Lenovo XClarity Management Hub
Guia do Usuário e Instalação

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

Conteúdo i

Capítulo 1. Planejando o Lenovo XClarity Management Hub 1

Hardware e software compatíveis 1

Firewalls e servidores proxy 2

Disponibilidade de porta 3

Considerações de rede 5

Considerações sobre alta disponibilidade 6

Capítulo 2. Configurando o XClarity Management Hub para dispositivos cliente de borda 9

Fazendo login no XClarity Management Hub para dispositivos cliente de borda. 9

Criando contas de usuário para Lenovo XClarity Management Hub dispositivos cliente de borda . . 11

Definindo configurações de rede para XClarity Management Hub para dispositivos cliente de borda 12

Configurando data e hora para o XClarity Management Hub para dispositivos cliente de borda 14

Gerenciando certificados de segurança para Lenovo XClarity Management Hub para dispositivos cliente de borda 15

Gerando novamente o certificado de servidor autoassinado para XClarity Management Hub para dispositivos cliente de borda 17

Instalando um certificado de servidor assinado externamente confiável para XClarity Management Hub para dispositivos cliente de borda 19

Importando o certificado do servidor para um navegador da Web para Lenovo XClarity Management Hub para dispositivos cliente de borda 21

Conectando o XClarity Management Hub para dispositivos cliente de borda ao XClarity Orchestrator 23

Capítulo 3. Desinstalando o XClarity Management Hub para dispositivos cliente de borda 25

Capítulo 1. Planejando o Lenovo XClarity Management Hub

Revise as seguintes considerações e pré-requisitos para ajudá-lo a planejar a instalação do Lenovo XClarity Management Hub.

Hardware e software compatíveis

Assegure-se de que seu ambiente atenda aos requisitos de hardware e software do Lenovo XClarity Management Hub.

Sistemas host

Requisitos do hipervisor

Os hipervisores a seguir são suportados para instalação do Lenovo XClarity Management Hub.
- VMware ESXi 7.0, U1, U2 e U3
- VMware ESXi 6.7, U1, U2[1] e U3

Para VMware ESXi, o dispositivo virtual é um modelo OVF.

Importante:

- Para VMware ESXi 6.7 U2, você deve usar a imagem ISO VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso ou posterior.

Requisitos de Hardware

A tabela a seguir lista as configurações *mínimas recomendadas* para XClarity Management Hub com base no número de dispositivos cliente de borda gerenciados. Dependendo do ambiente, recursos adicionais podem ser necessários para obter o desempenho ideal.

Número de dispositivos cliente de borda gerenciados	Processadores	Memória	Armazenamento
0 - 100 dispositivos	6	32 GB	340 GB
100 - 200 dispositivos	8	34 GB	340 GB
200 - 400 dispositivos	10	36 GB	340 GB
400 - 600 dispositivos	12	40 GB	340 GB
600 - 800 dispositivos	14	44 GB	340 GB
800 - 1.000 dispositivos	16	48 GB	340 GB

1. Essa é a quantidade mínima de armazenamento para uso pelo dispositivo virtual XClarity Management Hub, como um armazenamento de dados SSD.

Requisitos de Software

O XClarity Management Hub requer o software a seguir.

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

Dispositivos gerenciáveis

O XClarity Management Hub pode gerenciar, monitorar e provisionar no máximo 10,000 dispositivos ThinkEdge Client (sem Baseboard Management Controllers).

É possível encontrar uma lista completa de dispositivos e opções compatíveis do ThinkEdge Client (como E/S, DIMM e adaptadores de armazenamento), níveis mínimos de firmware necessários e considerações sobre limitações nos Servidores XClarity Management Hub.

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

Navegadores da Web

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

Firewalls e servidores proxy

Algumas funções de serviço e suporte, incluindo Call Home e status de garantia, requerem acesso à Internet. Se você tiver firewalls em sua rede, configure os firewalls para habilitar o XClarity Orchestrator e os gerenciadores de recursos para executar essas operações. Se o Lenovo XClarity Orchestrator e os gerenciadores de recursos não tiverem acesso direto à Internet, configure-os para usar um servidor proxy.

Firewalls

Verifique se os nomes e as portas DNS a seguir estão abertos no firewall para XClarity Orchestrator e gerenciadores de recursos aplicáveis (Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub e Lenovo XClarity Administrator), conforme aplicável. Cada DNS representa um sistema distribuído geograficamente com um endereço IP dinâmico.

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

Nome DNS	Portas	Protocolos
Baixar atualizações (do servidor de gerenciamento, as atualizações de firmware, UpdateXpress System Packs (drivers de dispositivo do SO) e pacotes do repositório)		
download.lenovo.com	443	https
support.lenovo.com	443 e 80	https e http
Enviar dados de serviço para o Lenovo Support (Call Home) – XClarity Orchestratorsomente		
soaus.lenovo.com	443	https
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 e posterior) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/Logupload.ashx (XClarity Orchestrator v1.5 e anterior)	443	https
Enviar dados periódicos à Lenovo – XClarity Orchestrator somente		

Nome DNS	Portas	Protocolos
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 e posterior) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/uploadSnapshot.ashx (XClarity Orchestrator v1.5 e anterior)	443	https
Recuperar informações sobre garantia		
supportapi.lenovo.com	443	https e http

Servidor proxy

Se o XClarity Orchestrator ou os gerenciadores de recursos não têm acesso direto à Internet, verifique se eles estão configurados para usar um servidor proxy HTTP (consulte Configurando a redena documentação online do XClarity Orchestrator).

- 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.

Atenção: O XClarity Management Hub deve ter acesso direto à Internet. Um servidor proxy HTTP não é compatível atualmente.

Disponibilidade de porta

O Lenovo XClarity Orchestrator e os gerenciadores de recursos requerem que determinadas portas sejam abertas para facilitar a comunicação. Se as portas necessárias estiverem bloqueadas ou forem usadas por outro processo, algumas funções poderão não funcionar corretamente.

XClarity Orchestrator, Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub e o Lenovo XClarity Administrator são aplicativos RESTful que se comunicam com segurança por TCP na porta 443.

XClarity Orchestrator

O XClarity Orchestrator ouve e responde pelas portas que estão listadas na tabela a seguir. Se o XClarity Orchestrator e todos os recursos gerenciados estiverem atrás de um firewall, e você pretende acessar esses recursos de um navegador que está *fora* do firewall, certifique-se de que as portas necessárias estejam abertas.

