Modo AHCI SATA** habilitado para implantação do sistema operacional ou configurar discos bons não configurados como JBOD poderá funcionar em alguns casos.

  – Se um adaptador SATA estiver ativado, o modo SATA *não deverá* ser configurado como "IDE."
- O armazenamento NVMe que é conectado à placa-mãe do servidor ou controlador HBA não tem suporte e não deve ser instalado no dispositivo; caso contrário, a implantação do SO em armazenamento não NVMe falhará.
- Certifique-se que o modo de inicialização seguro esteja desabilitado para o servidor. Se estiver implantando um sistema operacional habilitado para o modo de inicialização seguro (como o Windows), desabilite o modo de inicialização seguro, implante o sistema operacional e então habilite novamente o modo de inicialização seguro.
- Para servidores ThinkServer, assegure que os seguintes requisitos sejam atendidos.

  – As configurações de inicialização no servidor devem incluir uma Política de OpROM de Armazenamento que é configurada para `UEFI Only`.

- Se estiver implantando o ESXi e houver adaptadores de rede inicializáveis em PXE, desabilite o suporte para PXE nesses adaptadores de rede antes de implantar o sistema operacional. A implantação será concluída, e você poderá reabilitar o suporte para PXE se desejar.
- Se estiver implantando o ESXi e houver dispositivos inicializáveis na lista de ordem de inicialização além da unidade na qual o sistema operacional deve ser instalado, remova-os dessa lista antes de implantar o sistema operacional. Após a conclusão da implantação, você poderá voltar a adicionar o dispositivo inicializável à lista. Certifique-se de que a unidade instalada esteja no topo da lista.

Para obter mais informações sobre as configurações de local de armazenamento, consulte Configurando perfis do sistema operacional.

Sistemas operacionais suportados

O Lenovo XClarity Orchestrator permite a implantação de diversos sistemas operacionais. Somente as versões compatíveis dos sistemas operacionais podem ser carregadas no repositório de imagens do SO do XClarity Orchestrator.

Importante:

- Para obter informações sobre limitações de implantação do sistema operacional para dispositivos específicos, consulte Hardware e software suportados na documentação online do XClarity Orchestrator.
- O recurso de gerenciamento criptográfico do XClarity Orchestrator permite limitar a comunicação com determinados modos SSL/TLS mínimos. Por exemplo, se o TLS 1.2 for selecionado, apenas os sistemas operacionais com um processo de instalação compatível com o TLS 1.2 e algoritmos criptográficos fortes poderão ser implantados por meio do XClarity Orchestrator.
- Imagens do sistema operacional no repositório de imagens do SO podem não ser compatíveis apenas em certas plataformas de hardware. É possível determinar se um sistema operacional é compatível com um servidor específico no Site do guia de interoperabilidade do SO da Lenovo.
- Para obter informações de suporte e compatibilidade relacionadas ao sistema operacional e hipervisor, bem como recursos para servidores e soluções Lenovo, consulte o Página da Web Centro de suporte do sistema operacional do servidor.

A seguinte tabela lista os sistemas operacionais de 64 bits em que o XClarity Orchestrator pode ser implantado.

Sistema Operacional	Versões	Notas
Red Hat® Enterprise Linux (RHEL) Server	7.2 and later 8.x	Inclui o KVM **Notas:** • Todas as versões secundárias existentes e futuras são compatíveis, a menos que seja indicado o contrário. • Ao importar a versão de DVD da imagem do SO, apenas o DVD1 é suportado. • Ao instalar o RHEL em servidores ThinkSystem, o RHEL v7.4 ou posterior é recomendado.
SUSE® Linux Enterprise Server (SLES)	12.3 and later 15.2 and later	Inclui hipervisores KVM e Xen **Notas:** • Todos os service packs existentes e futuros são compatíveis, a menos que seja indicado o contrário. • Ao importar a versão de DVD da imagem do SO, apenas o DVD1 é suportado.
VMware vSphere® Hypervisor (ESXi)	6.0.x 6.5.x 6.7.x 7.0.x	Imagens do Base VMware vSphere Hypervisor (ESXi) e imagens personalizadas do Lenovo VMware ESXi são compatíveis. Imagens personalizadas do Lenovo VMware ESXi são personalizadas para um hardware selecionado para fornecer gerenciamento de plataformas online, incluindo atualização e configuração de firmware, diagnósticos de plataformas e alertas de hardware aprimorados. Ferramentas de gerenciamento Lenovo também oferecem suporte ao gerenciamento simplificado do ESXi com servidores System x selecionados. Essa imagem está disponível para download no Suporte VMware – Página da Web de downloads. A licença fornecida com a imagem é uma versão de avaliação gratuita de 60 dias. Você é responsável por cumprir todos os requisitos de licenciamento do VMware. **Importante:** • Todos os pacotes de atualização existentes e futuros são compatíveis, a menos que seja indicado o contrário. • Imagens de base do ESXi (sem personalização da Lenovo) incluem apenas os drivers de dispositivo básicos predefinidos para armazenamento e rede. A imagem de base não inclui os drivers de dispositivo predefinidos (que são incluídos em imagens personalizadas do Lenovo VMware ESXi). • Para algumas versões de imagens personalizadas do Lenovo VMware ESXi, imagens separadas podem estar disponíveis para ThinkSystem, System x e ThinkServer. Somente uma imagem para uma versão específica pode existir no repositório de imagens do SO por vez. • Não há suporte para a implantação do ESXi para determinados servidores mais antigos. Para obter informações sobre quais servidores têm suporte, consulte o Site do guia de interoperabilidade do SO da Lenovo.

Perfis de imagem do sistema operacional

A importação de uma imagem do SO gera perfis predefinidos do SO. Cada perfil predefinido inclui opções de imagem de SO e opções de instalação para essa imagem.

É possível modificar os perfis para configurar credenciais, rede e configurações de armazenamento. Também é possível criar perfis com base nas políticas predefinidas do SO. Para obter mais informações, consulte Configurando perfis do sistema operacional.

A tabela a seguir lista os perfis predefinidos de imagem de SO que são criados quando você importa uma imagem do sistema operacional. Esta tabela lista também os pacotes que estão incluídos em cada perfil.

Sistema Operacional	Perfil	Pacotes incluídos no perfil	
Red Hat Enterprise Linux (RHEL) **Nota:** Inclui o KVM	Básico	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Mínima	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Virtualização	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
SUSE Linux Enterprise Server (SLES) 12.3 e posterior	Básico	<pattern>32bit</pattern> <pattern>Basis-Devel</pattern> <pattern>Minimal</pattern> <pattern>WBEM</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>gateway_server</pattern> <pattern>lamp_server</pattern> <pattern>mail_server</pattern> <pattern>ofed</pattern> <pattern>printing</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>	
	Mínima	<pattern>Minimal</pattern> <pattern>file_server</pattern> <pattern>sap_server</pattern>	

Sistema Operacional	Perfil	Pacotes incluídos no perfil
	Virtualização-KVM	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>kvm_server</pattern> <pattern>kvm_tools</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>
	Virtualização-Xen	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern>
SUSE Linux Enterprise Server (SLES) 15.2 e posterior	Básico	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	Mínima	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	Virtualização-KVM	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>

Sistema Operacional	Perfil	Pacotes incluídos no perfil
	Virtualização-Xen	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
VMware vSphere® Hypervisor (ESXi)	Virtualização	Imagens do Base VMware vSphere Hypervisor (ESXi) e imagens personalizadas do Lenovo VMware ESXi são compatíveis.

Disponibilidade da porta para sistemas operacionais implantados

Algumas portas são bloqueadas por determinados perfis de sistema operacional. As tabelas a seguir listam as portas que permanecem abertas (desbloqueadas).

Certifique-se de que o hipervisor que está executando o dispositivo Lenovo XClarity Orchestrator permita o tráfego de rede (TCP/UDP) nas portas 139, 445, 3001, 3900, 8443. Elas são necessárias para a implantação do sistema operacional.

Perfil de Virtualização de RHEL

Por padrão, o perfil de virtualização de Red Hat Enterprise Linux (RHEL) bloqueia todas as portas, exceto aquelas que estão listadas na tabela a seguir.

Tabela 1. Disponibilidade de portas para os perfis de virtualização de RHEL

Porta	TCP ou UDP	Direção	Descrição da Comunicação
22	TCP	Entrada	Comunicação SSH
53	TCP, UDP	Saída/Entrada	Comunicação com dispositivos de rede RHEL KVM
67	TCP, UDP	Saída/Entrada	Comunicação com dispositivos de rede RHEL KVM
161	UDP	Saída	Comunicação com agentes SNMP
162	UDP	Entrada	Comunicação com agentes SNMP
427	TCP, UDP	Saída/Entrada	Comunicação com agente de serviço SLP, agente do diretório SLP
3001	TCP	Saída/Entrada	Comunicação com serviço de implementação de imagem de software de gerenciamento
15988	TCP	Saída	Comunicação CIM-XML over HTTP

Tabela 1. Disponibilidade de portas para os perfis de virtualização de RHEL (continuação)

Porta	TCP ou UDP	Direção	Descrição da Comunicação
15989	TCP	Saída	Comunicação CIM-XML over HTTP
49152 - 49215	TCP	Saída/Entrada	Comunicação do Servidor Virtual KVM

Perfis Básico e Mínimo de RHEL

Por padrão, os perfis Básico e Mínimo de RHEL bloqueiam todas as portas, exceto aquelas que estão listadas na tabela a seguir.

Tabela 2. Disponibilidade de portas para os perfis básico e mínimo de RHEL

Porta	TCP ou UDP	Direção	Descrição da Comunicação
22	TCP	Entrada	Comunicação SSH
3001	TCP	Saída/Entrada	Comunicação de serviço de implementação de imagem de software de gerenciamento

SLES, virtualização, perfis básico e mínimo

Para o SUSE Linux Enterprise Server (SLES), algumas portas abertas são designadas dinamicamente com base na versão e nos perfis de sistema operacional. Para obter uma lista completa das portas abertas, consulte a documentação do SUSE Linux Enterprise Server.

Perfil de Virtualização de VMware ESXi

Para obter uma lista completa de portas abertas para VMware vSphere Hypervisor (ESXi) 5.1 com personalização da Lenovo, consulte a documentação do VMware para ESXi no Site da Base de conhecimento do VMware.

Importando imagens do sistema operacional

Antes de poder implantar um sistema operacional licenciado para servidores gerenciados, importe a imagem para o repositório de imagens do SO.

Sobre esta tarefa

Para obter informações sobre imagens do sistema operacional que você pode importar e implantar, incluindo sistemas operacionais de base e personalizados, consulte Sistemas operacionais suportados.

Somente para ESXi, é possível importar várias imagens ESXi com a mesma versão principal/secundária para o repositório de imagens do SO.

Somente para ESXi, é possível importar várias imagens ESXi personalizadas com a mesma versão principal/secundária e o número de build para o repositório de imagens do SO.

Ao importar uma imagem do sistema operacional, XClarity Orchestrator:

- Verifica se há espaço suficiente no repositório de imagens do SO antes de importar o sistema operacional. Se você não tiver espaço suficiente para importar uma imagem, exclua uma imagem existente do repositório e tente importar novamente a nova imagem.

- Cria um ou mais perfis dessa imagem e armazena o perfil no repositório de imagens do SO. Cada *perfil* inclui a imagem do SO e opções de instalação. Para obter informações adicionais sobre perfis predefinidos de imagem do SO, consulte Perfis de imagem do sistema operacional.

Nota: Os navegadores da Web Internet Explorer e Microsoft Edge têm um limite de upload de 4 GB. Se o arquivo que você está importando tiver mais do que 4 GB, considere usar outro navegador da Web (como o Chrome ou o Firefox).

Procedimento

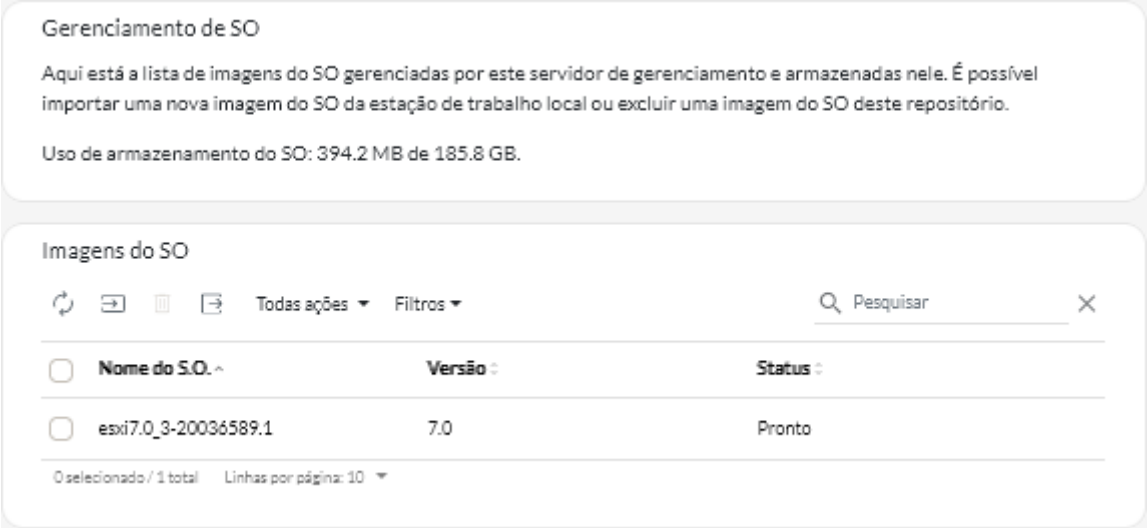
Para importar uma imagem do sistema operacional para o repositório de imagens do SO, conclua as seguintes etapas.

Etapa 1. Obtenha uma imagem ISO licenciada do sistema operacional.

Nota: Você é responsável por obter as licenças aplicáveis para o sistema operacional.

Etapa 2. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento** ( ) → **Implantação do OS** e, em seguida, clique na guia **Gerenciamento de SO** para exibir a página o Gerenciamento de SO.

Etapa 3. Clique em **Imagens do SO** na navegação à esquerda para exibir o cartão Imagens do SO.



Etapa 4. Clique no ícone **Importar arquivos** ( ) para exibir a caixa de diálogo Importar Imagens do SO.

Etapa 5. Arraste e solte a imagem .iso que você deseja importar ou clique em **Procurar** para encontrar a imagem ISO que você deseja importar

Etapa 6. **Opcional:** selecione um tipo de soma de verificação e copie e cole o valor de soma de verificação no campo de texto fornecido.

Se você selecionar um tipo de soma de verificação, especifique um valor de soma de verificação para verificar a integridade e a segurança da imagem de SO transferida por upload. O valor deve se originar de uma fonte segura de uma organização em que você confie. Se a imagem transferida por upload corresponde ao valor de soma de verificação, é seguro continuar com a implantação. Caso contrário, você deverá fazer upload da imagem novamente ou verificar o valor de soma de verificação.

Os tipos de verificação a seguir são compatíveis: MD5, SHA1 e SHA256.

Etapa 7. Clique em **Importar**.

O XClarity Orchestratorfaz upload da imagem do SO no repositório de imagens do SO e adiciona os perfis de SO predefinidos na guia **Perfis do SO**.

Dica: a imagem ISO é transferida por upload por uma conexão de rede segura. Dessa forma, a confiabilidade e o desempenho da rede afetam o tempo necessário para importar a imagem.

Depois de concluir

Nesta página, é possível executar as ações a seguir:

- Exclua uma imagem do SO selecionada clicando no ícone **Excluir** ().
- Exiba e edite perfis de SO clicando na barra de menus XClarity Orchestrator, clique em **Provisionamento () → Implantação do SO** e clique na guia **Perfis do SO**, selecione o perfil e clique no ícone de **Edição** () (consulte Configurando perfis do sistema operacional).
- Exclua perfis de SO clicando na barra de menus do XClarity Orchestrator, clique em **Provisionamento () → Implantação do SO** e clique na guia **Perfis do SO**, selecione o ícone de **Exclusão** ().

  Nota: Se você excluir o último perfil predefinido restante de um sistema operacional, o sistema operacional também será excluído.

Configurando perfis do sistema operacional

Os perfis do sistema operacional são criados automaticamente ao importar um sistema operacional. Os perfis criados são baseados no tipo e na versão do sistema operacional. É possível modificar o perfil, incluindo credenciais do SO, nome do host, configurações de rede e armazenamento, chaves de licença e local de armazenamento.

Antes de iniciar

Revise as considerações antes de implantar um sistema operacional em um dispositivo do servidor gerenciado. Para obter informações, consulte Considerações sobre implantação do sistema operacional.

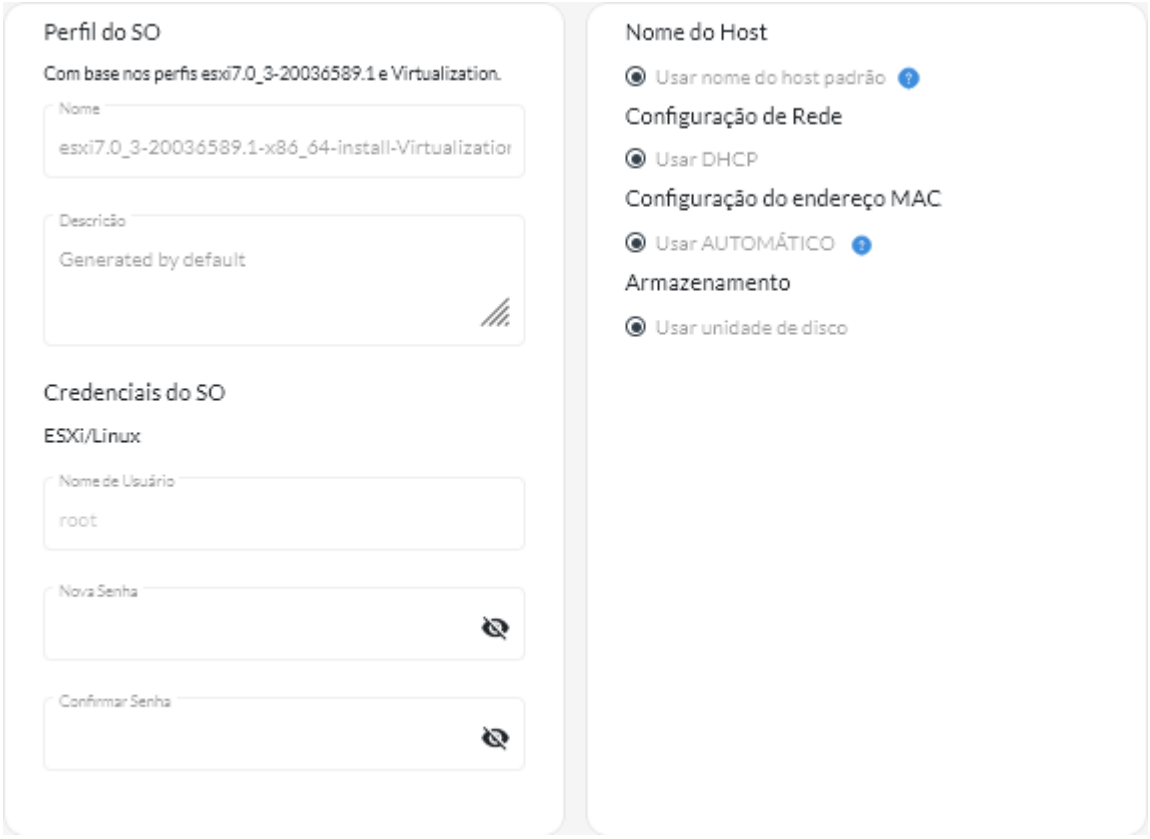
Procedimento

Para configurar um perfil do SO para implantação, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento () → Implantação do OS** e clique na guia **Perfis do SO** para exibir a página Perfis do SO.

Etapa 2. Selecione o perfil do SO.

Etapa 3. Clique no ícone de **Edição** () para exibir o cartão Detalhes do perfil do SO.



Etapa 4. Configure os atributos de perfil.

- **Nome**. Modificar o nome do perfil cria um perfil do SO.
- **Descrição**. Modifique a descrição desse perfil do SO.
- **Credenciais do SO**. Insira as credenciais do SO para a conta de administrador a ser usada para fazer login no sistema operacional.
- **Nome do host**. Selecione o que usar para o nome do host. É possível escolher um dos valores a seguir.
  - **Usar nome do host padrão**. (padrão) O nome do host é "nó" seguido pelos primeiros 11 caracteres do ID do dispositivo (por exemplo, `nodeABC31213310`).
- **Configuração de Rede**. Selecione as configurações de IP para esse perfil. É possível escolher um dos valores a seguir.
  - **DHCP**. (padrão) Use a infraestrutura DHCP existente para atribuir endereços IPv4 aos servidores.
- **Configuração do endereço MAC**. Selecione o endereço MAC da porta no host em que o sistema operacional será instalado. É possível escolher um dos valores a seguir.

  Nota: Não há suporte para portas de rede virtual. Não use uma porta de rede física para simular várias portas de rede virtual.

  - **Usar AUTO**. (padrão) Detecte automaticamente as portas Ethernet que podem ser configuradas e usadas para implantação. O primeiro endereço MAC (porta) detectado é usado por padrão. Se a conectividade for detectada em um endereço MAC diferente, o servidor será reiniciado automaticamente para usar o endereço MAC recém-detectado para a implantação. O Gerenciador de Recursos do XClarity Administrator pode detectar automaticamente portas de rede nos slots 1 a 16. Pelo menos uma porta nos slots 1 a 16 deve ter uma conexão com o Gerenciador de Recursos aplicável.

Se você quiser usar uma porta de rede no slot 17 ou superior para o endereço MAC, não poderá usar AUTOMÁTICO.

- **Storage**. Selecione o local de armazenamento onde você quer implantar a imagem do sistema operacional.
  - **Usar unidade de disco**. Instale a imagem do sistema operacional na primeira unidade de disco RAID local enumerada no servidor gerenciado.Somente unidades de disco conectadas a um controlador RAID ou SAS/SATA HBA são compatíveis.

    Se a configuração do RAID no servidor não estiver configurada corretamente, ou se estiver inativo, talvez o disco local não esteja visível para o servidor do Orchestrator. Para resolver o problema, habilite a configuração do RAID por meio de padrões de configuração (consulte Aprendendo um padrão de configuração de servidor de um servidor existente) ou pelo software de gerenciamento do RAID no servidor.

    Notas:
    - Se uma unidade M.2 também estiver presente, a unidade de disco deverá ser configurada para RAID de hardware.
    - Se um adaptador SATA estiver ativado, o modo SATA *não deverá* ser configurado como **IDE**.
    - Para servidores ThinkServer, a configuração só está disponível por meio do software de gerenciamento do RAID no servidor.

Etapa 5. Clique em **Salvar**.

Depois de concluir

É possível realizar as ações a seguir.

- Atribua um perfil do SO a um ou mais servidores na guia **Atribuir e implantar** clicando em selecionar servidores e, em seguida, no ícone **Atribuir** () ou clicando no ícone **Atribuir** () e, em seguida, selecionando um grupo de servidores. Depois de selecionar o perfil do SO, é possível escolher atribuir o perfil do SO a:
  - **Todos os dispositivos aplicáveis (substituir perfis atribuídos)**
  - **Dispositivos aplicáveis sem atribuição de perfil**
  - **Somente os dispositivos aplicáveis selecionados (substituir perfis atribuídos)**
  - **Somente dispositivos aplicáveis selecionados sem atribuição de perfil**
- Exclua os perfis do SO selecionados clicando no ícone **Excluir** ().

  Nota: Se você excluir o último perfil predefinido restante de um sistema operacional, o sistema operacional também será excluído.

Implantando uma imagem do sistema operacional

É possível usar o Lenovo XClarity Orchestrator para implantar um sistema operacional em seus servidores gerenciados.

