Execute tarefas de configuração e administração

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/pt-br/active-iq-unified-manager-918/config/concept_configure_unified_manager.html on November 13, 2026. Always check docs.netapp.com for the latest.

Índice

Execute tarefas de configuração e administração . . . 1
- Configurar o Active IQ Unified Manager . . . 1
  - Saiba mais sobre como configurar o Active IQ Unified Manager . . . 1
  - Saiba mais sobre a sequência de configuração no Active IQ Unified Manager . . . 1
  - Acesse a interface web no Active IQ Unified Manager . . . 1
  - Execute a configuração inicial da interface web do Active IQ Unified Manager . . . 2
  - Adicionar clusters ao Active IQ Unified Manager . . . 4
  - Configurar notificações . . . 6
  - Alterar a senha do usuário local no Active IQ Unified Manager . . . 15
  - Defina o tempo limite de inatividade da sessão no Active IQ Unified Manager . . . 15
  - Defina o tempo limite da sessão usando a CLI no Active IQ Unified Manager . . . 16
  - Alterar o nome do host do Unified Manager . . . 16
  - Ative e desative o gerenciamento de storage baseado em políticas no Active IQ Unified Manager . . . 21
- Configurar o Active IQ Unified Manager backup . . . 22
- Gerenciar configurações de recursos . . . 22
  - Saiba mais sobre as configurações de recursos no Active IQ Unified Manager . . . 22
  - Habilite o gerenciamento de storage baseado em políticas no Active IQ Unified Manager . . . 23
  - Saiba mais sobre o recurso API Gateway no Active IQ Unified Manager . . . 23
  - Especifique o tempo limite de inatividade no Active IQ Unified Manager . . . 24
  - Ative os eventos do portal Active IQ no Active IQ Unified Manager . . . 24
  - Ative e desative as configurações de segurança para conformidade no Active IQ Unified Manager . . . 25
  - Ativar e desativar o upload de scripts no Active IQ Unified Manager . . . 26
  - Adicione um banner de login no Active IQ Unified Manager . . . 26
- Use o console de manutenção . . . 26
  - Saiba mais sobre o console de manutenção no Active IQ Unified Manager . . . 26
  - Saiba mais sobre o usuário de manutenção no Active IQ Unified Manager . . . 27
  - Funcionalidades de diagnóstico do usuário no Active IQ Unified Manager . . . 27
  - Acesse o console de manutenção no Active IQ Unified Manager . . . 27
  - Acesse o console de manutenção usando o console da VM do vSphere no Active IQ Unified Manager . . . 28
  - Menus do console de manutenção . . . 28
  - Altere a senha do usuário de manutenção no Windows no Active IQ Unified Manager . . . 34
  - Altere a senha umadmin do Active IQ Unified Manager em sistemas Linux . . . 34
  - Altere as portas que o Active IQ Unified Manager utiliza para os protocolos HTTP e HTTPS . . . 35
  - Adicionar interfaces de rede ao Active IQ Unified Manager . . . 35
  - Regere o certificado de cliente no Active IQ Unified Manager . . . 36
  - Adicionar espaço de disco . . . 36
- Gerencie o acesso do usuário . . . 40
  - Adicionar usuários . . . 40
  - Editar configurações de usuário no Active IQ Unified Manager . . . 41
  - Visualizar usuários no Active IQ Unified Manager . . . 42
  - Excluir usuários ou grupos no Active IQ Unified Manager . . . 42
  - Saiba mais sobre controle de acesso baseado em funções no Active IQ Unified Manager . . . 43
  - Saiba mais sobre os tipos de usuários no Active IQ Unified Manager . . . 43

Saiba mais sobre as funções de usuário no Active IQ Unified Manager . . . 44
Saiba mais sobre funções e capacidades de usuário no Active IQ Unified Manager . . . 45
Gerenciar configurações de autenticação SAML . . . 46
Ative a autenticação SAML no Active IQ Unified Manager . . . 46
Utilize um provedor de identidade no Active IQ Unified Manager . . . 47
Ative a autenticação SAML no Active IQ Unified Manager . . . 48
Altere o provedor de identidade de autenticação SAML no Active IQ Unified Manager . . . 49
Atualize as configurações de autenticação SAML após uma alteração no certificado de segurança do Active IQ Unified Manager . . . 50
Desative a autenticação SAML no Active IQ Unified Manager . . . 51
Desative a autenticação SAML no console de manutenção do Active IQ Unified Manager . . . 51
Utilize a página de autenticação SAML no Active IQ Unified Manager . . . 52
Gerenciar autenticação . . . 53
Editar servidores de autenticação no Active IQ Unified Manager . . . 53
Excluir servidores de autenticação no Active IQ Unified Manager . . . 53
Autentique com o Active Directory ou OpenLDAP no Active IQ Unified Manager . . . 54
Registro de auditoria . . . 54
Utilize a página de autenticação remota no Active IQ Unified Manager . . . 57
Gerenciar certificados de segurança . . . 60
Visualize o certificado de segurança HTTPS no Active IQ Unified Manager . . . 60
Faça o download de uma solicitação de assinatura de certificado HTTPS no Active IQ Unified Manager . . . 60
Instale um certificado HTTPS assinado por uma Autoridade Certificadora (CA) no Active IQ Unified Manager . . . 61
Saiba mais sobre certificados HTTPS gerados usando ferramentas externas no Active IQ Unified Manager Unified Manager . . . 62
Descrições de páginas para gerenciamento de certificados . . . 64

Execute tarefas de configuração e administração

Configurar o Active IQ Unified Manager

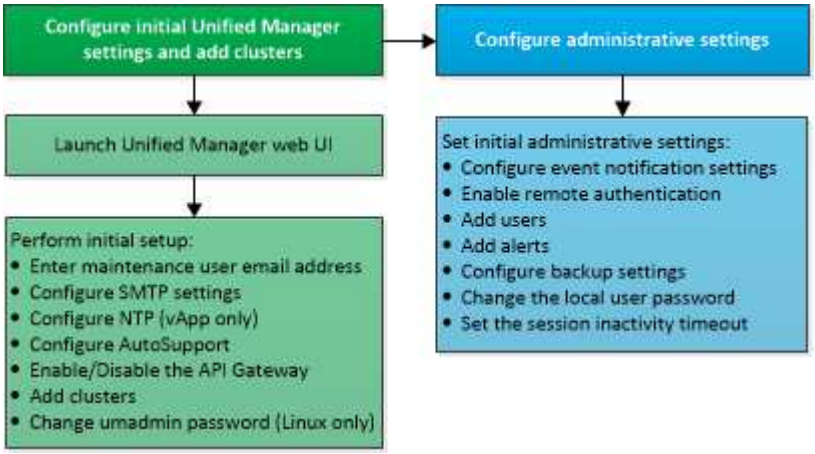
Saiba mais sobre como configurar o Active IQ Unified Manager

Após instalar o Active IQ Unified Manager (anteriormente o OnCommand Unified Manager), você deve concluir a configuração inicial (também chamada de assistente de primeira experiência) para acessar a interface de usuário da web. Em seguida, você pode realizar tarefas de configuração adicionais, como adicionar clusters, configurar a autenticação remota, adicionar usuários e adicionar alertas.

Alguns dos procedimentos descritos neste manual são necessários para concluir a configuração inicial da sua instância do Unified Manager. Outros procedimentos são configurações recomendadas que podem ser úteis para configurar sua nova instância ou que é bom conhecer antes de iniciar o monitoramento regular dos seus sistemas ONTAP.

Saiba mais sobre a sequência de configuração no Active IQ Unified Manager

O fluxo de trabalho de configuração descreve as tarefas que você deve executar antes de poder usar o Unified Manager.



Acesse a interface web no Active IQ Unified Manager

Após instalar o Unified Manager, você poderá acessar a interface de usuário da web para configurar o Unified Manager e começar a monitorar seus sistemas ONTAP.

Antes de começar

- Se esta for a primeira vez que você está acessando a interface de usuário da web, você deve fazer login como o usuário de manutenção (ou o usuário umadmin para instalações do Linux).
- Se você planeja permitir que os usuários acessem o Unified Manager usando o nome curto em vez de usar o domínio totalmente qualificado (FQDN) ou o endereço IP, sua configuração de rede precisa resolver esse nome curto para um FQDN válido.
- Se o servidor usar um certificado digital autoassinado, o navegador poderá exibir um aviso indicando que o certificado não é confiável. Você pode aceitar o risco para continuar acessando ou instalar um certificado

digital assinado por uma Autoridade Certificadora (CA) para autenticação do servidor.

Passos

1. Inicie a interface web do Unified Manager no seu navegador usando a URL exibida no final da instalação. A URL é o endereço IP ou o nome de domínio totalmente qualificado (FQDN) do servidor Unified Manager.

   O link está no seguinte formato: `https://URL`.

2. Faça login na interface da web do Unified Manager usando suas credenciais de usuário de manutenção.

> Se você fizer três tentativas consecutivas sem sucesso de login na interface de usuário da web em uma hora, seu acesso ao sistema será bloqueado, e você precisará entrar em contato com o administrador do sistema. Isso se aplica somente a usuários locais.

Execute a configuração inicial da interface web do Active IQ Unified Manager

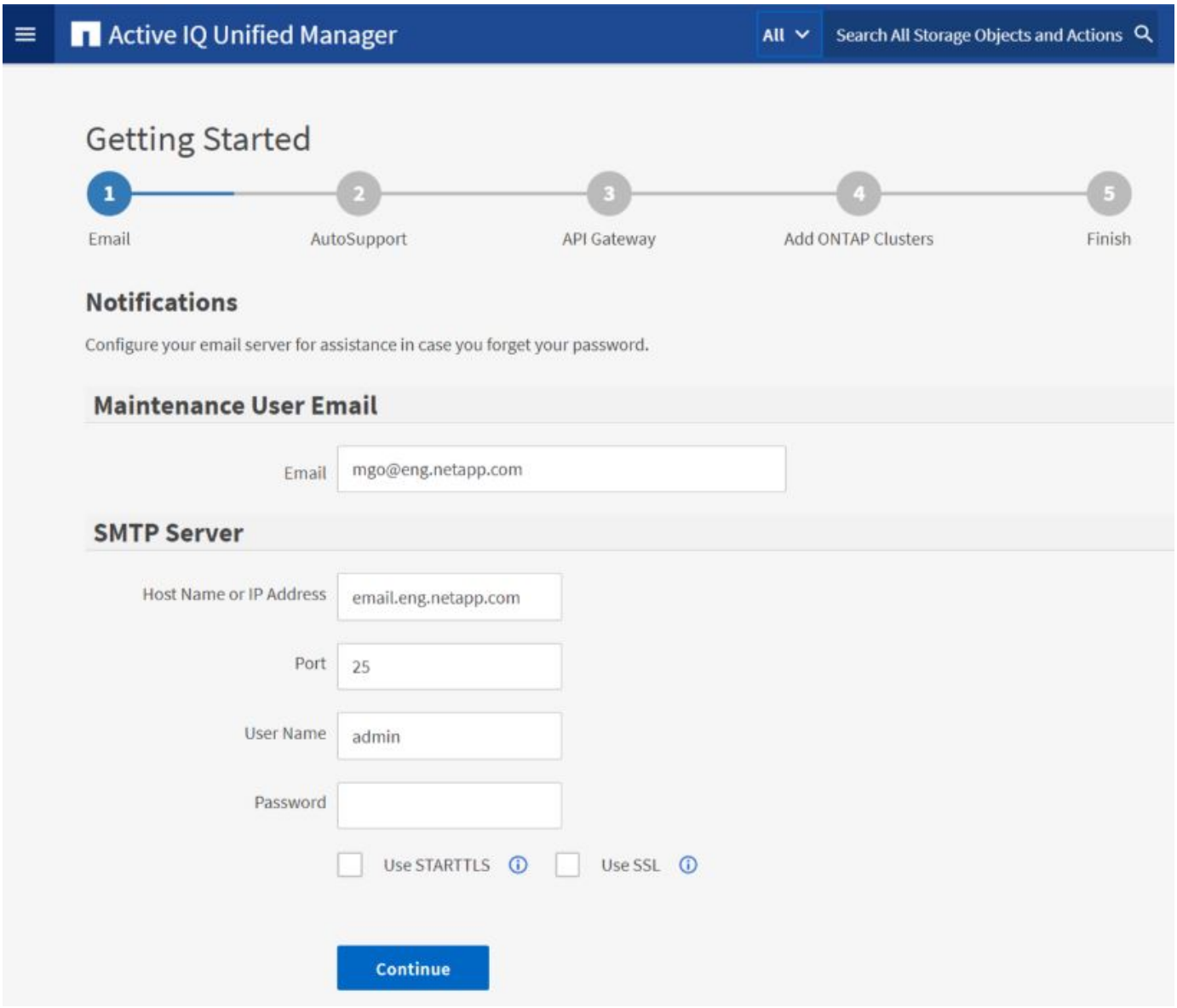
Para usar o Unified Manager, você deve primeiro configurar as opções de configuração inicial, incluindo o servidor NTP, o endereço de e-mail do usuário de manutenção, o host do servidor SMTP e a adição de clusters do ONTAP.

Antes de começar

Você deve ter realizado as seguintes operações:

- Iniciou a interface da web do Unified Manager usando a URL fornecida após a instalação
- Você fez login usando o nome de usuário e a senha de manutenção (usuário umadmin para instalações Linux) criados durante a instalação

A página Active IQ Unified ManagerGetting Started aparece somente quando você acessa a interface web pela primeira vez. A página abaixo é de uma instalação no VMware.



Se quiser alterar qualquer uma dessas opções posteriormente, você poderá selecionar sua escolha nas opções Gerais no painel de navegação à esquerda do Unified Manager. Observe que a configuração de NTP é exclusiva para instalações VMware e pode ser alterada posteriormente usando o console de manutenção do Unified Manager.

Passos

1. Na página de Configuração Inicial do Active IQ Unified Manager, insira o endereço de e-mail do usuário de manutenção, o nome do host do servidor SMTP, quaisquer opções adicionais de SMTP e o servidor NTP (somente para instalações VMware). Em seguida, clique em **Continuar**.

   Se você selecionou a opção **Usar STARTTLS** ou **Usar SSL**, uma página de certificado é exibida após clicar no botão **Continuar**. Verifique os detalhes do certificado e aceite-o para prosseguir com as configurações iniciais da interface web.

2. Na página AutoSupport, clique em **Agree and Continue** para habilitar o envio de mensagens de AutoSupport do Unified Manager para o NetAppActive IQ.

   Se você precisar designar um proxy para fornecer acesso à internet para enviar conteúdo do AutoSupport, ou se quiser desativar o AutoSupport, use a opção **Geral** > **AutoSupport** na interface da web.

3. Em sistemas Red Hat, altere a senha do usuário umadmin da string padrão “admin” para uma string personalizada.
4. Na página Configurar Gateway de API, selecione se deseja usar o recurso Gateway de API que permite ao Unified Manager gerenciar os clusters do ONTAP que você planeja monitorar usando as APIs REST do ONTAP. Em seguida, clique em **Continuar**.

   Você pode ativar ou desativar essa configuração posteriormente na interface da web em **Geral** > **Configurações de recursos** > **Gateway de API**. Para obter mais informações sobre as APIs, consulte "Primeiros passos com as APIs REST do Active IQ Unified Manager".

5. Adicione os clusters que você deseja que o Unified Manager gerencie e clique em **Avançar**. Para cada cluster que você planeja gerenciar, você deve ter o nome do host ou o endereço IP de gerenciamento do cluster (IPv4 ou IPv6), juntamente com o nome de usuário e as credenciais de senha; o usuário deve ter a função “admin”.

   Esta etapa é opcional. Você pode adicionar clusters posteriormente na interface de usuário da web em **Gerenciamento de armazenamento** > **Configuração de cluster**.

6. Na página de resumo, verifique se todas as configurações estão corretas e clique em **Concluir**.

A página de introdução é fechada e a página Dashboard do Unified Manager é exibida.

Adicionar clusters ao Active IQ Unified Manager

Você pode adicionar um cluster ao Active IQ Unified Manager para que você possa monitorar o cluster. Isso inclui a capacidade de obter informações do cluster, como a integridade, a capacidade, o desempenho e a configuração do cluster, para que você possa encontrar e resolver quaisquer problemas que possam ocorrer.

Antes de começar

- Você precisa ter a função de Application Administrator ou Storage Administrator.
- Você precisa ter as seguintes informações:
  - O Unified Manager oferece suporte a clusters ONTAP locais, ao ONTAP Select e ao Cloud Volumes ONTAP.
  - Nome do host ou endereço IP de gerenciamento do cluster

    O nome do host é o FQDN ou nome abreviado que o Unified Manager usa para se conectar ao cluster. O nome do host deve ser resolvido para o endereço IP de gerenciamento do cluster.

    O endereço IP de gerenciamento do cluster deve ser a LIF de gerenciamento do cluster da máquina virtual de armazenamento administrativa (SVM). Se você usar uma LIF de gerenciamento de nó, a operação falhará.

  - O cluster deve estar executando o software ONTAP versão 9.1 ou superior.
  - Nome de usuário e senha do administrador do ONTAP

    Esta conta deve ter a função *admin* com acesso ao aplicativo definido como *ontapi*, *amqp*, *console* e *http*.