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

Serviço	Saída (portas abertas em sistemas externos)	Entrada (portas abertas no dispositivo XClarity Orchestrator)
Dispositivo XClarity Orchestrator	• DNS – TCP/UDP na porta **53**	• HTTPS – TCP na porta **443**
Servidores de autenticação externos	• LDAP – TCP na porta **389**[1]	Não aplicável

Serviço	Saída (portas abertas em sistemas externos)	Entrada (portas abertas no dispositivo XClarity Orchestrator)
Serviços de encaminhamento de eventos	• Servidor de emails (SMTP) – UDP na porta **25**[1] • REST Web Service (HTTP) – UPD na porta **80**[1] • Splunk – UDP na porta **8088**[11], **8089**[1] • Syslog – UDP na porta **514**[1]	Não aplicável
Serviços Lenovo (incluindo Call Home)	• HTTPS (Call Home) – TCP na porta **443**	Não aplicável

1. Esta é a porta padrão. É possível configurar essa porta na interface do usuário do XClarity Orchestrator.

XClarity Management Hub 2.0

O Lenovo XClarity Management Hub 2.0 exige que determinadas portas sejam abertas para facilitar a comunicação. Se as portas necessárias estiverem bloqueadas ou forem usadas por outro processo, algumas funções do hub de gerenciamento poderão não funcionar corretamente.

Se os dispositivos estiverem atrás de um firewall e se você pretender gerenciar esses dispositivos a partir de um hub de gerenciamento que está fora desse firewall, você deverá garantir que todas as portas envolvidas com comunicações entre o hub de gerenciamento e o Baseboard Management Controller em cada dispositivo estejam abertas.

Serviço ou componente	Saída (portas abertas para sistemas externos)	Entrada (portas abertas em dispositivos de destino)
XClarity Management Hub 2.0	• DNS – UDP na porta **53** • NTP – UDP na porta **123** • HTTPS – TCP na porta **443** • SSDP – UDP na porta **1900** • DHCP – UDP na porta **67**	• HTTPS – TCP na porta **443** • Reimplantação de SSDP - UDP nas portas **32768**-**65535**
Servidores ThinkSystem e ThinkAgile	• HTTPS – TCP na porta **443** • Descoberta de SSDP – UDP na porta **1900**	• HTTPS – TCP na porta **443**

XClarity Management Hub

O XClarity Management Hub ouve e responde pelas portas que estão listadas na tabela a seguir.

Serviço ou componente	Saída (portas abertas em sistemas externos)	Entrada (portas abertas no dispositivo XClarity Management Hub)
DispositivoXClarity Management Hub[1]	• DNS – TCP/UDP na porta **53**[2]	• HTTPS – TCP na porta **443** • MQTT – TCP na porta **8883**
Dispositivos ThinkEdge Client[3]	Não aplicável	• MQTT – TCP na porta **8883**

1. Ao usar o XClarity Management Hub para gerenciar dispositivos por meio do XClarity Orchestrator, determinadas portas devem estar abertas para facilitar a comunicação. Se as portas necessárias estiverem bloqueadas ou forem usadas por outro processo, algumas funções do XClarity Orchestrator poderão não funcionar corretamente.

2. O XClarity Management Hub pode ser configurado para estabelecer conexões de saída com vários serviços externos. Essas conexões podem requerer acesso a um servidor domain name service (DNS) na porta TCP ou UDP 53 para resolver nomes de servidor externo.
3. Se os dispositivos gerenciáveis estiverem atrás de um firewall e se você pretender gerenciar esses dispositivos a partir de um servidor XClarity Management Hub que está fora desse firewall, você deverá garantir que todas as portas envolvidas com comunicações entre o XClarity Management Hub e os dispositivos de borda estejam abertas.

XClarity Administrator

Ao usar o Lenovo XClarity Administrator para gerenciar dispositivos por meio do Lenovo XClarity Orchestrator, determinadas portas devem estar abertas para facilitar a comunicação. Se as portas necessárias estiverem bloqueadas ou forem usadas por outro processo, algumas funções do XClarity Orchestrator poderão não funcionar corretamente.

Para obter informações sobre as portas que devem ser abertas para o XClarity Administrator, consulte Disponibilidade de porta na documentação online do XClarity Administrator.

Considerações de rede

É possível configurar o Lenovo XClarity Management Hub para usar uma única interface de rede (eth0) ou duas interfaces de rede separadas (eth0 e eth1) para comunicação.

O Lenovo XClarity Management Hubcomunica-se nas redes a seguir.

- A *rede de gerenciamento* é usada para comunicação entre o Lenovo XClarity Management Hub e dispositivos gerenciados.
- A *rede de dados* é normalmente usada para comunicação entre sistemas operacionais instalados nos servidores e a intranet corporativa, a Internet ou ambos.

Interface única (eth0)

Ao usar uma única interface de rede (eth0), as comunicações de gerenciamento, as comunicações de dados e a implantação do sistema operacional ocorrem na mesma rede.

Quando você configurar o Lenovo XClarity Management Hub, defina a interface de rede eth0 usando as seguintes considerações.

- A interface de rede deve ser configurada para ser compatível com a descoberta e o gerenciamento de dispositivos (incluindo atualizações de firmware). O Lenovo XClarity Management Hub deve ser capaz de se comunicar com todos os dispositivos que ele gerenciará a partir da rede de gerenciamento.O Lenovo XClarity Management Hub deve ser capaz de se comunicar com todos os dispositivos que ele gerenciará a partir da rede.
- Para implantar imagens do SO, a interface eth0 deve ter conectividade de rede IP com a interface de rede do servidor que é usada para acessar o sistema operacional do host.
- **Importante:** implementar uma rede de gerenciamento e de dados compartilhada que inclui o chassi pode causar interrupções no tráfego, como conjuntos sendo descartados ou problemas de conectividade de rede de gerenciamento, dependendo da configuração de rede (por exemplo, tráfego de servidores com uma alta prioridade e tráfego de controladores de gerenciamento que tenham baixa prioridade). A rede de gerenciamento usa o tráfego UDP além do TCP. O tráfego UDP pode ter uma prioridade inferior quando o tráfego de rede for alto.

Duas interfaces separadas (eth0 e eth1)

Ao usar duas interfaces de rede (eth0 e eth1), é possível configurá-las como redes separadas fisicamente ou virtualmente separadas.

