Executar tarefas de configuração e administrativas

Active IQ Unified Manager

NetApp
October 15, 2025

Índice

Executar tarefas de configuração e administrativas

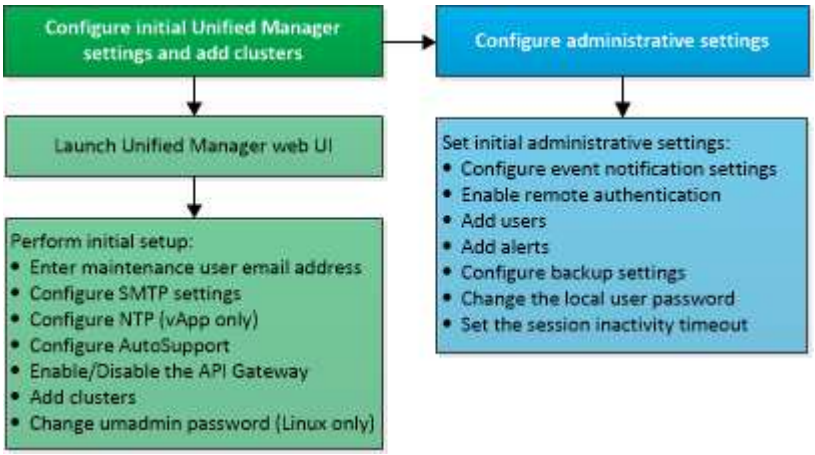
Configurar o Active IQ Unified Manager

Após instalar o Active IQ Unified Manager (antigo OnCommand Unified Manager), você deve concluir a configuração inicial (também chamada de assistente de primeira experiência) para acessar a interface da web. Em seguida, você pode executar tarefas de configuração adicionais, como adicionar clusters, configurar 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 definições de configuração recomendadas que são úteis para configurar em sua nova instância ou que é bom saber antes de iniciar o monitoramento regular de seus sistemas ONTAP .

Visão geral da sequência de configuração

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



Acesse a interface da Web do Unified Manager

Depois de instalar o Unified Manager, você pode 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 acessa a interface da web, você deve efetuar login como usuário de manutenção (ou usuário umadmin para instalações Linux).
- Se você planeja permitir que os usuários acessem o Unified Manager usando o nome curto em vez de usar o nome de domínio totalmente qualificado (FQDN) ou 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 reconhecer o risco de continuar o acesso ou instalar um certificado digital assinado pela Autoridade de Certificação (CA) para autenticação do servidor.

Passos

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

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

2. Efetue 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 da web em uma hora, seu acesso ao sistema será bloqueado e você precisará entrar em contato com o administrador do sistema. Isso é aplicável somente a usuários locais.

Execute a configuração inicial da interface da Web do Unified Manager

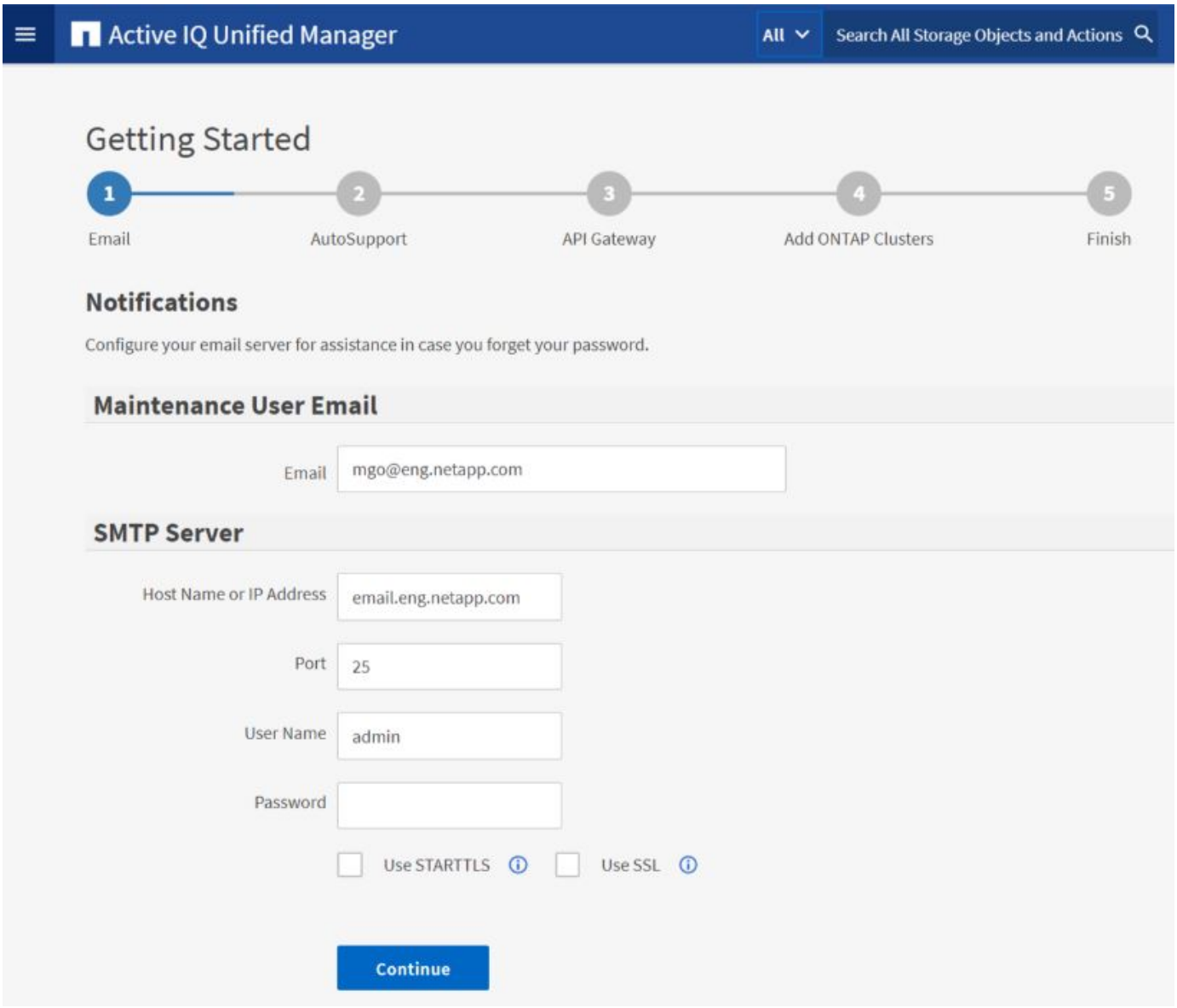
Para usar o Unified Manager, você deve primeiro configurar as opções de instalação inicial, incluindo o servidor NTP, o endereço de e-mail do usuário de manutenção, o host do servidor SMTP e a adição de clusters ONTAP .

Antes de começar

Você deve ter realizado as seguintes operações:

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

A página de introdução do Active IQ Unified Manager aparece somente quando você acessa a interface da Web pela primeira vez. A página abaixo é de uma instalação no VMware.



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

Passos

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

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

2. Na página AutoSupport , clique em **Concordar e continuar** 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 desabilitar 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 API Gateway, selecione se deseja usar o recurso API Gateway que permite ao Unified Manager gerenciar os clusters ONTAP que você planeja monitorar usando APIs REST ONTAP . Em seguida, clique em **Continuar**.