  - O número da porta para conectar-se ao cluster usando o protocolo HTTPS (normalmente a porta 443)

- Você possui os certificados necessários:

  Certificado SSL (HTTPS): este certificado pertence ao Unified Manager. Um certificado SSL (HTTPS) autoassinado padrão é gerado com uma nova instalação do Unified Manager. NetApp recomenda que você o atualize para um certificado assinado por CA para maior segurança. Se o certificado do servidor expirar, você deverá regenerá-lo e reiniciar o Unified Manager para que os serviços incorporem o novo certificado. Para obter mais informações sobre como regenerar o certificado SSL, consulte "Gerando um certificado de segurança HTTPS".

  Certificado EMS: Este certificado pertence ao Unified Manager. Ele é usado durante a autenticação para notificações EMS recebidas do ONTAP.

  Certificados para comunicação TLS mútua: utilizados durante a comunicação TLS mútua entre o Unified Manager e o ONTAP. A autenticação baseada em certificado é habilitada para um cluster, dependendo da versão do ONTAP. Se o cluster que executa a versão do ONTAP for inferior a 9.5, a autenticação baseada em certificado não será habilitada.

  A autenticação baseada em certificado não é habilitada automaticamente para um cluster se você estiver atualizando uma versão mais antiga do Unified Manager. No entanto, você pode habilitá-la modificando e salvando os detalhes do cluster. Se o certificado expirar, você deverá regenerá-lo para incorporar o novo certificado. Para obter mais informações sobre como visualizar e regenerar o certificado, consulte "Editando clusters".

  - Você pode adicionar um cluster pela interface de usuário da web, e a autenticação baseada em certificado é ativada automaticamente.
  - Você pode adicionar um cluster pela CLI do Unified Manager; a autenticação baseada em certificado não está habilitada por padrão. Se você adicionar um cluster usando a CLI do Unified Manager, precisará editar o cluster usando a interface do usuário do Unified Manager. Consulte "Comandos da CLI do Unified Manager suportados" para adicionar um cluster usando a CLI do Unified Manager.
  - Se a autenticação baseada em certificado estiver habilitada para um cluster e você fizer o backup do Unified Manager de um servidor e restaurá-lo em outro servidor do Unified Manager em que o nome do host ou o endereço IP foi alterado, o monitoramento do cluster poderá falhar. Para evitar essa falha, edite e salve os detalhes do cluster. Para obter mais informações sobre como editar os detalhes do cluster, consulte "Editando clusters".

  + **Certificados de cluster**: Este certificado pertence ao ONTAP. Não é possível adicionar um cluster ao Unified Manager com um certificado expirado e, caso o certificado já tenha expirado, você deve regenerá-lo antes de adicionar o cluster. Para obter informações sobre a geração de certificados, consulte o artigo da base de conhecimento (KB) "Como renovar um certificado autoassinado do ONTAP na interface de usuário do System Manager".

- Você precisa ter espaço suficiente no servidor do Unified Manager. A adição de um cluster ao servidor não será possível se mais de 90% do espaço no diretório do banco de dados já estiver ocupado.

Para uma configuração do MetroCluster, você precisa adicionar os clusters local e remoto, e ambos devem estar configurados corretamente.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de cluster**.

2. Na página de Configuração do Cluster, clique em **Adicionar**.
3. Na caixa de diálogo Add Cluster, especifique os valores necessários, como o nome do host ou o endereço IP do cluster, o nome de usuário, a senha e o número da porta.

   Você pode alterar o endereço IP de gerenciamento do cluster de IPv6 para IPv4 ou de IPv4 para IPv6. O novo endereço IP será refletido na grade do cluster e na página de configuração do cluster após a conclusão do próximo ciclo de monitoramento.

4. Clique em **Enviar**.
5. Na caixa de diálogo Authorize Host, clique em **View Certificate** para visualizar as informações do certificado do cluster.
6. Clique em **Yes**.

   Após salvar os detalhes do cluster, você poderá visualizar o certificado para a comunicação TLS mútua de um cluster.

   Se a autenticação baseada em certificado não estiver habilitada, o Unified Manager verificará o certificado apenas quando o cluster for adicionado inicialmente. O Unified Manager não verifica o certificado para cada chamada de API ao ONTAP.

Após todos os objetos de um novo cluster serem descobertos, o Unified Manager começa a coletar dados históricos de desempenho dos 15 dias anteriores. Essas estatísticas são coletadas usando a funcionalidade de coleta de continuidade de dados. Esse recurso fornece a você mais de duas semanas de informações de desempenho de um cluster imediatamente após sua adição. Após a conclusão do ciclo de coleta de continuidade de dados, os dados de desempenho do cluster em tempo real são coletados, por padrão, a cada cinco minutos.

Como a coleta de 15 dias de dados de desempenho exige muito da CPU, recomenda-se que você adicione novos clusters de forma escalonada para que as sondagens da coleta de continuidade de dados não sejam executadas em muitos clusters ao mesmo tempo. Além disso, se você reiniciar o Unified Manager durante o período de coleta de continuidade de dados, a coleta será interrompida e você verá lacunas nos gráficos de desempenho referentes ao período ausente.

Se você receber uma mensagem de erro informando que não é possível adicionar o cluster, verifique se os relógios dos dois sistemas não estão sincronizados e se a data de início do certificado HTTPS do Unified Manager é posterior à data no cluster. Você deve garantir que os relógios estejam sincronizados usando o NTP ou um serviço similar.

Informações relacionadas

"Instalando um certificado HTTPS assinado e retornado por uma Autoridade Certificadora (CA)"

Configurar notificações

Configure o Active IQ Unified Manager para enviar notificações de alerta

Você pode configurar o Unified Manager para enviar notificações que alertem você sobre eventos em seu ambiente. Antes que as notificações possam ser enviadas, você deve configurar várias outras opções do Unified Manager.

Antes de começar

Você precisa ter a função de Application Administrator.

Após implantar o Unified Manager e concluir a configuração inicial, você deve considerar configurar seu ambiente para disparar alertas e gerar e-mails de notificação ou traps SNMP com base no recebimento de eventos.

Passos

1. "Configure as definições de notificação de eventos".

   Se você quiser que as notificações de alerta sejam enviadas quando determinados eventos ocorrerem em seu ambiente, será necessário configurar um servidor SMTP e fornecer um endereço de e-mail a partir do qual a notificação de alerta será enviada. Se você quiser usar traps SNMP, poderá selecionar essa opção e fornecer as informações necessárias.

2. "Habilitar autenticação remota".

   Se você quiser que usuários remotos do LDAP ou do Active Directory acessem a instância do Unified Manager e recebam notificações de alerta, você deverá habilitar a autenticação remota.

3. "Adicionar servidores de autenticação".

   Você pode adicionar servidores de autenticação para que usuários remotos no servidor de autenticação possam acessar o Unified Manager.

4. "Adicionar usuários".

   Você pode adicionar vários tipos diferentes de usuários locais ou remotos e atribuir funções específicas. Ao criar um alerta, você atribui um usuário para receber as notificações de alerta.

5. "Adicionar alertas".

   Depois de adicionar o endereço de e-mail para envio de notificações, adicionar os usuários que receberão as notificações, configurar as definições de rede e configurar as opções SMTP e SNMP necessárias para o seu ambiente, você poderá atribuir alertas.

Configure as definições de notificação de eventos no Active IQ Unified Manager

Você pode configurar o Unified Manager para enviar notificações de alerta quando um evento é gerado ou quando um evento é atribuído a um usuário. Você pode configurar o servidor SMTP usado para enviar o alerta e definir vários mecanismos de notificação, por exemplo, as notificações de alerta podem ser enviadas como e-mails ou traps SNMP.

Antes de começar

Você precisa ter as seguintes informações:

- Endereço de e-mail a partir do qual a notificação de alerta é enviada

  O endereço de e-mail aparece no campo “From” nas notificações de alerta enviadas. Se o e-mail não puder ser entregue por algum motivo, esse endereço de e-mail também será usado como destinatário para mensagens não entregues.

- Nome do host do servidor SMTP, nome de usuário e senha para acessar o servidor

- Nome do host ou endereço IP do host de destino do trap que receberá o trap SNMP, juntamente com a versão SNMP, a porta de saída do trap, a comunidade e outros valores de configuração SNMP necessários

  Para especificar vários destinos de traps, separe cada host com uma vírgula. Nesse caso, todas as outras configurações de SNMP, como versão e porta de trap de saída, devem ser as mesmas para todos os hosts da lista.

Você precisa ter a função de Application Administrator ou Storage Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Notificações**.
2. Na página de Notificações, configure as definições apropriadas.

   Notas:

   - Se o campo "De" estiver preenchido automaticamente com o endereço "ActiveIQUnifiedManager@localhost.com", você deve alterá-lo para um endereço de e-mail real e funcional para garantir que todas as notificações por e-mail sejam entregues com sucesso.
   - Caso o nome do host do servidor SMTP não possa ser resolvido, você pode especificar o endereço IP (IPv4 ou IPv6) do servidor SMTP em vez do nome do host.
3. Clique em **Salvar**.
4. Se você selecionou a opção **Usar STARTTLS** ou **Usar SSL**, uma página de certificado é exibida após clicar no botão **Salvar**. Verifique os detalhes do certificado e aceite-o para salvar as configurações de notificação.

   Você pode clicar no botão **Exibir detalhes do certificado** para visualizar os detalhes do certificado. Se o certificado atual estiver expirado, desmarque a caixa **Usar STARTTLS** ou **Usar SSL**, salve as configurações de notificação e marque novamente a caixa **Usar STARTTLS** ou **Usar SSL** para visualizar um novo certificado.

Ative a autenticação remota no Active IQ Unified Manager

Você pode habilitar a autenticação remota para que o servidor do Unified Manager possa se comunicar com seus servidores de autenticação. Os usuários do servidor de autenticação podem acessar a interface gráfica do Unified Manager para gerenciar objetos de storage e dados.

Antes de começar

Você precisa ter a função de Application Administrator.

> O servidor do Unified Manager deve estar conectado diretamente ao servidor de autenticação. Você deve desativar quaisquer clientes LDAP locais, como SSSD (System Security Services Daemon) ou NSLCD (Name Service LDAP Caching Daemon).

Você pode habilitar a autenticação remota usando o Open LDAP ou o Active Directory. Se a autenticação remota estiver desabilitada, os usuários remotos não poderão acessar o Unified Manager.

A autenticação remota é suportada via LDAP e LDAPS (Secure LDAP). O Unified Manager utiliza a porta 389 como padrão para comunicação não segura e a porta 636 como padrão para comunicação segura.

O certificado utilizado para autenticar usuários deve estar em conformidade com o formato X.509.

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Marque a caixa **Ativar autenticação remota…**.
3. No campo Serviço de Autenticação, selecione o tipo de serviço e configure o serviço de autenticação.

Para o tipo de autenticação…	Insira as seguintes informações…
Active Directory	• Nome do administrador do servidor de autenticação em um dos seguintes formatos: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (usando a notação LDAP apropriada) • Senha de administrador • Nome diferenciado base (usando a notação LDAP apropriada)
Open LDAP	• Nome diferenciado de bind (na notação LDAP apropriada) • Senha de vinculação • Nome diferenciado base

Se a autenticação de um usuário do Active Directory demorar muito ou expirar, o servidor de autenticação provavelmente está demorando muito para responder. Desativar o suporte a grupos aninhados no Unified Manager pode reduzir o tempo de autenticação.

Se você selecionar a opção Usar conexão segura para o servidor de autenticação, o Unified Manager se comunicará com o servidor de autenticação usando o protocolo Secure Sockets Layer (SSL).

4. **Opcional:** adicione servidores de autenticação e teste a autenticação.
5. Clique em **Salvar**.

Desative grupos aninhados na autenticação remota no Active IQ Unified Manager

Se você tiver a autenticação remota habilitada, poderá desabilitar a autenticação de grupos aninhados para que somente usuários individuais, e não membros de grupos, possam se autenticar remotamente no Unified Manager. Você pode desabilitar grupos aninhados quando quiser melhorar o tempo de resposta da autenticação do Active Directory.

Antes de começar

- Você precisa ter a função de Application Administrator.
- Desativar grupos aninhados só se aplica ao uso do Active Directory.

Desativar o suporte a grupos aninhados no Unified Manager pode reduzir o tempo de autenticação. Se o suporte a grupos aninhados estiver desativado e um grupo remoto for adicionado ao Unified Manager, os usuários individuais deverão ser membros do grupo remoto para se autenticarem no Unified Manager.

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Marque a caixa de seleção para **Disable Nested Group Lookup**.
3. Clique em **Salvar**.

Configure os serviços de autenticação no Active IQ Unified Manager

Os serviços de autenticação permitem a autenticação de usuários remotos ou grupos remotos em um servidor de autenticação antes de conceder a eles acesso ao Unified Manager. Você pode autenticar usuários usando serviços de autenticação predefinidos, como Active Directory ou OpenLDAP, ou configurando seu próprio mecanismo de autenticação.

Antes de começar

- Você deve ter habilitado a autenticação remota.
- Você precisa ter a função de Application Administrator.

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Selecione um dos seguintes serviços de autenticação:

Se você selecionar…	Então faça isso…
Active Directory	a. Digite o nome do administrador e a senha. b. Especifique o nome diferenciado base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, então o nome diferenciado base será **cn=ou,dc=domain,dc=com**.
O OpenLDAP	a. Insira o nome diferenciado de vinculação e a senha de vinculação. b. Especifique o nome diferenciado base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, então o nome diferenciado base será **cn=ou,dc=domain,dc=com**.

Se você selecionar…	Então faça isso…
Outros	a. Insira o nome diferenciado de vinculação e a senha de vinculação. b. Especifique o nome diferenciado base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, então o nome diferenciado base será **cn=ou,dc=domain,dc=com**. c. Especifique a versão do protocolo LDAP compatível com o servidor de autenticação. d. Insira o nome de usuário, a associação a grupos, o grupo de usuários e os atributos do membro.

Se você quiser modificar o serviço de autenticação, deverá excluir todos os servidores de autenticação existentes e, em seguida, adicionar novos servidores de autenticação.

3. Clique em **Salvar**.

Adicionar servidores de autenticação ao Active IQ Unified Manager

Você pode adicionar servidores de autenticação e habilitar a autenticação remota no servidor de gerenciamento para que usuários remotos no servidor de autenticação possam acessar o Unified Manager.

Antes de começar

- As informações a seguir devem estar disponíveis:
  - Nome do host ou endereço IP do servidor de autenticação
  - Número da porta do servidor de autenticação
- Você deve ter habilitado a autenticação remota e configurado seu serviço de autenticação para que o servidor de gerenciamento possa autenticar usuários ou grupos remotos no servidor de autenticação.
- Você precisa ter a função de Application Administrator.

Se o servidor de autenticação que você está adicionando fizer parte de um par de alta disponibilidade (HA) (usando o mesmo banco de dados), você também poderá adicionar o servidor de autenticação parceiro. Isso permite que o servidor de gerenciamento se comunique com o parceiro quando um dos servidores de autenticação estiver inacessível.

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Ative ou desative a opção **Use secure connection**:

Se você quiser…	Então faça isso…
Habilite-o	a. Selecione a opção **Usar conexão segura**. b. Na área Servidores de Autenticação, clique em **Adicionar**. c. Na caixa de diálogo Adicionar Servidor de Autenticação, insira o nome de autenticação ou o endereço IP (IPv4 ou IPv6) do servidor. d. Na caixa de diálogo Authorize Host, clique em View Certificate. e. Na caixa de diálogo Exibir Certificado, verifique as informações do certificado e clique em **Fechar**. f. Na caixa de diálogo "Authorize Host", clique em **Yes**. Quando você ativa a opção **Use Secure Connection authentication**, o Unified Manager se comunica com o servidor de autenticação e exibe o certificado. O Unified Manager usa a porta 636 como porta padrão para comunicação segura e a porta 389 para comunicação não segura.
Desative-o	a. Desmarque a opção **Usar conexão segura**. b. Na área Servidores de Autenticação, clique em **Adicionar**. c. Na caixa de diálogo Adicionar servidor de autenticação, especifique o nome do host ou o endereço IP (IPv4 ou IPv6) do servidor, bem como os detalhes da porta. d. Clique em **Add**.

O servidor de autenticação que você adicionou é exibido na área Servidores.

3. Realize um teste de autenticação para confirmar que você consegue autenticar usuários no servidor de autenticação que você adicionou.

Teste a configuração dos servidores de autenticação no Active IQ Unified Manager

Você pode validar a configuração dos seus servidores de autenticação para garantir que o servidor de gerenciamento consiga se comunicar com eles. Você pode validar a configuração pesquisando um usuário remoto ou grupo remoto nos seus servidores de autenticação e autenticando esse usuário ou grupo usando as configurações definidas.

Antes de começar

- Você deve ter habilitado a autenticação remota e configurado seu serviço de autenticação para que o servidor do Unified Manager possa autenticar o usuário remoto ou o grupo remoto.
- Você deve ter adicionado seus servidores de autenticação para que o servidor de gerenciamento possa procurar o usuário remoto ou o grupo remoto nesses servidores e autenticá-los.
- Você precisa ter a função de Application Administrator.

Se o serviço de autenticação estiver configurado para o Active Directory e se você estiver validando a autenticação de usuários remotos que pertencem ao grupo primário do servidor de autenticação, as informações sobre o grupo primário não serão exibidas nos resultados da autenticação.

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Clique em **Test Authentication**.
3. Na caixa de diálogo Test User, especifique o nome de usuário e a senha do usuário remoto ou o nome do grupo remoto e clique em **Test**.

   Se você estiver autenticando um grupo remoto, não deve inserir a senha.