Revise as considerações a seguir ao definir as interfaces de rede eth0 e eth1.

- A interface de rede eth0 deve ser conectada à rede de gerenciamento e configurada para dar suporte à descoberta e ao gerenciamento de dispositivos. O Lenovo XClarity Management Hub deve ser capaz de se comunicar com todos os dispositivos que ele gerenciará a partir da rede de gerenciamento.
- A interface de rede eth1 pode ser configurada geralmente para se comunicar com uma rede de dados interna, rede de dados pública ou ambas.
- Para implantar imagens do sistema operacional, a interface de rede eth1 deve ter conectividade de rede IP com a interface de rede do servidor que é usada para acessar o sistema operacional do host.
- As funções podem ser executadas em qualquer rede.
- Para redes separadas virtualmente, os pacotes da rede de gerenciamento e os pacotes da rede de dados são enviados pela mesma conexão física. Use a marcação de VLAN em todos os pacotes de dados da rede de gerenciamento para manter o tráfego separado entre as duas redes.

Considerações sobre endereço IP

Revise as considerações de endereço IP a seguir antes de configurar a rede.

- Alterar o endereço IP do dispositivo virtual depois que o XClarity Management Hub é ligado e está em execução causará problemas de conectividade com o XClarity Orchestrator e todos os dispositivos gerenciados. Se você precisar alterar o endereço IP, desconecte o XClarity Management Hub do XClarity Orchestrator e cancele o gerenciamento de todos os dispositivos gerenciados antes de alterar o endereço IP e, em seguida, gerencie novamente os dispositivos e reconecte o XClarity Management Hub ao XClarity Orchestrator após a alteração do endereço IP ser concluída
- Configure os dispositivos e os componentes de forma a minimizar as alterações de endereço IP. Considere utilizar endereços IP estáticos em vez de Dynamic Host Configuration Protocol (DHCP). Se o DHCP for usado, garanta que as alterações de endereço IP sejam minimizadas, como basear o endereço DHCP em um endereço MAC ou configurar o DHCP para que o arrendamento não expire.Se o endereço IP de um dispositivo gerenciado (diferente de um dispositivo ThinkEdge Client) for alterado, você deverá cancelar o gerenciamento do dispositivo e, em seguida, gerenciá-lo novamente.
- A conversão de endereço de rede (NAT), que remapeia um espaço de endereço IP em outro, não é suportada.
- As interfaces de rede devem ser configuradas com um endereço IPv4 para gerenciar os dispositivos a seguir. Endereços IPv6 não têm suporte.
  - Servidores ThinkServer
  - Dispositivos de armazenamento Lenovo
- O gerenciamento de dispositivos RackSwitch usando link IPv6 local por meio da porta de dados ou porta de gerenciamento não tem suporte.

Considerações sobre alta disponibilidade

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

Microsoft Hyper-V

Use a função de alta disponibilidade fornecida para o ambiente Hyper-V.

VMware ESXi

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

O VMware High Availability requer os seguintes componentes.

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

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

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

Capítulo 2. Configurando o XClarity Management Hub para dispositivos cliente de borda

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

Procedimento

Conclua as etapas a seguir para configurar inicialmente o XClarity Management Hub.

Etapa 1. Faça login na Interface da web do XClarity Management Hub.

Etapa 2. Leia e aceite o contrato de licença.

Etapa 3. Crie contas de usuário adicionais.

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

Etapa 5. Configure data e hora.

Etapa 6. Registre o XClarity Management Hub com o servidor do Orchestrator.

Fazendo login no XClarity Management Hub para dispositivos cliente de borda

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

Antes de iniciar

Use um dos seguintes navegadores da Web suportados.
- 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**.

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

O XClarity Management Hub desconecta automaticamente as sessões do usuário após 60 minutos, independentemente da atividade do usuário.

Procedimento

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

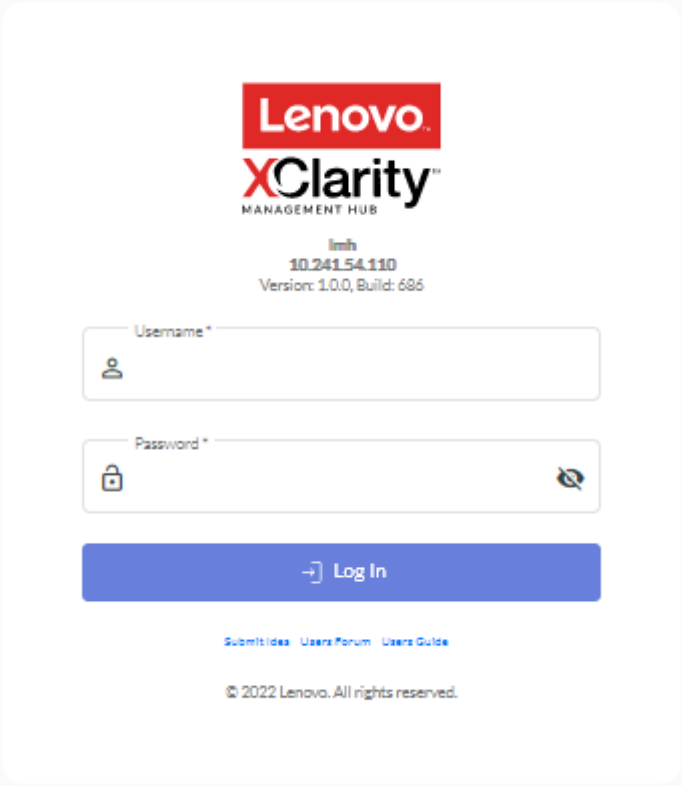
Etapa 1. Aponte seu navegador para o endereço IP do XClarity Management Hub.
`https://<IPv4_address>`

Exemplo:
`https://192.0.2.10`

O endereço IP utilizado depende de como seu ambiente é definido.

- Se você especificou um endereço IPv4 em eth0_config, use esse endereço IPv4 para acessar o XClarity Management Hub.
- Se um servidor DHCP estiver configurado no mesmo domínio de transmissão de XClarity Management Hub, use o endereço IPv4 que é exibido no console de máquina virtual do XClarity Management Hub para acessar o XClarity Management Hub.
- Se você tiver as redes eth0 e eth1 em sub-redes diferentes e se DHCP for usado nas sub-redes, use o endereço IP de *eth1* ao acessar a interface da Web para configuração inicial. Quando o XClarity Management Hub é iniciado pela primeira vez, eth0 e eth1 obtêm um endereço IP designado por DHCP e o gateway padrão do XClarity Management Hub é configurado para o gateway designado por DHCP para *eth1*.