Antes de iniciar

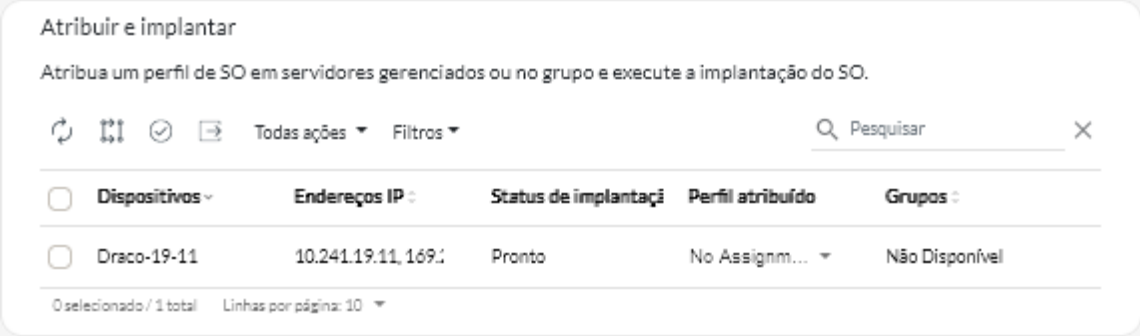
Leia as considerações de implantação do sistema operacional antes de tentar implantar sistemas operacionais em servidores gerenciados (consulte Considerações sobre implantação do sistema operacional).

Atenção: Se o servidor possui, atualmente, um sistema operacional, a implantação de um perfil de imagem do SO substituirá o sistema operacional atual.

Procedimento

Para implantar uma imagem do sistema operacional em um ou mais servidores gerenciados, conclua um dos procedimentos a seguir.

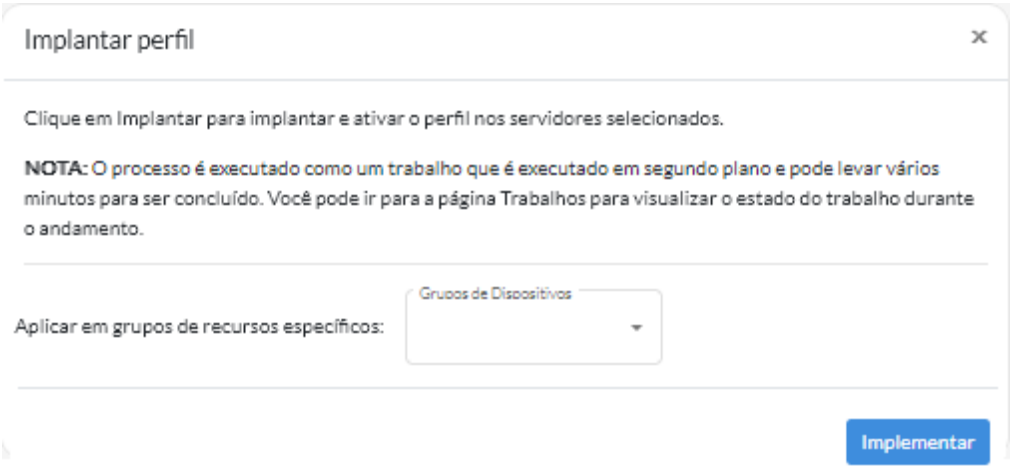
- **Para dispositivos específicos**
  1. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento ( ) → Implantação do OS** e clique na guia **Atribuir e implantar** para exibir o cartão Atribuir e Implantar.



  2. Selecione um ou mais servidores nos quais você deseja implantar o sistema operacional.
  3. Para cada servidor de destino, selecione o perfil do SO a ser implantado na lista suspensa na coluna **Perfis do SO**. Certifique-se de selecionar um perfil do SO compatível com o servidor de destino.
  4. Verifique se o status da implantação na coluna **Status** é Pronto para todos os servidores selecionados.
  5. Clique no ícone **Implantar** ( ) para exibir a caixa de diálogo Implantar perfil.
  6. Clique em **Implantar** para iniciar a implantação do sistema operacional. 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 .)
- **Para todos os dispositivos em um grupo específico**
  1. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento ( ) → Implantação do OS** e clique na guia **Atribuir e implantar** para exibir o cartão Atribuir e Implantar.
  2. Atribua um perfil de SO ao grupo de servidores.
     a. Clique no ícone **Atribuir** ( ) para exibir a caixa de diálogo Atribuir perfil.

b. Selecione o perfil a ser atribuído.
c. Selecione o grupo de dispositivos a serem atribuídos.
d. Escolha quais dispositivos do grupo atribuir.
   - **Todos os dispositivos aplicáveis (substituir perfis atribuídos)**
   - **Dispositivos aplicáveis sem atribuição de perfil**
   - **Somente os dispositivos aplicáveis selecionados (substituir perfis atribuídos)**
   - **Somente dispositivos aplicáveis selecionados sem atribuição de perfil**
e. Clique em **Implantar**.

3. Clique no ícone **Implantar** (⊘) para exibir a caixa de diálogo Implantar perfil.



4. Selecione o grupo de dispositivos em que deseja implantar o perfil de SO atribuído.

5. Clique em **Implantar** para iniciar a implantação do sistema operacional. 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 .)

Fornecimento de atualizações para recursos gerenciados

É possível usar o Lenovo XClarity Orchestrator para manter níveis atuais de software nos gerenciadores de recursos do Lenovo XClarity Administrator e servidores gerenciados. É possível usar o catálogo de atualizações para saber quais níveis de software estão disponíveis, usar as políticas de conformidade de atualização para identificar quais recursos precisam ser atualizados com base em critérios personalizados e, em seguida, implantar as atualizações desejadas nesses recursos.

Procedimento

A figura a seguir ilustra o fluxo de trabalho para atualizar recursos gerenciados.

Etapa 1. **Atualizar o catálogo**

O *repositório de atualizações* contém um catálogo e os pacotes de atualização que podem ser aplicados aos recursos gerenciados.

O *catálogo* contém informações sobre as atualizações que estão disponíveis atualmente. O catálogo organiza as atualizações por tipos de recurso (plataformas) e componentes. Quando você atualiza o catálogo, o XClarity Orchestrator recupera informações sobre as atualizações mais recentes disponíveis do site de suporte da Lenovo e armazena as informações no repositório de atualizações.

Importante: O XClarity Orchestrator deve estar conectado à Internet para atualizar o catálogo.

Quando novos pacotes de atualização ficarem disponíveis, você deverá importar os pacotes de atualização aplicáveis antes de aplicar uma atualização. A atualização do catálogo não importa automaticamente os pacotes de atualização.

Quando o XClarity Orchestrator, o repositório de atualizações está vazio.

Etapa 2. **Baixar ou importar pacotes de atualização para o repositório**

Se o XClarity Orchestrator estiver conectado à Internet, você poderá baixar pacotes de atualização listados no catálogo de atualizações diretamente do site de suporte da Lenovo. Se o XClarity Orchestrator não estiver conectado à Internet, você poderá importar manualmente os pacotes de atualização previamente baixados do Site de Suporte a data center da Lenovo para uma estação de trabalho que tenha acesso de rede ao host do XClarity Orchestrator.

Se você optar por baixar uma versão secundária, os pacotes de atualização de pré-requisito também serão baixados.

Ao importar manualmente pacotes do repositório, você deve importar a carga útil (.tgz), os metadados (.xml), o log de alterações (.chg) e o leiame (.txt).

Ao importar atualizações manualmente, você deve importar a base de arquivos necessários no tipo de recurso.

- Para servidores ThinkSystem V3, importe o pacote de atualização único (*.zip). Esse arquivo zip contém a carga útil, os arquivos de metadados (vários arquivos *.json), o arquivo de log de alterações (*.chg) e o arquivo leiame (*.txt).
- Para dispositivos ThinkEdge Client, importe a carga útil (Windows .exe). O arquivo leiame (.txt) é opcional. Observe que apenas o **pacote de utilitário flash BIOS para atualização do Windows** é aceito atualmente.
- Para XClarity Management Hub, eXClarity Management Hub 2.0, importe o arquivo do pacote de atualização único (.tgz). Este arquivo contém a carga útil, metadados, histórico de alterações e leiame.
- Para todos os outros recursos (incluindo XClarity Administrator, servidores ThinkEdge, ThinkSystem V1 e V2 e dispositivos legados), importe a carga útil (.zip, .uxz, .tar.gz, .tar, .bin), metadados (.xml), log de alterações (.chg) e leiame (.txt).

Para obter mais informações sobre a importação de atualizações, consulte Baixando e importando atualizações.

Etapa 3. **Criar e atribuir políticas de conformidade de atualização**

As políticas de conformidade de atualização garantem que o software ou o firmware em alguns recursos gerenciados esteja no nível atual ou específico sinalizando os recursos que precisam de atenção. Cada política de conformidade de atualização identifica quais recursos são monitorados e qual nível de software ou firmware deve ser instalado para manter os recursos em conformidade. Em seguida, o XClarity Orchestrator usa essas políticas para verificar o status de recursos gerenciados e identificar os recursos que não estão em conformidade.

Ao criar uma política de conformidade de atualização, é possível fazer o XClarity Orchestrator sinalizar um recurso quando o software ou firmware no recurso estiver em um nível inferior.

Depois que uma política de conformidade de atualização é atribuída a um recurso, o XClarity Orchestrator verifica o status de conformidade do recurso quando o repositório de atualizações é alterado. Se o software ou firmware no recurso não está em conformidade com a política atribuída, o XClarity Orchestrator sinaliza esse recurso como não conforme na página Aplicar/Ativar, com base nas regras que você especificou na política de conformidade de atualização.

Por exemplo, é possível criar uma política de conformidade de atualização que defina o nível de software de linha de base para o XClarity Administrator e, em seguida, atribuir essa política a todos os gerenciadores de recursos do XClarity Administrator. Quando o catálogo de atualizações é atualizado e uma nova atualização é baixada ou importada, as instâncias do XClarity Administrator podem ficar fora de conformidade. Quando isso acontece, o XClarity Orchestrator atualiza a página Aplicar/Ativar para mostrar quais instâncias do XClarity Administrator não estão em conformidade e gera um alerta.

Para obter mais informações sobre como criar políticas de conformidade de atualização, consulte Criando e atribuindo políticas de conformidade de atualização.

Etapa 4. **Aplicar e ativar atualizações**

O XClarity Orchestrator não aplica atualizações automaticamente. Para atualizar os recursos de software, você deve aplicar e ativar manualmente a atualização nos recursos selecionados que não são compatíveis com a política de conformidade de atualização atribuída.

O XClarity Orchestrator não atualiza recursos diretamente. Em vez disso, ele envia uma solicitação ao gerenciador de recursos aplicável para executar a atualização e rastreia o progresso da solicitação. O XClarity Orchestrator identifica as dependências que são necessárias para executar a atualização, garante que os recursos de destino sejam atualizados na ordem correta, transfira os pacotes de atualização aplicáveis ao gerenciador de recursos e cria uma solicitação para iniciar um trabalho no gerenciador de recursos para executar a atualização.

Para obter mais informações sobre como aplicar atualizações, consulte Aplicando e ativando atualizações aos gerenciadores de recursos e Aplicando e ativando atualizações aos servidores gerenciados.

Atualizar considerações de implantação

Antes de implantar atualizações usando o Lenovo XClarity Orchestrator, revise as seguintes considerações importantes.

- Para obter o melhor desempenho, certifique-se de que os gerenciadores de recursos do Lenovo XClarity Administrator estejam executando a versão v3.2.1 ou posterior
- Verifique se o repositório de atualizações contém os pacotes de atualização que você pretende aplicar. Se não contiver, atualize o catálogo de produtos e baixe as atualizações apropriadas (consulte Baixando e importando atualizações).
- Certifique-se de que nenhum trabalho esteja em execução atualmente no recurso de destino. Se houver trabalhos em execução, o trabalho de atualização será enfileirado até que todos os outros trabalhos sejam concluídos.
- Se o recurso tiver uma política de conformidade de atualização atribuída que resulte em violações de conformidade, você deverá corrigir as violações ajustando a política de conformidade ou atribuindo uma política alternativa.
- Se você optar por instalar um pacote de atualização que contenha atualizações para vários componentes, todos os componentes aos quais o pacote de atualização se aplica serão atualizados.

Considerações do recurso

- A função de atualizações oferece suporte à atualização apenas de servidores e gerenciadores de recursos.No ThinkSystem SR635 e SR655, somente as atualizações de firmware UEFI e BMC são aceitas.

  Para dispositivos ThinkSystem e ThinkAgile, as atualizações de firmware não são suportadas para controlador gerenciado do baseboard e bancos de backup UEFI. Em vez disso, atualize o banco principal e, em seguida, habilite a promoção automática.
- Antes de atualizar os dispositivos gerenciados, leia as considerações importantes sobre atualização (consulte Considerações de atualização de firmware na documentação online do XClarity Administrator).
- Antes de atualizar os Gerenciadores de Recursos do XClarity Administrator, leia as considerações de atualização do XClarity Administrator (consulte Atualizando o servidor de gerenciamento do XClarity Administrator na documentação online do XClarity Administrator).
- Antes de atualizar os Gerenciadores de Recursos do XClarity Administrator, faça backup do dispositivo virtual criando um clone (consulte Fazendo backup do XClarity Administrator na documentação online do XClarity Administrator).
- Certifique-se de que os recursos que você deseja atualizar tenham uma política de conformidade de atualização atribuída.
- O XClarity Orchestrator transfere as atualizações aplicáveis para o gerenciador de recursos durante o processo de atualização. Certifique-se de que haja espaço em disco suficiente no servidor de gerenciamento para conter as atualizações.

- Para dispositivos ThinkEdge Client, somente atualizações de BIOS em servidores que executam o Windows 10 versão 1809 ou sistema operacional de 64 bits posteriores são compatíveis. Edições especiais (como 10 S ou 10x) não são compatíveis atualmente.
- Não é possível baixar atualizações de firmware para servidores a seguir da interface da Web. Em vez disso, baixe manualmente atualizações pelo ibm.com e, em seguida, importe as atualizações.
  - IBM System x iDataPlex dx360 M4
  - IBM System série M4
  - IBM System x3100 M5 e x3250 M
  - IBM System x3850 X5 e x3950 X5
  - IBM System x3850 X6 e x3950 X6
  - IBM Flex System

Considerações do repositório

- Verifique se o repositório de atualizações contém os pacotes de atualização que você pretende aplicar. Se não contiver, atualize o catálogo de produtos e baixe as atualizações apropriadas (consulte Baixando e importando atualizações).É possível optar por instalar as atualizações de pré-requisito além da atualização de destino. Todas as atualizações de pré-requisito deve ser baixadas para o repositório para que possam ser aplicadas.

  Em alguns casos, várias versões podem ser necessárias para aplicar uma atualização, e todas as versões precisam ser baixadas para o repositório.

Considerações do processo de atualização

- Se você optar por instalar um pacote de atualização que contenha atualizações para vários componentes, todos os componentes aos quais o pacote de atualização se aplica serão atualizados.
- Quando uma solicitação é feita para aplicar atualizações a um gerenciador de recursos e a um ou mais dispositivos que são gerenciados por esse gerenciador de recursos, as atualizações são aplicadas primeiro ao gerenciador de recursos.
- Enquanto uma atualização estiver em andamento, o recurso de destino ficará bloqueado. Não é possível iniciar outras tarefas de gerenciamento no recurso de destino até o processo de atualização ser concluído.
- Após uma atualização ser aplicada a um recurso, uma ou mais reinicializações podem ser necessárias para ativar totalmente a atualização. Você pode optar por reiniciar o recurso imediatamente, atrasar a ativação ou priorizar a ativação. Se você optar por reiniciar imediatamente, o XClarity Orchestrator minimizará o número de reinicializações necessárias. Se optar por atrasar a ativação, as atualizações serão ativadas na próxima vez que o recurso for reiniciado. Se você escolher a ativação priorizada, as atualizações serão ativadas imediatamente no Baseboard Management Controller e todas as outras atualizações serão ativadas na próxima vez em que o dispositivo for reiniciado.
- Se você optar por reiniciar o recurso durante o processo de atualização (*ativação imediata*), certifique-se de que as cargas de trabalho em execução sejam interrompidas ou, se estiverem funcionando em um ambiente virtualizado, sejam movidas para um recurso diferente.
- Algumas atualizações de firmware requerem que um monitor seja conectado ao dispositivo de destino. O processo de atualização poderá falhar se um monitor não estiver conectado.

Baixando e importando atualizações

Os pacotes de atualizações devem estar disponíveis no repositório atualizações para que você possa aplicar atualizações aos recursos gerenciados.

Antes de iniciar

Para recuperar as informações mais recentes sobre os pacotes de atualização, selecione o tipo de recurso e clique em **Verificar se há atualizações → Atualização selecionada** para obter informações sobre todos os

pacotes de atualização disponíveis ou clique em **Verificar se há atualizações → Atualização selecionada – Somente Mais Recente** para obter apenas informações sobre o pacote de atualização mais recente para esse recurso. Em seguida, classifique a tabela usando a coluna **Nome** para ordenar as atualizações por versão.

O XClarity Orchestrator usa uma unidade separada para o repositório de atualizações. O requisito de tamanho mínimo para essa unidade é 100 GB.

Sobre esta tarefa

Você pode baixar ou importar um único pacote de repositório do XClarity Administrator ou um ou mais pacotes de atualização por vez.

- **Pacotes de repositórios do XClarity Administrator**Os pacotes do repositório do Lenovo XClarity Administrator contêm as mais recentes atualizações de firmware disponíveis em um período específico para a maioria dos dispositivos compatíveis e uma política de conformidade de firmware padrão atualizada. Quando você baixa um pacote de repositório do Página da Web de download do XClarity Administrator, cada pacote de atualização no pacote de repositório é extraído e importado para o repositório de atualizações e, em seguida, o arquivo de carga do repositório é excluído. A política de conformidade de firmware padrão atualizada também é importada como uma política predefinida. Não é possível modificar essa política predefinida.

  Os pacotes do repositório a seguir estão disponíveis.
  - **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os CMMs e comutadores Flex System.
  - **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os comutadores RackSwitch e dispositivos Lenovo Storage.
  - **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos servidores Converged HX Series, Flex System e System x.
  - **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os servidores ThinkSystem.
  - **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Contém atualizações de firmware para todos os servidores ThinkSystem V2.
  - **lnvgy_sw_lxca_thinksystemv3repo*x-x.x.x*_anyos_noarc**. Contém atualizações de firmware para todos os servidores ThinkAgile e ThinkSystem V3.

  Ao importar manualmente pacotes do repositório, você deve importar a carga útil (.tgz), os metadados (.xml), o log de alterações (.chg) e o leiame (.txt).

  Você pode determinar o status de um pacote de repositório da coluna **Status** na página Gerenciamento de repositórios. Essa coluna contém os seguintes valores.
  - **Não baixado**. O pacote de repositório está disponível na Web, mas não é baixado e extraído para o repositório de atualizações.
  - **Download pendente**. O pacote de repositórios está na fila para download da Internet.
  - **Baixando**. O pacote de repositórios está sendo baixado da Internet.
  - **Aplicação pendente**. O pacote de repositórios está na fila para extrair pacotes de atualização no pacote de repositórios para o repositório de atualizações.
  - **Aplicando**. Os pacotes de atualização no pacote de repositórios estão sendo extraídos para o repositório de atualizações.
  - *x* **de** *y* **Baixado**. Alguns, mas nem todos os pacotes de repositório são baixados e extraídos para o repositório de atualizações. Os números entre parênteses indicam o número de atualizações baixadas e o número de atualizações disponíveis.
  - **Baixado**. Todos os pacotes de atualização no pacote de repositórios são armazenados no repositório de atualizações, e o arquivo de carga do pacote de repositórios é excluído.
- **Pacotes de atualização**Se o XClarity Orchestrator estiver conectado à Internet, você poderá baixar pacotes de atualização listados no catálogo de atualizações diretamente do site de suporte da Lenovo.

Se o XClarity Orchestrator não estiver conectado à Internet, você poderá importar manualmente os pacotes de atualização previamente baixados do Site de Suporte a data center da Lenovo para uma estação de trabalho que tenha acesso de rede ao host do XClarity Orchestrator.

Se você optar por baixar uma versão secundária, os pacotes de atualização de pré-requisito também serão baixados.

Ao importar atualizações manualmente, você deve importar a base de arquivos necessários no tipo de recurso.

- Para servidores ThinkSystem V3, importe o pacote de atualização único (*.zip). Esse arquivo zip contém a carga útil, os arquivos de metadados (vários arquivos *.json), o arquivo de log de alterações (*.chg) e o arquivo leiame (*.txt).
- Para dispositivos ThinkEdge Client, importe a carga útil (Windows .exe). O arquivo leiame (.txt) é opcional. Observe que apenas o **pacote de utilitário flash BIOS para atualização do Windows** é aceito atualmente.
- Para XClarity Management Hub, eXClarity Management Hub 2.0, importe o arquivo do pacote de atualização único (.tgz). Este arquivo contém a carga útil, metadados, histórico de alterações e leiame.
- Para todos os outros recursos (incluindo XClarity Administrator, servidores ThinkEdge, ThinkSystem V1 e V2 e dispositivos legados), importe a carga útil (.zip, .uxz, .tar.gz, .tar, .bin), metadados (.xml), log de alterações (.chg) e leiame (.txt).

Importante: O tamanho máximo de todos os arquivos a serem importados ao mesmo tempo é 8 GB.

É possível determinar se os arquivos de atualização específicos estão armazenados no repositório de atualizações na coluna **Status** na página Gerenciamento do Repositório. Essa coluna contém os seguintes valores.

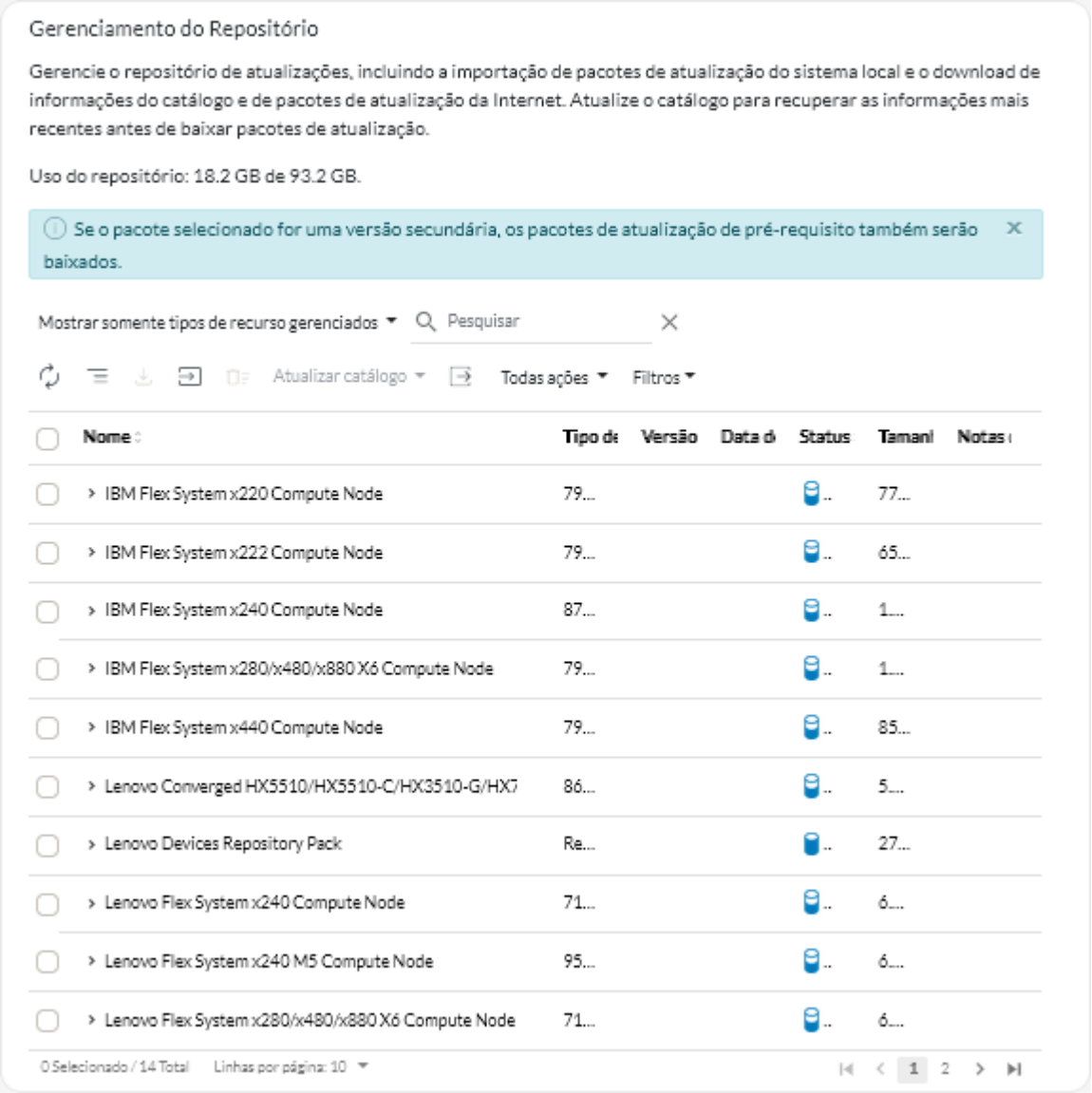
- **Não baixado**. O pacote de atualização inteiro ou a atualização individual está disponível na Web, mas não armazenado atualmente no repositório.
- **Download pendente**. O pacote de atualizações está na fila para download da Internet.
- **Baixando**. O pacote de atualizações está sendo baixado da Internet.
- *x* **de** *y* **Baixado**. Algumas atualizações (não todas) no pacote de atualização estão armazenadas no repositório. Os números entre parênteses indicam o número de atualizações armazenadas e o número de atualizações disponíveis.
- **Baixado**. O pacote de atualização inteiro ou a atualização individual é armazenada no repositório.