Adicione alertas no Active IQ Unified Manager

Você pode configurar alertas para receber notificações quando um evento específico for gerado. Você pode configurar alertas para um único recurso, para um grupo de recursos ou para eventos de um determinado tipo de gravidade. Você pode especificar a frequência com que deseja ser notificado e associar um script ao alerta.

Antes de começar

- Você precisa ter configurado as definições de notificação, como o endereço de e-mail do usuário, o servidor SMTP e o host de trap SNMP, para permitir que o servidor Active IQ Unified Manager use essas configurações para enviar notificações aos usuários quando um evento for gerado.
- Você precisa saber os recursos e eventos para os quais deseja acionar o alerta, bem como os nomes de usuário ou endereços de e-mail dos usuários que deseja notificar.
- Se você quiser que um script seja executado com base no evento, deve ter adicionado o script ao Unified Manager usando a página Scripts.
- Você precisa ter a função de Application Administrator ou Storage Administrator.

Além de criar um alerta na página de Configuração de Alertas, conforme descrito aqui, você pode criá-lo diretamente na página de detalhes do evento após receber um evento.

Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de alertas**.
2. Na página Configuração de alertas, clique em **Adicionar**.
3. Na caixa de diálogo Adicionar alerta, clique em **Nome** e insira um nome e uma descrição para o alerta.
4. Clique em **Recursos**, e selecione os recursos que deseja incluir ou excluir do alerta.

   Você pode definir um filtro especificando uma cadeia de texto no campo **Nome contém** para selecionar um grupo de recursos. Com base na cadeia de texto que você especificar, a lista de recursos disponíveis exibe apenas os recursos que correspondem à regra de filtro. A cadeia de texto que você especificar

diferencia maiúsculas de minúsculas.

Se um recurso estiver em conformidade com as regras de inclusão e exclusão que você especificou, a regra de exclusão tem precedência sobre a regra de inclusão, e o alerta não é gerado para eventos relacionados ao recurso excluído.

5. Clique em **Eventos** e selecione os eventos com base no nome do evento ou no tipo de gravidade do evento para os quais você deseja acionar um alerta.



Para selecionar mais de um evento, pressione a tecla Ctrl enquanto você faz suas seleções.

6. Clique em **Ações** e selecione os usuários que você deseja notificar, escolha a frequência de notificação, defina se um trap SNMP será enviado ao receptor de traps e atribua um script para executar quando um alerta for gerado.



Se você modificar o endereço de e-mail especificado para o usuário e reabrir o alerta para edição, o campo Nome aparecerá em branco, pois o endereço de e-mail modificado não estará mais vinculado ao usuário selecionado anteriormente. Além disso, se você modificar o endereço de e-mail do usuário selecionado na página Usuários, o endereço de e-mail modificado não será atualizado para o usuário selecionado.

Você também pode optar por notificar os usuários por meio de traps SNMP.

7. Clique em **Salvar**.

Exemplo de como adicionar um alerta

Este exemplo mostra como criar um alerta que atenda aos seguintes requisitos:

- Nome do alerta: HealthTest
- Recursos: inclui todos os volumes cujo nome contém “abc” e exclui todos os volumes cujo nome contém “xyz”
- Eventos: inclui todos os eventos críticos de saúde
- Ações: inclui "sample@domain.com", um script “Test” e o usuário deve ser notificado a cada 15 minutos

Execute as etapas a seguir na caixa de diálogo Add Alert:

Passos

1. Clique em **Nome** e digite **HealthTest** no campo **Nome do alerta**.
2. Clique em **Resources** e, na guia Include, selecione **Volumes** na lista suspensa.
   a. Digite **abc** no campo **Nome contém** para exibir os volumes cujo nome contém “abc”.
   b. Selecione **<<All Volumes whose name contains 'abc'>>** na área Recursos Disponíveis e mova-o para a área Recursos Selecionados.
   c. Clique em **Excluir**, digite **xyz** no campo **Nome contém** e, em seguida, clique em **Adicionar**.
3. Clique em **Eventos** e selecione **Crítico** no campo Severidade do evento.
4. Selecione **Todos os eventos críticos** na área Eventos correspondentes e mova-o para a área Eventos selecionados.
5. Clique em **Actions**, e digite **sample@domain.com** no campo Alert these users.

6. Selecione **Lembrar a cada 15 minutos** para notificar o usuário a cada 15 minutos.

   Você pode configurar um alerta para enviar notificações repetidamente aos destinatários durante um período específico. Você deve determinar o horário a partir do qual a notificação do evento estará ativa para o alerta.

7. No menu Selecionar Script para Executar, selecione o script **Teste**.
8. Clique em **Salvar**.

Alterar a senha do usuário local no Active IQ Unified Manager

Você pode alterar a senha de login do seu usuário local para evitar possíveis riscos de segurança.

Antes de começar

Você precisa estar conectado como um usuário local.

As senhas do usuário de manutenção e dos usuários remotos não podem ser alteradas seguindo estas etapas. Para alterar a senha de um usuário remoto, entre em contato com seu administrador de senhas. Para alterar a senha do usuário de manutenção, consulte "Usando o console de manutenção".

Passos

1. Faça login no Unified Manager.
2. Na barra de menu superior, clique no ícone do usuário e em seguida clique em **Alterar senha**.

   A opção **Change Password** não é exibida se você for um usuário remoto.

3. Na caixa de diálogo Change Password, insira a senha atual e a nova senha.
4. Clique em **Salvar**.

Se o Unified Manager estiver configurado em uma configuração de alta disponibilidade, você deverá alterar a senha no segundo nó da configuração. Ambas as instâncias devem ter a mesma senha.

Defina o tempo limite de inatividade da sessão no Active IQ Unified Manager

Você pode especificar o valor de tempo limite de inatividade para o Unified Manager, para que a sessão seja encerrada automaticamente após um determinado período de inatividade. Por padrão, o tempo limite é definido como 4.320 minutos (72 horas).

Antes de começar

Você precisa ter a função de Application Administrator.

Essa configuração afeta todas as sessões de usuários conectados.

Esta opção não está disponível se você tiver ativado a autenticação SAML (Security Assertion Markup Language).

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Configurações de recursos**.
2. Na página **Configurações de recursos**, especifique o tempo limite de inatividade escolhendo uma das

seguintes opções:

Se você quiser…	Então faça isso…
Não defina um tempo limite para que a sessão nunca seja fechada automaticamente	No painel **Tempo limite de inatividade**, mova o botão deslizante para a esquerda (desativado) e clique em **Aplicar**.
Defina um número específico de minutos como o valor de tempo limite	No painel **Tempo limite de inatividade**, mova o botão deslizante para a direita (ativado), especifique o valor do tempo limite de inatividade em minutos e clique em **Aplicar**.

Defina o tempo limite da sessão usando a CLI no Active IQ Unified Manager

Você pode definir um valor máximo de tempo limite de sessão para o Unified Manager usando a CLI para que a sessão seja encerrada automaticamente após um determinado período. Por padrão, o tempo limite da sua sessão está definido para o valor máximo, que é de 4.320 minutos (72 horas). Isso significa que sua sessão termina automaticamente após 72 horas, mesmo se você estiver conectado e usando o Unified Manager.

Sobre esta tarefa

Você precisa ter a função de Application Administrator.

A configuração de tempo limite da sessão afeta todas as sessões de usuários conectados.

Passos

1. Faça login na CLI do Unified Manager digitando o `um cli login` comando. Use um nome de usuário e uma senha válidos para autenticação.
2. Digite o `um option set max.session.timeout.value=<in mins>` comando para modificar o valor do tempo limite da sessão.

Alterar o nome do host do Unified Manager

Alterar o nome do host da máquina virtual do Active IQ Unified Manager

O host de rede recebe um nome quando o dispositivo virtual do Unified Manager é implantado pela primeira vez. Você pode alterar o nome do host após a implantação. Se você alterar o nome do host, também deverá regenerar o certificado HTTPS.

Antes de começar

Para executar essas tarefas, você precisa estar conectado ao Unified Manager como usuário de manutenção ou ter a função de Application Administrator atribuída.

Você pode usar o nome do host (ou o endereço IP do host) para acessar a interface do usuário da Web do Unified Manager. Se você configurou um endereço IP estático para sua rede durante a implantação, então você terá atribuído um nome ao host da rede. Se você configurou a rede usando DHCP, o nome do host deve ser obtido do DNS. Se o DHCP ou o DNS não estiverem configurados corretamente, o nome do host “Unified Manager” será atribuído automaticamente e associado ao certificado de segurança.

Independentemente de como o nome do host foi atribuído, se você alterar o nome do host e pretender usar o novo nome do host para acessar a interface da web do Unified Manager, você deverá gerar um novo certificado de segurança.

Se você acessar a interface web usando o endereço IP em vez do nome do host, não precisará gerar um novo certificado caso altere o nome do host. No entanto, a melhor prática é atualizar o certificado para que o nome do host no certificado corresponda ao nome do host real.

Se você alterar o nome do host no Unified Manager, deverá atualizá-lo manualmente no OnCommand Workflow Automation (WFA). O nome do host não é atualizado automaticamente no WFA.

O novo certificado só entrará em vigor após a reinicialização da máquina virtual do Unified Manager.

Passos

1. Gere um certificado de segurança HTTPS

   Se você quiser usar o novo nome de host para acessar a interface da web do Unified Manager, será necessário gerar novamente o certificado HTTPS para associá-lo ao novo nome de host.

2. Reinicie a máquina virtual do Unified Manager

   Após regenerar o certificado HTTPS, você deve reiniciar a máquina virtual do Unified Manager.

Gere um certificado de segurança HTTPS no Active IQ Unified Manager

Quando o Active IQ Unified Manager é instalado pela primeira vez, um certificado HTTPS padrão é instalado. Você pode gerar um novo certificado de segurança HTTPS para substituir o certificado existente.

Antes de começar

Você precisa ter a função de Application Administrator.

Pode haver vários motivos para regenerar o certificado, por exemplo, se você quiser valores melhores para o Nome distinto (DN), um tamanho de chave maior, um período de expiração mais longo ou se o certificado atual tiver expirado.

Se você não tiver acesso à interface web do Unified Manager, poderá regenerar o certificado HTTPS com os mesmos valores usando o console de manutenção. Ao regenerar os certificados, você pode definir o tamanho da chave e a duração de validade da chave. Se você usar a opção `Reset Server Certificate` no console de manutenção, um novo certificado HTTPS será criado e será válido por 397 dias. Este certificado terá uma chave RSA de 2048 bits.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Certificado HTTPS**.
2. Clique em **Regenerate HTTPS Certificate**.

   A caixa de diálogo "Regenerate HTTPS Certificate" é exibida.

3. Selecione uma das seguintes opções dependendo de como você deseja gerar o certificado:

Se você quiser…	Faça isso…
Gere novamente o certificado com os valores atuais	Clique na opção **Regenerar usando os atributos do certificado atual**.

Se você quiser…	Faça isso…
Gere o certificado usando valores diferentes	Clique na opção **Atualizar os atributos do certificado atual**. Os campos Nome Comum e Nomes Alternativos usarão os valores do certificado existente se você não inserir novos valores. O “Nome Comum” deve ser definido como o FQDN do host. Os outros campos não exigem valores, mas você pode inserir valores, por exemplo, para E-MAIL, EMPRESA, DEPARTAMENTO, Cidade, Estado e País, se quiser que esses valores sejam preenchidos no certificado. Você também pode selecionar entre o TAMANHO DA CHAVE disponível (o algoritmo da chave é “RSA”.) e o PERÍODO DE VALIDADE. • Os valores permitidos para o tamanho da chave são `2048`, `3072` e `4096`. • Os períodos de validade variam de um mínimo de 1 dia a um máximo de 36.500 dias. Embora seja permitido um período de validade de 36500 dias, recomenda-se que você utilize um período de validade de no máximo 397 dias ou 13 meses. Isso porque, se você selecionar um período de validade superior a 397 dias e planejar exportar um CSR para este certificado e obtê-lo assinado por uma CA reconhecida, a validade do certificado assinado retornado a você pela CA será reduzida para 397 dias. • Você pode selecionar a caixa de seleção "Excluir informações de identificação local (ex.: localhost)" se quiser remover as informações de identificação local do campo Nomes Alternativos no certificado. Quando essa caixa de seleção estiver marcada, somente o que você inserir no campo será usado no campo Nomes Alternativos. Se deixado em branco, o certificado resultante não terá nenhum campo Nomes Alternativos.

4. Clique em **Sim** para regenerar o certificado.
5. Reinicie o servidor do Unified Manager para que o novo certificado entre em vigor.
6. Verifique as novas informações do certificado ao visualizar o certificado HTTPS.

Reinicie a máquina virtual do Active IQ Unified Manager

Você pode reiniciar a máquina virtual a partir do console de manutenção do Unified Manager. Você deve reiniciar após gerar um novo certificado de segurança ou se houver um problema com a máquina virtual.

Antes de começar

O appliance virtual está ligado.

Você está conectado ao console de manutenção como o usuário de manutenção.

Você também pode reiniciar a máquina virtual a partir do vSphere usando a opção **Restart Guest**. Consulte a documentação da VMware para obter mais informações.

Passos

1. Acesse o console de manutenção.
2. Selecione **Configuração do sistema** > **Reiniciar máquina virtual**.

Altere o nome do host do Active IQ Unified Manager em sistemas Linux

Em algum momento, você poderá querer alterar o nome do host da máquina Red Hat Enterprise Linux na qual instalou o Unified Manager. Por exemplo, você pode querer renomear o host para identificar mais facilmente os seus servidores do Unified Manager por tipo, grupo de trabalho ou grupo de cluster monitorado ao listar suas máquinas Linux.

Antes de começar

Você deve ter acesso de usuário raiz ao sistema Linux no qual o Unified Manager está instalado.

Você pode usar o nome do host (ou o endereço IP do host) para acessar a interface da web do Unified Manager. Se você configurou um endereço IP estático para sua rede durante a implantação, então terá designado um nome para o host da rede. Se você configurou a rede usando DHCP, o nome do host deve ser obtido do servidor DNS.

Independentemente de como o nome do host foi atribuído, se você alterar o nome do host e pretender usar o novo nome do host para acessar a interface da Web do Unified Manager, será necessário gerar um novo certificado de segurança.

Se você acessar a interface da web usando o endereço IP do servidor em vez do nome do host, não precisará gerar um novo certificado se alterar o nome do host. No entanto, a prática recomendada é atualizar o certificado para que o nome do host no certificado corresponda ao nome real do host. O novo certificado só entrará em vigor depois que a máquina Linux for reiniciada.

Se você alterar o nome do host no Unified Manager, deverá atualizá-lo manualmente no OnCommand Workflow Automation (WFA). O nome do host não é atualizado automaticamente no WFA.

Passos

1. Faça login como usuário raiz no sistema do Unified Manager que você deseja modificar.

2. Pare o software Unified Manager e o software MySQL associado digitando o seguinte comando:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Altere o nome do host usando o comando Linux `hostnamectl`:

   ```
   hostnamectl set-hostname new_FQDN
   ```

   ```
   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. Gere novamente o certificado HTTPS para o servidor:

   ```
   /opt/netapp/essentials/bin/cert.sh create
   ```

5. Reinicie o serviço de rede:

   ```
   systemctl restart NetworkManager.service
   ```

6. Após reiniciar o serviço, verifique se o novo nome do host consegue dar ping em si mesmo:

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Este comando deve retornar o mesmo endereço IP que você definiu anteriormente para o nome do host original.

7. Após concluir e verificar a alteração do nome do host, reinicie o Unified Manager digitando o seguinte comando:

   ```
   systemctl start mysqld ocie ocieau
   ```

Ative e desative o gerenciamento de storage baseado em políticas no Active IQ Unified Manager

A partir do Unified Manager 9.7, você pode provisionar cargas de trabalho de storage (volumes e LUNs) em seus clusters ONTAP e gerenciar essas cargas de trabalho com base nos níveis de serviço de desempenho atribuídos. Essa funcionalidade é semelhante à criação de cargas de trabalho no ONTAP System Manager e à associação de políticas de QoS, mas, quando aplicada usando o Unified Manager, permite provisionar e gerenciar cargas de trabalho em todos os clusters que a sua instância do Unified Manager está monitorando.

Você precisa ter a função de Application Administrator.

Essa opção está habilitada por padrão, mas você pode desativá-la se não quiser provisionar e gerenciar cargas de trabalho usando o Unified Manager.

Quando ativada, esta opção fornece vários novos itens na interface de usuário:

Novo conteúdo	Localização
Uma página para provisionar novas cargas de trabalho	Disponível em **Tarefas comuns** > **Provisionamento**
Uma página para criar políticas de nível de serviço de desempenho	Disponível em **Configurações** > **Políticas** > **Níveis de serviço de desempenho**
Uma página para criar políticas de eficiência de storage de desempenho	Disponível em **Configurações** > **Políticas** > **Eficiência de storage**
Painéis que descrevem o desempenho atual da sua carga de trabalho e as IOPS da sua carga de trabalho	Disponível no painel de controle

Consulte a ajuda online do produto para obter mais informações sobre essas páginas e sobre essa funcionalidade.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Configurações de recursos**.
2. Na página **Configurações de Recursos**, desative ou ative o gerenciamento de storage baseado em políticas escolhendo uma das seguintes opções:

Se você quiser…	Então faça isso…
Desativar o gerenciamento de storage baseado em políticas	No painel **gerenciamento de storage baseado em políticas**, mova o botão deslizante para a esquerda.
Habilitar o gerenciamento de storage baseado em políticas	No painel **gerenciamento de storage baseado em políticas**, mova o botão deslizante para a direita.

Configurar o Active IQ Unified Manager backup

Você pode configurar a funcionalidade de backup no Unified Manager por meio de um conjunto de etapas de configuração a serem executadas nos sistemas host e pelo console de manutenção.

Para obter informações sobre as etapas de configuração, consulte "Gerenciamento de operações de backup e restauração".

Gerenciar configurações de recursos

Saiba mais sobre as configurações de recursos no Active IQ Unified Manager

A página Configurações de recursos permite ativar e desativar recursos específicos no Active IQ Unified Manager. Isso inclui a criação e o gerenciamento de objetos de storage com base em políticas, a ativação do API Gateway e do Login Banner, o upload de scripts para gerenciar alertas, o encerramento automático de uma sessão da interface de usuário da web com base no tempo de inatividade e a desativação do recebimento de eventos da plataforma Active IQ.

A página Configurações de recursos está disponível apenas para usuários com a função

Administrador de Aplicativos.

Para obter informações sobre Scripts Upload, consulte "Ativar e desativar o upload de scripts".

Habilite o gerenciamento de storage baseado em políticas no Active IQ Unified Manager

A opção **Gerenciamento de storage baseado em políticas** permite o gerenciamento de storage com base em objetivos de nível de serviço (SLOs). Essa opção está habilitada por padrão.

Ao ativar esse recurso, você pode provisionar cargas de trabalho de storage nos clusters do ONTAP adicionados à sua instância do Active IQ Unified Manager e gerenciar essas cargas de trabalho com base nos níveis de serviço de desempenho e nas políticas de eficiência de storage atribuídos.

Você pode optar por ativar ou desativar esse recurso em **Geral** > **Configurações de recursos** > **gerenciamento de storage baseado em política**. Ao ativar esse recurso, as seguintes páginas ficam disponíveis para operação e monitoramento:

- Provisionamento (provisionamento de cargas de trabalho de storage)
- **Políticas** > **Níveis de Serviço de Desempenho**
- **Políticas** > **Eficiência de storage**
- Coluna Cargas de trabalho gerenciadas por nível de serviço de desempenho na página Configuração de clusters
- Painel de desempenho da carga de trabalho no **Painel de controle**

Você pode usar as telas para criar níveis de serviço de desempenho e políticas de eficiência de storage, além de provisionar cargas de trabalho de storage. Você também pode monitorar as cargas de trabalho de storage que estão em conformidade com os níveis de serviço de desempenho atribuídos, bem como aquelas que não estão em conformidade. O painel Desempenho da Carga de Trabalho e IOPS da Carga de Trabalho também permite avaliar a capacidade e o desempenho (IOPS) totais, disponíveis e usados dos clusters em todo o seu data center, com base nas cargas de trabalho de storage provisionadas neles.

Após ativar esse recurso, você pode executar as APIs REST do Unified Manager para realizar algumas dessas funções em **Menu Bar** > **Help button** > **API Documentation** > categoria **storage-provider**. Como alternativa, você pode inserir o nome do host ou o endereço IP e a URL para acessar a página da API REST no formato https://<hostname>/docs/api/

Para obter mais informações sobre as APIs, consulte "Primeiros passos com as APIs REST do Active IQ Unified Manager".

Saiba mais sobre o recurso API Gateway no Active IQ Unified Manager

O recurso API Gateway permite que o Active IQ Unified Manager seja um plano de controle único a partir do qual você pode gerenciar múltiplos clusters ONTAP, sem precisar fazer login em cada um individualmente.

Você pode ativar esse recurso nas páginas de configuração que aparecem quando você faz login pela primeira vez no Unified Manager. Como alternativa, você pode ativar ou desativar esse recurso em **General** > **Feature Settings** > **API Gateway**.

As APIs REST do Unified Manager são diferentes das APIs REST do ONTAP, e nem todas as funcionalidades das APIs REST do ONTAP podem ser usadas com as APIs REST do Unified Manager. No entanto, se você tiver um requisito empresarial específico para acessar as APIs do ONTAP e gerenciar recursos específicos que não são expostos ao Unified Manager, poderá habilitar o recurso API Gateway e executar as APIs do ONTAP. O gateway atua como um proxy para encapsular as solicitações de API, mantendo as solicitações de cabeçalho e corpo no mesmo formato das APIs do ONTAP. Você pode usar suas credenciais do Unified Manager e executar as APIs específicas para acessar e gerenciar os clusters do ONTAP sem fornecer credenciais individuais de cluster. O Unified Manager funciona como um ponto único de gerenciamento para executar as APIs nos clusters do ONTAP gerenciados pela sua instância do Unified Manager. A resposta retornada pelas APIs é a mesma que a resposta retornada pelas respectivas APIs REST do ONTAP executadas diretamente do ONTAP.

Após habilitar esse recurso, você poderá executar as APIs REST do Unified Manager em **Barra de menu** > **Botão Ajuda** > **Documentação da API** > categoria **gateway**. Como alternativa, você pode inserir o nome do host ou o endereço IP e a URL para acessar a página da API REST no formato `https://<hostname>/docs/api/`

Para obter mais informações sobre as APIs, consulte "Primeiros passos com as APIs REST do Active IQ Unified Manager".

Especifique o tempo limite de inatividade no Active IQ Unified Manager

Você pode especificar o valor do tempo limite de inatividade para o Active IQ Unified Manager. Após o tempo de inatividade especificado, o aplicativo faz logout automaticamente. Essa opção está habilitada por padrão.

Você pode desativar este recurso ou modificar o tempo limite em **Geral** > **Configurações de Recursos** > **Tempo Limite de Inatividade**. Após ativar este recurso, você deve especificar o limite de tempo de inatividade (em minutos) no campo **SAIR APÓS**, após o qual o sistema encerra a sessão automaticamente. O valor padrão é 4320 minutos (72 horas).

Esta opção não está disponível se você tiver ativado a autenticação SAML (Security Assertion Markup Language).

Ative os eventos do portal Active IQ no Active IQ Unified Manager

Você pode especificar se deseja ativar ou desativar os eventos do portal Active IQ. Essa configuração permite que o portal Active IQ descubra e exiba eventos adicionais sobre a configuração do sistema, o cabeamento e assim por diante. Essa opção está ativada por padrão.

Ao ativar esse recurso, o Active IQ Unified Manager exibe os eventos descobertos pelo portal Active IQ. Esses eventos são criados ao executar um conjunto de regras nas mensagens AutoSupport geradas por todos os sistemas de storage monitorados. Esses eventos são diferentes dos outros eventos do Unified Manager e identificam incidentes ou riscos relacionados à configuração do sistema, ao cabeamento, às melhores práticas e aos problemas de disponibilidade.

Você pode optar por ativar ou desativar esse recurso em **Geral** > **Configurações de recursos** > **Active IQ Portal Events**. Em sites sem acesso externo à rede, você deve carregar as regras manualmente em **Gerenciamento de storage** > **Configuração de eventos** > **Carregar regras**.

Este recurso está ativado por padrão. Desativar esse recurso impede que os eventos do Active IQ sejam

descobertos ou exibidos no Unified Manager. Quando estiver desativado, ativar esse recurso permitirá que o Unified Manager receba os eventos do Active IQ em um cluster no horário predefinido de 00:15 para o fuso horário desse cluster.

Ative e desative as configurações de segurança para conformidade no Active IQ Unified Manager

Ao usar o botão **Customize** no painel **Security Dashboard** da página Configurações de recursos, você pode ativar ou desativar os parâmetros de segurança para o monitoramento de conformidade no Unified Manager.

As configurações ativadas ou desativadas nesta página controlam o status geral de conformidade dos clusters e das VMs de storage no Unified Manager. Com base nas seleções, as colunas correspondentes ficam visíveis na visualização **Segurança: todos os clusters** da página de inventário de Clusters e na visualização **Segurança: todas as VMs de storage** da página de inventário de VMs de storage.

Somente usuários com função de administrador podem editar essas configurações.

Os critérios de segurança para seus clusters ONTAP, VMs de storage e volumes são avaliados em relação às recomendações definidas no "Guia de fortalecimento da segurança para o NetApp ONTAP 9". O painel Segurança no dashboard e a página Segurança exibem o status de conformidade de segurança padrão de seus clusters, VMs de storage e volumes. Eventos de segurança também são gerados, e ações de gerenciamento são habilitadas para os clusters e VMs de storage que apresentam violações de segurança.

Personalize as configurações de segurança

Para personalizar as configurações de monitoramento de conformidade de acordo com o seu ambiente ONTAP, siga estas etapas:

Passos

1. Clique em **Geral > Configurações de recursos > Painel de segurança > Personalizar**. A janela pop-up **Personalizar configurações do Painel de segurança** aparece.

   Os parâmetros de conformidade de segurança que você habilita ou desabilita podem afetar diretamente as visualizações de segurança padrão, os relatórios e os relatórios agendados nas telas Clusters e Storage VMs. Se você tiver carregado um relatório do Excel dessas telas antes de modificar os parâmetros de segurança, os relatórios do Excel baixados podem estar incorretos.

2. Para ativar ou desativar as configurações personalizadas para seus clusters do ONTAP, selecione a configuração geral necessária em **Cluster**. Para obter informações sobre as opções de personalização da conformidade do cluster, consulte "Categorias de conformidade do cluster".
3. Para ativar ou desativar as configurações personalizadas para suas VMs de storage, selecione a configuração geral necessária em **Storage VM**. Para obter informações sobre as opções para personalizar a conformidade da VM de storage, consulte "Categorias de conformidade de VMs de storage".

Personalize as configurações do AutoSupport e da autenticação

Na seção **AutoSupport Settings**, você pode especificar se o transporte HTTPS deve ser usado para enviar mensagens de AutoSupport do ONTAP.

Na seção **Configurações de Autenticação**, você pode habilitar o Unified Manager para gerar alertas para o

usuário administrador padrão do ONTAP.

Ativar e desativar o upload de scripts no Active IQ Unified Manager

A capacidade de carregar scripts no Unified Manager e executá-los está habilitada por padrão. Se sua organização não deseja permitir essa atividade por motivos de segurança, você pode desabilitar essa funcionalidade.

Antes de começar

Você precisa ter a função de Application Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Configurações de recursos**.
2. Na página **Configurações de Recursos**, desative ou ative a execução de scripts escolhendo uma das seguintes opções:

Se você quiser…	Então faça isso…
Desativar scripts	No painel **Script Upload**, mova o botão deslizante para a esquerda.
Ativar scripts	No painel **Script Upload**, mova o botão deslizante para a direita.

Adicione um banner de login no Active IQ Unified Manager

Adicionar um banner de login permite que sua organização exiba informações como quem tem permissão para acessar o sistema e os termos e condições de uso durante o login e o logout.

Qualquer usuário, como operadores de storage ou administradores, pode visualizar este banner pop-up de login durante o login, logout e o tempo limite da sessão.

Use o console de manutenção

Saiba mais sobre o console de manutenção no Active IQ Unified Manager

O console de manutenção do Unified Manager permite que você mantenha as configurações do seu sistema Unified Manager e faça as alterações necessárias para evitar a ocorrência de problemas.

Dependendo do sistema operacional no qual você instalou o Unified Manager, o console de manutenção oferece as seguintes funções:

- Solucione quaisquer problemas com seu dispositivo virtual, especialmente se a interface da web do Unified Manager não estiver disponível
- Atualize para versões mais recentes do Unified Manager
- Gere pacotes de suporte para enviar ao suporte técnico

- Configurar as configurações de rede
- Alterar a senha do usuário de manutenção
- Conecte-se a um provedor de dados externo para enviar estatísticas de desempenho
- Alterar a coleta interna de dados de desempenho
- Restaure o banco de dados e as configurações do o Unified Manager a partir de uma versão com backup anterior.

Saiba mais sobre o usuário de manutenção no Active IQ Unified Manager

O usuário de manutenção é criado durante a instalação do Unified Manager em um sistema Red Hat Enterprise Linux. O nome do usuário de manutenção é o usuário “umadmin”. O usuário de manutenção tem a função Application Administrator na IU da web, e esse usuário pode criar usuários subsequentes e atribuir funções a eles.

O usuário de manutenção, ou usuário umadmin, também pode acessar o console de manutenção do Unified Manager.

Funcionalidades de diagnóstico do usuário no Active IQ Unified Manager

O objetivo do acesso para diagnóstico é permitir que o suporte técnico ajude você na solução de problemas, e você só deve usá-lo quando instruído pelo suporte técnico.

O usuário de diagnóstico pode executar comandos no nível do sistema operacional quando orientado pelo suporte técnico, para fins de solução de problemas.

Acesse o console de manutenção no Active IQ Unified Manager

Caso a interface de usuário do Unified Manager não esteja em funcionamento, ou se você precisar executar funções que não estão disponíveis na interface de usuário, você pode acessar o console de manutenção para gerenciar seu sistema Unified Manager.

Antes de começar

Você precisa ter instalado e configurado o Unified Manager.

Após 15 minutos de inatividade, o console de manutenção encerra sua sessão.

Quando instalado no VMware, se você já tiver feito login como usuário de manutenção por meio do console do VMware, não poderá fazer login simultaneamente usando o Secure Shell.

Etapa

1. Siga estes passos para acessar o console de manutenção:

Neste sistema operacional…	Siga estes passos…
VMware	a. Usando o Secure Shell, conecte-se ao endereço IP ou ao nome de domínio totalmente qualificado do dispositivo virtual do Unified Manager. b. Faça login no console de manutenção usando seu nome de usuário e senha de manutenção.
Linux	a. Usando o Secure Shell, conecte-se ao endereço IP ou ao nome de domínio totalmente qualificado do sistema Unified Manager. b. Faça login no sistema com o nome e a senha do usuário de manutenção (umadmin). c. Digite o comando `maintenance_console` e pressione Enter.
Windows	a. Faça login no sistema Unified Manager com as credenciais de administrador. b. Inicie o PowerShell como administrador do Windows. c. Digite o comando `maintenance_console` e pressione Enter.

O menu do console de manutenção do Unified Manager é exibido.

Acesse o console de manutenção usando o console da VM do vSphere no Active IQ Unified Manager

Se a interface de usuário do Unified Manager não estiver em funcionamento, ou se você precisar executar funções que não estejam disponíveis na interface de usuário, poderá acessar o console de manutenção para reconfigurar seu dispositivo virtual.

Antes de começar

- Você deve ser o usuário de manutenção.
- O appliance virtual deve estar ligado para acessar o console de manutenção.

Passos

1. No vSphere Client, localize o dispositivo virtual do Unified Manager.
2. Clique na aba **Console**.
3. Clique dentro da janela do console para fazer login.
4. Faça login no console de manutenção usando seu nome de usuário e senha.

   Após 15 minutos de inatividade, o console de manutenção encerra sua sessão.

Menus do console de manutenção

Saiba mais sobre os menus do console de manutenção no Active IQ Unified Manager