   Você pode habilitar ou desabilitar essa configuração mais tarde na interface da web em **Geral** > **Configurações de recursos** > **Gateway de API**. Para obter mais informações sobre as APIs, consulte"Introdução às 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 as credenciais de nome de usuário e senha - o usuário deve ter a função “admin”.

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

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

A página Introdução é fechada e a página Painel do Unified Manager é exibida.

Adicionar clusters

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

Antes de começar

- Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.
- Você deve ter as seguintes informações:
  - O Unified Manager oferece suporte a clusters ONTAP locais, ONTAP Select e Cloud Volumes ONTAP.
  - Nome do host ou endereço IP de gerenciamento de 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 de cluster deve ser o LIF de gerenciamento de cluster da máquina virtual de armazenamento administrativo (SVM). Se você usar um LIF de gerenciamento de nós, 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*, *console* e *http*.

  - O número da porta para conectar ao cluster usando o protocolo HTTPS (normalmente porta 443)
  - Você possui os certificados necessários:

    Certificado SSL (HTTPS): Este certificado é de propriedade do Unified Manager. Um certificado SSL

autoassinado padrão (HTTPS) é gerado com uma nova instalação do Unified Manager. A NetApp recomenda que você 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 a regeneração do certificado SSL, consulte"Gerando um certificado de segurança HTTPS" .

Certificado EMS: Este certificado é de propriedade do Unified Manager. É usado durante a autenticação para notificações EMS recebidas do ONTAP.

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

A autenticação baseada em certificado não será habilitada automaticamente para um cluster se você estiver atualizando uma versão mais antiga do Unified Manager. No entanto, você pode habilitá-lo 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 a partir da interface da web, e a autenticação baseada em certificado será ativada automaticamente.
- Você pode adicionar um cluster por meio do Unified Manager CLI; a autenticação baseada em certificado não está habilitada por padrão. Se você adicionar um cluster usando a CLI do Unified Manager, será necessário editar o cluster usando a interface do usuário do Unified Manager. Você pode ver"Comandos CLI do Unified Manager suportados" para adicionar um cluster usando o Unified Manager CLI.
- Se a autenticação baseada em certificado estiver habilitada para um cluster e você fizer o backup do Unified Manager de um servidor e restaurar em outro servidor do Unified Manager onde o nome do host ou endereço IP for alterado, o monitoramento do cluster poderá falhar. Para evitar a falha, edite e salve os detalhes do cluster. Para obter mais informações sobre a edição de detalhes do cluster, consulte"Editando clusters" .

+ **Certificados de cluster**: Este certificado é de propriedade da ONTAP. Não é possível adicionar um cluster ao Unified Manager com um certificado expirado e, se o certificado já tiver expirado, você deverá 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 ONTAP na interface de usuário do System Manager" .

- Você deve ter espaço adequado no servidor do Unified Manager. Você não poderá adicionar um cluster ao servidor quando mais de 90% do espaço no diretório do banco de dados já estiver consumido.

Para uma configuração do MetroCluster , você deve adicionar os clusters locais e remotos, e os clusters devem ser configurados corretamente.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de cluster**.
2. Na página Configuração do cluster, clique em **Adicionar**.
3. Na caixa de diálogo Adicionar cluster, especifique os valores necessários, como o nome do host ou endereço IP do cluster, nome de usuário, senha e número da porta.

Você pode alterar o endereço IP de gerenciamento de cluster de IPv6 para IPv4 ou de IPv4 para IPv6. O novo endereço IP é 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 Autorizar Host, clique em **Exibir Certificado** para visualizar as informações do certificado sobre o cluster.
6. Clique em **Sim**.

   Depois de salvar os detalhes do cluster, você pode ver o certificado para comunicação TLS mútua de um cluster.

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

Depois que todos os objetos de um novo cluster são 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. Este recurso fornece mais de duas semanas de informações de desempenho para um cluster imediatamente após ele ser adicionado. 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 muita CPU, é recomendável escalonar a adição de novos clusters para que as pesquisas de 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 para o período ausente.

Se você receber uma mensagem de erro informando que não é possível adicionar o cluster, verifique se os relógios nos 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 NTP ou um serviço similar.

Informações relacionadas

"Instalando um certificado HTTPS assinado e retornado por uma CA"

Configurar o Unified Manager para enviar notificações de alerta

Você pode configurar o Unified Manager para enviar notificações que o alertam sobre eventos no seu ambiente. Antes que as notificações possam ser enviadas, você deve configurar várias outras opções do Unified Manager.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

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

Passos

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

   Se você quiser que notificações de alerta sejam enviadas quando determinados eventos ocorrerem em seu ambiente, você deve configurar um servidor SMTP e fornecer um endereço de e-mail do qual a notificação de alerta será enviada. Se você quiser usar traps SNMP, você pode 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, será necessário habilitar a autenticação remota.

3. "Adicionar servidores de autenticação".

   Você pode adicionar servidores de autenticação para que usuários remotos dentro do 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 enviar notificações, adicionar usuários para receber as notificações, configurar suas configurações de rede e configurar as opções SMTP e SNMP necessárias para seu ambiente, você poderá atribuir alertas.

Configurar as definições de notificação de eventos

Você pode configurar o Unified Manager para enviar notificações de alerta quando um evento for gerado ou quando um evento for 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 interceptações SNMP.

Antes de começar

Você deve ter as seguintes informações:

- Endereço de e-mail de onde a notificação de alerta é enviada

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

- Nome do host do servidor SMTP e o nome de usuário e senha para acessar o servidor
- Nome do host ou endereço IP do host de destino da armadilha que receberá a armadilha SNMP, juntamente com a versão SNMP, porta da armadilha de saída, comunidade e outros valores de configuração SNMP necessários

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

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Passos

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

   Notas:

   - Se o Endereço De estiver preenchido com o endereço "ActiveIQUnifiedManager@localhost.com", você deverá alterá-lo para um endereço de e-mail real e funcional para garantir que todas as notificações por e-mail sejam entregues com sucesso.
   - Se o nome do host do servidor SMTP não puder ser resolvido, você poderá 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 será exibida depois que você clicar no botão **Salvar**. Verifique os detalhes do certificado e aceite o certificado para salvar as configurações de notificação.

   Você pode clicar no botão **Exibir detalhes do certificado** para visualizar os detalhes do certificado. Se o certificado existente 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.

Habilitar autenticação remota

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 armazenamento e dados.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

> O servidor do Unified Manager deve ser conectado diretamente ao servidor de autenticação. Você deve desabilitar todos os 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 por LDAP e LDAPS (LDAP seguro). O Unified Manager usa 389 como a porta padrão para comunicação não segura e 636 como a porta padrão para comunicação segura.

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

Passos

1. No painel de navegação esquerdo, 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 tipo de autenticação…	Insira as seguintes informações…
Diretório ativo	• 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 do administrador • Nome distinto base (usando a notação LDAP apropriada)
Abra o LDAP	• Vincular nome distinto (na notação LDAP apropriada) • Vincular senha • Nome distinto base

Se a autenticação de um usuário do Active Directory demorar muito ou atingir o tempo limite, o servidor de autenticação provavelmente está demorando muito para responder. Desabilitar o suporte para 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**.