A página de login inicial de XClarity Management Hub é exibida:



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

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

Etapa 3. Insira suas credenciais do usuário e clique em **Fazer login**

Se você estiver fazendo login no XClarity Management Hub pela primeira vez, insira as credenciais padrão **USERID** e **PASSW0RD** (em que 0 é zero).

Etapa 4. Leia e aceite o contrato de licença.

Etapa 5. Se você fez login pela primeira vez usando credenciais padrão, será solicitado a 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.
- (1) Devem conter pelo menos um caractere alfabético maiúsculo

- (2) Devem conter pelo menos um caractere alfabético minúsculo
- (3) Devem conter pelo menos um número
- (4) Devem conter pelo menos um caractere especial
- (5) Não devem ser iguais ao nome do usuário

Etapa 6. Se você fez login pela primeira vez, será solicitado que você opte por usar o certificado autoassinado atual ou um certificado assinado pela CA externamente. Se você optar por usar um certificado assinado externamente, a página Certificado do Servidor será exibida.

Atenção: O certificado autoassinado não é seguro. É recomendável gerar e instalar seu próprio certificado assinado externamente.

Para obter informações sobre como usar um certificado assinado externamente, consulte Instalando um certificado de servidor assinado externamente confiável para XClarity Management Hub para dispositivos cliente de borda.

Depois de concluir

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

- Faça logout da sessão atual clicando em **Fazer logout**. A página de login do XClarity Management Hub será exibida.
- Faça perguntas e encontre respostas usando o Site do fórum da comunidade do Lenovo XClarity.
- Enviar ideias sobre o XClarity Management Hub clicando em **Enviar ideias** no menu **Conta do Usuário** ( ) na interface da Web do canto superior direito ou indo diretamente para o Web site de concepção do Lenovo XClarity.
- Exiba a documentação online clicando no **Guia do usuário**.
- Exiba informações sobre a versão do XClarity Management Hub clicando em **Sobre**.
- 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)

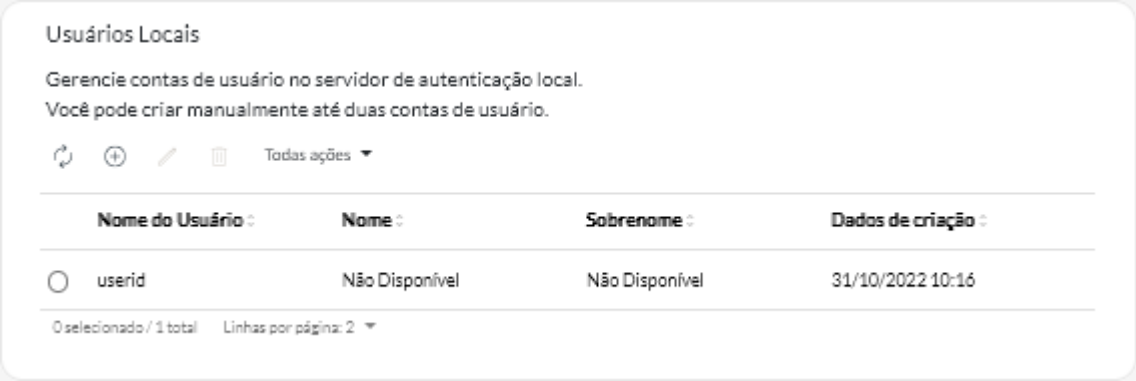
Criando contas de usuário para Lenovo XClarity Management Hub dispositivos cliente de borda

É possível criar até dez contas de usuário para o Lenovo XClarity Management Hub.

Procedimento

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

Etapa 1. Na barra de menus do Lenovo XClarity Management Hub, clique em **Segurança (⚙) → Usuários Locais** para exibir o cartão 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.
  - (1) Devem conter pelo menos um caractere alfabético maiúsculo
  - (2) Devem conter pelo menos um caractere alfabético minúsculo
  - (3) Devem conter pelo menos um número
  - (4) Devem conter pelo menos um caractere especial
  - (5) Não devem ser iguais ao nome do usuário

Etapa 4. 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.

- Modifique a senha e as propriedades de sua conta de usuário clicando no ícone **Editar** (✎). Observe que as senhas não expiram.
- Exclua um usuário selecionado clicando no ícone **Excluir** (🗑).

Definindo configurações de rede para XClarity Management Hub para dispositivos cliente de borda

É possível configurar uma única interface de rede IPv4 e configurações de roteamento da Internet.

Antes de iniciar

Revise as considerações sobre rede antes de configurá-la (consulte Considerações de rede).

Procedimento

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

- **Configurar definições de IP**Para a interface eth0, clique na guia **Interface Eth0**, defina as configurações de endereço IPv4 aplicáveis e, em seguida, clique em **Aplicar**.

  Atenção:

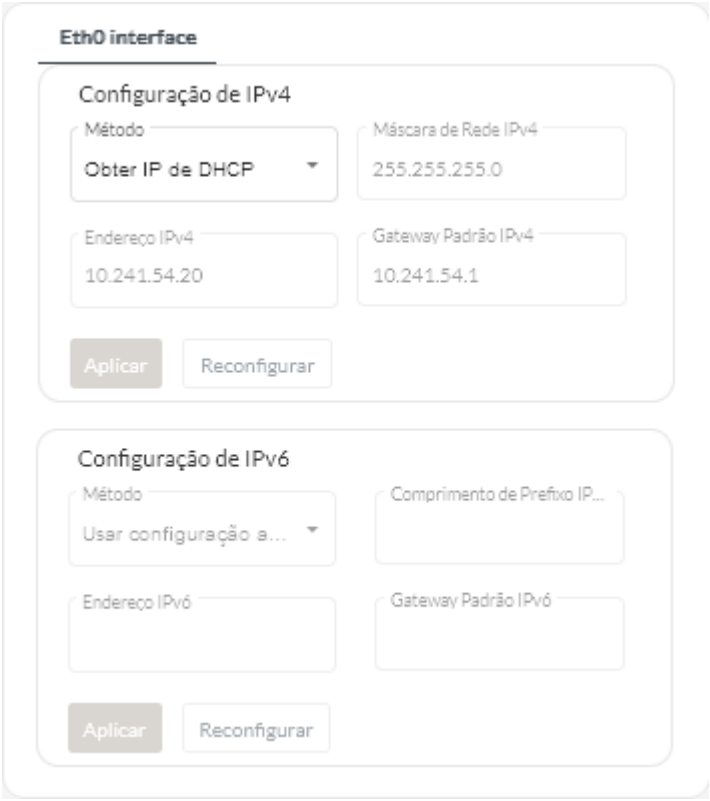
  – Alterar o endereço IP do dispositivo virtual depois que o XClarity Management Hub é ligado e está em execução causará problemas de conectividade com o XClarity Orchestrator e todos os dispositivos gerenciados. Se você precisar alterar o endereço IP, desconecte o XClarity Management Hub do XClarity Orchestrator e cancele o gerenciamento de todos os dispositivos gerenciados antes de alterar o endereço IP e, em seguida, gerencie novamente os dispositivos e reconecte o XClarity Management Hub ao XClarity Orchestrator após a alteração do endereço IP ser concluída