Nota: Alguns pacotes de atualização são usados por várias plataformas. Se você selecionar um pacote de atualização na tabela, ele será selecionado em todas as plataformas que o utilizam.

Procedimento

Para baixar ou importar manualmente pacotes de atualização e pacotes de repositório, execute uma das etapas a seguir.

- Se o XClarity Orchestrator estiver conectado à Internet, baixe os pacotes de atualização listados no catálogo.
  1. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento** ( ) → **Atualizações** e, em seguida, clique em **Gerenciamento do Repositório** para exibir o cartão Gerenciamento do Repositório.O cartão Gerenciamento do Repositório lista informações sobre pacotes de atualização em uma estrutura de árvore, organizada por tipos de recurso, componentes e pacotes de atualização. Por padrão, os tipos de recursos para apenas *recursos* gerenciados são listados na tabela. Clique em **Mostrar Tipos de Recurso Disponíveis** para listar *todos os tipos* de recurso disponíveis no catálogo.



2. (Opcional) Baixe as informações sobre as atualizações mais recentes disponíveis para tipos de recursos específicos selecionando um ou mais tipos na tabela, clicando em **Verificar se há atualizações** e, em seguida, clicando em uma das opções a seguir.
   - **Atualizar Selecionado**. Recupera informações sobre todas as versões de atualização disponíveis para o recurso selecionado.
   - **Atualizar Selecionado – Somente Mais Recente**. Recupera informações sobre a versão de atualização mais atual disponível para o recurso selecionado.Para dispositivos ThinkEdge Client, somente **Atualizar Selecionado – Somente Mais Recente** é compatível.

   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 .)
3. Selecione um ou mais pacotes de repositório, recursos, componentes e versões de atualização das quais você deseja baixar.É possível expandir os tipos de recurso e componentes para exibir a lista de versões de atualização que estão disponíveis no catálogo para cada tipo de recurso e componente.
4. Clique no ícone **Baixar Atualizações** ( ) para baixar as atualizações selecionadas.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 .)

Quando o download estiver concluído, o **Estado de Download** das atualizações selecionadas será alterado para "Baixado".

- Se o XClarity Orchestrator não estiver conectado à Internet, importe manualmente os pacotes de atualização e os pacotes de repositório.
  1. Baixe os arquivos de cada pacote de repositório e pacote de atualização para uma estação de trabalho que tenha acesso de rede ao host do XClarity Orchestrator usando um navegador da Web. Use estes links para baixar as atualizações aplicáveis.
     - Para atualizações do Lenovo XClarity Administrator, acesse Página da Web de download do XClarity Administrator.Também é possível baixar atualizações do XClarity Administrator usando os comandos do Lenovo XClarity Essentials OneCLI. O exemplo a seguir baixa a atualização mais recente (incluindo a carga útil) para o diretório /lxca-updates e armazena os arquivos de log no diretório /logs/lxca-updates. Para obter mais informações sobre o OneCLI, consulte comando de aquisição na documentação online do Lenovo XClarity Essentials OneCLI.
       ```
       Onecli.exe update acquire --lxca --ostype none --mt lxca --scope latest --superseded --xml
       --dir ./lxca-updates --output ./logs/lxca-updates
       ```
     - Para pacotes do repositório de atualizações de firmware, acesse Página da Web de download do XClarity Administrator.
     - Para atualizações de firmware, acesse Site de Suporte a data center da Lenovo.
  2. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento (**) **→ Atualizações** e, em seguida, clique em **Gerenciamento do Repositório** para exibir o cartão Gerenciamento do Repositório.
  3. Clique no ícone **Importar** ( ) para exibir a caixa de diálogo Importar Atualizações.
  4. Arraste e solte os arquivos baixados na caixa de diálogo Importar ou clique em **Procurar** para localizar os arquivos.

     Atenção:

     - Para dispositivos ThinkEdge Client, você deve importar o arquivo de carga útil para cada pacote de atualização. O arquivo readme é opcional.
     - Para todos os outros dispositivos, é necessário importar o arquivo de metadados e o arquivo de imagem ou carga útil, o arquivo de histórico de alterações e o arquivo readme para pacote de repositório e pacote de atualização. Os arquivos que estiverem selecionados, mas não especificados no arquivo de metadados, serão descartados. Se você não incluir o arquivo de metadados, a atualização não será importada.
     - Não importe outros arquivos que possam ser encontrados nos sites de download da Lenovo.
     - Se você não incluir o arquivo de metadados (.xml ou .json) para o pacote de repositório nem para o pacote de atualização, o pacote de repositório ou o pacote de atualização não será importado.
  5. Clique em **Importar**.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 .)

     Quando os arquivos forem importados e armazenados no repositório, a coluna **Estado de Download** será alterada para "Baixado".

Depois de concluir

É possível executar as ações a seguir a partir do cartão Gerenciamento do Repositório.

- Revise o arquivo leia-me, o histórico de alterações e a lista de vulnerabilidades e exposições comuns (CVEs) fixas para obter uma atualização específica clicando no ícone de informações ( ) na coluna **Notas de versão**.Também é possível encontrar uma lista de CVEs fixas ao passar o cursor sobre a coluna **CVEs fixas**. Clique no ID da CVE para exibir informações detalhadas sobre a CVE no site de Dados de Vulnerabilidade Nacional.

  As colunas **Notas de versão** e **CVEs fixas** são ocultas por padrão. Para mostrar essas colunas na tabela, clique em **Todas as Ações → Alternar Colunas**.
- Exclua apenas o arquivo de imagem (carga útil) para cada atualização selecionada clicando no ícone **Excluir somente arquivos de carga útil** ( ). As informações sobre a atualização (o arquivo de metadados XML) permanecem no repositório e o status de download muda para "Não baixado".

  Importante:

  – A carga útil dos pacotes de repositório é excluída automaticamente após os pacotes de atualização serem extraídos durante o processo de download ou importação.
  – Você não pode excluir cargas de pacotes de atualização que sejam usados nas políticas de conformidade de atualização. Você deve primeiro remover o pacote de atualização das políticas (consulte Criando e atribuindo políticas de conformidade de atualização).
  – Alguns pacotes de atualização são comuns para várias plataformas e componentes. A exclusão de um pacote de atualização comum afeta todas as plataformas e componentes que o usam.

Criando e atribuindo políticas de conformidade de atualização

É possível criar uma política de conformidade de atualização baseada nas atualizações adquiridas no repositório de atualizações. Em seguida, é possível atribuir a política a um ou mais gerenciadores de recursos ou servidores gerenciados.

Antes de iniciar

Ao criar uma política de conformidade de atualização, selecione a versão de atualização de destino a ser aplicada aos recursos que serão atribuídos à política. Certifique-se de que os arquivos de atualização da versão de destino estejam no repositório de atualizações antes de criar a política.

Quando você baixa ou importa um pacote de repositório de atualização de firmware, as políticas de conformidade de firmware predefinidas no pacote de repositório são adicionadas ao repositório de atualizações. Trata-se de uma *política predefinida*, que não pode ser modificada nem excluída.

Sobre esta tarefa

As políticas de conformidade de atualização garantem que o software ou o firmware em alguns recursos gerenciados esteja no nível atual ou específico sinalizando os recursos que precisam de atenção. Cada política de conformidade de atualização identifica quais recursos são monitorados e qual nível de software ou firmware deve ser instalado para manter os recursos em conformidade. Em seguida, o XClarity Orchestrator usa essas políticas para verificar o status de recursos gerenciados e identificar os recursos que não estão em conformidade.

Ao criar uma política de conformidade de atualização, é possível fazer o XClarity Orchestrator sinalizar um recurso quando o software ou firmware no recurso estiver em um nível inferior.

Depois que uma política de conformidade de atualização é atribuída a um recurso, o XClarity Orchestrator verifica o status de conformidade do recurso quando o repositório de atualizações é alterado. Se o software ou firmware no recurso não está em conformidade com a política atribuída, o XClarity Orchestrator sinaliza

esse recurso como não conforme na página Aplicar/Ativar, com base nas regras que você especificou na política de conformidade de atualização.

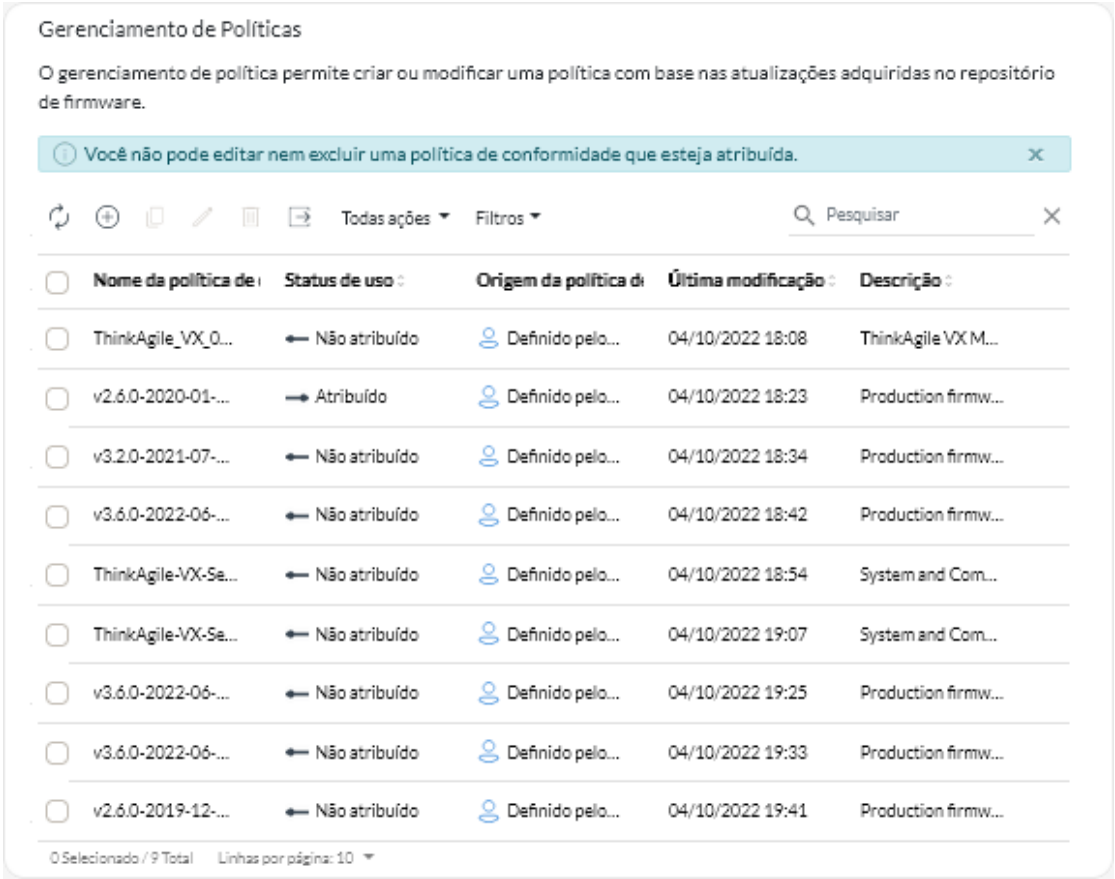
Por exemplo, é possível criar uma política de conformidade de atualização que defina o nível de software de linha de base para o XClarity Administrator e, em seguida, atribuir essa política a todos os gerenciadores de recursos do XClarity Administrator. Quando o catálogo de atualizações é atualizado e uma nova atualização é baixada ou importada, as instâncias do XClarity Administrator podem ficar fora de conformidade. Quando isso acontece, o XClarity Orchestrator atualiza a página Aplicar/Ativar para mostrar quais instâncias do XClarity Administrator não estão em conformidade e gera um alerta.

Procedimento

Para criar e atribuir uma política de conformidade de atualização, conclua as etapas a seguir.

Etapa 1. Crie uma política de conformidade de atualização.

1. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento** ( ) → **Atualizações** e, em seguida, clique em **Gerenciamento de Políticas** para exibir o cartão Gerenciamento de Políticas.



2. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Criar política de conformidade.
3. Especifique o nome e a descrição opcional da política.
4. Especifique o acionador da política. Este pode ser um dos valores a seguir.
   - **Sinalizar se a correspondência não for exata**. Se a versão de software ou firmware instalada no recurso for *anterior ou posterior* à versão de firmware de destino na política de conformidade de atualização, o recurso será sinalizado como não compatível. Por exemplo, se você substituir um adaptador de rede em um servidor, e o firmware nesse

adaptador de rede for diferente da versão de firmware padrão na política de conformidade de atualização atribuída, o servidor será sinalizado como não compatível.

- **Não sinalizar**. Recursos que estão fora de conformidade não são sinalizados.

5. Clique na guia **Regras** para adicionar regras de conformidade para essa política.
   a. Selecione o tipo de recurso para essa política.
   b. Especifique o destino de conformidade para recursos e componentes aplicáveis.Para recursos com componentes, é possível escolher um dos valores a seguir.
      - **Personalizar**. O destino de conformidade de cada componente de recurso será padronizado para a versão mais recente atual no repositório desse componente.
      - **Não atualizar**. O destino de conformidade de cada componente do recurso será padronizado para **Não atualizar**. Observe que se você alterar o valor padrão para qualquer componente, o destino de conformidade do recurso geral mudará para **Personalizar**.Para recursos sem componentes e para cada componente, é possível escolher um dos valores a seguir.
        – *{firmware_level}*. Especifica que o firmware no componente deve estar na versão de firmware da linha de base selecionada.
        – **Não atualizar**. Especifica que o firmware no componente não deve ser atualizado. Observe que o firmware no controlador de gerenciamento de backup (secundário) não é atualizado por padrão.
   c. Clique no ícone **Adicionar** (⊕) para incluir regras adicionais e clique no ícone **Excluir** (🗑) para excluir regras.
6. Clique em **Criar**.

Etapa 2. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento (🛒) → Atualizações** e clique em **Aplicar e Ativar** para exibir o cartão Aplicar e Ativar.

Etapa 3. Atribua a política de conformidade de atualização a recursos.

- **A um único recurso**Para cada recurso, selecione uma política na lista suspensa da coluna **Política de Conformidade Atribuída**.

  Você pode selecionar uma opção em uma lista de políticas de conformidade aplicáveis ao recurso. Se não houver uma política atualmente atribuída ao recurso, a política atribuída será definida como **Sem atribuição**. Se nenhuma política for aplicável ao recurso, a política atribuída será definida como **Sem políticas aplicáveis**.

- **A vários recursos**
  1. Selecione um ou mais recursos aos quais você deseja atribuir a política.
  2. Clique no ícone **Atribuir** (📋) para exibir a caixa de diálogo Atribuir Política.
  3. Selecione a política que deseja atribuir.Você pode selecionar uma opção em uma lista de políticas de conformidade aplicáveis a todos os recursos selecionados. Se não houver uma política atualmente atribuída ao recurso, a política atribuída será definida como **Sem atribuição**. Se nenhuma política for aplicável ao recurso, a política atribuída será definida como **Sem políticas aplicáveis**. Se os recursos não foram selecionados antes de abrir a caixa de diálogo, todas as políticas serão listadas.

     Nota: Selecione **Sem atribuição** para remover a atribuição de política do recurso selecionado.
  4. Selecione um dos seguintes escopos para a atribuição de política.
     – **Todos os dispositivos aplicáveis que são...**
     – **Somente dispositivos aplicáveis selecionados que são...**

5. Selecione um ou mais critérios de política.
   - **Sem uma política atribuída**
   - **Não compatível (substituir política atribuída atual)**
   - **Compatível (substituir política atribuída atual)**
6. Clique em **Aplicar**.A política listada na coluna Política Atribuída na página Atualizações de Firmware: Repositório altera o nome da política de conformidade de firmware selecionada.

- **Para grupos de recursos**

1. Clique no ícone **Atribuir** ( ) para exibir a caixa de diálogo Atribuir Política.
2. Selecione a política que deseja atribuir.Você pode selecionar uma opção em uma lista de políticas de conformidade aplicáveis a todos os recursos no grupo. Se não houver uma política atualmente atribuída ao recurso, a política atribuída será definida como **Sem atribuição**. Se nenhuma política for aplicável ao recurso, a política atribuída será definida como **Sem políticas aplicáveis**.

   Nota: Selecione **Sem atribuição** para remover a atribuição de política dos recursos no grupo.
3. Selecione um ou mais grupos de recursos aos quais você deseja atribuir a política.
4. Selecione um dos seguintes escopos para a atribuição de política.
   - **Todos os dispositivos aplicáveis que são...**
   - **Somente dispositivos aplicáveis selecionados que são...**
5. Selecione um ou mais critérios de política.
   - **Sem uma política atribuída**
   - **Não compatível (substituir política atribuída atual)**
   - **Compatível (substituir política atribuída atual)**
6. Clique em **Aplicar**.A política listada na coluna Política Atribuída na página Atualizações de Firmware: Repositório altera o nome da política de conformidade de firmware selecionada.

Depois de concluir

É possível executar as ações a seguir a partir do cartão Gerenciamento de Políticas.

- Exiba detalhes da política clicando na linha na tabela.
- Modifique uma política selecionada clicando no ícone **Editar** ( ).

  Nota: Não é possível modificar uma política atribuída a um ou mais recursos. Você deve primeiro cancelar a atribuição da política.
- Copiar e modificar uma política selecionada clicando no ícone **Copiar** ( ).
- Exclua uma política *definida pelo usuário* selecionada clicando no ícone **Excluir** ( ).

  Nota: Não é possível excluir uma política atribuída a um ou mais recursos. Você deve primeiro cancelar a atribuição da política.

No cartão Aplicar e Ativar, você pode cancelar a atribuição de uma política para um recurso selecionado clicando no ícone **Atribuir** ( ), selecionando **Sem atribuição** e, em seguida, selecionando se deve aplicar a alteração a todos os recursos com uma atribuição de política ou apenas aos recursos selecionados.

Aplicando e ativando atualizações aos gerenciadores de recursos

O XClarity Orchestrator não aplica atualizações automaticamente. Para atualizar o software, você deve aplicar e ativar manualmente a atualização nos gerenciadores de recursos selecionados do Lenovo XClarity Administrator que não são compatíveis com a política de conformidade de atualização atribuída.

Antes de iniciar

Antes de tentar aplicar e ativar atualizações em algum recurso, verifique se você leu as considerações de atualização (consulte Atualizar considerações de implantação).

Certifique-se de que uma política de conformidade de atualização esteja atribuída ao recurso de destino (consulte Criando e atribuindo políticas de conformidade de atualização).

Não é possível aplicar uma atualização do mesmo nível de software ou anterior à do atualmente instalado.

Sobre esta tarefa

É possível aplicar atualizações de firmware a gerenciadores de recursos do XClarity Administrator que tenham uma política de conformidade de atualizações atribuída e não estejam em conformidade com essa política. É possível atualizar o software das maneiras a seguir.

- Para gerenciadores específicos não compatíveis
- Para todos os gerenciadores não compatíveis em grupos específicos
- Para todos os gerenciadores não compatíveis com uma política específica de conformidade de atualização atribuída
- Para todos os gerenciadores não compatíveis em grupos específicos com uma política específica de conformidade de atualização atribuída
- Para todos os gerenciadores não compatíveis com qualquer política atribuída e que não estão em conformidade com essa política

O XClarity Orchestrator não atualiza recursos diretamente. Em vez disso, ele envia uma solicitação ao gerenciador de recursos aplicável para executar a atualização e rastreia o progresso da solicitação. O XClarity Orchestrator identifica as dependências que são necessárias para executar a atualização, garante que os recursos de destino sejam atualizados na ordem correta, transfira os pacotes de atualização aplicáveis ao gerenciador de recursos e cria uma solicitação para iniciar um trabalho no gerenciador de recursos para executar a atualização.

Durante o processo de atualização, o recurso de destino poderá ser reiniciado automaticamente várias vezes até a conclusão de todo o processo de atualização. Certifique-se de fechar todos os aplicativos no recurso de destino antes de continuar.

Se ocorrer um erro ao atualizar qualquer um dos componentes em um recurso de destino, o processo de atualização não atualizará esse componente; entretanto, o processo de atualização continuará a atualizar os outros componentes no recurso e todos os outros recursos de destino no trabalho de atualização atual.

As atualizações de pré-requisito não são aplicadas automaticamente.

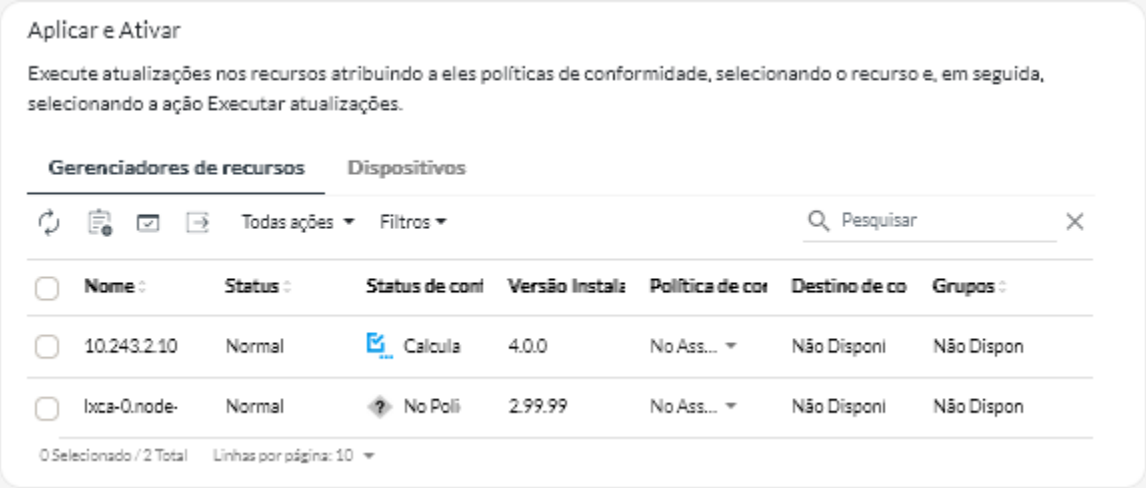
Dica:

- A tabela lista apenas gerenciadores de recursos que podem ser atualizados.
- As colunas **Número do Build** e **Número do Build do Destino de Conformidade** são ocultas da exibição por padrão. É possível mostrar essas colunas clicando em **Todas as Ações → Alternar Colunas**.