Desabilitar grupos aninhados da autenticação remota

Se você tiver a autenticação remota habilitada, poderá desabilitar a autenticação de grupo aninhada para que somente usuários individuais, e não membros do grupo, 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 deve ter a função de Administrador do Aplicativo.
- A desabilitação de grupos aninhados só é aplicável ao usar o Active Directory.

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

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação Remota**.
2. Marque a caixa **Desativar pesquisa de grupo aninhado**.

3. Clique em **Salvar**.

Configurar serviços de autenticação

Os serviços de autenticação permitem a autenticação de usuários remotos ou grupos remotos em um servidor de autenticação antes de fornecer 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 deve ter a função de Administrador do Aplicativo.

Passos

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

Se você selecionar…	Então faça isto…
Diretório ativo	a. Digite o nome e a senha do administrador. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, o nome distinto base será **cn=ou,dc=domain,dc=com**.
OpenLDAP	a. Digite o nome distinto e a senha de vinculação. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for ou@domain.com, o nome distinto base será **cn=ou,dc=domain,dc=com**.

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

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

3. Clique em **Salvar**.

Adicionar servidores de autenticação

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

Antes de começar

- As seguintes informações 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 deve ter a função de Administrador do Aplicativo.

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 do 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 esquerdo, clique em **Geral** > **Autenticação Remota**.
2. Habilite ou desabilite a opção **Usar conexão segura**:

Se você quiser…	Então faça isto…
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 endereço IP (IPv4 ou IPv6) do servidor. d. Na caixa de diálogo Autorizar Host, clique em Exibir Certificado. e. Na caixa de diálogo Exibir certificado, verifique as informações do certificado e clique em **Fechar**. f. Na caixa de diálogo Autorizar Host, clique em **Sim**. Quando você habilita a opção **Usar autenticação de conexão segura**, o Unified Manager se comunica com o servidor de autenticação e exibe o certificado. O Unified Manager usa 636 como porta padrão para comunicação segura e a porta número 389 para comunicação não segura.
Desabilite-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 e os detalhes da porta. d. Clique em **Adicionar**.

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

3. Execute um teste de autenticação para confirmar se você pode autenticar usuários no servidor de autenticação que você adicionou.

Teste a configuração dos servidores de autenticação

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 em seus servidores de autenticação e autenticando-os 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 ou grupo remoto.
- Você deve ter adicionado seus servidores de autenticação para que o servidor de gerenciamento possa procurar o usuário remoto ou grupo remoto nesses servidores e autenticá-los.
- Você deve ter a função de Administrador do Aplicativo.

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

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação Remota**.
2. Clique em **Testar autenticação**.
3. Na caixa de diálogo Testar usuário, especifique o nome de usuário e a senha do usuário remoto ou o nome de usuário do grupo remoto e clique em **Testar**.

   Se você estiver autenticando um grupo remoto, não deverá digitar a senha.

Adicionar alertas

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

Antes de começar

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

Você pode criar um alerta diretamente na página Detalhes do evento após receber um evento, além de criar um alerta na página Configuração de alerta, conforme descrito aqui.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de alerta**.
2. Na página Configuração de alerta, 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 a serem incluídos ou excluídos do alerta.

   Você pode definir um filtro especificando uma sequência de texto no campo **Nome contém** para selecionar um grupo de recursos. Com base na sequência de texto especificada, a lista de recursos

disponíveis exibe apenas aqueles que correspondem à regra de filtro. A sequência de texto que você especificar diferencia maiúsculas de minúsculas.

Se um recurso estiver em conformidade com as regras de inclusão e exclusão especificadas, a regra de exclusão terá precedência sobre a regra de inclusão, e o alerta não será 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 o qual você deseja acionar um alerta.

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

6. Clique em **Ações** e selecione os usuários que deseja notificar, escolha a frequência de notificação, escolha se uma armadilha SNMP será enviada ao receptor da armadilha e atribua um script a ser executado 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 porque o endereço de e-mail modificado não estará mais mapeado para o 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 adição de um alerta

Este exemplo mostra como criar um alerta que atende 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 "Teste", e o usuário deve ser notificado a cada 15 minutos

Execute as seguintes etapas na caixa de diálogo Adicionar alerta:

Passos

1. Clique em **Nome** e insira **HealthTest** no campo **Nome do alerta**.
2. Clique em **Recursos** e, na guia Incluir, 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'] +** da área Recursos Disponíveis e mova-o para a área Recursos Selecionados.
   c. Clique em **Excluir** e insira **xyz** no campo **Nome contém** e depois clique em **Adicionar**.
3. Clique em **Eventos** e selecione **Crítico** no campo Gravidade do Evento.
4. Selecione **Todos os Eventos Críticos** na área Eventos Correspondentes e mova-os para a área Eventos Selecionados.
5. Clique em **Ações** e insira **sample@domain.com** no campo Alertar estes usuários.

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 por um período específico. Você deve determinar o horário a partir do qual a notificação de 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

Você pode alterar sua senha de login de usuário local para evitar potenciais riscos de segurança.

Antes de começar

Você deve estar logado como usuário local.

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

Passos

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

   A opção **Alterar senha** não será exibida se você for um usuário remoto.

3. Na caixa de diálogo Alterar senha, digite 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.

Definir o tempo limite de inatividade da sessão

Você pode especificar o valor do tempo limite de inatividade do 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 deve ter a função de Administrador do Aplicativo.

Esta configuração afeta todas as sessões de usuários conectados.

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

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 isto…
Não defina nenhum tempo limite para que a sessão nunca seja fechada automaticamente	No painel **Tempo limite de inatividade**, mova o botão deslizante para a esquerda (desligado) e clique em **Aplicar**.
Defina um número específico de minutos como valor de tempo limite	No painel **Tempo limite de inatividade**, mova o botão deslizante para a direita (ligado), especifique o valor do tempo limite de inatividade em minutos e clique em **Aplicar**.

Defina o tempo limite da sessão por meio da CLI

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 de tempo. Por padrão, o tempo limite da sessão é definido para o valor máximo, que é 4.320 minutos (72 horas). Isso significa que sua sessão termina automaticamente após 72 horas, mesmo que você esteja conectado e usando ativamente o Unified Manager.

Sobre esta tarefa

Você deve ter a função de Administrador do Aplicativo.

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

Passos

1. Efetue login no Unified Manager CLI inserindo o `um cli login` comando. Use um nome de usuário e senha válidos para autenticação.
2. Entre no `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

Em algum momento, você pode querer alterar o nome do host do sistema no qual instalou o Unified Manager. Por exemplo, você pode querer renomear o host para identificar mais facilmente seus servidores do Unified Manager por tipo, grupo de trabalho ou grupo de cluster monitorado.

As etapas necessárias para alterar o nome do host são diferentes dependendo se o Unified Manager está sendo executado em um servidor VMware ESXi, em um servidor Red Hat Linux ou em um servidor Microsoft Windows.

Alterar o nome do host do appliance virtual do 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 gerar novamente o certificado HTTPS.