  Atualmente, apenas endereços IPv4 são suportados.

  – **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 usar a mesma máscara de rede (a mesma sub-rede) da interface habilitada (eth0).

    Se uma das interfaces usar DHCP para obter um endereço IP, o gateway padrão também usará DHCP.



- **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.

  É possível alterar o endereço IP para o servidor DNS.

O nome de domínio totalmente qualificado (FQDN) e o nome do host para o servidor DNS são os mesmos do servidor XClarity Management Hub e não podem ser alterados.

Configurando data e hora para o XClarity Management Hub para dispositivos cliente de borda

É necessário configurar pelo menos um (e até quatro) servidor Network Time Protocol (NTP) para sincronizar os registros de data e hora entre o XClarity Management Hub e todos os dispositivos gerenciados.

Antes de iniciar

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

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

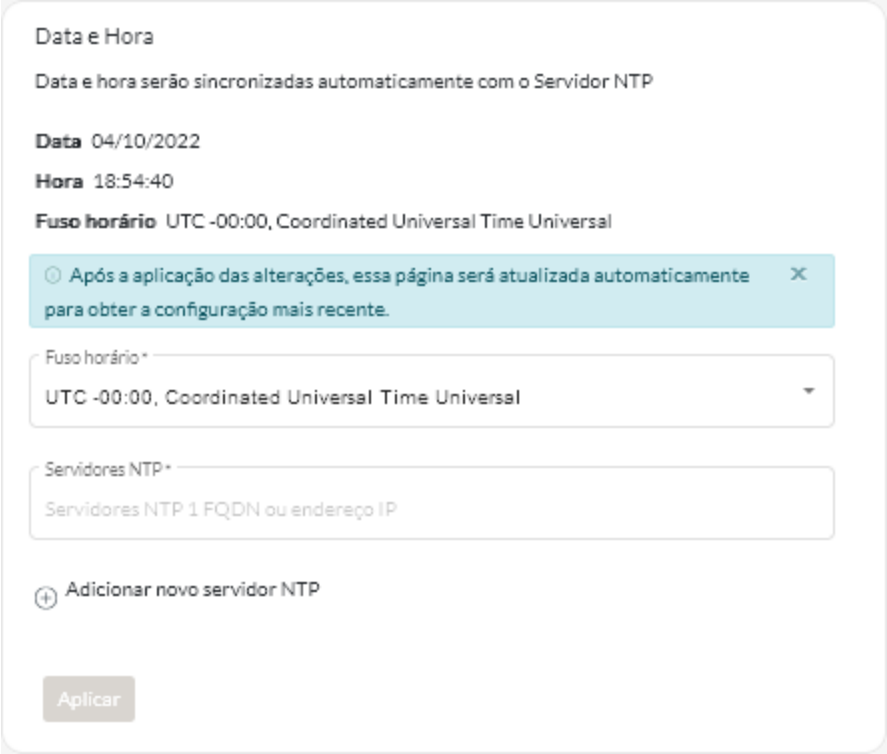
Atenção: O dispositivo virtual do XClarity Management Hub e seu host devem ser configurados para sincronização com a mesma origem de horário para evitar a falta de sincronização de horário acidental entre o XClarity Management Hub e seu host. Normalmente, o host é configurado para que seus dispositivos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

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

Procedimento

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

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



Etapa 2. Escolha o fuso horário onde o host para XClarity Management Hub 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**.

Gerenciando certificados de segurança para Lenovo XClarity Management Hub para dispositivos cliente de borda

O Lenovo XClarity Management Hub usa certificados SSL para estabelecer uma comunicação segura e confiável entre o Lenovo XClarity Management Hub e seus dispositivos gerenciados, bem como a comunicação com o Lenovo XClarity Management Hub por usuários ou com serviços diferentes. Por padrão, o Lenovo XClarity Management Hub e o XClarity Orchestrator 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 Lenovo XClarity Management Hub, fornece segurança adequada para muitos ambientes. É possível escolher se você quer deixar o Lenovo XClarity Management Hub gerenciar certificados, ou se você pode ter uma função mais

ativa personalizando e substituindo os certificados de servidor. O Lenovo XClarity Management Hub 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 Lenovo XClarity Management Hub 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 Lenovo XClarity Management Hub 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 Lenovo XClarity Management Hub 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 Lenovo XClarity Management Hub não estiver incluído na lista do cliente, o cliente se desconectará do Lenovo XClarity Management Hub para evitar a troca de qualquer informação confidencial de segurança com uma origem não confiável.

O Lenovo XClarity Management Hub age como um cliente ao se comunicar com dispositivos gerenciados e serviços externos. Quando isso ocorre, o dispositivo gerenciado ou o serviço externo fornece seu certificado de servidor a ser verificado pelo Lenovo XClarity Management Hub. O Lenovo XClarity Management Hub mantém uma lista de certificados em que ele confia. Se o *certificado confiável* fornecido pelo dispositivo gerenciado ou serviço externo não estiver listado, o Lenovo XClarity Management Hub 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 Lenovo XClarity Management Hub 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 Lenovo XClarity Management Hub. 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 autoassinado para XClarity Management Hub para dispositivos cliente de borda).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 Lenovo XClarity Management Hub. Ele é gerado de novo automaticamente sempre que o Lenovo XClarity Management Hub 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 autoassinado para XClarity Management Hub para dispositivos cliente de borda).