Procedimento

Para aplicar as atualizações aos gerenciadores de recursos do XClarity Orchestrator, conclua um dos procedimentos a seguir.

- **Para gerenciadores de recursos não compatíveis**
  1. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento** ( ) **→ Atualizações** e clique em **Aplicar e Ativar** para exibir o cartão Aplicar e Ativar.



2. Clique na guia **Gerenciadores de Recursos**.
3. Selecione um ou mais gerenciadores de recursos nos quais você deseja aplicar atualizações.
4. Clique no ícone **Aplicar Atualização** () para exibir a caixa de diálogo Atualizar resumo.
5. Clique em **Realizar Atualizações** para aplicar as atualizações. 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 .)

- **Para todos os gerenciadores de recursos não compatíveis em grupos específicos ou que tenham uma política específica de conformidade de atualização atribuída**

1. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento** () → **Atualizações** e clique em **Aplicar e Ativar** para exibir o cartão Aplicar e Ativar.
2. Clique na guia **Gerenciadores de Recursos**.
3. Clique no ícone **Aplicar Atualização** () para exibir a caixa de diálogo Atualizar resumo.
4. Selecione os grupos e a política de conformidade de atualização.
   - Se você não selecionar uma política nem um grupo, todos os gerenciadores que tenham uma política atribuída e que não estejam em conformidade com ela serão atualizados.
   - Se você selecionar uma política, mas não um grupo, todos os gerenciadores que tenham essa política atribuída e que não estiverem em conformidade com ela serão atualizados.
   - Se você selecionar um ou mais grupos e não uma política, todos os gerenciadores do grupo que não estiverem em conformidade com a política atribuída serão atualizados.
   - Se você selecionar uma política e um ou mais grupos, todos os gerenciadores do grupo que tiverem essa política atribuída e não estiverem em conformidade com ela serão atualizados.
5. Clique em **Realizar Atualizações** para aplicar as atualizações. 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 .)

Aplicando e ativando atualizações aos servidores gerenciados

O Lenovo XClarity Orchestrator não aplica atualizações automaticamente. Para atualizar o firmware, você deve aplicar e ativar manualmente a atualização nos dispositivos selecionados que não são compatíveis com a política de conformidade de atualização atribuída.

Antes de iniciar

Antes de tentar aplicar e ativar atualizações em algum dispositivo, verifique se você leu as considerações de atualização (consulte Atualizar considerações de implantação).

Certifique-se de que uma política de conformidade de atualização esteja atribuída ao dispositivo de destino (consulte Criando e atribuindo políticas de conformidade de atualização).

É possível aplicar atualizações de firmware somente aos servidores gerenciados.

Ao atualizar o firmware em muitos dispositivos ao mesmo tempo, use o XClarity Orchestrator v1.3.1 ou posterior e o Lenovo XClarity Administrator v3.2.1 ou posterior para obter melhor desempenho.

Sobre esta tarefa

É possível aplicar atualizações de firmware a dispositivos que tenham uma política de conformidade de atualizações atribuída e não estejam em conformidade com essa política. É possível atualizar o firmware das maneiras a seguir.

- Para dispositivos específicos não compatíveis
- Para todos os dispositivos não compatíveis em grupos específicos
- Para todos os dispositivos não compatíveis com uma política específica de conformidade de atualização atribuída
- Para todos os dispositivos não compatíveis em grupos específicos com uma política específica de conformidade de atualização atribuída
- A todos os dispositivos não compatíveis com qualquer política atribuída e não estão em conformidade com essa política

Um servidor é sinalizado como Não compatível quando a versão de firmware instalada de um ou mais componentes é *anterior ou posterior* à versão de firmware de destino na política de conformidade de atualização. Se a versão de firmware for *posterior* à instalada, você deverá selecionar a opção **Forçar atualização** ao aplicar a atualização para fazer downgrade do firmware nos componentes. Se a opção **Forçar atualização** não estiver selecionada, apenas as versões de firmware de destino posteriores às versões instaladas serão aplicadas.

Nota: Apenas determinadas opções de dispositivo, adaptadores e unidades são compatíveis com downgrade. Consulte a documentação do hardware para determinar se o downgrade é compatível.

O XClarity Orchestrator não atualiza recursos diretamente. Em vez disso, ele envia uma solicitação ao gerenciador de recursos aplicável para executar a atualização e rastreia o progresso da solicitação. O XClarity Orchestrator identifica as dependências que são necessárias para executar a atualização, garante que os recursos de destino sejam atualizados na ordem correta, transfira os pacotes de atualização aplicáveis ao gerenciador de recursos e cria uma solicitação para iniciar um trabalho no gerenciador de recursos para executar a atualização.

Durante o processo de atualização, o dispositivo de destino poderá ser reiniciado automaticamente várias vezes até a conclusão de todo o processo de atualização. Certifique-se de fechar todos os aplicativos no dispositivo de destino antes de continuar.

Se ocorrer um erro ao atualizar qualquer um dos componentes em um dispositivo de destino, o processo de atualização não atualizará esse componente; entretanto, o processo de atualização continuará a atualizar os outros componentes no dispositivo e todos os outros dispositivos de destino no trabalho de atualização atual.

As atualizações de pré-requisito não são aplicadas automaticamente.

Dicas:

- A tabela lista apenas dispositivos que podem ser atualizados.
- As colunas **Número do Build**, **Número do Build do Destino de Conformidade** e **Nome do Produto** são ocultas da exibição por padrão. É possível mostrar essas colunas clicando em **Todas as Ações → Alternar Colunas**.
- Para servidores ThinkSystem SR635, SR645, SR655 e SR665, para aplicar firmware dentro e fora da banda, primeiro aplique atualizações aos Baseboard Management Controllers e, em seguida, aplique atualizações de firmware às opções restantes.

Procedimento

Para aplicar as atualizações aos dispositivos gerenciados, conclua um dos procedimentos a seguir.

- **Para dispositivos específicos não compatíveis**
  1. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento ( ) → Atualizações** e clique em **Aplicar e Ativar** para exibir o cartão Aplicar e Ativar.
  2. Clique na guia **Dispositivos**.
  3. Selecione um ou mais dispositivos nos quais você deseja aplicar atualizações.
  4. Clique no ícone **Aplicar Atualização** ( ) para exibir a caixa de diálogo Atualizar Resumo.
  5. Selecione quando ativar as atualizações.
     - **Ativação priorizada**. As atualizações de firmware no Baseboard Management Controller são ativadas imediatamente. Todas as outras atualizações de firmware são ativadas na próxima vez em que o dispositivo é reiniciado. Em seguida, as reinicializações adicionais são executadas até o término do processo de atualização. Um evento é gerado quando o status muda para o Modo de Manutenção de Firmware Pendente para notificá-lo quando o servidor precisa ser reiniciado.
     - **Ativação atrasada**. Algumas, mas nem todas as operações de atualização, são executadas. É necessário reiniciar os dispositivos de destino manualmente para prosseguir com o processo de atualização. Em seguida, as reinicializações adicionais são executadas até o término do processo de atualização.Um evento é gerado quando o status muda para o Modo de Manutenção de Firmware Pendente para notificá-lo quando o servidor precisa ser reiniciado.

       Se o dispositivo de destino for reiniciado por algum motivo, o processo de atualização atrasado será concluído.

       Importante:

       - Use **Reiniciar normalmente** para reiniciar o servidor para continuar o processo de atualização. *Não* use **Reiniciar Imediatamente**.
       - Não escolha Ativação Atrasada para mais de 50 dispositivos ao mesmo tempo. O XClarity Orchestrator monitora ativamente dispositivos com ativação atrasada, para que a ativação atrasada seja realizada quando o dispositivo é reiniciado. Se desejar aplicar atualizações com ativação atrasada para mais de 50 dispositivos, separe a seleção de atualização em lotes de 50 dispositivos por vez.
     - **Ativação imediata**. Durante o processo de atualização, o dispositivo de destino poderá ser reiniciado automaticamente várias vezes até a conclusão de todo o processo de atualização. Certifique-se de fechar todos os aplicativos no dispositivo de destino antes de continuar.

     Notas:

     - Para servidores gerenciados pelo XClarity Management Hub 2.0 e para dispositivos ThinkEdge Client, apenas a ativação imediata é aceita, independentemente da regra de ativação selecionada.

– Quando ativada, a opção de inicialização Wake-on-LAN pode interferir nas operações do Lenovo XClarity Administrator que desligam que o servidor, incluindo atualizações de firmware se houver um cliente Wake-on-LAN na rede que emite comandos "Wake on Magic Packet".

6. **Opcional:** selecione **Forçar atualização** para atualizar o firmware em componentes selecionados mesmo se o nível de firmware estiver atualizado ou aplique uma atualização de firmware que seja anterior à atualmente instalada nos componentes selecionados.
7. **Opcional:** selecione **Agendar atualização** para escolher a data e hora em que deseja que a atualização de firmware seja executada. Se não for selecionado, o firmware será atualizado imediatamente.
8. Clique em **Realizar Atualizações** para aplicar as atualizações. 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 .)

- **Para todos os dispositivos não compatíveis em grupos específicos com uma política específica de conformidade de atualização atribuída**

1. Na barra de menus do XClarity Orchestrator, clique em **Fornecimento ( ) → Atualizações** e clique em **Aplicar e Ativar** para exibir o cartão Aplicar e Ativar.
2. Clique na guia **Dispositivos**.
3. Selecione um ou mais grupos de dispositivos nos quais você deseja aplicar atualizações.
4. Clique no ícone **Aplicar Atualização** ( ) para exibir a caixa de diálogo Atualizar Resumo.
5. Selecione os grupos e a política de conformidade de atualização.
   – Se você não selecionar uma política ou grupo, todos os dispositivos que tenham uma política atribuída e que não estejam em conformidade com ela serão atualizados.
   – Se você selecionar uma política, mas não um grupo, todos os dispositivos que tenham essa política atribuída e que não estiverem em conformidade com ela serão atualizados.
   – Se você selecionar um ou mais grupos e não uma política, todos os dispositivos do grupo que não estiverem em conformidade com a política atribuída serão atualizados.
   – Se você selecionar uma política e um ou mais grupos, todos os dispositivos do grupo que tiverem essa política atribuída e não estiverem em conformidade com ela serão atualizados.
6. Selecione quando ativar as atualizações.

   – **Ativação priorizada**. As atualizações de firmware no Baseboard Management Controller são ativadas imediatamente. Todas as outras atualizações de firmware são ativadas na próxima vez em que o dispositivo é reiniciado. Em seguida, as reinicializações adicionais são executadas até o término do processo de atualização. Um evento é gerado quando o status muda para o Modo de Manutenção de Firmware Pendente para notificá-lo quando o servidor precisa ser reiniciado.
   – **Ativação atrasada**. Algumas, mas nem todas as operações de atualização, são executadas. É necessário reiniciar os dispositivos de destino manualmente para prosseguir com o processo de atualização. Em seguida, as reinicializações adicionais são executadas até o término do processo de atualização.Um evento é gerado quando o status muda para o Modo de Manutenção de Firmware Pendente para notificá-lo quando o servidor precisa ser reiniciado.

     Se o dispositivo de destino for reiniciado por algum motivo, o processo de atualização atrasado será concluído.

     Importante:

     – Use **Reiniciar normalmente** para reiniciar o servidor para continuar o processo de atualização. *Não* use **Reiniciar Imediatamente**.
     – Não escolha Ativação Atrasada para mais de 50 dispositivos ao mesmo tempo. O XClarity Orchestrator monitora ativamente dispositivos com ativação atrasada, para que a ativação atrasada seja realizada quando o dispositivo é reiniciado. Se desejar aplicar atualizações com

ativação atrasada para mais de 50 dispositivos, separe a seleção de atualização em lotes de 50 dispositivos por vez.

– **Ativação imediata**. Durante o processo de atualização, o dispositivo de destino poderá ser reiniciado automaticamente várias vezes até a conclusão de todo o processo de atualização. Certifique-se de fechar todos os aplicativos no dispositivo de destino antes de continuar.

Notas:

– Para servidores gerenciados pelo XClarity Management Hub 2.0 e para dispositivos ThinkEdge Client, apenas a ativação imediata é aceita, independentemente da regra de ativação selecionada.

– Quando ativada, a opção de inicialização Wake-on-LAN pode interferir nas operações do Lenovo XClarity Administrator que desligam que o servidor, incluindo atualizações de firmware se houver um cliente Wake-on-LAN na rede que emite comandos "Wake on Magic Packet".

7. **Opcional:** selecione **Forçar atualização** para atualizar o firmware em componentes selecionados mesmo se o nível de firmware estiver atualizado ou aplique uma atualização de firmware que seja anterior à atualmente instalada nos componentes selecionados.
8. **Opcional:** selecione **Agendar atualização** para escolher a data e hora em que deseja que a atualização de firmware seja executada. Se não for selecionado, o firmware será atualizado imediatamente.
9. Clique em **Realizar Atualizações** para aplicar as atualizações. 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 .)

Depois de concluir

É possível executar as ações a seguir na placa Padrões.

- Encaminhe relatórios sobre conformidade de firmware de forma recorrente em um ou mais endereços de e-mail clicando no ícone **Criar encaminhador de relatórios** ( ). O relatório é enviado usando os filtros de dados que estão aplicados atualmente à tabela. Todas as colunas da tabela mostradas e ocultas são incluídas no relatório. Para obter mais informações, consulte Encaminhando relatórios.
- Adicione um relatório de conformidade de firmware a um encaminhador de relatórios específico usando os filtros de dados que estão aplicados atualmente à tabela clicando no ícone **Adicionar ao encaminhador de relatórios** ( ). Se o encaminhador de relatórios já incluir um relatório de conformidade de firmware, ele será atualizado para usar os filtros de dados atuais.

É possível cancelar um trabalho de atualização de firmware programado que ainda não foi executado clicando em **Monitoramento ( ) → Trabalhos** na barra de menus do XClarity Orchestrator e clique na guia **Programações** para exibir o cartão Tarefas programadas. Selecione a tarefa programada e, em seguida, clique no ícone **Cancelado** ( ).

Capítulo 6. Analisando tendências e prevendo problemas

O Lenovo XClarity Orchestrator gera alertas de análise com base em problemas conhecidos de hardware e firmware, monitora tendências para detectar anomalias que ocorrem em seus recursos gerenciados e cria heurísticas que podem calcular a probabilidade de problemas ou falhas iminentes. As tendências são visualizadas como consultas e gráficos que mostram o status de conformidade, o histórico de problemas e a divisão dos recursos que têm a maioria dos problemas. Em seguida, é possível analisar essas tendências para obter informações sobre a causa dos problemas e resolvê-los rapidamente.

Importante:

- As funções de análise são compatíveis com servidores ThinkAgile, ThinkSystem e ThinkEdge executando o firmware XCC v1.4 ou posterior.
- Para usar as funções de análise, uma licença do Lenovo XClarity Orchestrator Analytics é necessária para cada dispositivo que ofereça suporte às funções de análise. Uma licença *não* está vinculada a dispositivos específicos. Para obter mais informações, consulte Aplicando licenças do XClarity Orchestrator na documentação online do XClarity Orchestrator.

Criando relatórios de análise personalizados

Os relatórios analíticos são executados continuamente em segundo plano para entender como o data center está operando em tempo real.

Sobre esta tarefa

O Lenovo XClarity Orchestrator fornece diversos relatórios de análise predefinidos que são baseados em eventos, inventário ou dados métricos coletados dos recursos gerenciados. Eles são exibidos como estatísticas (na forma tabular) ou graficamente como gráficos de barras ou pizza. Você pode ver exemplos desses relatórios nas páginas **Análise ( ) → Análises predefinidas**.

Também é possível criar seus próprios relatórios personalizados para representar dados que lhe interessam mais.

Procedimento

Para criar relatórios de análise personalizados, conclua as etapas a seguir.

Etapa 1. Crie alertas personalizados.

O XClarity Orchestrator gera alertas de análise com base em problemas conhecidos de hardware e firmware. Também é possível criar alertas personalizados para usar em seus relatórios personalizados.

Etapa 2. Crie relatórios personalizados (consultas).

É possível incluir relatórios gráficos personalizados ao XClarity Orchestrator definindo consultas baseadas nos dados que mais interessam a você.

Criando regras para alertas de análise personalizados

Lenovo XClarity Orchestrator gera alertas com base em problemas conhecidos de hardware e firmware. É possível definir *regras de alerta* personalizadas para gerar alertas de análise quando um evento específico ocorre ou quando uma métrica específica é violada. Em seguida, é possível usar esses alertas para gerar relatórios de análise personalizados (consultas).

Sobre esta tarefa

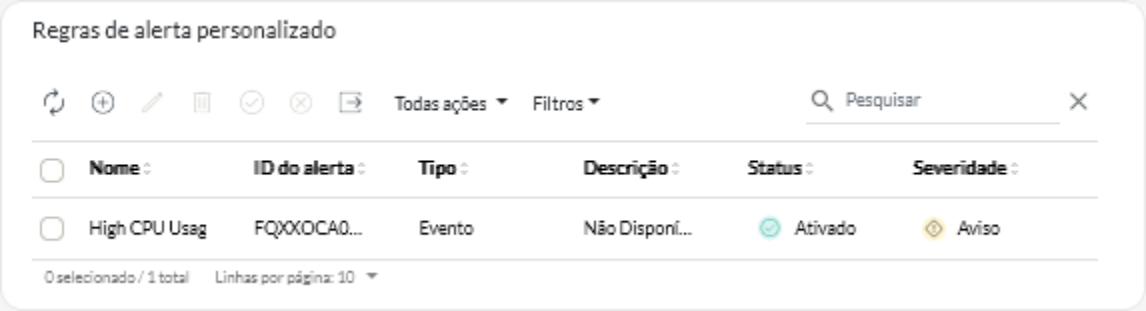
Os eventos são gerados para todos os alertas, incluindo alertas de análise personalizados. O mesmo código de evento é usado para o alerta ativo e o evento usando o formato `FQXXOCA`*xxxxc*, em que *xxxx* é o identificador exclusivo e *c* é a severidade

Alertas personalizados são incluídos na lista de alertas ativos para status de funcionamento. Todos os alertas ativos, incluindo alertas personalizados, são exibidos em uma só exibição unificada (consulte Monitorando alertas ativos).

Procedimento

Para criar uma regra de alertas personalizados, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Análise (**) → **Alertas personalizados**para exibir o cartão Regras de alerta personalizado.



Etapa 2. Clique no ícone **Criar** (⊕) para exibir a caixa de diálogo Criar Regra de Alertas Personalizados.

Etapa 3. Especifique um nome exclusivo e uma descrição opcional para o alerta personalizado.

Etapa 4. Selecione o tipo de origem para essa regra.
- **Evento**. Gera um alerta quando um evento específico ocorre, com base nos critérios de regra.
- **Métrica**. Gera um alerta quando uma métrica específica é violada, com base nos critérios de regra.

Etapa 5. Clique em **Detalhes do Acionador de Regra** e especifique os critérios para essa regra. Os critérios variam dependendo do tipo de origem.

- **Regras de alertas com base em eventos**
  - Especifique o tipo de destino para esse alerta.
    - **Dispositivo**. Gera um alerta quando o evento ocorre em qualquer dispositivo. O nome do dispositivo está incluído neste alerta.
    - **Grupo de dispositivos**. Gera um alerta quando o evento ocorre em um dispositivo em qualquer grupo de dispositivos. O nome do grupo está incluído no alerta.
  - Especifique o ID do evento que aciona um alerta. Para obter uma lista de IDs de eventos, consulte Mensagens de eventos e alertas na documentação online do XClarity Orchestrator.
  - Especifique o número de vezes (contagem) que o evento deve ocorrer no intervalo especificado antes que um alerta seja gerado.
  - Selecione o período (intervalo), em minutos, no qual o evento ocorre antes de um alerta ser gerado.
- **Regras de alertas com base em métricas**
  - Selecione o modo de critérios.

- **média**. Gera um alerta quando o valor médio da métrica viola o limite (com base no comparador) durante um intervalo específico.

  Por exemplo, é possível criar uma regra para gerar um alerta quando a temperatura média da CPU (**metric**) durante um período de 24 horas (**interval**) é maior que (**operator**) 40 graus C (**threshold**).
- **contagem**. Gera um alerta quando a métrica viola o limite (com base no comparador) em determinadas vezes durante um intervalo específico.

  Por exemplo, é possível criar uma regra para gerar um alerta quando a temperatura média da CPU (**metric**) é maior que (**operator**) 40 graus C (**threshold**) por 5 vezes (**count**) em um período de 24 horas (**interval**).
- **simples**. Gera um alerta quando a métrica viola o limite (com base no comparador).

  Por exemplo, é possível criar uma regra para gerar um alerta quando a temperatura média da CPU (**metric**) é maior que (**operator**) 40 graus C (**threshold**).

– Selecione a medida (métrica) para esse alerta em uma lista de medidas suportadas para os recursos gerenciados.
– Se o modo de critérios for "contagem", especifique o número de vezes que o valor foi violado no intervalo especificado antes que um alerta seja gerado.
– Selecione a função de comparação.
  – **>=**. Maior ou igual a
  – **<=**. Menor ou igual a
  – **>**. Maior que
  – **<**. Menor que
  – **=**. Igual a
  – **!=**. Diferente de
– Especifique o valor limite para comparar com o valor da métrica.
– Se o modo de critérios for "média" ou "contagem", selecione o período (intervalo), em minutos, no qual a métrica é avaliada.

Etapa 6. Clique em **Alerta e Detalhes do Evento** e especifique as informações a serem exibidas para o alerta e o evento.

1. Especifique a mensagem, a descrição e a ação do usuário a serem exibidas para o alerta e o evento associados. É possível incluir variáveis, colocando o nome do campo (variável) em colchetes duplos, por exemplo, `[[DeviceName]]`. Uma lista de campos disponíveis (com base na medida selecionada) é exibida na tabela à direita dos campos de entrada.
2. Selecione a gravidade para essa regra de alerta.
   - **Aviso**. O usuário pode decidir se a ação é necessária.
   - **Crítico**. A ação é necessária imediatamente, e o escopo é amplo (talvez resultará em uma falha iminente em um recurso crítico).
3. Especifique um número exclusivo de 4 dígitos a ser usado para o código do evento desse alerta. É possível especificar um número de 0001 a 9999 que ainda não seja usado.

Etapa 7. Opcionalmente, altere o status para **Ativado** para permitir que o XClarity Orchestrator gere um alerta de análise quando os critérios para o alerta personalizado forem atendidos.

Etapa 8. Clique em **Criar**.

Depois de concluir

É possível exibir a lista de alertas de análise que foram gerados com base nas regras de alertas personalizados ativadas clicando em **Monitoramento ( ) → Alertas**.

É possível executar as ações a seguir a partir do cartão Regras de Alertas Personalizados.

- Modifique as propriedades de uma regra de alertas personalizados clicando no ícone **Editar** ( ).
- Exclua uma regra de alertas personalizados clicando no ícone **Excluir** ( ).
- Ative ou desative uma ou mais regras de alertas personalizados clicando no ícone **Ativar** ( ) ou no ícone **Desativar** ( ).

Criando relatórios personalizados (consultas)

É possível incluir relatórios gráficos e tabulares personalizados para o Lenovo XClarity Orchestrator definindo consultas baseadas em dados coletados, como alertas, eventos, inventário, métricas de dispositivo ou métricas personalizadas (agregações).