O console de manutenção consiste em diferentes menus que permitem a você manter e gerenciar recursos especiais e definições de configuração do servidor do Unified Manager.

Dependendo do sistema operacional no qual você instalou o Unified Manager, o console de manutenção consiste nos seguintes menus:

- Atualizar o Unified Manager (somente VMware)
- Configuração de rede (somente VMware)
- Configuração do sistema (somente o VMware)
  a. Suporte/Diagnóstico
  b. Redefinir certificado do servidor
  c. Regenerar certificado do cliente
  d. Backup e restauração
  e. Fornecedor de dados externo
  f. Configuração do intervalo de sondagem de desempenho
  g. Desativar autenticação SAML
  h. Visualizar/alterar portas do aplicativo
  i. Configuração do log de depuração
  j. Controlar o acesso à porta 3306 do MySQL
  k. Sair

Você seleciona o número da lista para acessar a opção específica do menu. Por exemplo, para backup e restauração, você seleciona *4*.

Menu de configuração de rede no Active IQ Unified Manager

O menu Configuração de Rede permite que você gerencie as configurações de rede. Você deve usar este menu quando a interface de usuário do Unified Manager não estiver disponível.

Este menu não está disponível se o Unified Manager estiver instalado no Red Hat Enterprise Linux ou no Microsoft Windows.

As seguintes opções de menu estão disponíveis.

- **Exibir configurações de endereço IP**

  Exibe as configurações de rede atuais do dispositivo virtual, incluindo o endereço IP, a rede, o endereço de broadcast, a máscara de rede, o gateway e os servidores DNS.

- **Alterar configurações de endereço IP**

  Permite que você altere qualquer configuração de rede do appliance virtual, incluindo o endereço IP, a máscara de rede, o gateway ou os servidores DNS. Se você alterar suas configurações de rede de DHCP

para rede estática usando o console de manutenção, não poderá editar o nome do host. Você deve selecionar **Commit Changes** para que as alterações entrem em vigor.

- **Exibir configurações de pesquisa de nome de domínio**

  Exibe a lista de pesquisa de nomes de domínio usada para resolver nomes de host.

- **Alterar configurações de pesquisa de nomes de domínio**

  Permite alterar os nomes de domínio que você deseja pesquisar ao resolver nomes de host. Você deve selecionar **Confirmar alterações** para que as alterações entrem em vigor.

- **Exibir rotas estáticas**

  Exibe as rotas de rede estáticas atuais.

- **Alterar rotas estáticas**

  Permite adicionar ou excluir rotas de rede estáticas. Você deve selecionar **Commit Changes** para que as alterações entrem em vigor.

  - **Adicionar rota**

    Permite adicionar uma rota estática.

  - **Excluir Rota**

    Permite excluir uma rota estática.

  - **Voltar**

    Retorna ao **Menu Principal**.

  - **Sair**

    Sai do console de manutenção.

- **Desativar interface de rede**

  Desativa todas as interfaces de rede disponíveis. Se houver apenas uma interface de rede disponível, você não poderá desativá-la. Você deve selecionar **Commit Changes** para que as alterações entrem em vigor.

- **Habilitar interface de rede**

  Habilita as interfaces de rede disponíveis. Você deve selecionar **Confirmar alterações** para que as alterações entrem em vigor.

- **Confirmar alterações**

  Aplica quaisquer alterações feitas nas configurações de rede do dispositivo virtual. Você deve selecionar esta opção para que quaisquer alterações feitas entrem em vigor, caso contrário, as alterações não ocorrerão.

- **Enviar ping para um host**

Envia um ping para um host de destino para confirmar alterações de endereço IP ou configurações de DNS.

- **Restaurar configurações padrão**

  Redefine todas as configurações para o padrão de fábrica. Você deve selecionar **Commit Changes** para que as alterações entrem em vigor.

- **Voltar**

  Retorna ao **Menu Principal**.

- **Sair**

  Sai do console de manutenção.

Utilize o menu Configuração do Sistema no Active IQ Unified Manager

O menu Configuração do Sistema permite que você gerencie seu appliance virtual, oferecendo várias opções, como visualizar o status do servidor, reiniciar e desligar a máquina virtual.

Quando o Unified Manager está instalado em um sistema Linux ou Microsoft Windows, somente a opção “Restore from a Unified Manager Backup” está disponível neste menu.

As seguintes opções de menu estão disponíveis:

- **Exibir status do servidor**

  Exibe o status atual do servidor. As opções de status incluem "Em execução" e "Não em execução".

  Se o servidor não estiver funcionando, talvez seja necessário entrar em contato com o suporte técnico.

- **Reiniciar máquina virtual**

  Reinicia a máquina virtual, interrompendo todos os serviços. Após a reinicialização, a máquina virtual e os serviços reiniciam.

- **Desligar a máquina virtual**

  Encerra a máquina virtual, interrompendo todos os serviços.

  Você pode selecionar esta opção somente no console da máquina virtual.

- **Alterar <logged in user> senha do usuário**

  Altera a senha do usuário que está conectado no momento, que só pode ser o usuário de manutenção.

- **Aumentar o tamanho do disco de dados**

  Aumenta o tamanho do disco de dados (disco 3) na máquina virtual.

- **Aumentar o tamanho do disco de swap**

  Aumenta o tamanho do disco de swap (disco 2) na máquina virtual.

- **Alterar fuso horário**

  Altera o fuso horário para o da sua localização.

- **Alterar servidor NTP**

  Altera as configurações do servidor NTP, como endereço IP ou nome de domínio totalmente qualificado (FQDN).

- **Alterar o serviço NTP**

  Alterna entre os serviços `ntp` e `systemd-timesyncd`.

- **Restaurar a partir de um backup do Unified Manager**

  Restaura o banco de dados e as configurações do o Unified Manager a partir de uma versão de backup anterior.

- **Redefinir certificado do servidor**

  Redefine o certificado de segurança do servidor.

- **Alterar nome do host**

  Altera o nome do host no qual o appliance virtual está instalado.

- **Voltar**

  Sai do menu Configuração do Sistema e retorna ao menu principal.

- **Sair**

  Sai do menu do console de manutenção.

Utilize o menu Suporte e Diagnóstico no Active IQ Unified Manager

O menu Suporte e Diagnóstico permite gerar um pacote de suporte que você pode enviar ao suporte técnico para obter assistência na resolução de problemas.

As seguintes opções de menu estão disponíveis:

- **Gerar pacote de suporte leve**

  Permite que você crie um pacote de suporte leve que contém apenas 30 dias de logs e registros do banco de dados de configuração, excluindo dados de desempenho, arquivos de gravação de aquisição e heap dump do servidor.

- **Gerar pacote de suporte**

  Permite criar um pacote de suporte completo (arquivo 7-Zip) contendo informações de diagnóstico no diretório base do usuário de diagnóstico. Se o seu sistema estiver conectado à internet, você também pode enviar o pacote de suporte para NetApp.

  O arquivo inclui informações geradas por uma mensagem AutoSupport, o conteúdo do banco de dados do Unified Manager, dados detalhados sobre os componentes internos do servidor do Unified Manager e logs

de nível detalhado que normalmente não são incluídos em mensagens AutoSupport nem no pacote de suporte simplificado.

Saiba mais sobre as opções adicionais do menu do console de manutenção no Active IQ Unified Manager

As opções de menu a seguir permitem que você execute diversas tarefas administrativas no servidor Unified Manager.

As seguintes opções de menu estão disponíveis:

- **Redefinir certificado do servidor**

  Regenera o certificado do servidor HTTPS.

  Você pode regenerar o certificado do servidor na GUI do Unified Manager clicando em **Geral** > **Certificados HTTPS** > **Regenerar certificado HTTPS**.

- **Desativar a autenticação SAML**

  Desativa a autenticação SAML para que o provedor de identidade (IdP) não forneça mais autenticação de logon para os usuários que acessam a GUI do Unified Manager. Essa opção de console normalmente é usada quando um problema com o servidor IdP ou com a configuração SAML impede que os usuários acessem a GUI do Unified Manager.

- **Fornecedor de dados externo**

  Oferece opções para conectar o Unified Manager a um provedor de dados externo. Após estabelecer a conexão, os dados de desempenho são enviados para um servidor externo para que especialistas em desempenho de storage possam gerar gráficos das métricas usando software de terceiro. As seguintes opções são exibidas:

  - **Exibir configuração do servidor**--Exibe as configurações atuais de conexão e de configuração de um provedor de dados externo.
  - **Adicionar / Modificar conexão com o servidor**--Permite inserir novas configurações de conexão para um provedor de dados externo ou alterar as configurações existentes.
  - **Modificar Configuração do Servidor** permite inserir novas configurações para um provedor de dados externo ou alterar as configurações existentes.
  - **Excluir conexão com o servidor**--Exclui a conexão com um provedor de dados externo.

    Após a exclusão da conexão, o Unified Manager perde a conexão com o servidor externo.

- **Backup e Restauração**

  Para obter mais informações, consulte os tópicos em "Gerenciamento de operações de backup e restauração".

- **Configuração do intervalo de sondagem de desempenho**

  Oferece uma opção para configurar a frequência com que o Unified Manager coleta dados estatísticos de desempenho dos clusters. O intervalo de coleta padrão é de 5 minutos.

  Você pode alterar esse intervalo para 10 ou 15 minutos se perceber que as coletas de dados de clusters grandes não terminam no prazo.

- **Visualizar/Alterar portas do aplicativo**

  Oferece uma opção para alterar as portas padrão que o Unified Manager usa para os protocolos HTTP e HTTPS, se necessário para a segurança. As portas padrão são 80 para HTTP e 443 para HTTPS.

- **Controlar o acesso à porta 3306 do MySQL**

  Controla o acesso do host à porta padrão do MySQL 3306. Por motivos de segurança, o acesso por meio dessa porta é restrito apenas ao localhost durante uma nova instalação do Unified Manager em sistemas Linux, Windows e VMware vSphere. Esta opção permite alternar a visibilidade dessa porta entre o localhost e hosts remotos, ou seja, se ela estiver habilitada apenas para localhost em seu ambiente, você poderá disponibilizar essa porta também para hosts remotos. Como alternativa, quando ela estiver habilitada para todos os hosts, você poderá restringir o acesso a essa porta apenas ao localhost. Se o acesso tiver sido habilitado anteriormente em hosts remotos, a configuração será mantida em um cenário de upgrade. Você deve verificar as configurações do firewall em sistemas Windows após alternar a visibilidade da porta e desabilitar as configurações do firewall se elas estiverem configuradas para restringir o acesso à porta 3306 do MySQL.

- **Sair**

  Sai do menu do console de manutenção.

Altere a senha do usuário de manutenção no Windows no Active IQ Unified Manager

Você pode alterar a senha do usuário de manutenção do Unified Manager quando necessário.

Passos

1. Na página de login da interface web do Unified Manager, clique em **Esqueci minha senha**.

   Uma página é exibida solicitando o nome do usuário cuja senha você deseja redefinir.

2. Digite o nome de usuário e clique em **Enviar**.

   Um e-mail com um link para redefinir a senha é enviado ao endereço de e-mail definido para esse nome de usuário.

3. Clique no **link de redefinição de senha** no e-mail e defina a nova senha.
4. Retorne à interface web e faça login no Unified Manager usando a nova senha.

Altere a senha umadmin do Active IQ Unified Manager em sistemas Linux

Por motivos de segurança, você deve alterar a senha padrão do usuário umadmin do Unified Manager imediatamente após concluir o processo de instalação. Se necessário, você poderá alterar a senha novamente a qualquer momento.

Antes de começar

- O Unified Manager deve ser instalado em um sistema Red Hat Enterprise Linux.
- Você deve ter as credenciais do usuário raiz do sistema Linux no qual o Unified Manager está instalado.

Passos

1. Faça login como usuário raiz no sistema Linux em que o Unified Manager está em execução.
2. Altere a senha do umadmin:

   ```
   passwd umadmin
   ```

   O sistema solicita que você insira uma nova senha para o usuário umadmin.

Altere as portas que o Active IQ Unified Manager utiliza para os protocolos HTTP e HTTPS

As portas padrão que o Unified Manager usa para os protocolos HTTP e HTTPS podem ser alteradas após a instalação, se necessário por motivos de segurança. As portas padrão são 80 para HTTP e 443 para HTTPS.

Antes de começar

Você precisa ter um ID de usuário e uma senha autorizados para fazer login no console de manutenção do servidor Unified Manager.

> Algumas portas são consideradas inseguras ao usar os navegadores Mozilla Firefox ou Google Chrome. Verifique no seu navegador antes de atribuir um novo número de porta para o tráfego HTTP e HTTPS. Selecionar uma porta insegura pode tornar o sistema inacessível, o que exigiria que você entrasse em contato com o suporte ao cliente para obter uma solução.

A instância do Unified Manager é reiniciada automaticamente após você alterar a porta, portanto certifique-se de que este seja um bom momento para desligar o sistema por um curto período.

1. Faça login usando SSH como usuário de manutenção no host do Unified Manager.

   Os prompts do console de manutenção do Unified Manager são exibidos.

2. Digite o número da opção de menu rotulada **View/Change Application Ports** e pressione Enter.
3. Caso seja solicitado, digite novamente a senha do usuário de manutenção.
4. Digite os novos números de porta para as portas HTTP e HTTPS, e pressione Enter.

   Deixar o número da porta em branco atribui a porta padrão ao protocolo.

   Será perguntado a você se deseja alterar as portas e reiniciar o Unified Manager agora.

5. Digite **y** para alterar as portas e reiniciar o Unified Manager.
6. Saia do console de manutenção.

Após essa alteração, os usuários devem incluir o novo número da porta na URL para acessar a interface web do Unified Manager, por exemplo https://host.company.com:1234, https://12.13.14.15:1122, ou https://[2001:db8:0:1]:2123.

Adicionar interfaces de rede ao Active IQ Unified Manager

Você pode adicionar novas interfaces de rede se precisar separar tráfego de rede.

Antes de começar

Você deve ter adicionado a interface de rede ao dispositivo virtual usando o vSphere.

O appliance virtual precisa estar ligado.

> Não é possível executar esta operação se o Unified Manager estiver instalado no Red Hat Enterprise Linux ou no Microsoft Windows.

Passos

1. No menu principal do console do vSphere, selecione **Configuração do sistema** > **Reiniciar sistema operacional**.

   Após a reinicialização, o console de manutenção poderá detectar a interface de rede recém-adicionada.

2. Acesse o console de manutenção.
3. Selecione **Configuração de rede** > **Ativar interface de rede**.
4. Selecione a nova interface de rede e pressione **Enter**.

   Selecione **eth1** e pressione **Enter**.

5. Digite **y** para ativar a interface de rede.
6. Insira as configurações de rede.

   Você deverá inserir as configurações de rede se estiver usando uma interface estática ou se o DHCP não for detectado.

   Após inserir as configurações de rede, você retorna automaticamente ao menu **Configuração de Rede**.

7. Selecione **Confirmar alterações**.

   Você precisa confirmar as alterações para adicionar a interface de rede.

Regere o certificado de cliente no Active IQ Unified Manager

Você pode usar o console de manutenção para regenerar o certificado de cliente do Unified Manager. Seu certificado tem um período de validade estendido de cinco anos.

Passos

1. Faça login como usuário de manutenção.
2. Selecione **Regenerar certificado do cliente** e pressione **Enter**.
3. Se o sistema solicitar autenticação, insira as credenciais necessárias.
4. Selecione **Confirm Regeneration** e pressione **Enter**.
5. Após a regeneração do certificado, reinicie o serviço Unified Manager para aplicar as alterações.
6. Para verificar o certificado atualizado, faça login no ONTAP. Visualize o status do certificado do cliente e o status de validade.

Informações relacionadas "Gerencie os certificados do ONTAP com o System Manager"

Adicionar espaço de disco

Adicione espaço de disco ao diretório do banco de dados do Active IQ Unified Manager

O diretório do banco de dados do Unified Manager contém todos os dados de integridade e desempenho coletados dos sistemas ONTAP. Em algumas circunstâncias, pode ser necessário aumentar o tamanho do diretório do banco de dados.

Por exemplo, o diretório do banco de dados pode ficar cheio se o Unified Manager estiver coletando dados de um grande número de clusters onde cada cluster tem muitos nós. Você receberá um evento de aviso quando o diretório do banco de dados estiver 90% cheio e um evento crítico quando o diretório estiver 95% cheio.

Nenhum dado adicional é coletado dos clusters depois que o diretório atinge 95% de ocupação.

As etapas necessárias para adicionar capacidade ao diretório de dados variam dependendo de o Unified Manager estar em execução em um servidor VMware ESXi, em um servidor Red Hat ou em um servidor Microsoft Windows.

Adicione espaço ao diretório de dados em um host Linux no Active IQ Unified Manager

Se você alocou espaço de disco insuficiente ao `/opt/netapp/data` diretório para oferecer suporte ao Unified Manager quando configurou originalmente o host Linux e depois instalou o Unified Manager, você pode adicionar espaço de disco após a instalação, aumentando o espaço de disco no `/opt/netapp/data` diretório.

Antes de começar

Você deve ter acesso de usuário raiz à máquina Red Hat Enterprise Linux na qual o Unified Manager está instalado.

Recomendamos que você faça backup do banco de dados do Unified Manager antes de aumentar o tamanho do diretório de dados.

Passos

1. Faça login como usuário raiz na máquina Linux na qual você deseja adicionar espaço de disco.
2. Pare o serviço do Unified Manager e o software MySQL associado na ordem mostrada:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Crie uma pasta de backup temporária (por exemplo, `/backup-data`) com espaço de disco suficiente para conter os dados no diretório atual `/opt/netapp/data`.
4. Copie o conteúdo e a configuração de privilégios do diretório existente `/opt/netapp/data` para o diretório de dados de backup:

   ```
   cp -arp /opt/netapp/data/* /backup-data
   ```

5. Se o SE Linux estiver ativado:

   a. Obtenha o tipo do SE Linux para pastas em uma pasta `/opt/netapp/data` existente:

      ```
      se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
      head -1
      ```

      O sistema retorna uma confirmação semelhante à seguinte:

```
echo $se_type
mysqld_db_t
```

a. Execute o comando chcon para definir o tipo de SE Linux para o diretório de backup:

```
chcon -R --type=mysqld_db_t /backup-data
```

6. Remova o conteúdo do `/opt/netapp/data` diretório:
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. Aumente o tamanho do `/opt/netapp/data` diretório para um mínimo de 150 GB por meio de comandos LVM ou adicionando discos extras.

> Se você criou `/opt/netapp/data` a partir de um disco, não tente montar `/opt/netapp/data` como um compartilhamento NFS ou CIFS. Isso porque, nesse caso, ao tentar expandir o espaço de disco, alguns comandos LVM, como `resize` e `extend`, podem não funcionar como esperado.

8. Confirme se o `/opt/netapp/data` proprietário do diretório (mysql) e o grupo (root) permanecem inalterados:

```
ls -ltr /opt/netapp/ | grep data
```

O sistema retorna uma confirmação semelhante à seguinte:

```
drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
```

9. Se o SE Linux estiver ativado, confirme se o contexto do `/opt/netapp/data` diretório ainda está definido como mysqld_db_t:
   a. `touch /opt/netapp/data/abc`
   b. `ls -Z /opt/netapp/data/abc`

O sistema retorna uma confirmação semelhante à seguinte:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Exclua o arquivo abc para que esse arquivo desnecessário não cause um erro no banco de dados no futuro.
11. Copie o conteúdo de backup-data de volta para o diretório expandido `/opt/netapp/data`:

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. Se o SE Linux estiver ativado, execute o seguinte comando:

    ```
    chcon -R --type=mysqld_db_t /opt/netapp/data
    ```

13. Inicie o serviço MySQL:

    ```
    systemctl start mysqld
    ```

14. Após iniciar o serviço MySQL, inicie os serviços ocie e ocieau na ordem mostrada:

    ```
    systemctl start ocie ocieau
    ```

15. Após todos os serviços serem iniciados, exclua a pasta de backup `/backup-data`:

    ```
    rm -rf /backup-data
    ```

Adicione espaço ao disco de dados em uma máquina virtual no Active IQ Unified Manager

Se você precisar aumentar a quantidade de espaço no disco de dados para o banco de dados do Unified Manager, poderá adicionar capacidade após a instalação aumentando o espaço de disco por meio do console de manutenção do Unified Manager.

Antes de começar

- Você precisa ter acesso ao vSphere Client.
- A máquina virtual não deve ter nenhum snapshot armazenado localmente.
- Você precisa ter as credenciais do usuário de manutenção.

Recomendamos que você faça um backup da sua máquina virtual antes de aumentar o tamanho dos discos virtuais.

Passos

1. No cliente vSphere, selecione a máquina virtual do Unified Manager e, em seguida, adicione mais capacidade de disco aos dados `disk 3`. Consulte a documentação da VMware para obter detalhes.

   Em alguns casos raros, a implantação do Unified Manager usa “Hard Disk 2” para o disco de dados em vez de “Hard Disk 3”. Se isso ocorreu na sua implantação, aumente o espaço do disco que for maior. O disco de dados sempre terá mais espaço do que o outro disco.

2. No cliente vSphere, selecione a máquina virtual do Unified Manager e, em seguida, selecione a guia **Console**.
3. Clique na janela do console e, em seguida, faça login no console de manutenção usando seu nome de usuário e senha.
4. No menu principal, digite o número da opção **Configuração do sistema**.
5. No menu de configuração do sistema, insira o número da opção **Aumentar o tamanho do disco de dados**.

Adicionar espaço à unidade lógica em um servidor Windows no Active IQ Unified Manager

Se precisar aumentar a quantidade de espaço de disco para o banco de dados do Unified Manager, você pode adicionar capacidade à unidade lógica na qual o Unified

Manager está instalado.

Antes de começar

Você precisa ter privilégios de administrador do Windows.

Recomendamos que você faça backup do banco de dados do Unified Manager antes de adicionar espaço de disco.

Passos

1. Faça login como administrador no servidor Windows no qual deseja adicionar espaço de disco.
2. Siga o passo a passo correspondente ao método que deseja usar para adicionar mais espaço:

Opção	Descrição
Em um servidor físico, adicione capacidade à unidade lógica na qual o servidor do Unified Manager está instalado.	Siga os passos descritos no tópico da Microsoft: "Ampliar um Volume Básico"
Em um servidor físico, adicione um disco rígido.	Siga os passos descritos no tópico da Microsoft: "Adicionando discos rígidos"
Em uma máquina virtual, aumente o tamanho de uma partição de disco.	Siga os passos descritos no tópico da VMware: "Aumentar o tamanho de uma partição de disco"

Gerencie o acesso do usuário

Adicionar usuários

Adicionar usuários no Active IQ Unified Manager

Você pode adicionar usuários locais ou usuários de banco de dados usando a página Usuários. Também é possível adicionar usuários remotos ou grupos que pertencem a um servidor de autenticação. Você pode atribuir funções a esses usuários e, com base nos privilégios dessas funções, os usuários podem gerenciar os objetos de armazenamento e os dados com Unified Manager ou visualizar os dados em um banco de dados.

Antes de começar

- Você precisa ter a função de Application Administrator.
- Para adicionar um usuário ou grupo remoto, você precisa ter habilitado a autenticação remota e configurado seu servidor de autenticação.
- Se você planeja configurar a autenticação SAML para que um provedor de identidade (IdP) autentique os usuários que acessam a interface gráfica, certifique-se de que esses usuários sejam definidos como usuários “remote”.

  O acesso à interface do usuário não é permitido para usuários do tipo “local” ou “maintenance” quando a autenticação SAML está habilitada.

Se você adicionar um grupo do Active Directory do Windows, todos os membros diretos e subgrupos aninhados poderão se autenticar no Unified Manager, a menos que os subgrupos aninhados estejam

desativados. Se você adicionar um grupo do OpenLDAP ou de outros serviços de autenticação, somente os membros diretos desse grupo poderão se autenticar no Unified Manager.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Usuários**.
2. Na página Users, clique em **Add**.
3. Na caixa de diálogo Add User, selecione o tipo de usuário que você deseja adicionar e insira as informações necessárias.

   Ao inserir as informações de usuário necessárias, você deve especificar um endereço de e-mail exclusivo para esse usuário. Evite especificar endereços de e-mail compartilhados por vários usuários.

4. Clique em **Add**.

Crie um usuário de banco de dados no Active IQ Unified Manager

Para oferecer suporte a uma conexão entre o Workflow Automation e o Unified Manager, ou para acessar visualizações do banco de dados, você deve primeiro criar um usuário de banco de dados com a função Integration Schema ou Report Schema na interface da web do Unified Manager.

Antes de começar

Você precisa ter a função de Application Administrator.

Os usuários do banco de dados fornecem integração com o Workflow Automation e acesso a visualizações de banco de dados específicas de relatórios. Os usuários do banco de dados não têm acesso à interface da web do Unified Manager nem ao console de manutenção, e não podem executar chamadas de API.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Usuários**.
2. Na página Users, clique em **Add**.
3. Na caixa de diálogo Adicionar Usuário, selecione **Usuário do Banco de Dados** na lista suspensa **Tipo**.
4. Digite um nome e uma senha para o usuário do banco de dados.
5. Na lista suspensa **Função**, selecione a função apropriada.

Se você é…	Escolha esta função
Conectando o Unified Manager com o Workflow Automation	Esquema de integração
Acesso a relatórios e outras visualizações do banco de dados	Esquema do relatório

6. Clique em **Add**.

Editar configurações de usuário no Active IQ Unified Manager

Você pode editar as configurações do usuário, como o endereço de e-mail e a função, que são especificadas para cada usuário. Por exemplo, você pode querer alterar a função de um usuário que é operador de storage e atribuir privilégios de administrador

de storage a esse usuário.

Antes de começar

Você precisa ter a função de Application Administrator.

Ao modificar a função atribuída a um usuário, as alterações são aplicadas quando ocorre uma das seguintes ações:

- Você faz logout e login novamente no Unified Manager.
- A sessão atingiu o tempo limite de 24 horas.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Usuários**.
2. Na página Users, selecione o usuário para o qual você deseja editar as configurações e clique em **Edit**.
3. Na caixa de diálogo Edit User, edite as configurações apropriadas especificadas para o usuário.
4. Clique em **Salvar**.

Visualizar usuários no Active IQ Unified Manager

Você pode usar a página Usuários para visualizar a lista de usuários que gerenciam objetos de storage e dados usando o Unified Manager. Você pode visualizar detalhes sobre os usuários, como nome de usuário, tipo de usuário, endereço de e-mail e a função atribuída a eles.

Antes de começar

Você precisa ter a função de Application Administrator.

Etapa

1. No painel de navegação esquerdo, clique em **Geral** > **Usuários**.

Excluir usuários ou grupos no Active IQ Unified Manager

Você pode excluir um ou mais usuários do banco de dados do servidor de gerenciamento para impedir que usuários específicos acessem o Unified Manager. Você também pode excluir grupos para que todos os usuários do grupo não possam mais acessar o servidor de gerenciamento.

Antes de começar

- Ao excluir grupos remotos, você deve ter reatribuído os eventos atribuídos aos usuários desses grupos.

  Se você excluir usuários locais ou usuários remotos, os eventos atribuídos a esses usuários terão a atribuição removida automaticamente.

- Você precisa ter a função de Application Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Usuários**.
2. Na página Usuários, selecione os usuários ou grupos que deseja excluir e clique em **Excluir**.

3. Clique em **Sim** para confirmar a exclusão.

Saiba mais sobre controle de acesso baseado em funções no Active IQ Unified Manager

O RBAC (controle de acesso baseado em funções) oferece a capacidade de controlar quem tem acesso a vários recursos e funcionalidades no servidor do Active IQ Unified Manager. O RBAC permite que os administradores gerenciem grupos de usuários definindo funções. Se você precisar restringir o acesso a funcionalidades específicas para administradores selecionados, será necessário configurar contas de administrador para eles. Se você quiser restringir as informações que os administradores podem visualizar e as operações que podem executar, será necessário aplicar funções às contas de administrador que você criar.

O servidor de gerenciamento usa RBAC para login de usuários e permissões de função. Se você não alterou as configurações padrão do servidor de gerenciamento para acesso de usuários administrativos, não precisa fazer login para visualizá-las.

Ao iniciar uma operação que requer privilégios específicos, o servidor de gerenciamento solicita que você faça login. Por exemplo, para criar contas de administrador, você deve fazer login com acesso à conta Application Administrator.

Saiba mais sobre os tipos de usuários no Active IQ Unified Manager

Um tipo de usuário especifica o tipo de conta que o usuário possui e inclui usuários remotos, grupos remotos, usuários locais, usuários de banco de dados e usuários de manutenção. Cada um desses tipos tem sua própria função, que é atribuída por um usuário com a função de Administrator.

Os tipos de usuários do Unified Manager são os seguintes:

- **Usuário de manutenção**

  Criado durante a configuração inicial do Unified Manager. O usuário de manutenção cria outros usuários e atribui funções. O usuário de manutenção também é o único usuário com acesso ao console de manutenção. Quando o Unified Manager é instalado em um sistema Red Hat Enterprise Linux, o usuário de manutenção recebe o nome de usuário “umadmin.”

- **Usuário local**

  Acessa a interface de usuário do Unified Manager e executa funções com base na função atribuída pelo usuário de manutenção ou por um usuário com a função Application Administrator.

- **Grupo remoto**

  Um grupo de usuários que acessa a interface do usuário do Unified Manager usando as credenciais armazenadas no servidor de autenticação. O nome dessa conta deve corresponder ao nome de um grupo armazenado no servidor de autenticação. Todos os usuários do grupo remoto recebem acesso à interface do usuário do Unified Manager usando suas credenciais individuais de usuário. Os grupos remotos podem executar funções de acordo com os papéis atribuídos.

- **Usuário remoto**

  Acessa a interface do Unified Manager usando as credenciais armazenadas no servidor de autenticação. Um usuário remoto executa funções com base na função atribuída pelo usuário de manutenção ou por um usuário com a função Application Administrator.

- **Usuário do banco de dados**

  Possui acesso somente leitura aos dados no banco de dados do Unified Manager, não tem acesso à interface da web do Unified Manager nem ao console de manutenção e não pode executar chamadas de API.

Saiba mais sobre as funções de usuário no Active IQ Unified Manager

O usuário de manutenção ou o administrador de aplicativos atribui uma função a cada usuário. Cada função contém determinados privilégios. O escopo das atividades que você pode executar no Unified Manager depende da função atribuída e dos privilégios que essa função contém.

O Unified Manager inclui as seguintes funções de usuário predefinidas:

- **Operador**

  Exibe informações do sistema de storage e outros dados coletados pelo Unified Manager, incluindo históricos e tendências de capacidade. Essa função permite que o operador de storage visualize, atribua, reconheça, resolva e adicione notas aos eventos.

- **Administrador de storage**

  Configura operações de gerenciamento de storage no Unified Manager. Essa função permite que o administrador de storage configure limites e crie alertas, além de outras opções e políticas específicas de gerenciamento de storage.

- **Administrador de aplicativos**

  Configura definições não relacionadas ao gerenciamento de storage. Essa função permite o gerenciamento de usuários, certificados de segurança, acesso ao banco de dados e opções administrativas, incluindo autenticação, SMTP, rede e AutoSupport.

  Quando o Unified Manager é instalado em sistemas Linux, o usuário inicial com a função Application Administrator é automaticamente nomeado como “umadmin”.

- **Esquema de Integração**

  Esta função permite acesso somente leitura às visualizações do banco de dados do Unified Manager para integrar o Unified Manager com o OnCommand Workflow Automation (WFA).

- **Esquema do relatório**

  Esta função permite acesso somente leitura a relatórios e outras visualizações do banco de dados diretamente do banco de dados do Unified Manager. Os bancos de dados que podem ser visualizados incluem:

- netapp_model_view
- netapp_performance
- ocum
- ocum_report
- ocum_report_birt
- opm
- scalemonitor

Saiba mais sobre funções e capacidades de usuário no Active IQ Unified Manager

Com base na sua função de usuário atribuída, você pode determinar quais operações pode executar no Unified Manager.

A tabela a seguir exibe as funções que cada perfil de usuário pode executar:

Função	Operador	Administrador de storage	Administrador de Aplicativos	Esquema de integração	Esquema do relatório
Visualizar informações do sistema de storage	•	•	•	•	•
Veja outros dados, como históricos e tendências de capacidade	•	•	•	•	•
Visualizar, atribuir e resolver eventos	•	•	•		
Visualize objetos de serviço de storage, como associações de SVM e pools de recursos	•	•	•		
Ver políticas de limite	•	•	•		
Gerenciar objetos de serviço de storage, como associações de SVM e pools de recursos		•	•		
Definir alertas		•	•		

Função	Operador	Administrador de storage	Administrador de Aplicativos	Esquema de integração	Esquema do relatório
Gerencie as opções de gerenciamento de storage		•	•		
Gerenciar políticas de gerenciamento de storage		•	•		
Gerenciar usuários			•		
Gerenciar opções administrativas			•		
Definir políticas de limite			•		
Gerenciar o acesso ao banco de dados			•		
Gerencie a integração com o WFA e forneça acesso às visualizações do banco de dados				•	
Agendar e salvar relatórios		•	•		
Execute operações “Fix It” em Management Actions		•	•		
Fornecer acesso somente leitura às visualizações do banco de dados					•

Gerenciar configurações de autenticação SAML

Ative a autenticação SAML no Active IQ Unified Manager

Após configurar as definições de autenticação remota, você pode ativar a autenticação Security Assertion Markup Language (SAML) para que os usuários remotos sejam autenticados por um provedor de identidade (IdP) seguro antes de poderem acessar a interface de usuário da web do Unified Manager.

Observe que somente os usuários remotos terão acesso à interface gráfica de usuário do Unified Manager após a autenticação SAML ter sido ativada. Os usuários locais e os usuários de manutenção não poderão acessar a interface. Essa configuração não afeta os usuários que acessam o console de manutenção.

Utilize um provedor de identidade no Active IQ Unified Manager

Ao configurar o Unified Manager para usar um provedor de identidade (IdP) para realizar autenticação SAML para todos os usuários remotos, você precisa estar ciente de algumas configurações obrigatórias para que a conexão com Unified Manager seja bem-sucedida.

Você deve inserir o URI e os metadados do Unified Manager no servidor IdP. Você pode copiar essas informações da página SAML Authentication do Unified Manager. O Unified Manager é considerado o provedor de serviços (SP) no padrão Security Assertion Markup Language (SAML).

Padrões de criptografia suportados

- Padrão de Criptografia Avançado (AES): AES-128 e AES-256
- Algoritmo de Hash Seguro (SHA): SHA-1 e SHA-256

Provedores de identidade validados

- O Shibboleth
- O Active Directory Federation Services (ADFS)

Requisitos de configuração do ADFS

- Você deve definir três regras de declaração na seguinte ordem, que são necessárias para que o Unified Manager analise as respostas SAML do ADFS para esta entrada de confiança da parte confiável.

Regra de reivindicação	Valor
SAM-account-name	ID do nome
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Grupos de tokens — nome não qualificado	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Você deve definir o método de autenticação como “Forms Authentication” ou os usuários poderão receber um erro ao sair do Unified Manager . Siga estas etapas:
  a. Abra o ADFS Management Console.
  b. Clique na pasta Políticas de Autenticação na exibição em árvore à esquerda.
  c. Em Ações, à direita, clique em Editar política de autenticação primária global.
  d. Defina o método de autenticação da intranet como “Forms Authentication” em vez do padrão “Windows Authentication”.
- Em alguns casos, o login pelo IdP é rejeitado quando o certificado de segurança do Unified Manager é assinado por uma CA. Existem duas soluções alternativas para resolver esse problema:
  - Siga as instruções indicadas no link para desativar a verificação de revogação no servidor ADFS da parte confiável associada ao certificado de AC encadeada:

    "Desativar a verificação de revogação por confiança de parte confiável"

◦ Faça com que o servidor CA resida no servidor ADFS para assinar a solicitação de certificado do servidor do Unified Manager.

Outros requisitos de configuração

- O desvio de relógio do Unified Manager está configurado para 5 minutos, portanto a diferença de horário entre o servidor IdP e o servidor Unified Manager não pode ser superior a 5 minutos, caso contrário, a autenticação falhará.

Ative a autenticação SAML no Active IQ Unified Manager

Você pode habilitar a autenticação Security Assertion Markup Language (SAML) para que os usuários remotos sejam autenticados por um provedor de identidade (IdP) seguro antes de acessarem a interface de usuário da web do Unified Manager.

Antes de começar

- Você deve ter configurado a autenticação remota e verificado se ela foi bem-sucedida.
- Você deve ter criado pelo menos um Usuário Remoto, ou um Grupo Remoto, com a função de Administrador do Aplicativo.
- O provedor de identidade (IdP) deve ser compatível com o Unified Manager e deve estar configurado.
- Você precisa ter a URL do IdP e os metadados.
- Você precisa ter acesso ao servidor IdP.

Após habilitar a autenticação SAML no Unified Manager, os usuários não poderão acessar a interface gráfica de usuário até que o IdP seja configurado com as informações de host do servidor do Unified Manager. Portanto, você deve estar preparado para concluir ambas as partes da conexão antes de iniciar o processo de configuração. O IdP pode ser configurado antes ou depois de configurar o Unified Manager.

Somente usuários remotos terão acesso à interface gráfica de usuário do Unified Manager após a autenticação SAML ser ativada. Usuários locais e usuários de manutenção não poderão acessar a interface do usuário. Essa configuração não afeta usuários que acessam o console de manutenção, os comandos do Unified Manager ou as ZAPIs.

O Unified Manager é reiniciado automaticamente após você concluir a configuração SAML nesta página.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação SAML**.
2. Selecione a caixa de seleção **Enable SAML authentication**.

   São exibidos os campos necessários para configurar a conexão IdP.

3. Insira o URI do IdP e os metadados necessários para conectar o servidor do Unified Manager ao servidor IdP.

   Se o servidor IdP estiver acessível diretamente a partir do servidor do Unified Manager, você pode clicar no botão **Obter metadados do IdP** após inserir o URI do IdP para preencher automaticamente o campo de metadados do IdP.

4. Copie o URI de metadados do host do Unified Manager ou salve os metadados do host em um arquivo de texto XML.

Você pode configurar o servidor IdP com essas informações agora.

5. Clique em **Salvar**.

   Uma caixa de mensagem será exibida para confirmar que você deseja concluir a configuração e reiniciar o Unified Manager.

6. Clique em **Confirmar e Sair** e o Unified Manager será reiniciado.

Na próxima vez que usuários remotos autorizados tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do IdP em vez da página de login do Unified Manager.

Caso ainda não tenha feito isso, acesse seu IdP e insira a URI e os metadados do servidor do Unified Manager para concluir a configuração.

> Ao usar o ADFS como seu provedor de identidade, a GUI do Unified Manager não respeita o tempo limite do ADFS e continuará funcionando até que o tempo limite da sessão do Unified Manager seja atingido. Você pode alterar o tempo limite da sessão da GUI clicando em **Geral** > **Configurações de recursos** > **Tempo limite de inatividade**.

Altere o provedor de identidade de autenticação SAML no Active IQ Unified Manager

Você pode alterar o provedor de identidade (IdP) que o Unified Manager usa para autenticar usuários remotos.

Antes de começar

- Você precisa ter a URL do IdP e os metadados.
- Você precisa ter acesso ao IdP.

O novo IdP pode ser configurado antes ou depois de configurar o Unified Manager.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação SAML**.
2. Insira o novo URI do IdP e os metadados do IdP necessários para conectar o servidor do Unified Manager ao IdP.

   Se o IdP estiver acessível diretamente do servidor do Unified Manager, você poderá clicar no botão **Fetch IdP Metadata** após inserir a URL do IdP para preencher automaticamente o campo IdP Metadata.

3. Copie o URI de metadados do Unified Manager ou salve os metadados em um arquivo de texto XML.
4. Clique em **Salvar configuração**.

   Uma caixa de mensagem é exibida para confirmar que você deseja alterar a configuração.

5. Clique em **OK**.

Acesse o novo IdP e insira a URI do servidor do Unified Manager e os metadados para concluir a configuração.

Na próxima vez que usuários remotos autorizados tentarem acessar a interface gráfica do Unified Manager, eles deverão inserir suas credenciais na nova página de login do IdP em vez da antiga página de login do IdP.

Atualize as configurações de autenticação SAML após uma alteração no certificado de segurança do Active IQ Unified Manager

Qualquer alteração no certificado de segurança HTTPS instalado no servidor do Unified Manager exige que você atualize as configurações de autenticação SAML. O certificado é atualizado se você renomear o sistema host, atribuir um novo endereço IP ao sistema host ou alterar manualmente o certificado de segurança do sistema.

Após a alteração do certificado de segurança e a reinicialização do servidor do Unified Manager, a autenticação SAML deixará de funcionar, e os usuários não poderão acessar a interface gráfica do Unified Manager. Você deve atualizar as configurações de autenticação SAML tanto no servidor IdP quanto no servidor do Unified Manager para reativar o acesso à interface de usuário.

Passos

1. Faça login no console de manutenção.
2. No **Menu Principal**, insira o número da opção **Desativar autenticação SAML**.

   Uma mensagem será exibida para confirmar que você deseja desativar a autenticação SAML e reiniciar o Unified Manager.

3. Inicie a interface de usuário do Unified Manager usando o FQDN ou endereço IP atualizado, aceite no seu navegador o certificado de servidor atualizado e faça login usando as credenciais do usuário de manutenção.
4. Na página **Configuração/Autenticação**, selecione a aba **Autenticação SAML** e configure a conexão com o IdP.
5. Copie o URI de metadados do host do Unified Manager ou salve os metadados do host em um arquivo de texto XML.
6. Clique em **Salvar**.

   Uma caixa de mensagem será exibida para confirmar que você deseja concluir a configuração e reiniciar o Unified Manager.

7. Clique em **Confirmar e Sair** e o Unified Manager será reiniciado.
8. Acesse o servidor IdP e insira o URI do servidor do Unified Manager e os metadados para concluir a configuração.

Provedor de identidade	Etapas de configuração
ADFS	a. Exclua a entrada de confiança da parte confiável existente na interface gráfica de gerenciamento do ADFS. b. Adicione uma nova entrada de confiança de terceira parte confiável usando o `saml_sp_metadata.xml`do servidor Unified Manager atualizado. c. Defina as três regras de declaração necessárias para que o Unified Manager analise as respostas SAML do ADFS para esta entrada de confiança da parte confiável. d. Reinicie o serviço ADFS do Windows.