Antes de começar

Você deve estar conectado ao Unified Manager como usuário de manutenção ou ter a função de Administrador de Aplicativos atribuída a você para executar essas tarefas.

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, você teria designado um nome para o 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 estiver configurado corretamente, o nome do host "Unified Manager" será automaticamente atribuído e associado ao certificado de segurança.

Independentemente de como o nome do host foi atribuído, se você alterar o nome do host e pretende usar o novo nome do host para acessar a interface de usuário 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 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 não entrará em vigor até que a máquina virtual do Unified Manager seja reiniciada.

Passos

1. Gerar um certificado de segurança HTTPS

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

2. Reinicie a máquina virtual do Unified Manager

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

Gerar um certificado de segurança HTTPS

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 que substitui o certificado existente.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Pode haver vários motivos para regenerar o certificado, como se você desejasse ter valores melhores para Nome Distinto (DN), se quisesse um tamanho de chave maior, um período de expiração mais longo ou se o certificado atual tivesse expirado.

Se você não tiver acesso à interface da Web do Unified Manager, poderá gerar novamente o certificado HTTPS com os mesmos valores usando o console de manutenção. Ao regenerar certificados, você pode definir o tamanho da chave e a duração da validade da chave. Se você usar o `Reset Server Certificate` opção do console de manutenção, então um novo certificado HTTPS é criado e é válido por 397 dias. Este certificado terá uma chave RSA de tamanho 2048 bits.

Passos

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

   A caixa de diálogo Regenerar certificado HTTPS é exibida.

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

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

Se você quiser…	Faça isso…
Gerar o certificado usando valores diferentes	Clique na opção **Atualizar os atributos atuais do certificado**. 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 são de no mínimo 1 dia e no máximo 36.500 dias. Embora seja permitido um período de validade de 36.500 dias, é recomendável usar um período de validade de no máximo 397 dias ou 13 meses. Porque se você selecionar um período de validade de mais de 397 dias e planejar exportar um CSR para este certificado e obtê-lo assinado por uma CA conhecida, a validade do certificado assinado devolvido a você pela CA será reduzida para 397 dias. • Você pode selecionar a caixa de seleção “Excluir informações de identificação local (por exemplo, host local)” se 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 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 visualizando o certificado HTTPS.

Reinicie a máquina virtual do Unified Manager

Você pode reiniciar a máquina virtual no 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 dispositivo virtual está ligado.

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

Você também pode reiniciar a máquina virtual do vSphere usando a opção **Reiniciar Convidado**. Consulte a documentação do VMware para obter mais informações.

Passos

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

Alterar o nome do host do Unified Manager em sistemas Linux

Em algum momento, você pode 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 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 root 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, você teria 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 pretende 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 melhor prática é atualizar o certificado para que o nome do host no certificado corresponda ao nome do host real. O novo certificado não entrará em vigor até que a máquina Linux seja 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. Efetue login como usuário root no sistema Unified Manager que você deseja modificar.

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

   ```
   systemctl stop ocieau ocie mysqld
   ```

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

   ```
   hostnamectl set-hostname new_FQDN

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

4. Regenere 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 o serviço ser reiniciado, verifique se o novo nome do host consegue fazer ping em si mesmo:

   ```
   ping new_hostname

   ping nuhost
   ```

   Este comando deve retornar o mesmo endereço IP que foi definido 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
   ```

Habilitar e desabilitar o gerenciamento de armazenamento baseado em políticas

A partir do Unified Manager 9.7, você pode provisionar cargas de trabalho de armazenamento (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 anexação de políticas de QoS, mas quando aplicada usando o Unified Manager, você pode provisionar e gerenciar cargas de trabalho em todos os clusters que sua instância do Unified Manager está monitorando.

Você deve ter a função de Administrador do Aplicativo.

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

Quando ativada, esta opção fornece muitos itens novos na interface do 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 armazenamento de desempenho	Disponível em **Configurações** > **Políticas** > **Eficiência de armazenamento**
Painéis que descrevem seu desempenho de carga de trabalho atual e IOPS de carga de trabalho	Disponível no Painel

Consulte a ajuda on-line do produto para obter mais informações sobre essas páginas e 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 armazenamento baseado em políticas escolhendo uma das seguintes opções:

Se você quiser…	Então faça isto…
Desabilitar o gerenciamento de armazenamento baseado em políticas	No painel **Gerenciamento de armazenamento baseado em políticas**, mova o botão deslizante para a esquerda.
Habilitar gerenciamento de armazenamento baseado em políticas	No painel **Gerenciamento de armazenamento baseado em políticas**, mova o botão deslizante para a direita.

Configurar backup do Unified Manager

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

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

Gerenciar configurações de recursos

A página Configurações de recursos permite que você habilite e desabilite recursos específicos no Active IQ Unified Manager. Isso inclui criar e gerenciar objetos de armazenamento com base em políticas, habilitar o API Gateway e o Login Banner, carregar scripts para gerenciar alertas, tempo limite de uma sessão da interface do usuário da Web com base no tempo de inatividade e desabilitar o recebimento de

eventos da plataforma Active IQ .

> A página Configurações de recursos está disponível somente para usuários com função de Administrador do aplicativo.

Para obter informações sobre o upload de scripts, consulte"Habilitando e desabilitando o upload de scripts" .

Habilitar gerenciamento de armazenamento baseado em políticas

A opção **Gerenciamento de armazenamento baseado em políticas** permite o gerenciamento de armazenamento com base em objetivos de nível de serviço (SLOs). Esta opção é habilitada por padrão.

Ao ativar esse recurso, você pode provisionar cargas de trabalho de armazenamento nos clusters 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 Políticas de Eficiência de Armazenamento atribuídos.

Você pode optar por ativar ou desativar esse recurso em **Geral** > **Configurações de recursos** > **Gerenciamento de armazenamento baseado em políticas**. Ao ativar este recurso, as seguintes páginas estarão disponíveis para operação e monitoramento:

- Provisionamento (provisionamento de carga de trabalho de armazenamento)
- **Políticas** > **Níveis de Serviço de Desempenho**
- **Políticas** > **Eficiência de Armazenamento**
- 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**

Você pode usar as telas para criar Níveis de Serviço de Desempenho e Políticas de Eficiência de Armazenamento, além de provisionar cargas de trabalho de armazenamento. Você também pode monitorar as cargas de trabalho de armazenamento que estão em conformidade com os Níveis de Serviço de Desempenho atribuídos, bem como as que não estão em conformidade. O painel Desempenho da carga de trabalho e IOPS da carga de trabalho também permite que você avalie a capacidade e o desempenho (IOPS) total, disponível e usado dos clusters em seu data center com base nas cargas de trabalho de armazenamento provisionadas neles.

Após ativar esse recurso, você pode executar as APIs REST do Unified Manager para executar algumas dessas funções em **Barra de menus** > **Botão Ajuda** > **Documentação da API** > categoria **provedor de armazenamento**. Como alternativa, você pode inserir o nome do host ou endereço IP e a URL para acessar a página da API REST no formato https://<nome do host>/docs/api/

Para obter mais informações sobre as APIs, consulte"Introdução às APIs REST do Active IQ Unified Manager" .