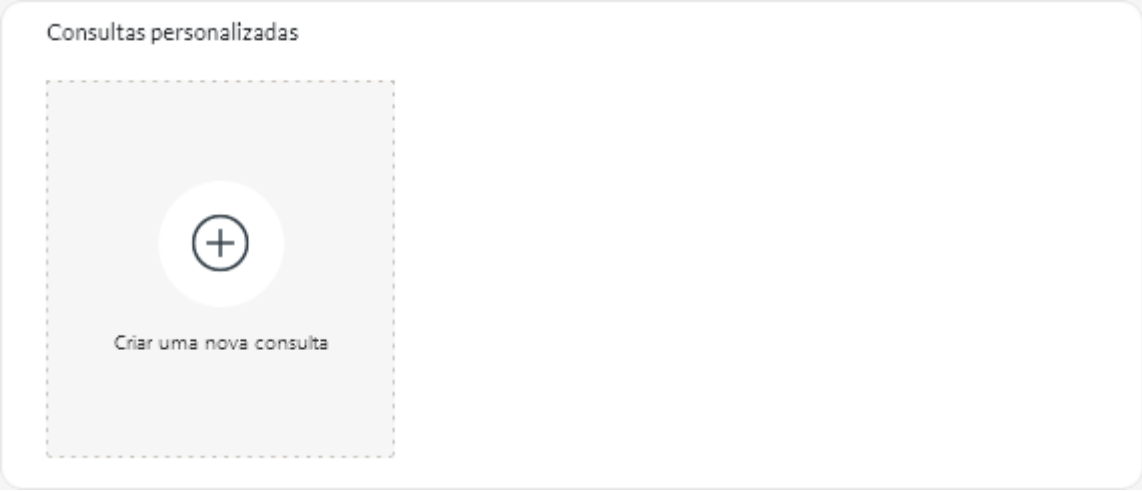
Antes de iniciar

Importante: A criação de relatórios de análises personalizados no XClarity Orchestrator requer um conhecimento básico de bancos de dados e consultas do banco de dados.

Sobre esta tarefa

Para criar um relatório personalizado, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Análise ( ) → Consultas personalizadas**, para exibir o cartão Consultas personalizadas.



Etapa 2. Clique no ícone **Criar** ( ) para exibir a caixa de diálogo Criar Consulta Personalizado.

Etapa 3. Especifique um nome exclusivo para a consulta personalizada.

Etapa 4. Selecione o tipo de dados que você deseja usar como fonte desta consulta.

É possível escolher um dos tipos de fonte de dados a seguir.

- **Alertas**. Condições de hardware ou gerenciamento que requerem investigação e ação do usuário
- **Eventos**. Eventos de auditoria e de recursos
- **Eventos-Recurso**. Condição de hardware ou do orquestrador que ocorreu em um dispositivo gerenciado, gerenciador de recursos ou no XClarity Orchestrator
- **Eventos-Auditoria**. Atividades do usuário que foram executadas a partir de um gerenciador de recursos ou XClarity Orchestrator
- **Inventários-Gerenciador**. Dados do inventário para gerenciadores de recursos

- **Inventários-Dispositivo**. Os dados do inventário para dispositivos gerenciados de todos os tipos
- **Inventários-Dispositivo-Servidor**. Dados do inventário para servidores gerenciados
- **Inventários-Dispositivo-Comutador**. Dados do inventário para comutadores gerenciados
- **Inventários-Dispositivo-Armazenamento**. Os dados do inventário para dispositivos de armazenamento gerenciados
- **Inventários-Dispositivo-Chassi**. Dados do inventário para chassi gerenciado
- **CPUTemp**. Dados métricos para temperatura, em graus Celsius, de cada processador em um dispositivo gerenciado. A métrica é capturada a cada minuto.
- **CPUUtilizationStats**. Dados métricos para o uso do processador, como uma porcentagem, para um dispositivo gerenciado. A métrica é capturada a cada minuto.
- **InletAirTemp**. Dados métricos para temperatura de entrada do ar, em graus Celsius, de um dispositivo gerenciado. A temperatura é capturada a cada minuto.
- **MemoryUtilizationStats**. Dados métricos para a memória usada, como uma porcentagem, por um dispositivo gerenciado. A métrica é capturada a cada minuto.
- **PowerMetrics**. Dados métricos para consumo de energia, em Watts, por todos os processadores, módulos de memória ou o sistema inteiro para um dispositivo gerenciado. Essas métricas são capturadas a cada 30 segundos.
- **PowerSupplyStats**. Dados métricos para entrada e saída da fonte de alimentação, em Watts, para um dispositivo gerenciado. Essas métricas são capturadas a cada 30 segundos.

Os tipos de fontes de dados (alertas, eventos, inventários e métricas) que são listados variam de acordo com os dados disponíveis no XClarity Orchestrator. Por exemplo, se os dados de alertas estiverem disponíveis, o tipo **Alertas** será listado. Se os dados de eventos estiverem disponíveis, todos os tipos de **Eventos-*** serão listados.

A fonte de dados selecionada afeta os dados disponíveis na guia **Condições da Consulta**. Se você selecionar um tipo genérico, como **Inventários-Dispositivos**, apenas os atributos comuns a todos os dispositivos serão listados. Se você selecionar **Inventários-Dispositivo-Servidor**, os atributos comuns a todos os servidores serão listados.

Etapa 5. Clique em **Condições da Consulta** para definir as condições de consulta do relatório.

1. Restrinja os dados que você deseja usar para essa consulta.
   a. Selecione um ou mais campos na lista suspensa **Campos Filtrados**. Os campos listados com base no tipo de fonte de dados selecionado na etapa 4.
   b. Se você selecionou vários campos de filtro, escolha o operador a ser usado para construir a consulta. Este pode ser um dos valores a seguir.
      - **E**. Todos os valores devem corresponder.
      - **OU**. Um ou mais valores devem corresponder.
      - **E (negado)**. Todos os valores não devem corresponder.
      - **OU (negado)**. Um ou mais valores não devem corresponder.
   c. Para cada campo filtrado selecionado, selecione o operador de comparação na lista suspensa **Comparação** e o valor do campo.Os operadores de comparação que estão disponíveis diferem com base no tipo de dados do atributo.
      - **>=**. Corresponde a valores *maiores ou iguais* a um valor especificado
      - **<=**. Corresponde a valores *menores ou iguais* a um valor especificado
      - **>**. Corresponde a valores *maiores que* um valor especificado
      - **<**. Corresponde a valores *menores que* um valor especificado
      - **=**. Corresponde a valores *iguais a* um valor especificado
      - **!=**. Corresponde a todos os valores *diferentes de* um valor especificado
      - **Contém**. (Somente consultas de inventário e eventos) Corresponde a quaisquer valores parciais especificados em uma matriz
      - **In**. (Somente consultas de inventário e eventos) Corresponde a quaisquer valores especificados em uma matriz

- **NotIn**. (Somente consultas de inventário e eventos) Não corresponde a nenhum valor especificados em uma matriz

Dica: para localizar os valores atuais de qualquer campo, crie uma nova consulta com o mesmo tipo de fonte de dados, selecione o nome do campo na lista suspensa **Campos Agrupados**, especifique 0 para o **Limite** e clique em **Salvar**. A guia **Opções de Gráfico** é exibida com uma lista de todos os valores atuais.

2. Opcionalmente, escolha uma função de agregação na seção **Agregação de Resultados** para criar um novo campo com base nos dados filtrados e especifique um nome (alias) para o novo campo.Para algumas funções de agregação como média e máximo, você também deve especificar o campo ao qual deseja aplicar a função.

   Para consultas de inventário e eventos, é possível escolher uma das funções a seguir.
   - **Média**. Média estatística de todos os valores
   - **Soma**. Soma de todos os valores
   - **Contagem**. Número de valores
   - **Máximo**. Valor mais alto
   - **Mínimo**. Menor valor
   - **Primeiro**. Valor com o carimbo de data/hora mais antigo
   - **Último**. Valor com o carimbo de data/hora mais recente

   Em consultas de métricas, é possível escolher uma das funções a seguir.
   - **Contagem**. Número de valores não Nulls
   - **Distinto**. Lista de valores exclusivos
   - **Integral**. Valor médio do campo
   - **Média**. Média aritmética de valores
   - **Mediana**. Valor do meio
   - **Modo**. Valor mais frequente
   - **Espalhamento**. Diferença entre os valores mínimo e máximo
   - **Stddev**. Desvio padrão
   - **Soma**. Soma de todos os valores
3. Opcionalmente, escolha os campos que você deseja usar para agrupar os resultados da consulta na lista suspensa **Campos agrupados**.Ao escolher um campo agrupado, o XClarity Orchestrator desenrolará (decomporá) os dados para que haja um ponto de dados para cada valor dos campos selecionados.
4. Opcionalmente, escolha como classificar os resultados da consulta selecionando um campo na lista suspensa **Classificar por Campo** e a ordem de classificação na lista suspensa **Ordem de Classificação**. Para consultas de métricas, é possível classificar apenas pela hora.
5. Opcionalmente, especifique o número de pontos de dados a serem retornados nos resultados da consulta no campo **Limite**. O limite padrão é 10. Se você especificar 0 ou deixá-lo vazio, todos os pontos de dados serão retornados.

   Também é possível especificar o número de pontos de dados que você deseja ignorar nos resultados da consulta no campo **Deslocamento**.
6. (Somente consultas de métricas) Se você escolher campos agrupados, opcionalmente, especifique o número de conjuntos de dados a serem retornados nos resultados da consulta no campo **Limite de Série**.O limite padrão é vazio (0). Se você especificar 0 ou deixá-lo vazio, todos os conjuntos de dados serão retornados.

   Também é possível especificar o número de conjuntos de dados que você deseja ignorar nos resultados da consulta no campo **Deslocamento de Série**.
7. Clique em **Salvar** para salvar a consulta e gerar o relatório.

Etapa 6. Clique em **Opções de Gráfico** para escolher a aparência do relatório. Os tipos de gráfico a seguir estão disponíveis.

- **Tabela**. Exibe dados em formato tabular.
- **Barra**. Exibe os dados como um gráfico de barras. Escolha os campos que você deseja usar para o eixo x e y.
- **Pizza**. Exibe os dados como um gráfico de pizza. Escolha os campos que você deseja usar para o eixo x e y.É possível optar por usar um gráfico de pizza apenas quando os dados não são agrupados.

Etapa 7. Clique em **Criar** para incluir um novo cartão que contenha um relatório com os resultados atuais da consulta.

Depois de concluir

É possível executar as ações a seguir no cartão Opções Personalizadas.

- Amplie um relatório personalizado clicando no ícone **Ampliar** ( ) no cartão de relatório personalizado. Para relatórios tabulares, o ícone de relatório no cartão Consultas Personalizadas mostra apenas as primeiras quatro colunas da tabela. É possível aumentar o relatório para ver todas as colunas na tabela.

  O link **Ver Detalhes** em uma coluna da tabela indica que a coluna contém vários campos de dados. Clique no link **Ver Detalhes** para exibir uma tabela pop-up que lista os dados adicionais.
- Modifique as propriedades de um relatório personalizado clicando no ícone **Editar** ( ) no cartão.
- Exclua um relatório personalizado clicando no ícone **Excluir** ( ) no cartão.

Analisando tempos de inicialização do dispositivo

O painel Análise contém placas de relatório que resumem os períodos de inicialização para dispositivos gerenciados. O *tempo de inicialização* é a quantidade de tempo, em segundos, que foi necessária para a inicialização do sistema ser concluída, antes de passar para o sistema operacional.

Para exibir os relatórios de tempo de inicialização, clique em **Análise ( ) → Análises predefinidas**e clique em **Períodos de inicializações** para exibir os cartões de análise relacionados.

Nota: As estatísticas de inicialização estão disponíveis somente para dispositivos ThinkSystem e ThinkAgile executando o firmware v1.40 ou posterior.

Períodos de inicializações

Esse cartão de relatório inclui um gráfico de barras que mostra a quantidade de tempo necessária para a conclusão das inicializações, para dispositivos com o mais logo dos últimos períodos de inicializações.

Analisando problemas de conectividade

O painel Análise contém placas de relatório que mostram estatísticas sobre problemas de conectividade.

A conectividade perdida é relatada usando o evento a seguir.

- **FQXHMDM0163J**. A conexão entre o gerenciador de recursos e o Baseboard Management Controller no dispositivo está offline.

Para exibir os relatórios de conectividade perdida, clique em **Análise ( ) → Análises predefinidas** e clique em **Problemas de Conectividade** para exibir os cartões de análise relacionados

Problemas de conectividade por tempo

Esse cartão de relatório inclui um gráfico de barras que mostra o número de problemas de conectividade ocorridos durante o dia ou o mês atual de cada recurso.

É possível optar por exibir dados de um intervalo específico selecionando o ícone **Configurações** (⚙) no canto superior direito do cartão.

10 principais dispositivos por número de problemas de conectividade

Esse cartão de relatório inclui um gráfico de barras que mostra os 10 principais dispositivos que estão relatando a maioria dos problemas de conectividade. É possível clicar em um item na legenda para obter mais informações sobre um recurso específico.

Analisando correções de segurança

O painel Análise contém boletins que mostram análises sobre correções de segurança para vulnerabilidades e exposições comuns e conhecidas (CVEs).

Para exibir os relatórios de CVE, clique em **Análise (🔍) → Análises predefinidas** e clique em **Correções de segurança** para exibir os cartões de análise relacionados.

Correções de segurança

Este boletim inclui as seguintes estatísticas e gráficos.

- Um gráfico circular que mostra o número de dispositivos gerenciados que têm vulnerabilidades e exposições comuns (CVEs) para as quais uma correção de segurança está disponível, pela gravidade de CVE mais alta
  - **Crítico**. Número de dispositivos que têm pelo menos uma CVE crítica
  - **Não crítico**. Número de dispositivos que têm pelo menos uma CVE alta, média ou baixa, mas nenhuma CVE crítica
  - **Protegidos**. Número de dispositivos que não têm CVEs e são protegidos
- Um gráfico circular que mostra o número de CVEs exclusivas para as quais as correções de segurança estão disponíveis, por gravidade (crítica, alta, média ou baixa)

É possível passar o mouse sobre cada barra colorida nos gráficos circulares para obter mais informações sobre o estado. Também é possível clicar no número ao lado de cada estado para exibir uma lista de todos os dispositivos que correspondem ao critério.

Dispositivos

A placa Dispositivos lista o número total de CVEs para as quais há uma correção de segurança disponível e a severidade mais alta de CVEs para cada dispositivo. É possível expandir o dispositivo para exibir uma lista de componentes nesse dispositivo que têm correções de segurança e o número de correções de segurança disponíveis nas atualizações de firmware que são baixadas no repositório das atualizações.

É possível clicar no número de correções de segurança para abrir uma caixa de diálogo com uma lista filtrada de CVEs aplicáveis para esse componente. Nessa caixa de diálogo, é possível clicar no link da CVE para obter informações detalhadas sobre essa CVE na Web.

É possível mostrar ou ocultar o cartão Dispositivos clicando no botão de alternância **Mostrar/Ocultar Dispositivos**. A alternância muda para **Mostrar dispositivos** automaticamente quando você clica em um número nos gráficos.

Analisando o funcionamento da unidade

O painel Análise contém cartões de relatório que mostram análises sobre a falha preditiva e de funcionamento de unidades de disco rígido e unidades de estado sólido em servidores gerenciados ThinkAgile e ThinkSystem.

Para exibir os relatórios de firmware, clique em **Análise ( ) → Análises predefinidas** e clique em **Análise Preditiva da Unidade** para exibir os cartões de análise relacionados.

As análises são compatíveis com os seguintes tipos de modelos de unidade.

Unidades de disco rígido
- ST2000NX0253
- ST8000NM0055
- ST10000NM0086
- ST12000NM0008

Unidades de estado sólido
- Intel SSDSC2BB800G4

Importante: Unidades com firmware mais antigo são qualificadas para análise. Atualize as unidades quanto ao nível de firmware mais recente a fim de habilitar a análise preditiva.

Unidades em risco

Este boletim contém um gráfico de pizza que mostra o número de unidades em cada estado de funcionamento (normal ou em risco).

Histórico de unidades em risco

Este cartão de relatório contém um gráfico de barras que mostra o número de unidades com falha durante a última semana ou o ano passado. Passe o cursor sobre cada barra no gráfico para exibir uma lista filtrada de unidades com falha, por dispositivo, nesse dia.

Unidades com falha preditiva

O boletim contém uma tabela que lista os dispositivos com unidades com falha. Você pode clicar em um dispositivo para listar os detalhes de cada unidade em risco nesse dispositivo.

Analisando o firmware

O painel Análise contém placas de relatório que mostram análises sobre firmware.

Para exibir os relatórios de firmware, clique em **Análise ( ) → Análises predefinidas** e clique em **Análise de firmware** para exibir os cartões de análise relacionados.

Análise de firmware

Esse cartão de relatório inclui um gráfico de barras que mostra o número de firmware instalado nos dispositivos gerenciados com base na categoria e idade do firmware.

O firmware é agrupado nas categorias a seguir.
- Controlador de gerenciamento
- Ferramentas do sistema
- UEFI

As idades do firmware são agrupadas nos seguintes intervalos
- **Menos de 6 meses**
- **6 – 12 meses**
- **1 – 2 anos**
- **Mais de 2 anos**

É possível filtrar os dispositivos que são incluídos no relatório usando os campos de entrada **Filtros**. Também é possível salvar as consultas filtradas que você deseja usar regularmente.

É possível mostrar ou ocultar o cartão Dispositivos clicando no botão de alternância **Mostrar/Ocultar Dispositivos**. O cartão Dispositivos lista os tipos de firmware e as idades de todos os dispositivos incluídos no gráfico.

Analisando eventos perdidos

O painel Análise contém placas de relatório que mostram estatísticas sobre eventos perdidos. Os eventos perdidos são determinados por uma lacuna nos números da sequência

Os eventos têm um número de sequência que indica a ordem na qual cada evento ocorreu em um dispositivo específico. Os números de sequência de eventos devem ser consecutivos para um dispositivo específico. Se houver números de sequência que não sejam consecutivos, a lacuna poderá indicar que um ou mais eventos foram perdidos.

Para exibir os relatórios de eventos perdidos, clique em **Análise** () → **Análises predefinidas** e clique em **Eventos Perdidos** para exibir os cartões de análise relacionados.

Eventos perdidos por tempo

Esse cartão de relatório inclui um gráfico de barras que mostra o número de eventos perdidos durante o dia ou o mês atual de cada recurso.

É possível optar por exibir dados de um intervalo específico selecionando o ícone **Configurações** () no canto superior direito do cartão.

10 principais dispositivos por número de eventos perdidos

Esse cartão de relatório inclui um gráfico de barras que mostra os 10 principais dispositivos que estão relatando a maioria dos eventos perdidos gerais.

Analisando e prevendo a capacidade do gerenciador de recursos

O painel Análise contém boletins que preveem quando os gerenciadores de recursos excederão o número máximo de dispositivos gerenciados. Para gerenciadores de recursos do Lenovo XClarity Administrator, há suporte para até 1.000 dispositivos gerenciados.

Para exibir os relatórios de capacidade do gerenciador de recursos, clique em **Análises Avançadas** () → **Análises predefinidas** e clique em **Previsão de Capacidade do Gerenciador** para exibir os cartões de análise relacionados.

Capacidade do gerenciador

Este relatório lista a capacidade do dispositivo para cada gerenciador de recursos, incluindo o número de dispositivos gerenciados e o status de capacidade, que indica se a capacidade está sobrecarregada. Os seguintes estados de capacidade são usados.

- () **Normal**. O número de dispositivos gerenciados menor que o número máximo de dispositivos suportados.
- () **Aviso.** O número de dispositivos gerenciados próximo do número máximo de dispositivos suportados.
- () **Crítico.** O número de dispositivos gerenciados maior que o número máximo de dispositivos suportados.

Gerenciar tendência de capacidade

Esse cartão de relatório inclui um gráfico de linhas que mostra o número de dispositivos que foram gerenciados, ao longo do tempo, para um gerenciador de recursos específico e a tendência prevista quando o número de dispositivos gerenciados alcançar a capacidade máxima suportada para esse gerenciador de recursos.

Clique em uma linha na tabela Capacidade do gerenciador para exibir tendências de capacidade para esse gerenciador de recursos.

É possível alterar o período de tempo exibido clicando no menu suspenso. É possível optar por exibir dados por ano, trimestre, mês ou dia. Também é possível alterar o número de períodos mostrados no gráfico usando a caixa Zoom no gráfico.

Analisando e prevendo tendências de utilização

O painel Análise contém boletins que mostra o uso histórico e previsto do processador, do armazenamento e da memória em dispositivos e recursos virtuais (como hosts, clusters e máquinas virtuais).

Importante: Essa função requer uma conexão com o gerenciador de recursos VMware vRealize Operations Manager (consulte Conectando gerenciadores de recursos).

Para exibir os relatórios de tendência de utilização, clique em **Análises avançadas ( ) → Análises predefinidas** e, em seguida, clique em **Tendência de utilização da carga de trabalho** para exibir os cartões de análise relacionados.

Seleção de recurso

Este relatório lista os dispositivos e recursos virtuais que são gerenciados pelo servidor do orquestrador.

Clique em uma linha na tabela para exibir tendências de utilização para esse recurso.

Tendência de utilização da CPU

Esse cartão de relatório inclui um gráfico de linhas que mostra o uso do processador, ao longo do tempo, para um recurso virtual, e a tendência prevista quando o uso do processador alcançar a capacidade máxima compatível com esse recurso virtual.

É possível alterar o período que é exibido para dados históricos e previstos nos menus suspenso **Histórico** e **Projeção**, respectivamente. Também é possível alterar o número de períodos mostrados no gráfico usando a caixa Zoom no gráfico.

Tendência de utilização da memória

Esse cartão de relatório inclui um gráfico de linhas que mostra o uso da memória, ao longo do tempo, para um recurso virtual, e a tendência prevista quando o uso da memória alcançar a capacidade máxima compatível com esse recurso virtual.

É possível alterar o período que é exibido para dados históricos e previstos nos menus suspenso **Histórico** e **Projeção**, respectivamente. Também é possível alterar o número de períodos mostrados no gráfico usando a caixa Zoom no gráfico.

Tendência de utilização do armazenamento

Esse cartão de relatório inclui um gráfico de linhas que mostra o uso do armazenamento, ao longo do tempo, para um recurso virtual, e a tendência prevista quando o uso do armazenamento alcançar a capacidade máxima compatível com esse recurso virtual.

É possível alterar o período que é exibido para dados históricos e previstos nos menus suspenso **Histórico** e **Projeção**, respectivamente. Também é possível alterar o número de períodos mostrados no gráfico usando a caixa Zoom no gráfico.

Analisando métricas de desempenho e uso

O painel Analítico contém cartões de relatório que mostram mapas de calor com base em métricas e recursos específicos nas últimas 24 horas.

Para exibir o heatmap de desempenho, clique em **Análises Avançadas ( ) → Análises predefinidas**e clique em **Heatmap de desempenho** para exibir os cartões de análise relacionados.