Provedor de identidade	Etapas de configuração
O Shibboleth	a. Atualize o novo FQDN do servidor do Unified Manager nos arquivos `attribute-filter.xml` e `relying-party.xml`. b. Reinicie o servidor web Apache Tomcat e aguarde até que a porta 8005 fique online.

9. Faça login no Unified Manager e verifique se a autenticação SAML está funcionando conforme o esperado por meio do seu IdP.

Desative a autenticação SAML no Active IQ Unified Manager

Você pode desativar a autenticação SAML quando desejar interromper a autenticação de usuários remotos por meio de um provedor de identidade (IdP) seguro antes que eles possam fazer login na interface web do Unified Manager. Quando a autenticação SAML está desativada, os provedores de serviço de diretório configurados, como o Active Directory ou o LDAP, realizam a autenticação de login.

Após desativar a autenticação SAML, os usuários locais e os usuários de manutenção poderão acessar a interface gráfica do usuário, além dos usuários remotos configurados.

Você também pode desativar a autenticação SAML usando o console de manutenção do Unified Manager, caso não tenha acesso à interface gráfica de usuário.

O Unified Manager é reiniciado automaticamente após a desativação da autenticação SAML.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação SAML**.
2. Desmarque a caixa de seleção **Ativar autenticação SAML**.
3. Clique em **Salvar**.

   Uma caixa de mensagem será exibida para confirmar que você deseja concluir a configuração e reiniciar o Unified Manager.

4. Clique em **Confirmar e Sair** e o Unified Manager será reiniciado.

Na próxima vez que os usuários remotos tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do Unified Manager em vez da página de login do IdP.

Acesse seu IdP e exclua o URI do servidor do Unified Manager e os metadados.

Desative a autenticação SAML no console de manutenção do Active IQ Unified Manager

Pode ser necessário desativar a autenticação SAML no console de manutenção quando não houver acesso à interface gráfica do Unified Manager. Isso pode ocorrer em casos de configuração incorreta ou se o IdP estiver inacessível.

Antes de começar

Você precisa ter acesso ao console de manutenção como o usuário de manutenção.

Quando a autenticação SAML está desativada, os provedores de serviço de diretório configurados, como Active Directory ou LDAP, realizam a autenticação de login. Os usuários locais e os usuários de manutenção poderão acessar a interface gráfica do usuário, além dos usuários remotos configurados.

Você também pode desativar a autenticação SAML na página Setup/Authentication da interface de usuário.

O Unified Manager é reiniciado automaticamente após a desativação da autenticação SAML.

Passos

1. Faça login no console de manutenção.
2. No **Menu Principal**, insira o número da opção **Desativar autenticação SAML**.

   Uma mensagem será exibida para confirmar que você deseja desativar a autenticação SAML e reiniciar o Unified Manager.

3. Digite **y** e pressione Enter para reiniciar o Unified Manager.

Na próxima vez que os usuários remotos tentarem acessar a interface gráfica do Unified Manager, eles inserirão suas credenciais na página de login do Unified Manager em vez da página de login do IdP.

Caso necessário, acesse seu IdP e exclua a URL do servidor do Unified Manager e os metadados.

Utilize a página de autenticação SAML no Active IQ Unified Manager

Você pode usar a página de autenticação SAML para configurar o Unified Manager para autenticar usuários remotos usando SAML por meio de um provedor de identidade (IdP) seguro antes que eles possam fazer login na interface web do Unified Manager.

- Você precisa ter a função Application Administrator para criar ou modificar a configuração do SAML.
- Você precisa ter configurado a autenticação remota.
- Você deve ter configurado pelo menos um usuário remoto ou um grupo remoto.

Após configurar a autenticação remota e os usuários remotos, você pode selecionar a caixa de seleção "Ativar autenticação SAML" para habilitar a autenticação usando um provedor de identidade seguro.

- **URI do IdP**

  O URI para acessar o IdP a partir do servidor Unified Manager. Veja abaixo alguns exemplos de URIs.

  Exemplo de URI do ADFS:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Exemplo de URI do Shibboleth:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Metadados do IdP**

Os metadados do IdP em formato XML.

Se o URL do IdP estiver acessível a partir do servidor do Unified Manager, você pode clicar no botão **Obter metadados do IdP** para preencher este campo.

- **Sistema host (FQDN)**

  O FQDN do sistema host do Unified Manager, conforme definido durante a instalação. Você pode alterar esse valor, se necessário.

- **URI do host**

  O URI para acessar o sistema host do Unified Manager a partir do IdP.

- **Metadados do host**

  Os metadados do sistema host em formato XML.

Gerenciar autenticação

Editar servidores de autenticação no Active IQ Unified Manager

Você pode alterar a porta que o servidor do Unified Manager usa para se comunicar com o seu servidor de autenticação.

Antes de começar

Você precisa ter a função de Application Administrator.

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Marque a caixa **Desativar pesquisa de grupo aninhado**.
3. Na área **Servidores de Autenticação**, selecione o servidor de autenticação que você deseja editar e clique em **Editar**.
4. Na caixa de diálogo **Editar Servidor de Autenticação**, edite os detalhes da porta.
5. Clique em **Salvar**.

Excluir servidores de autenticação no Active IQ Unified Manager

Você pode excluir um servidor de autenticação se quiser impedir que o servidor do Unified Manager se comunique com o servidor de autenticação. Por exemplo, se quiser alterar um servidor de autenticação com o qual o servidor de gerenciamento se comunica, você pode excluir o servidor de autenticação e adicionar um novo servidor de autenticação.

Antes de começar

Você precisa ter a função de Application Administrator.

Ao excluir um servidor de autenticação, os usuários ou grupos remotos desse servidor de autenticação não poderão mais acessar o Unified Manager.

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação Remota**.
2. Selecione um ou mais servidores de autenticação que você deseja excluir e clique em **Excluir**.
3. Clique em **Sim** para confirmar a solicitação de exclusão.

   Se a opção **Usar conexão segura** estiver ativada, os certificados associados ao servidor de autenticação serão excluídos juntamente com o servidor de autenticação.

Autentique com o Active Directory ou OpenLDAP no Active IQ Unified Manager

Você pode habilitar a autenticação remota no servidor de gerenciamento e configurar o servidor de gerenciamento para se comunicar com seus servidores de autenticação, para que os usuários desses servidores de autenticação possam acessar o Unified Manager.

Você pode usar um dos seguintes serviços de autenticação predefinidos ou especificar seu próprio serviço de autenticação:

- O Microsoft Active Directory

  Você não pode usar o Microsoft Lightweight Directory Services.

- O OpenLDAP

Você pode selecionar o serviço de autenticação necessário e adicionar os servidores de autenticação apropriados para permitir que os usuários remotos no servidor de autenticação acessem o Unified Manager. As credenciais de usuários ou grupos remotos são mantidas pelo servidor de autenticação. O servidor de gerenciamento usa o Protocolo Lightweight Directory Access Protocol (LDAP) para autenticar usuários remotos no servidor de autenticação configurado.

Para usuários locais criados no Unified Manager, o servidor de gerenciamento mantém seu próprio banco de dados de nomes de usuário e senhas. O servidor de gerenciamento realiza a autenticação e não utiliza o Active Directory ou o OpenLDAP para autenticação.

Registro de auditoria

Saiba mais sobre os registros de auditoria no Active IQ Unified Manager

É possível detectar se os logs de auditoria foram comprometidos usando os logs de auditoria. Todas as atividades realizadas por um usuário são monitoradas e registradas nos logs de auditoria. As auditorias são realizadas para todas as funcionalidades da interface de usuário e das APIs expostas publicamente do Active IQ Unified Manager.

Você pode usar a **Visualização de arquivos: log de auditoria** para visualizar e acessar todos os arquivos de log de auditoria disponíveis no seu Active IQ Unified Manager. Os arquivos na Visualização de arquivos: log de auditoria são listados com base na data de criação. Essa visualização exibe informações de todos os logs de auditoria capturados desde a instalação ou atualização até o momento no sistema. Sempre que você executa uma ação no Unified Manager, as informações são atualizadas e ficam disponíveis nos logs. O status de cada arquivo de log é capturado usando o atributo “File Integrity Status”, que é monitorado ativamente para detectar adulteração ou exclusão do arquivo de log. Os logs de auditoria podem ter um dos seguintes estados quando estão disponíveis no sistema:

Estado	Descrição
ATIVO	Arquivo no qual os logs estão sendo registrados atualmente.
NORMAL	Arquivo inativo, compactado e armazenado no sistema.
ADULTERADO	Arquivo comprometido por um usuário que editou o arquivo manualmente.
EXCLUSÃO MANUAL	Arquivo que foi excluído por um usuário autorizado.
ROLLOVER_DELETE	Arquivo excluído devido à remoção com base na Política de Configuração de Rotação.
UNEXPECTED_DELETE	Arquivo que foi excluído por motivos desconhecidos.

A página de log de auditoria inclui os seguintes botões de comando:

- Configurar
- Excluir
- Download

O botão **EXCLUIR** permite excluir qualquer um dos logs de auditoria listados na visualização Logs de auditoria. Você pode excluir um log de auditoria e, opcionalmente, fornecer um motivo para excluir o arquivo, o que ajuda no futuro a determinar se a exclusão foi válida. A coluna MOTIVO lista o motivo juntamente com o nome do usuário que realizou a operação de exclusão.

Excluir um arquivo de log remove o arquivo do sistema, mas não exclui a entrada na tabela do DB.

Você pode baixar os logs de auditoria do Active IQ Unified Manager usando o botão **DOWNLOAD** na seção Audit Logs e exportar os arquivos de log de auditoria. Os arquivos marcados como “NORMAL” ou “TAMPERED” são baixados em formato `.gzip` compactado.

Os arquivos de log de auditoria são arquivados periodicamente e salvos no banco de dados para referência. Antes do arquivamento, os logs de auditoria são assinados digitalmente para manter a segurança e a integridade.

Quando um pacote completo do AutoSupport é gerado, o pacote de suporte inclui arquivos de log de auditoria ativos e arquivados. Mas, quando um pacote de suporte simplificado é gerado, ele inclui apenas os logs de auditoria ativos. Os logs de auditoria arquivados não são incluídos.

Configurar os registros de auditoria do Active IQ Unified Manager

Você pode usar o botão **Configure** na seção Logs de Auditoria para configurar a política de rotação dos arquivos de log de auditoria e também habilitar o registro remoto dos Logs de Auditoria.

Você pode definir os valores em **MAX FILE SIZE** e **AUDIT LOG RETENTION DAYS** de acordo com a quantidade e a frequência de dados que deseja armazenar no sistema. O valor no campo **TOTAL AUDIT LOG SIZE** é o tamanho total dos dados do log de auditoria presentes no sistema. A política de rollover é determinada pelos valores no campo **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** e **TOTAL AUDIT LOG SIZE**. Quando o tamanho do backup do log de auditoria atinge o valor configurado em **TOTAL AUDIT LOG**

SIZE, o arquivo que foi arquivado primeiro é excluído. Isso significa que o arquivo mais antigo é excluído. Mas a entrada do arquivo continua disponível no banco de dados e é marcada como “Rollover Delete”. O valor de **AUDIT LOG RETENTION DAYS** corresponde ao número de dias durante os quais os arquivos de log de auditoria são preservados. Qualquer arquivo mais antigo que o valor definido neste campo passa por rollover.

Passos

1. Clique em **Logs de auditoria** > > **Configurar**.
2. Insira valores em **TAMANHO MÁXIMO DO ARQUIVO**, **TAMANHO TOTAL DO LOG DE AUDITORIA** e **DIAS DE RETENÇÃO DO LOG DE AUDITORIA**.

   Para ativar o registro remoto, selecione **Ativar registro remoto**.

Ative o registro remoto de logs de auditoria no Active IQ Unified Manager

Você pode selecionar a caixa de seleção **Habilitar registro remoto** na caixa de diálogo Configurar logs de auditoria para habilitar o registro remoto de auditoria. Você pode usar esse recurso para transferir logs de auditoria para um servidor Syslog remoto. Isso permitirá que você gerencie seus logs de auditoria quando houver restrições de espaço.

O registro remoto dos logs de auditoria fornece um backup à prova de adulteração caso os arquivos de log de auditoria no servidor Active IQ Unified Manager sejam adulterados.

Passos

1. Na caixa de diálogo **Configurar logs de auditoria**, selecione a caixa de seleção **Habilitar registro remoto**.

   São exibidos campos adicionais para configurar o registro remoto.

2. Digite o **HOSTNAME** e a **PORT** do servidor remoto ao qual você deseja se conectar.
3. No campo **CERTIFICADO DA CA DO SERVIDOR**, clique em **PROCURAR** para selecionar um certificado público do servidor de destino.

   O certificado deve ser carregado no formato `.pem`. Este certificado deve ser obtido do servidor Syslog de destino e não deve estar expirado. O certificado deve conter o “hostname” selecionado como parte do atributo `SubjectAltName`(SAN).

4. Insira os valores para os seguintes campos: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   Os valores devem estar em milissegundos para esses campos.

5. Selecione o formato Syslog necessário e a versão do protocolo TLS nos campos **FORMAT** e **PROTOCOL**.
6. Selecione a caixa de seleção **Habilitar autenticação de cliente** se o servidor Syslog de destino exigir autenticação baseada em certificado.

   Você precisará baixar o certificado de autenticação de cliente e carregá-lo no servidor Syslog antes de salvar a configuração do Log de Auditoria, caso contrário, a conexão falhará. Dependendo do tipo de servidor Syslog, talvez seja necessário criar um hash do certificado de autenticação de cliente.

   Exemplo: o syslog-ng requer que uma <hash> do certificado seja criada usando o comando `openssl x509 -noout -hash -in cert.pem`, e então você deve criar simbolicamente um link do certificado de autenticação de cliente para um arquivo nomeado com <hash> .0.

7. Clique em **Salvar** para configurar a conexão com o seu servidor e ativar o registro remoto.

   Você será redirecionado para a página de Registros de Auditoria.

   O valor de **Tempo limite de conexão** pode afetar a configuração. Se a configuração demorar mais para responder do que o valor definido, isso pode levar a uma falha na configuração devido a um erro de conexão. Para estabelecer uma conexão bem-sucedida, aumente o valor de **Tempo limite de conexão** e tente a configuração novamente.

Utilize a página de autenticação remota no Active IQ Unified Manager

Você pode usar a página de autenticação remota para configurar o Unified Manager para se comunicar com seu servidor de autenticação e autenticar usuários remotos que tentam fazer login na interface web do Unified Manager.

Você precisa ter a função de Application Administrator ou Storage Administrator.

Depois que você selecionar a caixa de seleção Ativar autenticação remota, poderá habilitar a autenticação remota usando um servidor de autenticação.

- **Serviço de Autenticação**

  Permite que você configure o servidor de gerenciamento para autenticar usuários em provedores de serviços de diretório, como o Active Directory, o OpenLDAP, ou para especificar seu próprio mecanismo de autenticação. Você só pode especificar um serviço de autenticação se tiver habilitado a autenticação remota.

  - **Active Directory**
    - Nome do administrador

      Especifica o nome do administrador do servidor de autenticação.

    - Senha

      Especifica a senha para acessar o servidor de autenticação.

    - Nome distinto base

      Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, o nome diferenciado base será **cn=ou,dc=domain,dc=com**.

    - Desativar pesquisa de grupo aninhado

      Especifica se a opção de pesquisa de grupos aninhados deve ser ativada ou desativada. Por padrão, essa opção está desativada. Se você usa o Active Directory, pode acelerar a autenticação desativando o suporte a grupos aninhados.

    - Usar conexão segura

      Especifica o serviço de autenticação usado para se comunicar com servidores de autenticação.

  - **O OpenLDAP**

- Nome diferenciado de bind

  Especifica o nome diferenciado de bind que é usado juntamente com o nome diferenciado base para encontrar usuários remotos no servidor de autenticação.

- Senha de bind

  Especifica a senha para acessar o servidor de autenticação.

- Nome distinto base

  Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, o nome diferenciado base será **cn=ou,dc=domain,dc=com**.

- Usar conexão segura

  Especifica que o LDAP seguro é usado para se comunicar com servidores de autenticação LDAP.

◦ **Outros**

- Nome diferenciado de bind

  Especifica o nome diferenciado de vinculação que é usado juntamente com o nome diferenciado base para encontrar usuários remotos no servidor de autenticação que você configurou.

- Senha de bind

  Especifica a senha para acessar o servidor de autenticação.

- Nome distinto base

  Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, o nome diferenciado base será **cn=ou,dc=domain,dc=com**.

- Versão do protocolo

  Especifica a versão do Lightweight Directory Access Protocol (LDAP) suportada pelo seu servidor de autenticação. Você pode especificar se a versão do protocolo deve ser detectada automaticamente ou definir a versão como 2 ou 3.

- Atributo de nome de usuário

  Especifica o nome do atributo no servidor de autenticação que contém os nomes de login dos usuários a serem autenticados pelo servidor de gerenciamento.

- Atributo de associação a grupo

  Especifica um valor que atribui a associação ao grupo de servidores de gerenciamento a usuários remotos com base em um atributo e valor especificados no servidor de autenticação do usuário.

- UGID

  Se os usuários remotos estiverem incluídos como membros de um objeto GroupOfUniqueNames no servidor de autenticação, esta opção permite atribuir aos usuários remotos a associação ao

grupo do servidor de gerenciamento com base em um atributo especificado nesse objeto GroupOfUniqueNames.

- Desativar pesquisa de grupo aninhado

  Especifica se a opção de pesquisa de grupos aninhados deve ser ativada ou desativada. Por padrão, essa opção está desativada. Se você usa o Active Directory, pode acelerar a autenticação desativando o suporte a grupos aninhados.

- Membro

  Especifica o nome do atributo que o seu servidor de autenticação usa para armazenar informações sobre os membros individuais de um grupo.

- Classe de objeto do usuário

  Especifica a classe de objeto de um usuário no servidor de autenticação remota.

- Classe de objeto de grupo

  Especifica a classe de objeto de todos os grupos no servidor de autenticação remoto.

> Os valores que você inserir para os atributos *Member*, *User Object Class* e *Group Object Class* devem ser os mesmos adicionados nas configurações do Active Directory, do OpenLDAP e do LDAP. Caso contrário, a autenticação poderá falhar.

- Usar conexão segura

  Especifica o serviço de autenticação usado para se comunicar com servidores de autenticação.

> Se você quiser modificar o serviço de autenticação, certifique-se de excluir todos os servidores de autenticação existentes e adicionar novos servidores de autenticação.

Área de servidores de autenticação

A área Servidores de Autenticação exibe os servidores de autenticação com os quais o servidor de gerenciamento se comunica para localizar e autenticar usuários remotos. As credenciais de usuários ou grupos remotos são mantidas pelo servidor de autenticação.

- **Botões de comando**

  Permite adicionar, editar ou excluir servidores de autenticação.

  - Adicionar

    Permite adicionar um servidor de autenticação.

  Se o servidor de autenticação que você está adicionando fizer parte de um par de alta disponibilidade (usando o mesmo banco de dados), você também poderá adicionar o servidor de autenticação parceiro. Isso permite que o servidor de gerenciamento se comunique com o parceiro quando um dos servidores de autenticação estiver inacessível.

  - Editar

    Permite que você edite as configurações de um servidor de autenticação selecionado.

◦ Excluir

Exclui os servidores de autenticação selecionados.

- **Nome ou endereço IP**

  Exibe o nome do host ou endereço IP do servidor de autenticação usado para autenticar o usuário no servidor de gerenciamento.

- **Porta**

  Exibe o número da porta do servidor de autenticação.

- **Teste de autenticação**

  Este botão valida a configuração do seu servidor de autenticação ao autenticar um usuário ou grupo remoto.

  Durante os testes, se você especificar apenas o nome de usuário, o servidor de gerenciamento procurará o usuário remoto no servidor de autenticação, mas não o autenticará. Se você especificar o nome de usuário e a senha, o servidor de gerenciamento procurará e autenticará o usuário remoto.

  Não é possível testar a autenticação se a autenticação remota estiver desativada.

Gerenciar certificados de segurança

Visualize o certificado de segurança HTTPS no Active IQ Unified Manager

Você pode comparar os detalhes do certificado HTTPS com o certificado obtido no seu navegador para garantir que a conexão criptografada do seu navegador com o Unified Manager não esteja sendo interceptada.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

A visualização do certificado permite verificar o conteúdo de um certificado regenerado ou visualizar os Nomes alternativos do assunto (SAN), a partir dos quais você pode acessar o Unified Manager.

Etapa

1. No painel de navegação esquerdo, clique em **Geral** > **Certificado HTTPS**.

   O certificado HTTPS é exibido na parte superior da página

Caso você precise visualizar informações mais detalhadas sobre o certificado de segurança do que as exibidas na página HTTPS Certificate, você pode visualizar o certificado de conexão no seu navegador.

Faça o download de uma solicitação de assinatura de certificado HTTPS no Active IQ Unified Manager

Você pode baixar uma solicitação de assinatura de certificado para o certificado de segurança HTTPS atual para que você possa fornecer o arquivo a uma Autoridade Certificadora (AC) para assiná-lo. Um certificado assinado por uma AC ajuda a evitar

ataques do tipo "man-in-the-middle" e oferece melhor proteção de segurança do que um certificado autoassinado.

Antes de começar

Você precisa ter a função de Application Administrator.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Certificado HTTPS**.
2. Clique em **Baixar Solicitação de Assinatura de Certificado HTTPS**.
3. Salve o `<hostname>.csr` arquivo.

Você pode fornecer o arquivo a uma autoridade de certificação para que ela o assine e, em seguida, instale o certificado assinado.

Instale um certificado HTTPS assinado por uma Autoridade Certificadora (CA) no Active IQ Unified Manager

Você pode fazer upload e instalar um certificado de segurança depois que uma Autoridade Certificadora (AC) o assinar e devolver. O arquivo que você faz upload e instala deve ser uma versão assinada do certificado autoassinado existente. Um certificado assinado por uma AC ajuda a evitar ataques "man-in-the-middle" e oferece melhor proteção de segurança do que um certificado autoassinado.

*O que. Antes de começar

Você deve ter concluído as seguintes ações:

- Baixou o arquivo de solicitação de assinatura de certificado e o enviou para assinatura por uma autoridade certificadora
- Salvou a cadeia de certificados no formato PEM
- Inclui todos os certificados na cadeia, do certificado do servidor do Unified Manager até o certificado raiz de assinatura, incluindo quaisquer certificados intermediários presentes

Você precisa ter a função de Application Administrator.

Se a validade do certificado para o qual um CSR foi criado for superior a 397 dias, a CA reduzirá essa validade para 397 dias antes de assinar e devolver o certificado

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Certificado HTTPS**.
2. Clique em **Instalar certificado HTTPS**.
3. Na caixa de diálogo que aparece, clique em **Escolher arquivo…** para localizar o arquivo que deseja carregar.
4. Selecione o arquivo e clique em **Instalar** para instalar o arquivo.

   Para informações, consulte "Instalando um certificado HTTPS gerado com ferramentas externas".

Exemplo de cadeia de certificados

O exemplo a seguir mostra como o arquivo da cadeia de certificados pode aparecer:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Saiba mais sobre certificados HTTPS gerados usando ferramentas externas no Active IQ Unified Manager Unified Manager

Você pode instalar certificados autoassinados ou assinados por uma Autoridade Certificadora (CA) e gerados usando uma ferramenta externa, como OpenSSL, BoringSSL, LetsEncrypt.

Você deve carregar a chave privada junto com a cadeia de certificados, porque esses certificados são um par de chaves pública-privada gerado externamente. Os algoritmos de par de chaves permitidos são “RSA” e “EC”. A opção **Install HTTPS Certificate** está disponível na página HTTPS Certificates, na seção General. O arquivo que você enviar deve estar no seguinte formato de entrada.

1. Chave privada do servidor que pertence ao host do Active IQ Unified Manager
2. Certificado do servidor que corresponde à chave privada
3. Certificados das ACs em ordem inversa até a raiz, que são usados para assinar o certificado acima

Formato para carregar um certificado com um par de chaves EC

As curvas permitidas são “prime256v1” e “secp384r1”. Exemplo de certificado com um par EC gerado externamente:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

Formato para carregar um certificado com um par de chaves RSA

Os tamanhos de chave permitidos para o par de chaves RSA pertencente ao certificado de host são 2048, 3072 e 4096. certificado com um **par de chaves RSA** gerado externamente:

```
-----BEGIN RSA PRIVATE KEY-----
<RSA private key of Server>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

Após o upload do certificado, você deverá reiniciar a instância do Active IQ Unified Manager para que as alterações entrem em vigor.

Verificações ao carregar certificados gerados externamente

O sistema realiza verificações durante o upload de um certificado gerado usando ferramentas externas. Se alguma das verificações falhar, o certificado será rejeitado. Há também validações incluídas para os certificados gerados a partir da CSR no produto e para os certificados gerados usando ferramentas externas.

- A chave privada informada é validada em relação ao certificado do host informado.
- O Common Name (CN) no certificado do host é verificado em relação ao FQDN do host.
- O nome comum (CN) do certificado do host não deve estar vazio ou em branco e não deve ser definido como localhost.
- A data de início da validade não deve estar no futuro, e a data de expiração da validade do certificado não deve estar no passado.

- Se existir CA intermediária ou CA, a data de início da validade do certificado não deve estar no futuro e a data de expiração da validade não deve estar no passado.

A chave privada na entrada não deve estar criptografada. Se houver chaves privadas criptografadas, elas serão rejeitadas pelo sistema.

Exemplo 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Exemplo 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Exemplo 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Se a instalação do certificado falhar, consulte o artigo da base de conhecimento (KB): "O ActiveIQ Unified Manager falha ao instalar um certificado gerado externamente"

Descrições de páginas para gerenciamento de certificados

Saiba mais sobre a página de certificado HTTPS em o Active IQ Unified Manager

A página de Certificado HTTPS permite visualizar o certificado de segurança atual, baixar uma solicitação de assinatura de certificado, gerar um novo certificado HTTPS autoassinado ou instalar um novo certificado HTTPS.

Se você não gerou um novo certificado HTTPS autoassinado, o certificado exibido nesta página é o certificado gerado durante a instalação.

Botões de comando

Os botões de comando permitem realizar as seguintes operações:

- **Baixar solicitação de assinatura de certificado HTTPS**

Faz o download de uma solicitação de certificação para o certificado HTTPS atualmente instalado. Seu navegador solicitará que você salve o arquivo <hostname>.csr para que você possa fornecê-lo a uma Autoridade Certificadora para assinatura.

- **Instalar certificado HTTPS**

  Permite fazer upload e instalar um certificado de segurança após uma Autoridade de Certificação tê-lo assinado e devolvido. O novo certificado entra em vigor após você reiniciar o servidor de gerenciamento.

- **Regenerar certificado HTTPS**

  Permite gerar um novo certificado HTTPS autoassinado, que substitui o certificado de segurança atual. O novo certificado entra em vigor após reiniciar o Unified Manager.

Regenerar a caixa de diálogo de certificado HTTPS em Active IQ Unified Manager

A caixa de diálogo "Regenerar certificado HTTPS" permite personalizar as informações de segurança e, em seguida, gerar um novo certificado HTTPS com essas informações.

As informações atuais do certificado aparecem nesta página.

As opções “Regenerar usando os atributos atuais do certificado” e “Atualizar os atributos atuais do certificado” permitem regenerar o certificado com as informações atuais ou gerar um certificado com novas informações.

- **Nome comum**

  Obrigatório. O nome de domínio totalmente qualificado (FQDN) que você deseja proteger.

  Em configurações de alta disponibilidade do Unified Manager, use o endereço IP virtual.

- **E-mail**

  Opcional. Um endereço de e-mail para contato com sua organização; normalmente, o endereço de e-mail do administrador de certificados ou do departamento de TI.

- **Empresa**

  Opcional. Normalmente, o nome registrado da sua empresa.

- **Departamento**

  Opcional. O nome do departamento em sua empresa.

- **Cidade**

  Opcional. A cidade onde sua empresa está localizada.

- **Estado**

  Opcional. O estado ou província onde sua empresa está localizada, sem abreviação.

- **País**

  Opcional. O país onde sua empresa está localizada. Normalmente, trata-se de um código ISO de duas letras do país.

- **Nomes Alternativos**

  Obrigatório. Nomes de domínio adicionais, não primários, que podem ser usados para acessar este servidor além do localhost existente ou de outros endereços de rede. Separe cada nome alternativo com uma vírgula.

  Selecione a caixa de seleção “Excluir informações de identificação local (por exemplo, localhost)” se você quiser remover as informações de identificação local do campo Nomes Alternativos no certificado. Quando esta caixa de seleção estiver marcada, somente o que você inserir no campo será usado no campo Nomes Alternativos. Se você deixar o campo em branco, o certificado resultante não terá um campo Nomes Alternativos.

- **TAMANHO DA CHAVE (ALGORITMO DA CHAVE: RSA)**

  O algoritmo de chave está definido como RSA. Você pode selecionar um dos tamanhos de chave: 2048, 3072 ou 4096 bits. O tamanho de chave padrão é 2048 bits.

- **PERÍODO DE VALIDADE**

  O período de validade padrão é de 397 dias. Se você atualizou de uma versão anterior, poderá ver que a validade do certificado anterior permaneceu inalterada.

Para obter mais informações, consulte "Gerando certificados HTTPS".

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.