Habilitar API Gateway

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

Você pode habilitar esse recurso nas páginas de configuração que aparecem quando você faz login pela

primeira vez no Unified Manager. Como alternativa, você pode habilitar ou desabilitar esse recurso em **Geral** > **Configurações de recursos** > **Gateway de API**.

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 aproveitadas usando as APIs REST do Unified Manager. No entanto, se você tiver um requisito comercial específico de acesso às APIs do ONTAP para gerenciar recursos específicos que não são expostos ao Unified Manager, você pode habilitar o recurso API Gateway e executar as APIs do ONTAP . O gateway atua como um proxy para encapsular as solicitações de API, mantendo o cabeçalho e o corpo das solicitações no mesmo formato das APIs ONTAP . Você pode usar suas credenciais do Unified Manager e executar as APIs específicas para acessar e gerenciar os clusters ONTAP sem passar credenciais de cluster individuais. O Unified Manager funciona como um único ponto de gerenciamento para executar as APIs nos clusters 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 pode 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 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"Introdução às APIs REST do Active IQ Unified Manager" .

Especificar tempo limite de inatividade

Você pode especificar o valor do tempo limite de inatividade para o Active IQ Unified Manager. Após um período de inatividade especificado, o aplicativo será desconectado automaticamente. Esta opção é habilitada por padrão.

Você pode desativar esse recurso ou modificar o tempo em **Geral** > **Configurações de recursos** > **Tempo limite de inatividade**. Depois de ativar esse recurso, você deve especificar o limite de tempo de inatividade (em minutos) no campo **SAIR APÓS**, após o qual o sistema efetuará logout automaticamente. O valor padrão é 4320 minutos (72 horas).

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

Habilitar eventos do portal Active IQ

Você pode especificar se deseja habilitar ou desabilitar eventos do portal Active IQ . Esta configuração permite que o portal Active IQ descubra e exiba eventos adicionais sobre configuração do sistema, cabeamento e assim por diante. Esta opção é habilitada por padrão.

Ao habilitar esse recurso, o Active IQ Unified Manager exibe eventos descobertos pelo portal Active IQ . Esses eventos são criados executando um conjunto de regras em mensagens do AutoSupport geradas de todos os sistemas de armazenamento monitorados. Esses eventos são diferentes dos outros eventos do Unified Manager e identificam incidentes ou riscos relacionados à configuração do sistema, cabeamento, práticas recomendadas e problemas de disponibilidade.

Você pode escolher ativar ou desativar esse recurso em **Geral** > **Configurações de recursos** > **Eventos Active IQ *. Em sites sem acesso à rede externa, você deve carregar as regras manualmente em**

***Gerenciamento de armazenamento** > **Configuração de evento** > **Carregar regras**.

Este recurso é habilitado por padrão. Desabilitar esse recurso impede que os eventos do Active IQ sejam descobertos ou exibidos no Unified Manager. Quando desabilitado, habilitar esse recurso permite que o Unified Manager receba os eventos do Active IQ em um cluster em um horário predefinido de 00:15 para o fuso horário desse cluster.

Habilitar e desabilitar configurações de segurança para conformidade

Ao usar o botão **Personalizar** no painel **Painel de Segurança** da página Configurações de Recursos, você pode habilitar ou desabilitar os parâmetros de segurança para monitoramento de conformidade no Unified Manager.

As configurações habilitadas ou desabilitadas nesta página controlam o status geral de conformidade dos clusters e VMs de armazenamento no Unified Manager. Com base nas seleções, as colunas correspondentes ficam visíveis na exibição **Segurança: Todos os clusters** da página de inventário de clusters e na exibição **Segurança: Todas as VMs de armazenamento** da página de inventário de VMs de armazenamento.

Somente usuários com função de administrador podem editar essas configurações.

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

Personalizar configurações de segurança

Para personalizar as configurações de monitoramento de conformidade aplicáveis ao seu ambiente ONTAP , siga estas etapas:

Passos

1. Clique em **Geral > Configurações de recursos > Painel de segurança > Personalizar**. O pop-up **Personalizar configurações do painel de segurança** é exibido.

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

2. Para habilitar ou desabilitar as configurações personalizadas para seus clusters 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 habilitar ou desabilitar as configurações personalizadas para suas VMs de armazenamento, selecione a configuração geral necessária em **VM de armazenamento**. Para obter informações sobre as opções de personalização da conformidade da VM de armazenamento, consulte"Categorias de conformidade de VM de armazenamento" .

Personalize as configurações de AutoSupport e autenticação

Na seção * Configurações do AutoSupport *, você pode especificar se o transporte HTTPS deve ser usado

para enviar mensagens do AutoSupport do ONTAP.

Na seção **Configurações de autenticação**, você pode habilitar alertas do Unified Manager para serem gerados para o usuário administrador padrão do ONTAP .

Habilitar e desabilitar upload de scripts

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

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Passos

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

Se você quiser…	Então faça isto…
Desabilitar scripts	No painel **Script Upload**, mova o botão deslizante para a esquerda.
Habilitar scripts	No painel **Script Upload**, mova o botão deslizante para a direita.

Adicionar banner de login

Adicionar um banner de login permite que sua organização exiba qualquer informação, 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 armazenamento ou administradores, pode visualizar este pop-up de banner de login durante o login, logout e tempo limite da sessão.

Use o console de manutenção

Você pode usar o console de manutenção para configurar configurações de rede, configurar e gerenciar o sistema no qual o Unified Manager está instalado e executar outras tarefas de manutenção que ajudam a prevenir e solucionar possíveis problemas.

Que funcionalidade o console de manutenção fornece

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 que problemas ocorram.

Dependendo do sistema operacional no qual você instalou o Unified Manager, o console de manutenção fornece 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
- Gerar 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 do Unified Manager e as definições de configuração de uma versão de backup anterior.

O que o usuário de manutenção faz

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 de Administrador do Aplicativo na interface do usuário da Web e 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.

Capacidades de diagnóstico do usuário

O objetivo do acesso de diagnóstico é permitir que o suporte técnico auxilie 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 instruído pelo suporte técnico, para fins de solução de problemas.

Acesse o console de manutenção

Se a interface do usuário do Unified Manager não estiver em operação ou se você precisar executar funções que não estão disponíveis na interface do usuário, você poderá acessar o console de manutenção para gerenciar seu sistema Unified Manager.

Antes de começar

Você deve ter instalado e configurado o Unified Manager.

Após 15 minutos de inatividade, o console de manutenção desconecta você.

Quando instalado no VMware, se você já tiver efetuado login como usuário de manutenção por meio do console do VMware, não será possível efetuar login simultaneamente usando o Secure Shell.

Etapa

1. Siga estas etapas 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. Efetue 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. Efetue login no sistema com o nome de usuário de manutenção (umadmin) e a senha. c. Digite o comando `maintenance_console` e pressione Enter.
Windows	a. Efetue login no sistema Unified Manager com 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

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

Antes de começar

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

Passos

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

   Após 15 minutos de inatividade, o console de manutenção desconecta você.