Heatmap de desempenho

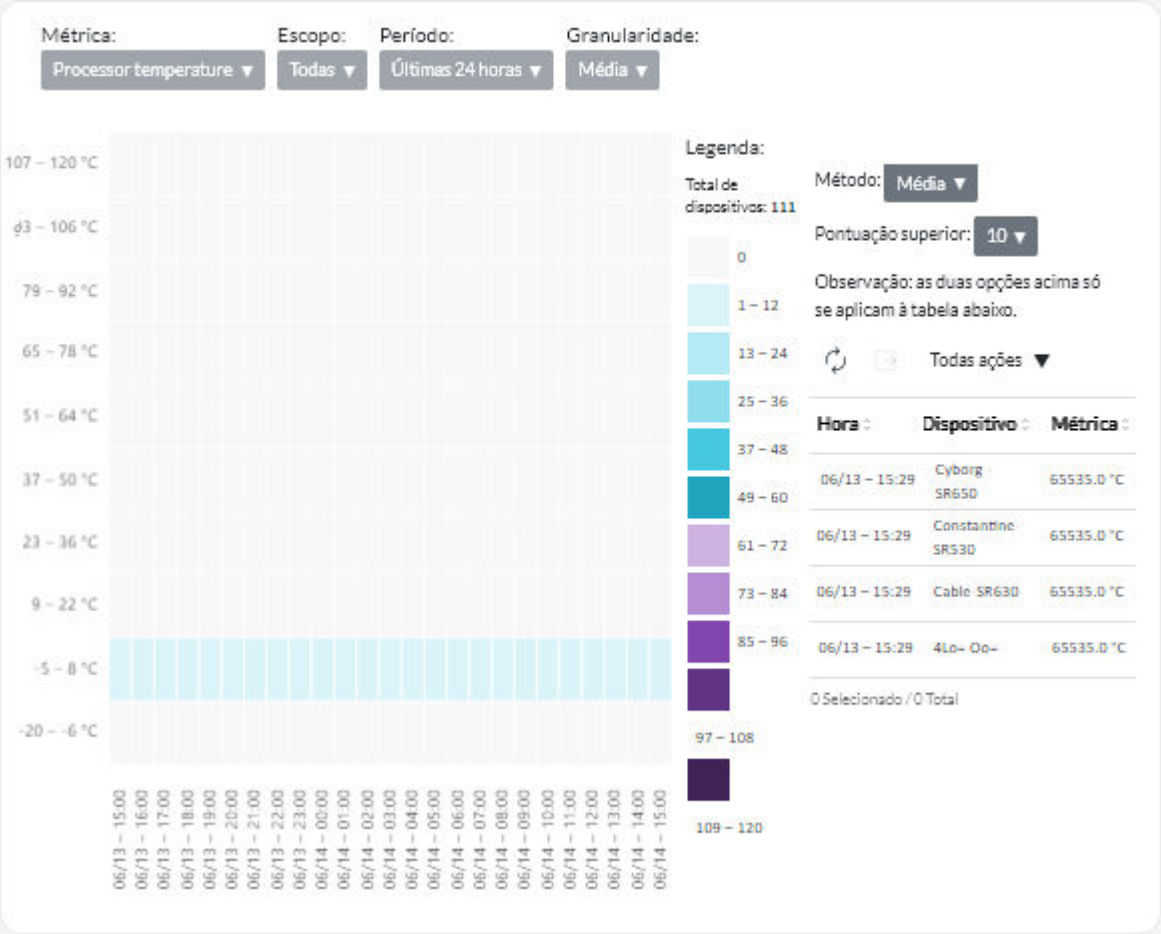
Este cartão de relatório inclui um mapa de calor que ilustra o número de dispositivos que têm valores métricos dentro de um número específico de intervalos por um determinado período.

É possível clicar em qualquer célula no mapa de calor para exibir uma lista pop-up de dispositivos representados por essa célula, com informações do valor de métrica real para cada dispositivo e carimbo de data/hora de quando a métrica foi coletada.

É possível configurar o mapa de calor para mostrar apenas as informações em que você está interessado.

- Você pode optar por mostrar dados para uma das métricas a seguir.
  - Temperatura do processador
  - Utilização do processador
  - Utilização da memória
- Você pode optar por agregar os dados métricos com base no valor médio ou máximo (mais alto).
- É possível filtrar o mapa de calor para incluir somente dados métricos para dispositivos em um grupo de dispositivos específico.

  Nota: Se você fizer o escopo da interface do usuário para um gerenciador de recursos específico, somente os dados dos dispositivos nos grupos selecionados que também são gerenciados pelo gerenciador de recursos serão incluídos no mapa de calor.
- Também é possível escolher o intervalo de valores de número a ser exibido no eixo x do mapa de calor. O número de valores entre o máximo e o mínimo é dividido em partes iguais com base no número escolhido. É possível escolher 10, 15 ou 20.
- Também é possível listar os 10, 15 ou 20 dispositivos principais com os valores mais altos e o carimbo de data/hora de quando a métrica foi coletada.



Analisando eventos repetidos

O painel Analítico contém cartões de relatório que resumem os eventos repetidos para cada dispositivo.

Eventos repetidos são gerados quando ocorrem as seguintes condições:

- **FQXXOIS0002J**. Um evento crítico ou de aviso com a mesma ID foi gerado uma ou mais vezes para o mesmo dispositivo em pelo menos três períodos consecutivos de 5 minutos.
- **FQXXOIS0003J**. Mais de cinco eventos críticos ou de aviso foram gerados para o mesmo dispositivo a cada hora por duas ou mais horas consecutivas.

Para exibir os relatórios de eventos repetidos, clique em **Análises Avançadas** ( ) → **Análises predefinidas** e clique em **Eventos Repetidos** para exibir os cartões de análise relacionados.

Eventos Repetidos

Esse cartão de relatório inclui um gráfico de barras que mostra o número de eventos repetidos geral para cada dispositivo.

Eventos repetidos por tempo

Esse cartão de relatório inclui um gráfico de barras que mostra o número de eventos repetidos gerados no dia atual, para cada dispositivo.

Analisando tentativas de acesso não autorizado

O painel Análise contém placas de relatório que resumem as tentativas de acesso não autorizado (login com falha).

Para exibir os relatórios de acesso não autorizado, clique em **Análise ( ) → Análises predefinidas** e clique em **Tentativas de acesso não autorizado** para exibir os cartões de análise de acesso não autorizado.

Número de tentativas de login com falha por usuário

Esse cartão de relatório inclui um gráfico que mostra o número de tentativas de acesso não autorizado geral para cada usuário (por nome de usuário). É possível exibir dados como um gráfico de barras ( ) ou gráfico de pizza ( ) clicando no ícone apropriado no canto superior esquerdo do cartão.

É possível passar o mouse sobre cada barra ou parte no gráfico para obter mais informações, como a última ocorrência.

Número de tentativas de login com falha por usuário, em cada período

Esse cartão de relatório inclui um gráfico de barras que mostra o número de tentativas de acesso não autorizado que ocorreram no dia atual para cada usuário (por nome de usuário).

Número de tentativas de login com falha por endereço IP do usuário

Esse cartão de relatório inclui um gráfico de barras que mostra o número total de todas as tentativas de acesso não autorizado geral para cada usuário (por endereço IP). É possível exibir dados como um gráfico de barras ( ) ou gráfico de pizza ( ) clicando no ícone apropriado no canto superior esquerdo do cartão.

É possível passar o mouse sobre cada barra ou parte no gráfico para obter mais informações, como a última ocorrência.

Número de tentativas de login com falha por endereço IP do usuário, em cada período

Esse cartão de relatório inclui um gráfico de barras que mostra o número de tentativas de acesso não autorizado que ocorreram no dia atual para cada usuário (por endereço IP).

Analisando o funcionamento do dispositivo

A placa Estados de Integridade Geral no painel e a placa Análise do Dispositivo em cada página de dispositivos resumem a integridade geral dos dispositivos gerenciados.

Resumo de status de todos os dispositivos

Na barra de menus do XClarity Orchestrator, clique em **Painel ( )** para exibir as placas de painel com uma visão geral e o status de todos os dispositivos gerenciados e outros recursos (consulte Exibindo um resumo do ambiente).

É possível alterar o escopo do resumo somente para os dispositivos gerenciados por um gerenciador de recursos específico ou em um grupo de recursos específico usando o menu suspenso **Selecionar gerenciador**.

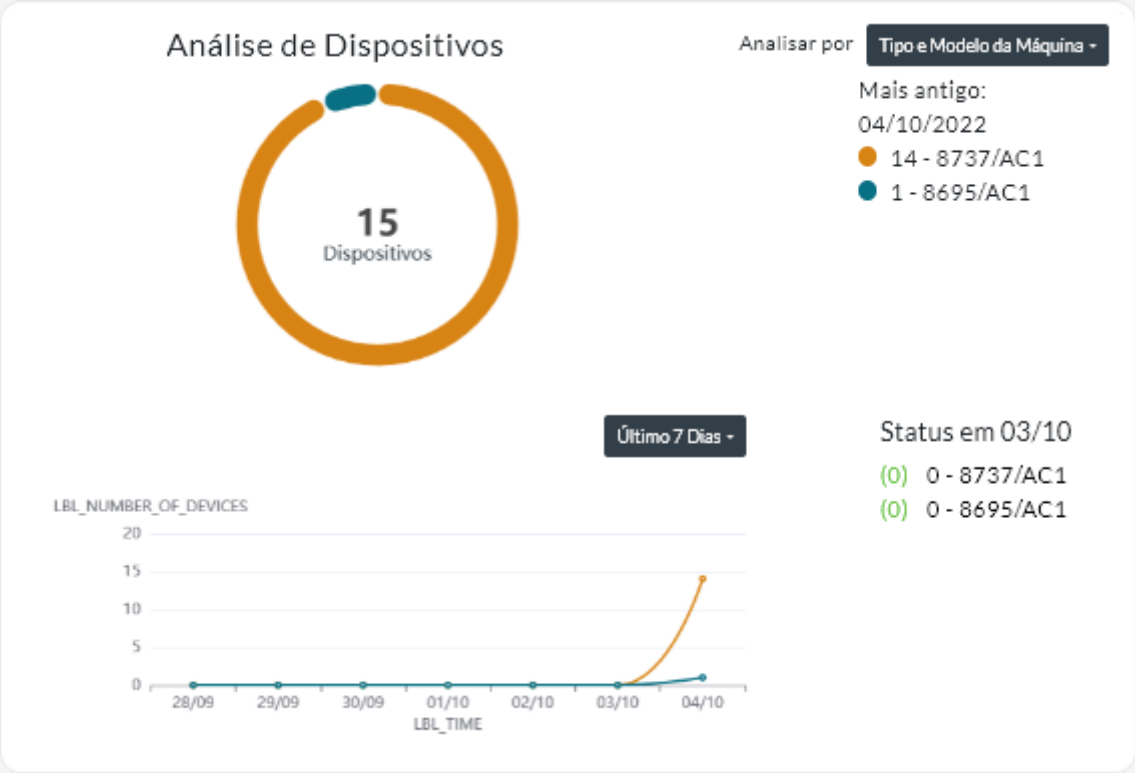
Cada barra colorida nos gráficos circulares e de barras indica o número de dispositivos em um estado específico. É possível passar o mouse sobre cada barra colorida para obter mais informações sobre o estado. Também é possível clicar no número de dispositivos em cada estado para exibir uma lista de todos os dispositivos que correspondem ao critério.

Resumo do status de todos os dispositivos de um tipo específico

Para exibir os resumos de alertas ativos, clique em **Recursos** () na barra de menus do XClarity Orchestrator e, em seguida, clique no tipo de dispositivo para exibir uma placa com uma exibição tabular de todos os dispositivos do tipo em questão. Por exemplo, se você selecionar **Servidores**, uma lista de todos os servidores em rack, em torre e densos e todos os servidores Flex System e ThinkSystem em um chassi será exibida.

É possível alterar o escopo do resumo com base na propriedade do dispositivo na lista suspensa **Analisar por**.

- **Tipo e Modelo da Máquina**. (padrão) Esse relatório resume a integridade do dispositivo por modelo e tipo de máquina (MTM).
- **Tipo de Máquina**. Esse relatório resume a integridade do dispositivo por tipo de máquina.
- **Nome do Produto**. Esse relatório resume a integridade do dispositivo por produto.



O XClarity Orchestrator resume a integridade do dispositivo com base em critérios específicos. Cada resumo inclui as seguintes informações.

- Um gráfico circular que mostra o número total de dispositivos que não estão íntegros e a porcentagem de dispositivos em cada estado não íntegro (crítico, aviso e desconhecido).

  Cada barra colorida nos gráficos circulares indica o número de dispositivos em um estado específico. É possível passar o mouse sobre cada barra colorida para obter mais informações sobre o estado.
- Um gráfico de linhas que mostra o número de dispositivos em cada estado de integridade por dia ao longo do número especificado de dias.

  Cada barra colorida no gráfico de linhas indica o número de dispositivos em um estado específico. É possível passar o mouse sobre cada barra colorida para obter mais informações sobre o estado.
- O número de dispositivos de cada tipo que não estão íntegros em um dia específico. O dia atual é mostrado por padrão. É possível alterar o dia passando o mouse sobre cada dia no gráfico de linhas.

Analisando o funcionamento dos recursos de infraestrutura

É possível determinar as tendências gerais de funcionamento e sensor de recursos de infraestrutura.

Status de funcionamento dos recursos de infraestrutura

Na barra de menus do Lenovo XClarity Orchestrator, clique em **Recursos (⚙) → Infraestrutura** para exibir a placa de infraestrutura. É possível determinar o status de funcionamento de cada recurso na coluna **Status**.

Tendências do sensor

Na barra de menus XClarity Orchestrator, clique em **Recursos (⚙) → Infraestrutura** para exibir a placa de infraestrutura e, em seguida, clique em um recurso de infraestrutura na tabela para exibir uma lista de sensores para esse recurso e a medida mais recente de cada um.

Selecione um ou mais sensores e, em seguida, clique no ícone **Gráfico** ( ) para exibir os gráficos de linha que mostram as medidas, com o tempo para cada sensor selecionado. Por padrão, os sensores com a mesma unidade (como watts ou amps) são representados no mesmo gráfico.

Nota: Schneider Electric EcoStruxure IT Expert coleta dados do sensor a cada 5 minutos e XClarity Orchestrator sincroniza esses dados a cada hora. Atualmente, o XClarity Orchestrator salva apenas os últimos 60 minutos de dados.

Analisando alertas ativos

A placa de Análise de Alertas resume os alertas ativos.

O Lenovo XClarity Orchestrator resume alertas ativos com base em critérios específicos. Cada resumo inclui as seguintes informações.

- Um gráfico circular que mostra o número total de alertas ativos e a porcentagem de alertas associados a cada tipo de resumo
- O número de alertas ativos para cada tipo de resumo
- Duração do alerta ativo mais antigo
- Um gráfico de linhas que mostra o número de alertas ativos para cada tipo de resumo por dia ao longo do número especificado de dias
- O número de alertas ativos para cada tipo de resumo em um dia específico. O dia atual é mostrado por padrão. É possível alterar o dia passando o mouse sobre cada dia no gráfico de linhas.

Alertas ativos gerais

Para visualizar os resumos gerais do alerta ativo, conclua as etapas a seguir.

1. Na barra de menus do XClarity Orchestrator, clique em **Monitoramento ( ) → Alertas** para exibir a placa Análises de Alertas.
2. Selecione o período na lista suspensa acima do gráfico de linhas. O padrão é os últimos sete dias.
3. Selecione o tipo de resumo na lista suspensa **Analisar por**.
   - **Gravidade**. (padrão) Esse relatório resume os alertas ativos por gravidade: crítico, aviso e informativo.
   - **Tipo de origem** Esse relatório resume os alertas ativos que foram gerados por cada tipo de origem, como dispositivo, gerenciamento e análise.
   - **Tipo de recurso**. Esse relatório resume os alertas ativos para cada tipo de recurso, como dispositivos, gerenciadores de recursos e XClarity Orchestrator.
   - **Capacidade de Manutenção**. Esse relatório resume os alertas ativos associados a cada tipo de capacidade de manutenção: **nenhum** (serviço não necessário), **usuário** (serviço é executado pelo usuário), **permite manutenção** (o serviço é executado pela Lenovo).

Alertas ativos de um dispositivo específico

Para exibir o alerta ativo de um dispositivo específico, conclua as etapas a seguir.

1. Na barra de menus do XClarity Orchestrator, clique em **Recursos ( )** e, em seguida, clique no tipo de dispositivo para exibir uma placa com uma exibição tabular de todos os dispositivos gerenciados do tipo em questão.
2. Clique na linha do dispositivo para exibir as placas de resumo desse dispositivo.
3. Clique em **Log de Alertas** para exibir a lista de alertas ativos do dispositivo e a placa de Análise de Alertas.

4. Na placa de Análises de Alertas, selecione o período na lista suspensa acima do gráfico de linhas. O padrão é os últimos sete dias.
5. Selecione o tipo de resumo na lista suspensa **Analisar por**.
   - **Tipo de origem** Esse relatório resume os alertas ativos que foram gerados por cada tipo de origem, como dispositivo, gerenciamento e análise.
   - **Tipo de Capacidade de Manutenção**. Esse relatório resume os alertas ativos associados a cada tipo de capacidade de manutenção: nenhum (serviço não necessário), usuário (serviço é executado pelo usuário), permite manutenção (o serviço é executado pela Lenovo).
   - **Gravidade**. Esse relatório resume os alertas ativos por gravidade: crítico, aviso e informativo.

Capítulo 7. Trabalhando com serviço e suporte

O Lenovo XClarity Orchestrator fornece um conjunto de ferramentas que você pode usar para coletar e enviar arquivos de serviço para o Suporte Lenovo, configurar a notificação automática para provedores de serviço quando ocorrerem certos eventos que permitem manutenção em dispositivos específicos, exibir o status do tíquete de serviço e informações de garantia. É possível entrar em contato com Suporte Lenovo para obter ajuda e assistência técnica quando você tiver problemas.

Enviando dados periódicos à Lenovo

Como opção, é possível permitir que o Lenovo XClarity Orchestrator colete informações sobre o seu ambiente de hardware e envie os dados para a Lenovo periodicamente. A Lenovo usa esses dados para melhorar sua experiência com os produtos Lenovo e com o Suporte Lenovo.

Antes de iniciar

Você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** é atribuída.

Atenção: Você deve aceitar o Instrução de privacidade da Lenovo para poder transferir dados para o Suporte Lenovo.

Sobre esta tarefa

Analisando dados de hardware de vários usuários, a Lenovo pode aprender sobre alterações de hardware que ocorrem regularmente. Esses dados podem ser usados para melhorar a análise de previsão e aprimorar sua experiência de serviço e suporte, estocando peças nas regiões corretas.

Quando você concorda em enviar dados de hardware para a Lenovo, os dados a seguir são coletados e enviados periodicamente.

- **Dados de hardware diários**. Somente alterações em dados de inventário e dados de análise de unidade (se a coleta de dados estiver habilitada) para cada dispositivo gerenciado
- **Dados de hardware semanais**. Todos os dados do inventário para dispositivos gerenciados e informações sobre gerenciadores de recursos conectados

Atenção: Esses dados *não são anônimos*.

- Os dados coletados *incluem* UUIDs, WWNs, IDs de dispositivo e números de série. O XClarity Orchestrator modifica o inventário efetuando hash dos UUIDs, WWNs e IDs de dispositivo usando SHA512.
- Os dados coletados *não incluem* informações de rede (endereços IP, nomes de domínio ou nomes de host) nem informações do usuário.

Quando os dados são enviados para a Lenovo, eles são transmitidos da instância do XClarity Orchestrator para o Recurso de Upload da Lenovo usando HTTPS. As APIs REST são chamadas sobre essa conexão HTTPS para enviar os dados. Um certificado pré-carregado no XClarity Orchestrator é usado para autenticação. Se uma instância do XClarity Orchestrator não tiver acesso direto à Internet e houver um proxy configurado no XClarity Orchestrator, os dados serão transmitidos por esse proxy.

Em seguida, os dados são movidos para o repositório Lenovo Customer Care, onde são armazenados por até 5 anos. Esse repositório é um local seguro que também é usado quando os dados de depuração são

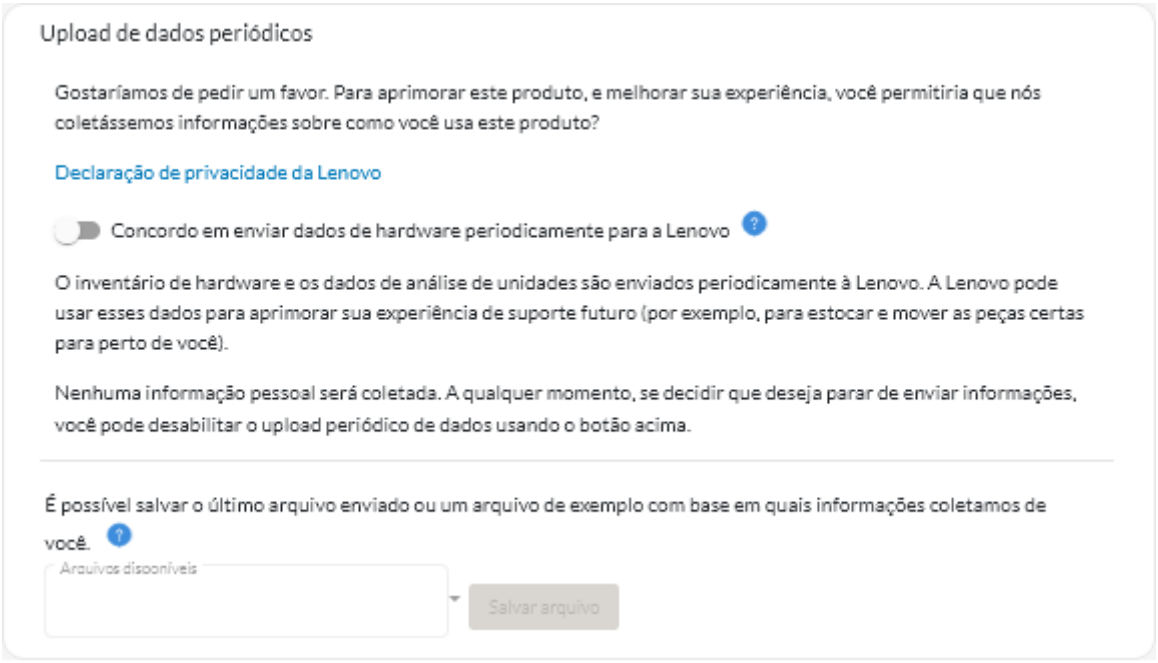
enviados para a Lenovo para solucionar problemas. Ele é usado pela maioria dos produtos de servidor, armazenamento e comutador da Lenovo.

No repositório Lenovo Customer Care, as consultas são executadas nos dados fornecidos e os gráficos são disponibilizados para a equipe de produtos Lenovo para análise.

Procedimento

Para permitir que o XClarity Orchestrator colete e envie os dados do cliente para a Lenovo, conclua as etapas a seguir.

Etapa 1. Na barra de menu do XClarity Orchestrator, clique em **Administração** (⚙) → **Serviço e Suporte** e clique em **Upload de Dados Periódico** na navegação esquerda para exibir o cartão Upload de Dados Periódico.



Etapa 2. Como opção, concorde em enviar dados de hardware para a Lenovo.

Etapa 3. Aceite o Instrução de privacidade da Lenovo.

Depois de concluir

É possível executar as seguintes ações nesta página se você concordou em enviar dados.

- É possível salvar os últimos arquivos de dados diários e semanais enviados para a Lenovo no sistema local selecionando o arquivo que você deseja baixar e clicando em **Salvar arquivo**.

Coletando dados de serviço do XClarity Orchestrator

É possível coletar dados de serviço do Lenovo XClarity Orchestrator e, em seguida, salvar as informações como um arquivo no formato tar. gz no sistema local. Em seguida, é possível enviar os arquivos serviço ao seu provedor de serviço preferencial para obter assistência na solução de problemas à medida que ocorrem.

Antes de iniciar

Saiba mais: Como coletar dados de serviço

Você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** é atribuída.

Certifique-se de que o navegador da Web não bloqueie pop-ups para o site XClarity Orchestrator ao baixar dados de serviço

Procedimento

Para coletar dados de serviço do XClarity Orchestrator, complete as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Administração** ( ) → **Serviço e Suporte** e, em seguida, clique em **Dados de Serviço** na navegação esquerda para exibir a placa Dados de Serviço de Gerenciamento.

Etapa 2. Clique em **Salvar como** para coletar dados de serviço e salvar o arquivo no sistema local.

Um trabalho é criado para coletar dados de serviço. 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 .)