  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 Lenovo XClarity Management Hub (consulte Instalando um certificado de servidor assinado externamente confiável para XClarity Management Hub para dispositivos cliente de borda).

  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 para um navegador da Web para Lenovo XClarity Management Hub para dispositivos cliente de borda).

- **Certificado de implantação do SO**. Um certificado separado é usado pelo serviço de implantação do sistema operacional para assegurar que o instalador do sistema operacional possa se conectar com segurança ao serviço de implantação durante o processo de implantação. Se a chave tiver sido comprometida, é possível gerá-la novamente reiniciando o Lenovo XClarity Management Hub.

Gerando novamente o certificado de servidor autoassinado para XClarity Management Hub para dispositivos cliente de borda

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

Antes de iniciar

Atenção: Se você gerar novamente o certificado de servidor XClarity Management Hub usando uma nova CA raiz, o XClarity Management Hub perderá sua conexão com os dispositivos gerenciados, e você deverá gerenciar novamente os dispositivos. Se você gerar novamente o certificado de servidor XClarity Management Hub assinado externamente sem alterar a CA raiz (por exemplo, quando o certificado expirou), não será necessário gerenciar os dispositivos novamente.

Sobre esta tarefa

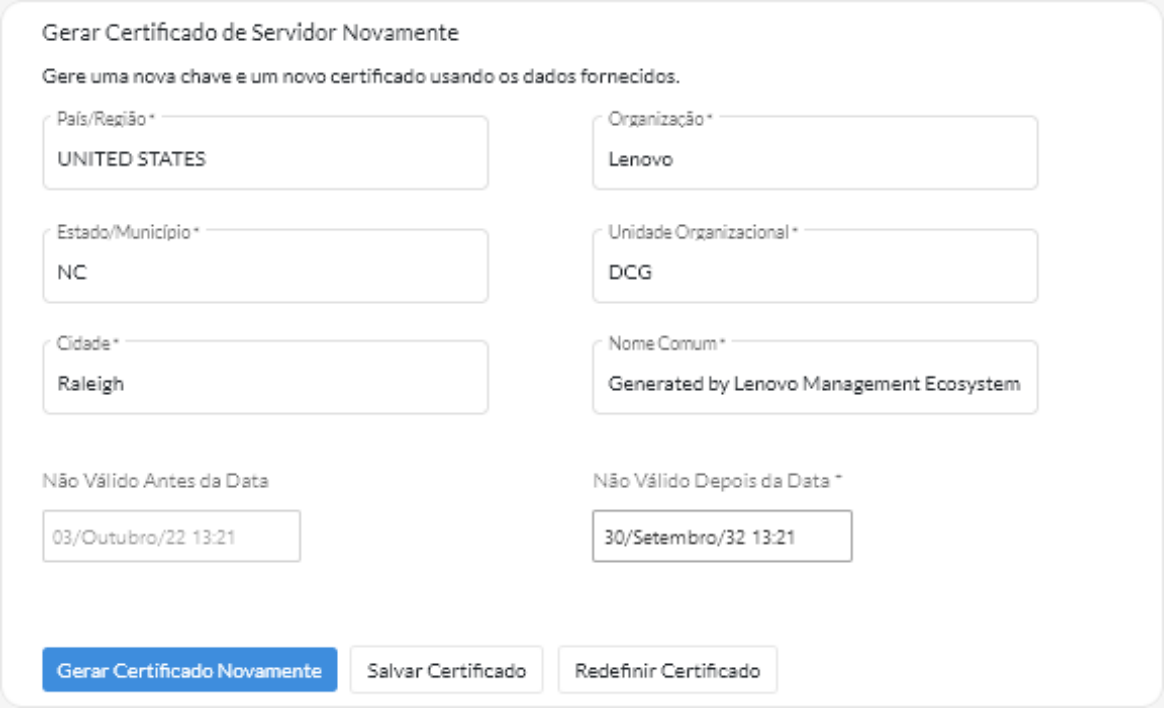
O certificado do servidor que está atualmente em uso, autoassinado ou assinado externamente, permanecerá em uso até que um novo certificado do servidor seja gerado, assinado e instalado.

Importante: Quando o certificado do servidor é modificado, o hub de gerenciamento é reiniciado, e todas as sessões do usuário são encerradas. Os usuários devem fazer login novamente para continuar trabalhando na interface da Web.

Procedimento

Para gerar um certificado de servidor autoassinado XClarity Management Hub, conclua as etapas a seguir.

Etapa 1. Na barra de menus do XClarity Management Hub, clique em **Segurança ( ) → Certificado do Servidor** para exibir o cartão **Gerar Novamente Certificado Autoassinado**.



Etapa 2. No cartão **Gerar Certificado de Servidor Autoassinado Novamente**, 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.

  Nota: Atualmente, esse atributo não afeta o certificado.
- Data e hora em que o certificado do servidor não será mais válido.

  Nota: Atualmente, esses atributos não afetam o certificado.

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

Etapa 3. Clique em **Gerar Certificado do Servidor Autoassinado Novamente** para gerar novamente o certificado autoassinado e, em seguida, clique em **Gerar Certificado Novamente** para confirmar. O hub de gerenciamento é reiniciado e todas as sessões de usuário estabelecidas são encerradas.

Etapa 4. Faça login novamente no navegador da web.

Depois de concluir

É possível executar as ações a seguir a partir do cartão Gerar Certificado de Servidor Autoassinado 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.

Instalando um certificado de servidor assinado externamente confiável para XClarity Management Hub para dispositivos cliente de borda

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.

Antes de iniciar

Atenção:

- Se você instalar um certificado de servidor Lenovo XClarity Management Hub assinado externamente usando uma nova CA raiz, o XClarity Management Hub perderá sua conexão com os dispositivos gerenciados, e você deverá gerenciar novamente os dispositivos. Se você instalar um certificado de servidor Lenovo XClarity Management Hub assinado externamente sem alterar a CA raiz (por exemplo, quando o certificado expirou), não será necessário gerenciar os dispositivos novamente.
- Se novos dispositivos forem adicionados após a CSR ser gerada e antes que o certificado do servidor assinado seja importado, esses dispositivos deverão ser reiniciados para receber o novo certificado do servidor.