Menus do console de manutenção

O console de manutenção consiste em diferentes menus que permitem 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 VMware)
  a. Suporte/Diagnóstico
  b. Redefinir certificado do servidor
  c. Provedor de dados externo
  d. Restauração de backup
  e. Configuração do intervalo de pesquisa de desempenho
  f. Desativar autenticação SAML
  g. Exibir/Alterar Portas do Aplicativo
  h. Configuração do log de depuração
  i. Controle o acesso à porta 3306 do MySQL
  j. Saída

Selecione o número na lista para acessar a opção de menu específica. Por exemplo, para backup e restauração, selecione *4*.

Menu de configuração de rede

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 estará 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 endereço IP, rede, endereço de transmissão, máscara de rede, gateway e servidores DNS.

- **Alterar configurações de endereço IP**

  Permite que você altere qualquer configuração de rede do dispositivo virtual, incluindo endereço IP, máscara de rede, gateway ou servidores DNS. Se você alternar suas configurações de rede de DHCP para rede estática usando o console de manutenção, não poderá editar o nome do host. Você deve

selecionar **Confirmar alterações** para que as alterações sejam aplicadas.

- **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 nome de domínio**

  Permite que você altere os nomes de domínio que deseja pesquisar ao resolver nomes de host. Você deve selecionar **Confirmar alterações** para que as alterações sejam aplicadas.

- **Exibir rotas estáticas**

  Exibe as rotas de rede estáticas atuais.

- **Alterar rotas estáticas**

  Permite adicionar ou excluir rotas de rede estáticas. Você deve selecionar **Confirmar alterações** para que as alterações sejam aplicadas.

  - **Adicionar Rota**

    Permite adicionar uma rota estática.

  - **Excluir Rota**

    Permite que você exclua uma rota estática.

  - **Voltar**

    Leva você de volta ao **Menu Principal**.

  - **Saída**

    Sai do console de manutenção.

- **Desabilitar interface de rede**

  Desabilita todas as interfaces de rede disponíveis. Se apenas uma interface de rede estiver disponível, você não poderá desativá-la. Você deve selecionar **Confirmar alterações** para que as alterações sejam aplicadas.

- **Habilitar interface de rede**

  Habilita interfaces de rede disponíveis. Você deve selecionar **Confirmar alterações** para que as alterações sejam aplicadas.

- **Confirmar alterações**

  Aplica quaisquer alterações feitas nas configurações de rede do dispositivo virtual. Você deve selecionar esta opção para aplicar quaisquer alterações feitas, ou as alterações não ocorrerão.

- **Fazer ping em um host**

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

- **Restaurar para as configurações padrão**

  Redefine todas as configurações para os padrões de fábrica. Você deve selecionar **Confirmar alterações** para que as alterações sejam aplicadas.

- **Voltar**

  Leva você de volta ao **Menu Principal**.

- **Saída**

  Sai do console de manutenção.

Menu de configuração do sistema

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

> Quando o Unified Manager é instalado em um sistema Linux ou Microsoft Windows, somente a opção “Restaurar de um backup do Unified Manager” 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 em execução, talvez seja necessário entrar em contato com o suporte técnico.

- **Reinicializar máquina virtual**

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

- **Desligar a máquina virtual**

  Desliga a máquina virtual, interrompendo todos os serviços.

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

- **Alterar senha do usuário <usuário conectado>**

  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 sua localização.

- **Alterar servidor NTP**

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

- **Alterar serviço NTP**

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

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

  Restaura o banco de dados e as definições de configuração do Unified Manager 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 dispositivo virtual está instalado.

- **Voltar**

  Sai do menu Configuração do Sistema e retorna ao Menu Principal.

- **Saída**

  Sai do menu do console de manutenção.

Menu de Suporte e Diagnóstico

O menu Suporte e Diagnóstico permite que você gere um pacote de suporte que pode ser enviado ao suporte técnico para obter assistência na solução de problemas.

As seguintes opções de menu estão disponíveis:

- **Gerar Pacote de Suporte de Luz**

  Permite que você produza um pacote de suporte leve que contém apenas 30 dias de logs e registros de banco de dados de configuração — ele exclui dados de desempenho, arquivos de gravação de aquisição e despejo de heap do servidor.

- **Gerar Pacote de Suporte**

  Permite que você crie um pacote de suporte completo (arquivo 7-Zip) contendo informações de diagnóstico no diretório inicial do usuário de diagnóstico. Se o seu sistema estiver conectado à Internet, você também poderá carregar o pacote de suporte para o NetApp.

  O arquivo inclui informações geradas por uma mensagem do 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 normalmente não incluídos em mensagens do AutoSupport ou no pacote de suporte leve.

Opções adicionais de menu

As seguintes opções de menu permitem que você execute várias tarefas administrativas no servidor do 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**.

- **Desabilitar autenticação SAML**

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

- **Provedor de dados externo**

  Fornece opções para conectar o Unified Manager a um provedor de dados externo. Depois de estabelecer a conexão, os dados de desempenho são enviados a um servidor externo para que especialistas em desempenho de armazenamento possam mapear as métricas de desempenho usando software de terceiros. As seguintes opções são exibidas:

  - **Exibir configuração do servidor** — Exibe as configurações atuais de conexão e configuração de um provedor de dados externo.
  - **Adicionar/Modificar conexão do servidor** — Permite que você insira novas configurações de conexão para um provedor de dados externo ou altere as configurações existentes.
  - **Modificar configuração do servidor** — Permite que você insira novas configurações para um provedor de dados externo ou altere as configurações existentes.
  - **Excluir conexão do servidor** — Exclui a conexão com um provedor de dados externo.

    Após a conexão ser excluída, o Unified Manager perde a conexão com o servidor externo.

- **Restauração de backup**

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

- **Configuração do intervalo de pesquisa de desempenho**

  Fornece uma opção para configurar a frequência com que o Unified Manager coleta dados estatísticos de desempenho de 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 grandes clusters não estão sendo concluídas no prazo.

- **Ver/Alterar Portas de Aplicativos**

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

- **Controle 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 essa porta é restrito apenas ao host local durante uma nova instalação do Unified Manager em sistemas Linux, Windows e VMware vSphere. Esta opção permite que você alterne a visibilidade desta porta entre o host local e os hosts remotos, ou seja, se ela estiver habilitada somente para o host local no seu ambiente, você também poderá disponibilizar esta porta para hosts remotos. Como alternativa, quando habilitado para todos os hosts, você pode restringir o acesso desta porta somente ao host local. Se o acesso foi habilitado em hosts remotos anteriormente, a configuração será mantida em um cenário de atualização. Você deve verificar as configurações de firewall em sistemas Windows depois de alternar a visibilidade da porta e desabilitar as configurações de firewall se as configurações estiverem definidas para restringir o acesso à porta 3306 do MySQL.

- **Saída**

  Sai do menu do console de manutenção.

Alterar a senha do usuário de manutenção no Windows

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

Passos

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

   É exibida uma página 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 para o endereço de e-mail definido para esse nome de usuário.

3. Clique no link **redefinir senha** no e-mail e defina a nova senha.
4. Retorne à interface da Web e faça login no Unified Manager usando a nova senha.

Alterar a senha do umadmin 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 pode alterar a senha novamente a qualquer momento.

Antes de começar

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

Passos

1. Efetue login como usuário root no sistema Linux no qual o Unified Manager está sendo executado.
2. Alterar a senha do umadmin:

   ```
   passwd umadmin
   ```

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

Alterar as portas que o Unified Manager usa 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 questões de segurança. As portas padrão são 80 para HTTP e 443 para HTTPS.