Depois de concluir

Também é possível executar estas ações relacionadas.

- Abra manualmente um tíquete de serviço para um dispositivo específico da placa Tíquetes de Serviço na página Serviço específica do dispositivo clicando no ícone **Abrir tíquete de serviço** ( ) (consulte Abrindo manualmente um tíquete de serviço no centro de suporte da Lenovo).
- Anexe um arquivo de dados de serviço a um tíquete de serviço ativo selecionado na placa Tíquetes de Serviço na página Serviço específico do dispositivo clicando no ícone **Anexar arquivo de serviço** ( ). É possível anexar um arquivo do XClarity Orchestrator ou do sistema local.

  Notas:

  – É possível anexar um único arquivo que não seja superior a 2 GB. O nome do arquivo não pode ter mais de 200 caracteres. Para obter informações sobre como criar arquivos de dados de serviço, (consulte Coletando dados de serviço para dispositivos).
  – O tíquete de serviço deve estar no estado aberto, em andamento ou em espera. Não é possível anexar um arquivo a um tíquete de serviço que esteja no estado fechado ou outro.
  – Não é possível anexar um arquivo a um tíquete de serviço de *software* que foi aberto para o gerenciador de recursos.
- Salve um ou mais arquivos de dados de serviço selecionados no sistema local na placa Dados de Serviço de Gerenciamento clicando no ícone **Salvar** ( ). Se vários arquivos forem selecionados, arquivos serão compactados em um único arquivo .tar.gz antes do download.
- Exclua um ou mais arquivos de dados de serviços selecionados que não são mais necessários no cartão Dados de Serviço de Gerenciamento clicando no ícone **Excluir** ( ) ou exclua todos os arquivos clicando no ícone **Excluir Tudo** ( ).

Coletando dados de serviço para dispositivos

Quando há um problema em um dispositivo que requeira a assistência de um provedor de serviço, como o suporte da Lenovo, para ser resolvido, é possível coletar manualmente dados de serviço (incluindo logs, informações de serviço e inventário) para esse dispositivo como um arquivo no formato tar.gz para ajudar a identificar a causa do problema. É possível salvar o arquivo morto no sistema local e, em seguida, enviar o arquivo para o provedor de serviço preferencial.

Antes de iniciar

Você deve aceitar o Instrução de privacidade da Lenovo para coletar dados de serviço. É possível aceitar a declaração de privacidade clicando em **Administração (⚙) → Serviço e Suporte** e clicando em **Configuração de Call Home** na navegação esquerda e, em seguida, selecionando **Concordo com a Declaração de Privacidade da Lenovo**.

Para obter informações sobre como salvar dados do XClarity Orchestratorde serviço para o sistema local, consulte "Coletando dados de serviço do XClarity Orchestrator" na página 202.

Para obter informações sobre como abrir manualmente um tíquete de serviço e enviar dados de serviço para o Centro de Suporte Lenovo, consulte "Abrindo manualmente um tíquete de serviço no centro de suporte da Lenovo" na página 212.

Para obter informações sobre como configurar o Call Home para abrir automaticamente um tíquete de serviço no centro de suporte da Lenovo e enviar o arquivo de dados de serviço quando ocorrer um evento que permite manutenção em um dispositivo, consulte "Abrindo automaticamente tíquetes de serviço usando Call Home" na página 208.

Sobre esta tarefa

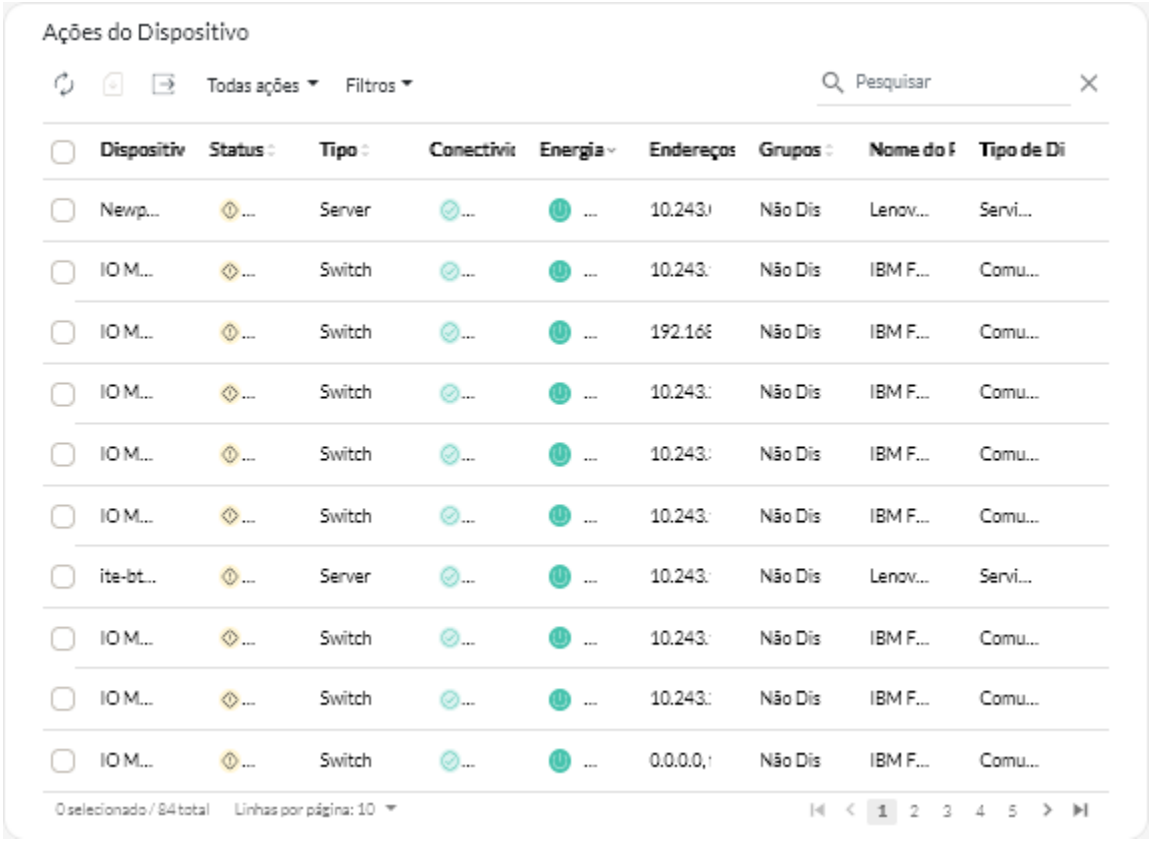
Quando você coleta dados de serviço por meio do Lenovo XClarity Orchestrator, o servidor do orquestrador envia a solicitação ao gerenciador de recursos (como o Lenovo XClarity Administrator). O gerenciador de recursos coleta e salva os dados como um arquivo morto em seu repositório local e transfere o arquivo morto ao XClarity Orchestrator.

É possível coletar dados de serviço para no máximo **50** dispositivos ao mesmo tempo.

Procedimento

Para coletar dados de serviço de um dispositivo específico, conclua as etapas a seguir.

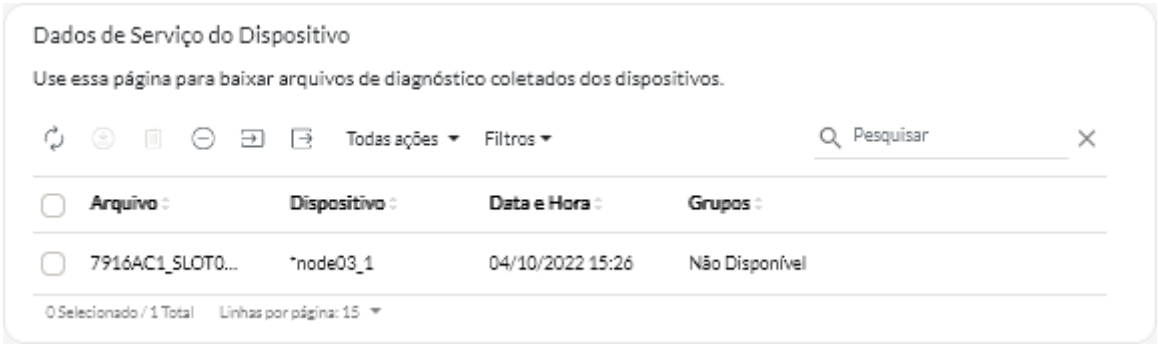
Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Administração (⚙) → Serviço e Suporte** e, em seguida, clique em **Ações do Dispositivo** na navegação esquerda para exibir a placa Ações do Dispositivo.



Etapa 2. Selecione o dispositivo para o qual você deseja coletar dados de serviço e clique no ícone **Coletar dados de serviço** ( )

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 .)

Etapa 3. Clique em **Dados de Serviço do Dispositivo** na navegação esquerda para exibir o cartão Dados de Serviço. O arquivo de dados de serviço é listado na tabela.



Etapa 4. Opcionalmente, salve o arquivo de serviço no sistema local. Para isso, selecione o arquivo clicando no ícone **Salvar** ( ).

Depois de concluir

Também é possível executar estas ações relacionadas.

- Abra manualmente um tíquete de serviço para um dispositivo específico da placa Tíquetes de Serviço na página Serviço específica do dispositivo clicando no ícone **Abrir tíquete de serviço** () (consulte Abrindo manualmente um tíquete de serviço no centro de suporte da Lenovo).
- Anexe um arquivo de dados de serviço a um tíquete de serviço ativo selecionado na placa Tíquetes de Serviço na página Serviço específico do dispositivo clicando no ícone **Anexar arquivo de serviço** (). É possível anexar um arquivo do XClarity Orchestrator ou do sistema local.

  Notas:

  – É possível anexar um único arquivo que não seja superior a 2 GB. O nome do arquivo não pode ter mais de 200 caracteres. Para obter informações sobre como criar arquivos de dados de serviço, (consulte Coletando dados de serviço para dispositivos).

  – O tíquete de serviço deve estar no estado aberto, em andamento ou em espera. Não é possível anexar um arquivo a um tíquete de serviço que esteja no estado fechado ou outro.

  – Não é possível anexar um arquivo a um tíquete de serviço de *software* que foi aberto para o gerenciador de recursos.
- Salve um ou mais arquivos de dados de serviço selecionados no sistema local na placa Dados de Serviço clicando no ícone **Salvar** (). Se vários arquivos forem selecionados, os arquivos serão salvos como um único arquivo .tar. gz.

  Nota: É possível salvar no máximo **50** arquivos de dados de serviço no sistema local ao mesmo tempo.
- Exclua um ou mais arquivos de dados de serviço selecionados que não são mais necessários da placa Dados de Serviço clicando no ícone **Excluir** () ou exclua todos os arquivos clicando no ícone **Excluir Tudo** ().

  Nota: Você deve ser um membro do grupo **SupervisorGroup** para excluir todos os arquivos.

Importando dados de serviço para dispositivos

É possível importar um arquivo de dados de serviço para um dispositivo específico. O arquivo pode ser recuperado de um gerenciador de recursos do Lenovo XClarity Administrator ou diretamente do Baseboard Management Controller.

Sobre esta tarefa

É possível importar até 10 arquivos por vez com total combinado de 2 GB ou menos.

Se você importar dados de serviço para o dispositivo de salvamento várias vezes, os dados do inventário serão substituídos pelos dados de serviço que foram importados por último.

Procedimento

Para importar um arquivo de dados de serviço, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Administração () → Serviço e Suporte** e, em seguida, clique em **Dados de Serviço** na navegação esquerda para exibir o cartão Dados de Serviço do Dispositivo.

Etapa 2. Clique no ícone **Importar** () para importar os arquivos de dados de serviço.

Etapa 3. Arraste e solte um ou mais arquivos de dados de serviço (no formato .tar.gz, .tzz ou .tgz) na caixa de diálogo Importar ou clique em **Procurar** para localizar o arquivo.

Etapa 4. Selecione **Adicionar o servidor nos dados de serviço ao inventário somente para revisão** se o arquivo for para um dispositivo que não seja gerenciado atualmente pelo XClarity Orchestrator

Etapa 5. Clique em **Importar** para importar e analisar o arquivo e, opcionalmente, gerenciar o dispositivo offline.

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 .)

Criando e atribuindo contatos para serviço e suporte

Quando os recursos necessitam de assistência do Suporte Lenovo, a Lenovo precisa saber com quem entrar em contato. É possível definir informações de contato em um local e, em seguida, atribuir esses contatos como os contatos primários e secundários padrão para recursos específicos.

Antes de iniciar

Certifique-se de aceitar a Instrução de privacidade da Lenovo. É possível ler e aceitar a declaração de privacidade na página **Administração → Serviço e Suporte → Configuração de Call Home**.

Sobre esta tarefa

É possível atribuir contatos primários e secundários a grupos de e recursos. Quando você atribui contatos a um grupo de recursos, os contatos são atribuídos a todos os recursos desse grupo.

A atribuição de contatos primários e secundários é opcional; entretanto, se você deseja atribuir um contato secundário, também deverá atribuir um contato primário.

Se um dispositivo for membro de vários grupos, é possível que a cada grupo seja atribuído um contato primário diferente. É possível optar por usar a atribuição de contato primário para o primeiro ou o último grupo ao qual o dispositivo foi designado (consulte Abrindo manualmente um tíquete de serviço no centro de suporte da Lenovo).

Se um dispositivo não for membro de um grupo com um contato primário atribuído, o contato de Call Home será atribuído por padrão. O contato de Call Home é usado quando os tíquetes de serviço são abertos automaticamente usando Call Home (consulte Abrindo automaticamente tíquetes de serviço usando Call Home). Contatos atribuídos a recursos e grupos têm precedência sobre o contato padrão de Call Home.

Ao abrir manualmente um tíquete de serviço, é possível optar por usar os contatos atribuídos ao recurso do problema ou escolher outro contato (consulte Abrindo manualmente um tíquete de serviço no centro de suporte da Lenovo).

Procedimento

- **Definir um contato**
  1. Na barra de menus do Lenovo XClarity Orchestrator, clique em **Administração** (⚙) → **Serviço e Suporte** e, em seguida, clique em **Informações de Contato** na navegação esquerda para exibir o cartão Informações de Contato.
  2. Clique no ícone **Criar** (⊕) para exibir a caixa de diálogo Adicionar Contato.
  3. Preencha o nome de contato, o e-mail, o número de telefone e o local.
  4. Selecione o método preferencial de contato.
  5. Clique em **Salvar** para criar o contato.
- **Atribuir contatos a grupos de recursos**

1. Na barra de menus do Lenovo XClarity Orchestrator, clique em **Recursos ( ) → Grupos** para exibir a placa Grupos.
2. Selecione o grupo e clique no ícone **Editar** ( ) para a caixa de diálogo Editar grupo.
3. Selecione o grupo de recursos.
4. Clique na guia **Informações de Contato**.
5. Selecione o contato de suporte primário e um ou mais contatos de suporte secundário para atribuir a todos os dispositivos do grupo.
6. Clique em **Salvar**.

Depois de concluir

É possível executar as ações a seguir a partir do cartão Informações de Contato.

- Modifique um contato selecionado clicando no ícone **Editar** ( ).
- Exclua um contato selecionado clicando em **Remover** ( ).

Abrindo automaticamente tíquetes de serviço usando Call Home

É possível definir o Lenovo XClarity Orchestrator para abrir automaticamente um tíquete de serviço e enviar dados de serviço coletados ao suporte da Lenovo usando a função de Call Home quando um dispositivo gera determinados eventos que permitem manutenção, como um erro de memória irrecuperável, para que o problema possa ser resolvido.

Antes de iniciar

Você deve ser membro de um grupo de usuários local ao qual a função predefinida de **Supervisor** é atribuída.

Verifique se todas as portas que são necessárias para o XClarity Orchestrator e para a função Call Home estão disponíveis antes de habilitar o Call Home. Para obter informações adicionais sobre portas, consulte Disponibilidade de porta na documentação online do XClarity Orchestrator.

Verifique se existe uma conexão aos endereços da Internet exigidos pelo Call Home. Para obter informações sobre firewalls, consulte Firewalls e servidores proxy na documentação online do XClarity Orchestrator.

Se o XClarity Orchestrator acessa a Internet com um proxy HTTP, verifique se o servidor proxy está configurado para usar autenticação básica e configurado como um proxy não encerrando. Para obter mais informações sobre como configurar o proxy, consulte Definindo configurações de rede na documentação online do XClarity Orchestrator.

Importante: Se Call Home estiver ativado no XClarity Orchestrator e no Lenovo XClarity Administrator, verifique se o Lenovo XClarity Administrator v2.7 ou posterior é usado para evitar tíquetes de serviço duplicados. Se Call Home estiver ativado no XClarity Orchestrator e desativado no Lenovo XClarity Administrator, o Lenovo XClarity Administrator v2.6 ou posterior será compatível.

Quando os contatos estão nos países a seguir, Call Home exige um contrato de Lenovo Premier Support. Para obter mais informações, entre em contato com seu representante Lenovo ou o parceiro de negócios autorizado.
- Catar
- Arábia Saudita
- Emirados Árabes Unidos

Sobre esta tarefa

Se o Call Home estiver configurado e habilitado e ocorre um evento que permite manutenção em um dispositivo específico, o XClarity Orchestrator abre *automaticamente* um tíquete de serviço e transfere dados de serviço para esse dispositivo para o centro de suporte da Lenovo.

Importante: A Lenovo está comprometida com a segurança. Os dados de serviço que você costuma fazer upload manualmente para o suporte da Lenovo são enviados automaticamente para o centro de suporte da Lenovo via HTTPS usando TLS 1.2 ou posterior. Seus dados corporativos nunca são transmitidos. O acesso aos dados de serviço no centro de suporte da Lenovo é restrito ao pessoal de serviço autorizado.

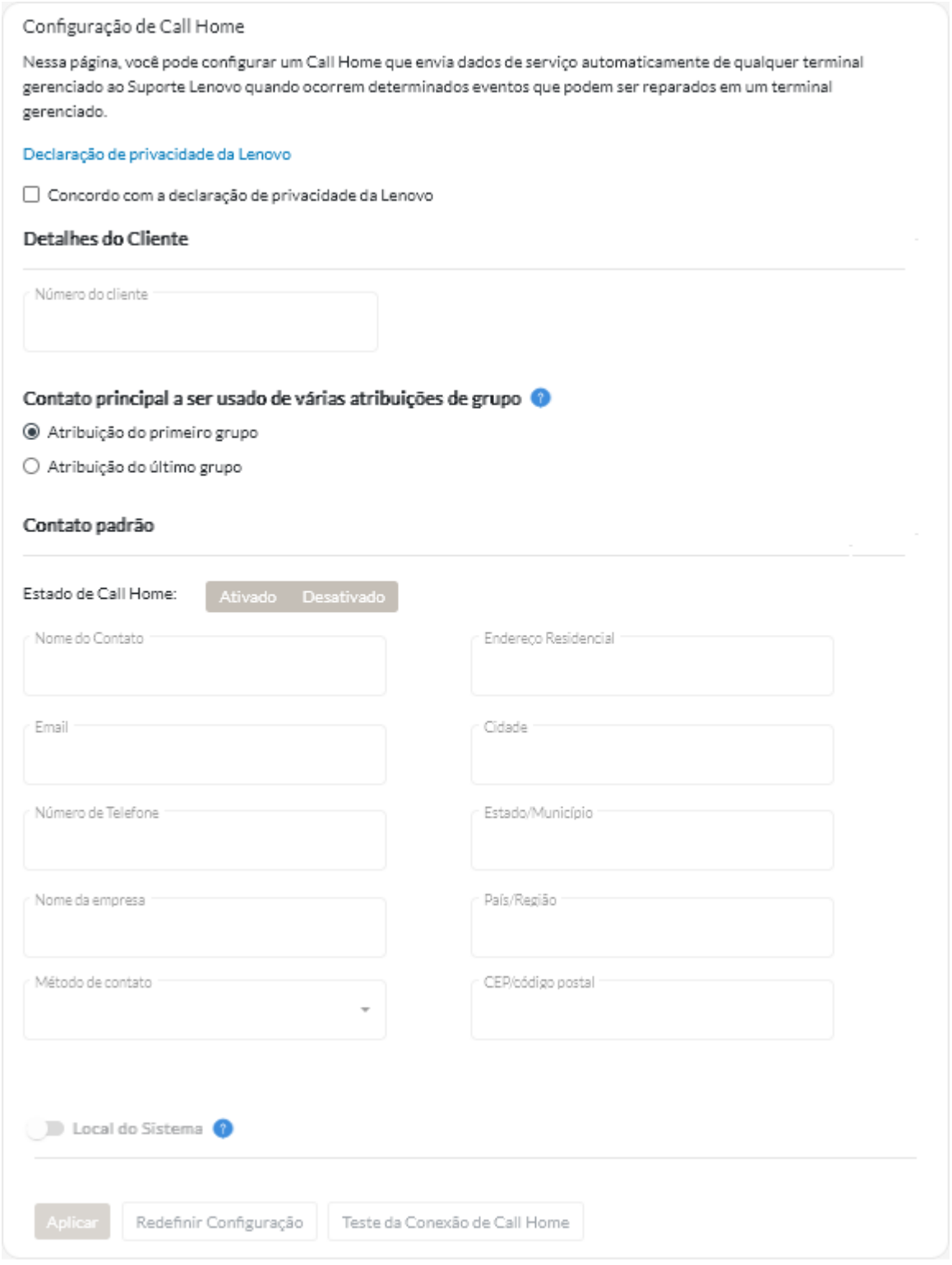
Quando Call Home não estiver habilitado, você poderá abrir manualmente um tíquete de serviço e enviar os arquivos de serviço para o Centro de Suporte da Lenovo seguindo as instruções em Como abrir uma página da Web de tíquete de suporte. Para obter informações sobre como coletar arquivos de serviço, consulte .

Para obter informações sobre como exibir tíquetes de serviço que foram abertos automaticamente pelo Call Home, consulte .

Procedimento

Para configurar o Call Home para notificação automática de problemas, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Orchestrator, clique em **Administração (⚙) → Serviço e Suporte** e, em seguida, clique em **Configuração de Call Home** na navegação esquerda para exibir a placa Configuração de Call Home.



Etapa 2. Revise a Instrução de privacidade da Lenovo e clique em **Concordo com a Declaração de Privacidade da Lenovo**

Etapa 3. Especifique o número do cliente Lenovo padrão a ser usado para relatar problemas.

Você pode localizar o número do seu cliente no e-mail com a prova de direito recebido ao comprar a licença do XClarity Orchestrator.

Etapa 4. Altere o status de Call Home para **Habilitar**.

Etapa 5. Selecione o contato primário a ser usado em várias atribuições de grupo.

É possível atribuir um contato de suporte primário a um grupo de dispositivos. Se um dispositivo for membro de vários grupos, é possível que a cada grupo seja atribuído um contato primário diferente. É possível optar por usar a atribuição de contato primário para o primeiro ou o último grupo ao qual o dispositivo foi designado.

Etapa 6. Preencha as informações de contato e o método preferencial de contato pelo Suporte Lenovo.

Se um dispositivo não for membro de um grupo com um contato primário atribuído, o contato padrão será usado para Call Home.

Etapa 7. Preencha as informações do local do sistema.

Etapa 8. Clique em **Teste da Conexão de Call Home** para verificar se o XClarity Orchestrator pode se comunicar com o Centro de suporte da Lenovo.

Etapa 9. Clique em **Aplicar**.

Depois de concluir

É possível executar as ações a seguir relacionadas a dados de serviço.