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 Lenovo XClarity Management Hub, 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 para um navegador da Web para Lenovo XClarity Management Hub para dispositivos cliente de borda).

O XClarity Management Hub 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.

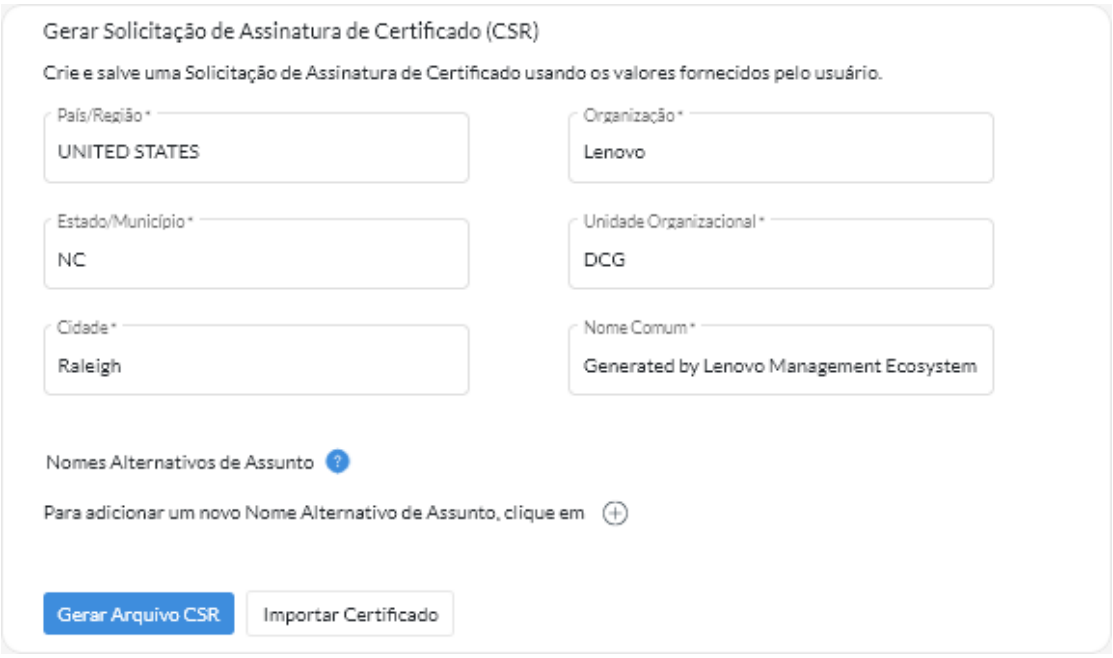
Importante: Quando o certificado do servidor for modificado, todas as sessões do usuário estabelecidas deverão aceitar o novo certificado clicando em CTRL + F5 para atualizar o navegador da Web e restabelecer a conexão com o XClarity Management Hub.

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 Management Hub, clique em **Segurança (⚙) → Certificado do Servidor** para exibir o cartão 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.

     Nota: Atualmente, esse atributo não afeta o certificado.
   - (Opcional) Nomes alternativos de assunto que serão personalizados, excluídos e adicionados à extensão X.509 "subjectAltName" quando a CSR for gerada. Os nomes alternativos de assunto especificados são validados (com base no tipo especificado) e adicionados à CSR somente depois que você gera a CSR. Por padrão, XClarity Management Hub 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 Management Hub.

Atenção: Os nomes alternativos de assunto devem incluir o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do hub de gerenciamento, e o nome do assunto deve ser definido como o FQDN do hub de gerenciamento. Verifique se esses campos obrigatórios estão presentes e corretos antes de iniciar o processo de CSR para assegurar que o certificado resultante seja concluído. Dados de certificado ausentes podem resultar em conexões que não são confiáveis ao tentar conectar o hub de gerenciamento ao Lenovo XClarity Orchestrator.

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)

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 Management Hub 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 Management Hub.

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.

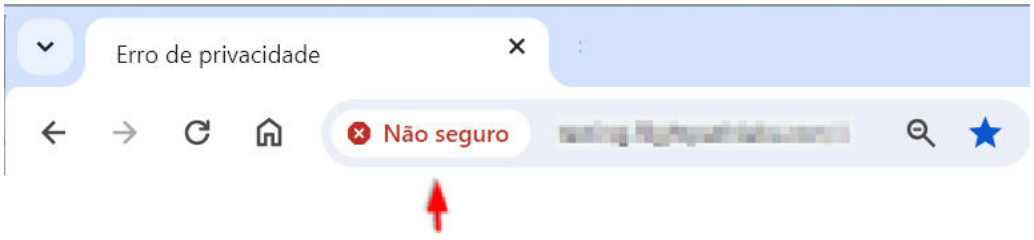
Importando o certificado do servidor para um navegador da Web para Lenovo XClarity Management Hub para dispositivos cliente de borda

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 a fim de evitar mensagens de aviso de segurança do navegador da Web ao acessar o Lenovo XClarity Management Hub.

Procedimento

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

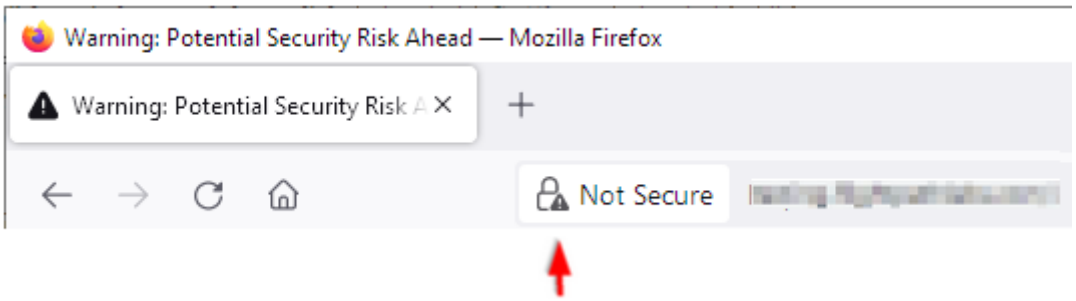
- **Chrome**
  1. Exporte o certificado do servidor Lenovo XClarity Management Hub.
     a. Clique no ícone de aviso "Não seguro" na barra de endereços superior, por exemplo:



b. Clique em **Certificado não é válido** para exibir a caixa de diálogo Certificado.
c. Clique na guia **Detalhes**.
d. Clique em **Exportar**.
e. Especifique o nome e o local do arquivo de certificado e clique em **Salvar** para exportar o certificado.
f. Feche a caixa de diálogo Visualizador de certificados.