Antes de começar

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

> Existem algumas portas que são consideradas inseguras ao usar os navegadores Mozilla Firefox ou Google Chrome. Verifique com seu navegador antes de atribuir um novo número de porta para tráfego HTTP e HTTPS. Selecionar uma porta insegura pode tornar o sistema inacessível, o que exigirá que você entre em contato com o suporte ao cliente para obter uma resolução.

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

1. Efetue 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 **Exibir/Alterar portas de aplicativo** e pressione Enter.
3. Se solicitado, digite a senha do usuário de manutenção novamente.
4. Digite os novos números de porta para as portas HTTP e HTTPS e pressione Enter.

   Deixar um número de porta em branco atribui a porta padrão para o protocolo.

   Você será perguntado 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 de porta na URL para acessar a interface de usuário da 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

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

Antes de começar

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

O dispositivo virtual deve 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** > **Reinicializar sistema operacional**.

   Após a reinicialização, o console de manutenção pode 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 habilitar a interface de rede.
6. Digite as configurações de rede.

   Você será solicitado a 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 retornará automaticamente ao menu **Configuração de rede**.

7. Selecione **Confirmar alterações**.

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

Adicionar espaço em disco ao diretório do banco de dados do Unified Manager

O diretório de banco de dados do Unified Manager contém todos os dados de integridade e desempenho coletados dos sistemas ONTAP . Algumas circunstâncias podem exigir que você aumente 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% da capacidade.

As etapas necessárias para adicionar capacidade ao diretório de dados são diferentes dependendo se o Unified Manager está sendo executado em um servidor VMware ESXi, em um servidor Red Hat ou em um servidor Microsoft Windows.

Adicionar espaço ao diretório de dados do host Linux

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

Antes de começar

Você deve ter acesso de usuário root 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. Efetue login como usuário root na máquina Linux na qual você deseja adicionar espaço em disco.
2. Pare o serviço 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 em disco suficiente para conter os dados no atual `/opt/netapp/data` diretório.
4. Copie o conteúdo e a configuração de privilégios do existente `/opt/netapp/data` diretório para o diretório de dados de backup:

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

5. Se o SE Linux estiver habilitado:

   a. Obtenha o tipo SE Linux para pastas existentes `/opt/netapp/data` pasta:

      ```
      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 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. Expandir 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` de um disco, então você não deve tentar montar `/opt/netapp/data` como um compartilhamento NFS ou CIFS. Porque, neste caso, se você tentar expandir o espaço em disco, alguns comandos LVM, como `resize` e `extend` pode não funcionar como esperado.

8. Confirme que o `/opt/netapp/data` o proprietário do diretório (mysql) e o grupo (root) não foram

alterados:

```
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 habilitado, confirme se o contexto para o `/opt/netapp/data` o 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 estranho não cause um erro no banco de dados no futuro.
11. Copie o conteúdo dos dados de backup de volta para o arquivo expandido `/opt/netapp/data` diretório:

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

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

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

13. Inicie o serviço MySQL:

```
systemctl start mysqld
```

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