- Redefina as configurações de Call Home para os valores padrão clicando em **Redefinir Configuração**.
- Exiba informações sobre *todos* os tíquetes de serviço que foram enviados ao Lenovo Support Center automaticamente ou manualmente usando Call Home clicando em **Tíquetes de Serviço** na navegação esquerda. Para obter mais informações, consulte Exibindo tíquetes de serviço e o status.
- Colete dados de serviço para um dispositivo selecionado da placa Ações do Dispositivo clicando no ícone **Coletar Dados de Serviço** (). Para obter mais informações, consulte Coletando dados de serviço para dispositivos.
- Anexe um arquivo de dados de serviço a um tíquete de serviço ativo selecionado na placa Tíquetes de Serviço na página Serviço específico do dispositivo clicando no ícone **Anexar arquivo de serviço** (). É possível anexar um arquivo do XClarity Orchestrator ou do sistema local.

  Notas:

  – É possível anexar um único arquivo que não seja superior a 2 GB. O nome do arquivo não pode ter mais de 200 caracteres. Para obter informações sobre como criar arquivos de dados de serviço, (consulte Coletando dados de serviço para dispositivos).

  – O tíquete de serviço deve estar no estado aberto, em andamento ou em espera. Não é possível anexar um arquivo a um tíquete de serviço que esteja no estado fechado ou outro.

  – Não é possível anexar um arquivo a um tíquete de serviço de *software* que foi aberto para o gerenciador de recursos.
- Abra manualmente um tíquete de serviço no Centro de Suporte da Lenovo, colete dados de serviço para um dispositivo específico e envie esses arquivos para o Centro de Suporte da Lenovo da placa Ações do Dispositivo, selecionando o dispositivo e, em seguida, clicando no ícone **Abrir tíquete de serviço** (). Para obter mais informações, consulte Abrindo manualmente um tíquete de serviço no centro de suporte da Lenovo.Se o Centro de Suporte da Lenovo precisar de dados adicionais, o suporte da Lenovo poderá instruir você a coletar novamente dados de serviço para esse ou para outro dispositivo.

Abrindo manualmente um tíquete de serviço no centro de suporte da Lenovo

Se Call Home estiver ativado usando um encaminhador de serviços e ocorrer um evento que permite manutenção em um dispositivo gerenciado, o Lenovo XClarity Orchestrator abrirá um tíquete de serviço automaticamente, coletará arquivos de serviço para o dispositivo gerenciado e enviará os arquivos para o centro de suporte da Lenovo. Também é possível coletar manualmente arquivos de serviço para um dispositivo gerenciado como um arquivo, salvar o arquivo no sistema local e enviar os arquivos para o centro de suporte da Lenovo a qualquer momento. A abertura de um tíquete de serviço inicia o processo de determinação de uma solução para seus problemas de hardware, tornando as informações pertinentes disponíveis para o Suporte Lenovo de maneira rápida e eficiente. Os técnicos de serviço Lenovo podem começar a trabalhar na sua solução, assim que você tiver concluído e aberto um tíquete de serviço.

Antes de iniciar

A Lenovo está comprometida com a segurança. Os dados de serviço que você costuma fazer upload manualmente para o suporte da Lenovo são enviados automaticamente para o centro de suporte da Lenovo via HTTPS usando TLS 1.2 ou posterior; seus dados corporativos nunca são transmitidos. O acesso aos dados de serviço no centro de suporte da Lenovo é restrito ao pessoal de serviço autorizado.

- Verifique se as informações de contato de Call Home estão configuradas e habilitadas (Abrindo automaticamente tíquetes de serviço usando Call Home).
- Garanta que XClarity Orchestratoro possa se comunicar com o centro de suporte da Lenovo clicando em **Administração** (⚙) → **Serviço e Suporte** na barra de menu do XClarity Orchestrator e clicando em **Configuração de Call Home** na navegação esquerda para exibir a página Configuração de Call Home. Em seguida, clique em **Teste de Configuração de Call Home** para gerar um evento de teste e verificar se o XClarity Orchestrator pode se comunicar com o Centro de Suporte Lenovo.
- Verifique se todas as portas que são necessárias para o XClarity Orchestrator (incluindo as portas necessárias para o Call Home) estão disponíveis antes de habilitar o Call Home. Para obter mais informações sobre portas, consulte Disponibilidade de porta na documentação online do XClarity Orchestrator.
- Verifique se existe uma conexão aos endereços da Internet exigidos pelo Call Home. Para obter informações sobre firewalls, consulte Firewalls e servidores proxy na documentação online do XClarity Orchestrator.
- Se o XClarity Orchestrator acessa a Internet com um proxy HTTP, verifique se o servidor proxy está configurado para usar autenticação básica e configurado como um proxy não encerrando. Para obter mais informações sobre como configurar o proxy, consulte Definindo configurações de rede.

Importante: A Lenovo está comprometida com a segurança. Os dados de serviço que você costuma fazer upload manualmente para o suporte da Lenovo são enviados automaticamente para o centro de suporte da Lenovo via HTTPS usando TLS 1.2 ou posterior. Seus dados corporativos nunca são transmitidos. O acesso aos dados de serviço no centro de suporte da Lenovo é restrito ao pessoal de serviço autorizado.

Sobre esta tarefa

Ao abrir manualmente um tíquete de serviço, é possível optar por usar os contatos atribuídos ao recurso do problema ou escolher outro contato.

Quando contatos primários e secundários são atribuídos a um grupo, esses contatos são atribuídos a cada dispositivo nesse grupo. A cada dispositivo pode ser atribuído um contato primário e um ou mais contatos secundários. Se um dispositivo for membro de vários grupos, todos os contatos secundários atribuídos a todos os grupos dos quais o dispositivo é membro serão atribuídos ao dispositivo. Se um dispositivo for membro de vários grupos, é possível que a cada grupo seja atribuído um contato primário diferente. É

possível optar por usar a atribuição de contato primário para o primeiro ou o último grupo ao qual o dispositivo foi designado (consulte Abrindo automaticamente tíquetes de serviço usando Call Home).

Se um dispositivo não for membro de um grupo com um contato primário atribuído, o contato de Call Home será atribuído por padrão. O contato de Call Home é usado quando os tíquetes de serviço são abertos automaticamente usando Call Home (consulte Abrindo automaticamente tíquetes de serviço usando Call Home). Contatos atribuídos a recursos e grupos têm precedência sobre o contato padrão de Call Home.

Procedimento

Para abrir um tíquete de serviço manualmente, conclua as etapas a seguir.

- Se o Call Home estiver configurado e habilitado, execute as etapas a seguir para abrir um tíquete de serviço, coletar e baixar os dados de serviço e enviar os arquivos para o centro de suporte da Lenovo.
  1. Na barra de menus do XClarity Orchestrator, clique em **Recursos (** **)** e, em seguida, clique no tipo de dispositivo para exibir uma placa com uma exibição tabular de todos os dispositivos gerenciados do tipo em questão.
  2. Clique na linha do dispositivo para exibir as placas de resumo desse dispositivo.
  3. Clique em **Serviço** na navegação esquerda para exibir a placa Tíquetes de Serviço.
  4. Clique no ícone **Abrir tíquete de serviço** ( ) para exibir a caixa de diálogo Adicionar Novo Tíquete.
  5. Forneça uma descrição do problema relatado, incluindo códigos de evento relevantes.
  6. Opcionalmente, escolha a gravidade do problema. Este pode ser um dos valores a seguir.
     - **Urgente**
     - **Alta**
     - **Média** (padrão)
     - **Baixa**
  7. Clique em **Enviar**.
- Se o Call Home estiver configurado e habilitado e ocorre um evento que permite manutenção em um dispositivo específico, o XClarity Orchestrator abre *automaticamente* um tíquete de serviço e transfere dados de serviço para esse dispositivo para o centro de suporte da Lenovo.

Depois de concluir

É possível executar as ações a seguir na página Serviço específica do dispositivo.

- Exiba informações sobre *todos* os tíquetes de serviço abertos clicando em **Serviço e Suporte → Tíquetes de Serviço** na barra de menus do XClarity Orchestrator.
- Adicione uma nota a um tíquete de serviço selecionado clicando no ícone **Adicionar nota de tíquete de serviço** ( ).

  Notas:

  - O tíquete de serviço deve estar no estado aberto, em andamento ou em espera. Você não pode adicionar uma nota a um tíquete de serviço no estado Fechado ou Outro.
  - É possível adicionar uma nota apenas a tíquetes de serviço da Lenovo. Não é possível adicionar uma nota aos tíquetes de serviço IBM, Service Now ou Cherwill.
  - Não é possível adicionar uma nota a um tíquete de serviço de *software* que foi aberto para o gerenciador de recursos.
- Anexe um arquivo de dados de serviço a um tíquete de serviço ativo selecionado na placa Tíquetes de Serviço na página Serviço específico do dispositivo clicando no ícone **Anexar arquivo de serviço** ( ). É possível anexar um arquivo do XClarity Orchestrator ou do sistema local.

Notas:

- É possível anexar um único arquivo que não seja superior a 2 GB. O nome do arquivo não pode ter mais de 200 caracteres. Para obter informações sobre como criar arquivos de dados de serviço, (consulte Coletando dados de serviço para dispositivos).
- O tíquete de serviço deve estar no estado aberto, em andamento ou em espera. Não é possível anexar um arquivo a um tíquete de serviço que esteja no estado fechado ou outro.
- Não é possível anexar um arquivo a um tíquete de serviço de *software* que foi aberto para o gerenciador de recursos.

Exibindo tíquetes de serviço e o status

É possível exibir informações sobre os tíquetes de serviço que foram criados manual e automaticamente ao Centro de Suporte Lenovo usando call home e os tíquetes de serviço gerados por serviços de suporte diferentes do call home.

Sobre esta tarefa

O status do tíquete de serviço é sincronizado com o Centro de Suporte Lenovo a cada 24 horas.

A coluna **Estado** identifica o status do tíquete de serviço. Um tíquete de serviço pode estar em um dos estados a seguir.

- **Ativo**
- **Atendido**
- **Cancelado**
- **Cancelado**
- **Criado**
- **Cancelado pelo Cliente**
- **Encerrado**
- **Parte Negada**
- **Duplicado**
- **Erro**
- **Estado de erro**
- **Em andamento**
- **Inicializado**
- **Mesclado**
- **Monitoramento - solução implantada**
- **Novo**
- **Em espera**
- **Pendente**
- **Início do problema**
- **Problema Resolvido**
- **Processando**
- **Rejeitado**
- **Pesquisando novamente**
- **Resolvido**
- **Solução fornecida**
- **Enviado**
- **Desconhecido**
- **Aguardando**
- **Aguardando detalhes**
- **Aguardando suporte interno Lenovo**
- **Aguardando parte de suporte externo**
- **Aguardando feedback do cliente sobre a solução**

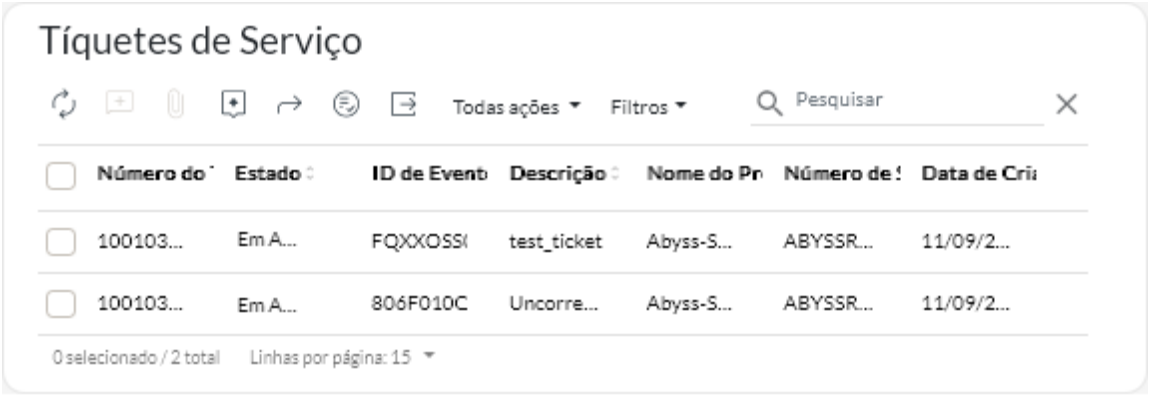
- **Aguardando a implantação da solução**
- **Transferido para Serviços Gerenciados**
- **Transferência a Quente**
- **Trabalho em andamento**

A coluna **Tipo** identifica o tipo de tíquete de serviço que é listado na coluna Número de ticket de serviço. O tipo de tíquete de serviço pode ser um dos valores a seguir.
- **Tíquete Cherwill**
- **Tíquete de Call Home da IBM**
- **Tíquete de Call Home da Lenovo**
- **Tíquete de passagem do Call Home da Lenovo**
- **Tíquete de Call Home de software da Lenovo**
- **ServiceNow**

Procedimento

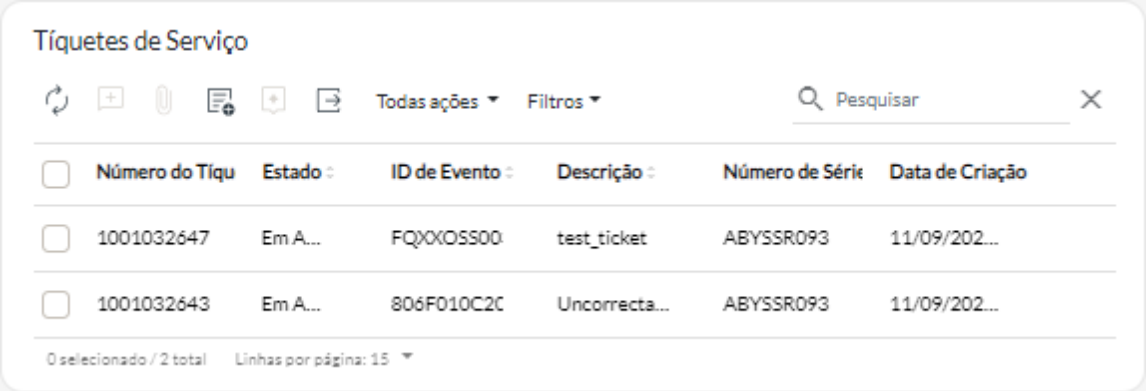
- **Exibir o status de todos os tíquetes de serviço**Clique em **Administração (⚙) → Serviço e Suporte** e, em seguida, clique em **Tíquetes de Serviço** na navegação esquerda para exibir o cartão Tíquetes de Serviço.

  Dica: clique no ID do evento para exibir um resumo do evento que gerou o tíquete de serviço, incluindo a ação do usuário, se houver.



- **Exibir o status de tíquetes de serviço para um dispositivo específico**
  1. Na barra de menus do XClarity Orchestrator, clique em **Recursos** (⚙) e, em seguida, clique no tipo de dispositivo para exibir uma placa com uma exibição tabular de todos os dispositivos gerenciados do tipo em questão.
  2. Clique na linha do dispositivo para exibir as placas de resumo desse dispositivo.
  3. Clique em **Serviço** na navegação esquerda para exibir a placa Tíquetes de Serviço com uma lista de todos os tíquetes de serviço do dispositivo.

     Dica: clique no ID do evento para exibir um resumo do evento que gerou o tíquete de serviço, incluindo a ação do usuário, se houver.



Depois de concluir

É possível executar as ações a seguir relacionadas a tíquetes de serviço.

- Configure o XClarity Orchestrator para abrir automaticamente um tíquete de serviço quando ocorrer um evento que permite manutenção (consulte "Abrindo automaticamente tíquetes de serviço usando Call Home" na página 208).
- Sincronize dados com o Centro de Suporte Lenovo e atualize o status de todos os tíquetes de serviço ativos clicando no ícone **Atualizar status do tíquete de serviço** ().
- Abra manualmente um tíquete de serviço para um dispositivo específico da placa Tíquetes de Serviço na página Serviço específico do dispositivo clicando no ícone **Abrir tíquete de serviço** ().
- Adicione uma nota a um tíquete de serviço selecionado clicando no ícone **Adicionar nota de tíquete de serviço** ().

  Notas:

  – O tíquete de serviço deve estar no estado aberto, em andamento ou em espera. Você não pode adicionar uma nota a um tíquete de serviço no estado Fechado ou Outro.

  – É possível adicionar uma nota apenas a tíquetes de serviço da Lenovo. Não é possível adicionar uma nota aos tíquetes de serviço IBM, Service Now ou Cherwill.

  – Não é possível adicionar uma nota a um tíquete de serviço de *software* que foi aberto para o gerenciador de recursos.
- Anexe um arquivo de dados de serviço a um tíquete de serviço ativo selecionado na placa Tíquetes de Serviço na página Serviço específico do dispositivo clicando no ícone **Anexar arquivo de serviço** (). É possível anexar um arquivo do XClarity Orchestrator ou do sistema local.

  Notas:

  – É possível anexar um único arquivo que não seja superior a 2 GB. O nome do arquivo não pode ter mais de 200 caracteres. Para obter informações sobre como criar arquivos de dados de serviço, (consulte Coletando dados de serviço para dispositivos).

  – O tíquete de serviço deve estar no estado aberto, em andamento ou em espera. Não é possível anexar um arquivo a um tíquete de serviço que esteja no estado fechado ou outro.

  – Não é possível anexar um arquivo a um tíquete de serviço de *software* que foi aberto para o gerenciador de recursos.
- Encaminhe relatórios sobre tíquetes de serviço ativos de forma recorrente em um ou mais endereços de e-mail clicando no ícone **Criar encaminhador de relatórios** (). O relatório é enviado usando os filtros

de dados que estão aplicados atualmente à tabela. Todas as colunas da tabela mostradas e ocultas são incluídas no relatório. Para obter mais informações, consulte .

- Adicione um relatório de tíquetes de serviço ativos a um encaminhador de relatórios específico usando os filtros de dados que são aplicados atualmente à tabela clicando no ícone **Adicionar ao encaminhador de relatórios** (↱). Se o encaminhador de relatórios já incluir um relatório de tíquetes de serviço ativos, ele será atualizado para usar os filtros de dados atuais.

Visualizando informações sobre garantia

É possível determinar os status de garantia (inclusive garantias prolongadas) dos dispositivos gerenciados.

Antes de iniciar

O Lenovo XClarity Orchestrator deve ter acesso aos URLs a seguir para coletar informações sobre garantia para os dispositivos gerenciados. Verifique se não há nenhum firewall bloqueando o acesso a esses URLs. Para obter mais informações, consulte Firewalls e servidores proxy na documentação online do XClarity Orchestrator.

- Banco de Dados da Lenovo Warranty (internacional) – https://ibase.lenovo.com/POIRequest.aspx
- Serviço da Web da Lenovo Warranty – http://supportapi.lenovo.com/warranty/ ou https://supportapi.lenovo.com/warranty/

Notas:

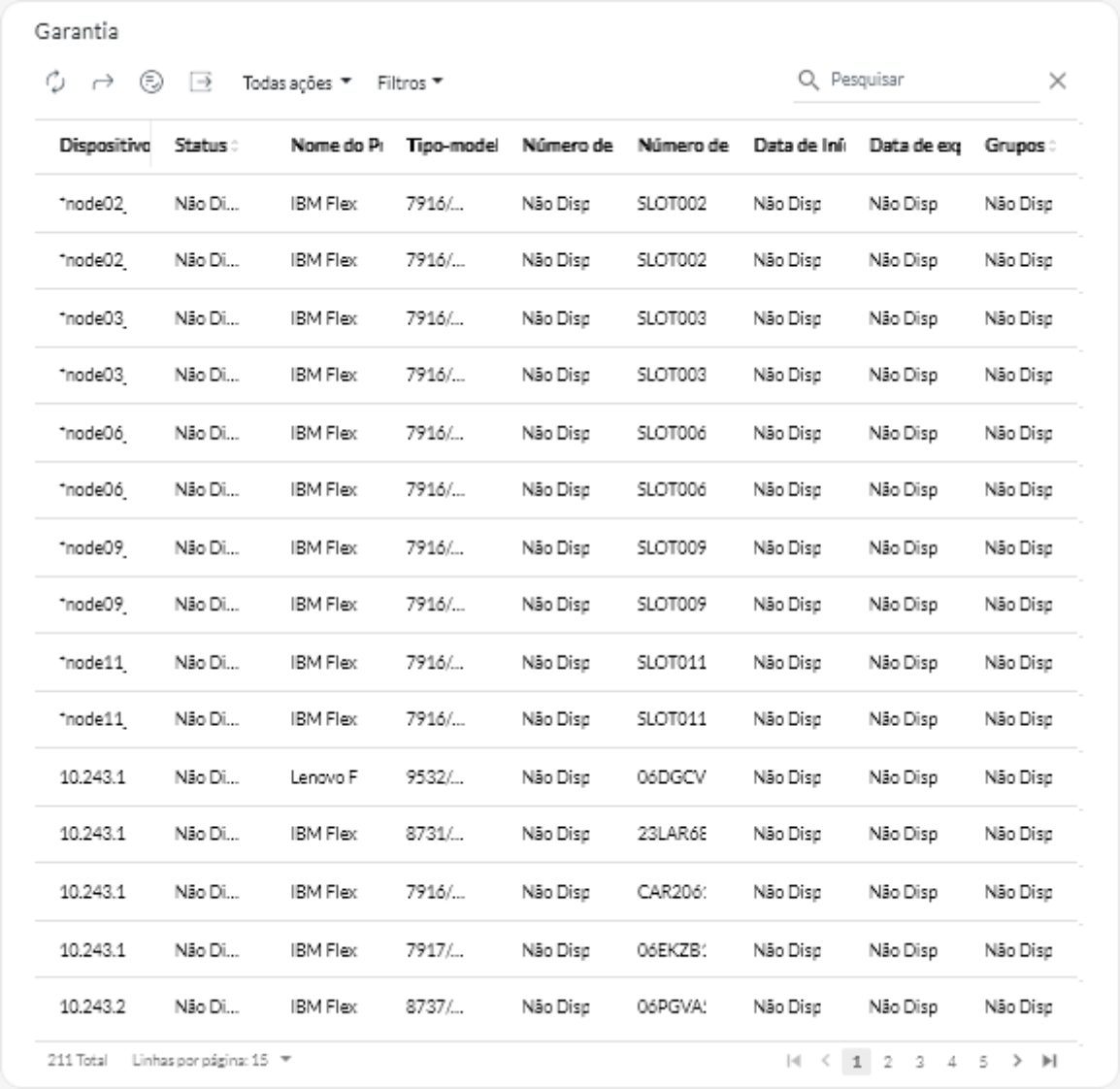
- O suporte de garantia para usuários não é suportado atualmente para usuários na China.
- As garantias são listadas para o chassi, mas não para os Chassis Management Modules (CMMs) correspondentes.

Sobre esta tarefa

As informações de garantia são recuperadas semanalmente para dispositivos que têm garantias, e diariamente para dispositivos que não têm garantias.

Procedimento

Para exibir informações de garantia, clique em **Administração** (⚙) → **Serviço e Suporte** e, em seguida, clique em **Garantia** na navegação esquerda para exibir o cartão Garantia.



Depois de concluir

É possível executar as ações a seguir a partir do cartão Garantia.

- Configure quando você quer ser notificado sobre as expirações de garantia para dispositivos gerenciados clicando no ícone **Definir configurações de garantia** (). É possível definir as configurações a seguir.
  - Habilite a geração de alertas quando a garantia do dispositivo está prestes a expirar.
  - Defina o número de dias antes da expiração das garantias quando você deseja gerar um alerta.
- Procure as informações sobre garantia (se disponíveis) para um dispositivo específico no site Suporte Lenovo clicando na coluna **Status**.
- Encaminhe relatórios sobre garantias de forma recorrente em um ou mais endereços de e-mail clicando em **Todas as Ações** → **Adicionar encaminhador de relatórios**. O relatório é enviado usando os filtros de dados que estão aplicados atualmente à tabela. Todas as colunas da tabela mostradas e ocultas são incluídas no relatório.
- Adicione um relatório de garantias a um encaminhador de relatórios específico usando os filtros de dados que são aplicados atualmente à tabela clicando no ícone **Adicionar ao encaminhador de relatórios** (). Se o encaminhador de relatórios já incluir um relatório de garantias, ele será atualizado para usar os filtros de dados atuais.

Lenovo