2. Importe o certificado de servidor Lenovo XClarity Management Hub 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** para abrir a página Configurações.
b. Clique em **Privacidade e Segurança** e, em seguida, em **Segurança** para exibir a página Segurança.
c. Role para a seção **Avançado** e, em seguida, clique em **Gerenciar certificados de dispositivo**.
d. Clique em **Importar** e clique em **Avançar**.
e. Selecione o arquivo de certificado que você exportou anteriormente e clique em **Avançar**.
f. Escolha onde armazenar o certificado e clique em **Avançar**.
g. Clique em **Concluir**.
h. Feche e abra novamente o navegador Chrome e, em seguida, abra o Lenovo XClarity Management Hub.

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



b. Clique em **Conexão não segura** e, em seguida, clique em **Mais informações**.
c. Clique em **Exibir Certificado**.
d. Role para baixo até a seção **Diversos** e clique no link **PEM (cert)** para salvar o arquivo no sistema local.

2. Importe o certificado de servidor Lenovo XClarity Management Hub para a lista de certificados confiáveis de autoridade raiz de seu navegador.
a. Abra o navegador e clique em **Ferramentas → Configurações**. Depois, clique em **Privacidade e Segurança**.
b. Role para baixo para a seção **Segurança**.
c. Clique em **Exibir certificados** para exibir a caixa de diálogo Gerenciador de Certificados.
d. Clique na guia **Seus Certificados**.
e. Clique em **Importar** e vá até o local onde o certificado foi baixado.
f. Selecione o certificado e clique em **Abrir**.
g. Feche a caixa de diálogo Gerenciador de Certificados.

Conectando o XClarity Management Hub para dispositivos cliente de borda ao XClarity Orchestrator

Depois de se registrar (conectar) o Lenovo XClarity Management Hubno Lenovo XClarity Orchestrator, é possível começar a gerenciar e monitorar seus dispositivos.

Antes de iniciar

Verifique se o XClarity Management Hub está acessível na rede em XClarity Orchestrator e se XClarity Orchestrator está acessível na rede do XClarity Management Hub.

Procedimento

Para registrar o XClarity Management Hub, conclua as seguintes etapas.

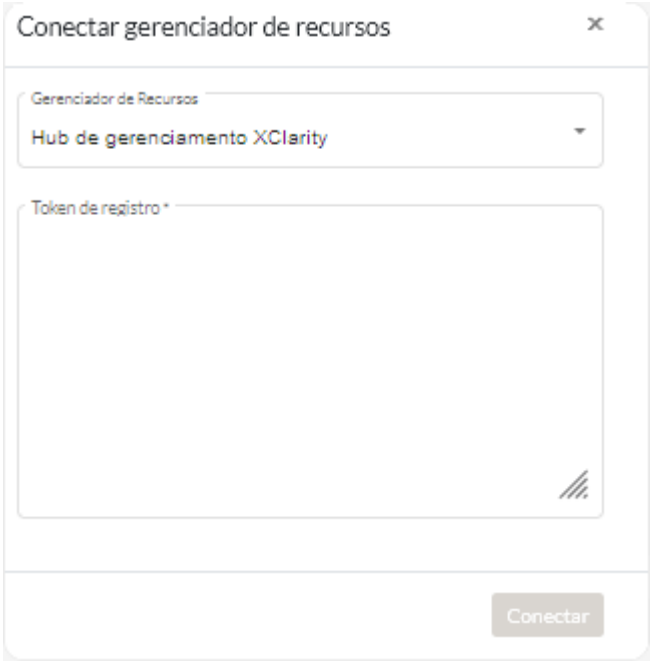
Etapa 1. Crie a chave de registro do hub de gerenciamento.

1. Na barra de menus do Management Hub, clique em **Registro** para exibir a página Registro.

2. Clique em **Criar chave de registro**.
3. Clique em **Copiar para área de transferência** para copiar a chave de registro e, em seguida, feche a caixa de diálogo.

Etapa 2. Adicione a chave de registro do hub de gerenciamento ao XClarity Orchestrator.

1. Na barra de menus do XClarity Orchestrator, clique em **Recursos ( ) → Gerenciadores de Recursos** para exibir o cartão Gerenciadores de Recursos.
2. Clique no ícone **Conectar** ( ) para exibir o gerenciador de recursos. A caixa de diálogo Conectar gerenciador de recursos.



3. Selecione **XClarity Management Hub** como o gerenciador de recursos.
4. Copie a chave de registro no campo **Token de registro**.
5. Clique em **Conectar** para exibir a caixa de diálogo Conectar Gerenciador de Recursos que contém a chave de registro do XClarity Orchestrator.
6. Clique em **Copiar para área de transferência** para copiar a chave de registro e, em seguida, feche a caixa de diálogo.

Etapa 3. Adicione a chave de registro do XClarity Orchestrator ao hub de gerenciamento.

1. Na barra de menus do Management Hub, clique em **Registro** para exibir a página Registro.
2. Clique em **Instalar chave de registro**.
3. Copie a chave de registro no campo **Token de registro**.
4. Clique em **Conectar**.

Depois de concluir

- Gerencie dispositivos usando o hub de gerenciamento (consulte Gerenciando dispositivos ThinkEdge Client na documentação online do XClarity Orchestrator).
- Exclua a chave de registro atual do hub de gerenciamento clicando em **Redefinir registro**.

Capítulo 3. Desinstalando o XClarity Management Hub para dispositivos cliente de borda

Conclua estas etapas para desinstalar um dispositivo virtual do XClarity Management Hub.

Procedimento

Para desinstalar o dispositivo virtual XClarity Management Hub, conclua as etapas a seguir.

Etapa 1. Cancele o gerenciamento de todos os dispositivos gerenciados atualmente por XClarity Management Hub.

Etapa 2. Desinstale o XClarity Management Hub, dependendo do sistema operacional.

- **ESXi**
  1. Conectar-se ao host pelo VMware vSphere Client.
  2. Clique com o botão direito na máquina virtual e clique em **Potência → Desligar**.
  3. Clique com o botão direito na máquina virtual novamente e clique em **Excluir do Disco**.

Lenovo