```
systemctl start ocie ocieau
```

15. Depois que todos os serviços forem iniciados, exclua a pasta de backup `/backup-data` :

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

Adicionar espaço ao disco de dados da máquina virtual VMware

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

Antes de começar

- Você deve ter acesso ao vSphere Client.

- A máquina virtual não deve ter instantâneos armazenados localmente.
- Você deve ter as credenciais de usuário de manutenção.

Recomendamos que você faça 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 adicione mais capacidade de disco aos dados `disk 3`. Consulte a documentação do VMware para obter detalhes.

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

2. No cliente vSphere, selecione a máquina virtual Unified Manager e, em seguida, selecione a guia **Console**.
3. Clique na janela do console e faça login no console de manutenção usando seu nome de usuário e senha.
4. No Menu Principal, insira o número da opção **Configuração do Sistema**.
5. No Menu de Configuração do Sistema, insira o número da opção **Aumentar Tamanho do Disco de Dados**.

Adicionar espaço à unidade lógica do servidor Microsoft Windows

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

Antes de começar

Você deve ter privilégios de administrador do Windows.

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

Passos

1. Efetue login como administrador no servidor Windows no qual você deseja adicionar espaço em disco.
2. Siga o passo que corresponde ao método que você deseja usar para adicionar mais espaço:

Opção	Descrição
Em um servidor físico, adicione capacidade à unidade lógica na qual o servidor Unified Manager está instalado.	Siga os passos do tópico da Microsoft: "Estender um volume básico"
Em um servidor físico, adicione uma unidade de disco rígido.	Siga os passos do tópico da Microsoft: "Adicionando unidades de disco rígido"

Opção	Descrição
Em uma máquina virtual, aumente o tamanho de uma partição de disco.	Siga os passos do tópico VMware: "Aumentando o tamanho de uma partição de disco"

Gerenciar acesso do usuário

Você pode criar funções e atribuir recursos para controlar o acesso do usuário ao Active IQ Unified Manager. Você pode identificar usuários que têm os recursos necessários para acessar objetos selecionados no Unified Manager. Somente os usuários que têm essas funções e capacidades podem gerenciar os objetos no Unified Manager.

Adicionar usuários

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

Antes de começar

- Você deve ter a função de Administrador do Aplicativo.
- Para adicionar um usuário ou grupo remoto, você deve 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 usuários que acessam a interface gráfica, certifique-se de que esses usuários estejam definidos como usuários "remotos".

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

Se você adicionar um grupo do Windows Active Directory, todos os membros diretos e subgrupos aninhados poderão ser autenticados no Unified Manager, a menos que os subgrupos aninhados estejam desabilitados. Se você adicionar um grupo do OpenLDAP ou 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 Usuários, clique em **Adicionar**.
3. Na caixa de diálogo Adicionar usuário, selecione o tipo de usuário que você deseja adicionar e insira as informações necessárias.

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

4. Clique em **Adicionar**.

Criar um usuário de banco de dados

Para dar suporte a uma conexão entre o Workflow Automation e o Unified Manager, ou para acessar visualizações de banco de dados, você deve primeiro criar um usuário de banco de dados com a função Esquema de Integração ou Esquema de Relatório na interface de usuário da Web do Unified Manager.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

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 ou 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 Usuários, clique em **Adicionar**.
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 a automação do fluxo de trabalho	Esquema de Integração
Acessando relatórios e outras visualizações de banco de dados	Esquema de Relatório

6. Clique em **Adicionar**.

Editar as configurações do usuário

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

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Quando você modifica a função atribuída a um usuário, as alterações são aplicadas quando ocorre uma das seguintes ações:

- O usuário efetua logout e login novamente no Unified Manager.
- O tempo limite da sessão de 24 horas foi atingido.

Passos

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

Ver usuários

Você pode usar a página Usuários para visualizar a lista de usuários que gerenciam objetos de armazenamento 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 aos usuários.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Etapa

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

Excluir usuários ou grupos

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 reatribuir os eventos atribuídos aos usuários dos grupos remotos.

  Se você estiver excluindo usuários locais ou remotos, os eventos atribuídos a esses usuários serão automaticamente desatribuídos.

- Você deve ter a função de Administrador do Aplicativo.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Usuários**.
2. Na página Usuários, selecione os usuários ou grupos que você deseja excluir e clique em **Excluir**.
3. Clique em **Sim** para confirmar a exclusão.

O que é RBAC

O RBAC (controle de acesso baseado em função) fornece a capacidade de controlar quem tem acesso a vários recursos e funcionalidades no servidor do Active IQ Unified Manager .

O que o controle de acesso baseado em função faz

O controle de acesso baseado em funções (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 quiser restringir as informações que os administradores podem visualizar e as operações que eles podem executar, você deve aplicar funções às contas de administrador que criar.

O servidor de gerenciamento usa RBAC para login de usuário e permissões de função. Se você não alterou as configurações padrão do servidor de gerenciamento para acesso de usuário administrativo, não será necessário efetuar login para visualizá-las.

Quando você inicia 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 de conta de administrador do aplicativo.

Definições de tipos de usuários

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 Administrador.

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 então cria usuários adicionais 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 do usuário do Unified Manager e executa funções com base na função atribuída pelo usuário de manutenção ou por um usuário com a função de Administrador do Aplicativo.

- **Grupo remoto**

  Um grupo de usuários que acessam a interface do usuário do Unified Manager usando as credenciais armazenadas no servidor de autenticação. O nome desta conta deve corresponder ao nome de um grupo armazenado no servidor de autenticação. Todos os usuários dentro do grupo remoto recebem acesso à interface do usuário do Unified Manager usando suas credenciais de usuário individuais. Grupos remotos podem executar funções de acordo com suas funções atribuídas.

- **Usuário remoto**

  Acessa a interface do usuário 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 de Administrador do Aplicativo.

- **Usuário do banco de dados**

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

Definições de funções de usuário

O usuário de manutenção ou administrador do aplicativo atribui uma função a cada usuário. Cada função contém certos privilégios. O escopo de atividades que você pode executar no Unified Manager depende da função atribuída a você e dos privilégios que a função contém.

O Unified Manager inclui as seguintes funções de usuário predefinidas:

- **Operador**

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

- **Administrador de Armazenamento**

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

- **Administrador do aplicativo**

  Configura definições não relacionadas ao gerenciamento de armazenamento. Esta 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 de Administrador de Aplicativos é automaticamente nomeado “umadmin”.

- **Esquema de Integração**

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

- **Esquema de Relatório**

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

  - netapp_model_view
  - netapp_desempenho
  - ocum
  - ocum_report

- ocum_report_birth
- opm
- monitor de escala

Funções e recursos do usuário do Unified Manager

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

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

Função	Operador	Administrador de Armazenamento	Administrador do aplicativo	Esquema de Integração	Esquema de Relatório
Exibir informações do sistema de armazenamento	•	•	•	•	•
Veja outros dados, como históricos e tendências de capacidade	•	•	•	•	•
Visualizar, atribuir e resolver eventos	•	•	•		
Exibir objetos de serviço de armazenamento, como associações de SVM e pools de recursos	•	•	•		
Ver políticas de limite	•	•	•		
Gerenciar objetos de serviço de armazenamento, como associações SVM e pools de recursos		•	•		

Função	Operador	Administrador de Armazenamento	Administrador do aplicativo	Esquema de Integração	Esquema de Relatório
Definir alertas		•	•		
Gerenciar opções de gerenciamento de armazenamento		•	•		
Gerenciar políticas de gerenciamento de armazenamento		•	•		
Gerenciar usuários			•		
Gerenciar opções administrativas			•		
Definir políticas de limite			•		
Gerenciar acesso ao banco de dados			•		
Gerenciar a integração com o WFA e fornecer acesso às visualizações do banco de dados				•	
Agendar e salvar relatórios		•	•		
Executar operações “Fix It” a partir de Ações de Gerenciamento		•	•		

Função	Operador	Administrador de Armazenamento	Administrador do aplicativo	Esquema de Integração	Esquema de Relatório
Forneça acesso somente leitura às visualizações do banco de dados					•

Gerenciar configurações de autenticação SAML

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

Observe que somente usuários remotos terão acesso à interface gráfica do usuário do Unified Manager após a autenticação SAML ser habilitada. Usuários locais e usuários de manutenção não poderão acessar a interface do usuário. Esta configuração não afeta os usuários que acessam o console de manutenção.

Requisitos do provedor de identidade

Ao configurar o Unified Manager para usar um provedor de identidade (IdP) para executar a autenticação SAML para todos os usuários remotos, você precisa estar ciente de algumas configurações necessárias para que a conexão com o 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 Autenticação SAML 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 Avançada (AES): AES-128 e AES-256
- Algoritmo de Hash Seguro (SHA): SHA-1 e SHA-256

Provedores de identidade validados

- Shibboleth
- Serviços de Federação do Active Directory (ADFS)

Requisitos de configuração do ADFS

- Você deve definir três regras de reivindicação 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
Nome da conta SAM	Nome ID
Nome da conta SAM	urna:oid:0.9.2342.19200300.100.1.1
Grupos de tokens — Nome não qualificado	urna:oide:1.3.6.1.4.1.5923.1.5.1.1

- Você deve definir o método de autenticação como “Autenticação de formulários” ou os usuários poderão receber um erro ao efetuar logout do Unified Manager. Siga estes passos:
  a. Abra o Console de Gerenciamento do ADFS.
  b. Clique na pasta Políticas de Autenticação na visualização 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 “Autenticação de Formulários” em vez do padrão “Autenticação do Windows”.
- Em alguns casos, o login pelo IdP é rejeitado quando o certificado de segurança do Unified Manager é assinado pela CA. Há duas soluções alternativas para resolver esse problema:
  - Siga as instruções identificadas no link para desabilitar a verificação de revogação no servidor ADFS para a parte confiável associada ao certificado de CA encadeado:

    "Desabilitar verificação de revogação por 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 é definido como 5 minutos, portanto a diferença de tempo entre o servidor IdP e o servidor do Unified Manager não pode ser maior que 5 minutos, ou a autenticação falhará.

Habilitar autenticação SAML

Você pode habilitar a autenticação SAML (Security Assertion Markup Language) para que usuários remotos sejam autenticados por um provedor de identidade seguro (IdP) antes de poderem acessar a interface 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 suportado pelo Unified Manager e deve ser configurado.
- Você deve ter o URL e os metadados do IdP.
- Você deve ter acesso ao servidor IdP.

Depois de habilitar a autenticação SAML do Unified Manager, os usuários não poderão acessar a interface gráfica do usuário até que o IdP tenha sido configurado com as informações do 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 da configuração do Unified Manager.

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

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

Passos

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

   Os campos necessários para configurar a conexão IdP são exibidos.

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

   Se o servidor IdP estiver acessível diretamente do servidor do Unified Manager, você poderá clicar no botão **Obter metadados do IdP** depois de inserir o URI do IdP para preencher o campo Metadados do IdP automaticamente.

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 neste momento.

5. Clique em **Salvar**.

   Uma caixa de mensagem é 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.

Se ainda não tiver concluído, acesse seu IdP e insira o 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**.

Alterar o provedor de identidade usado para autenticação SAML

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

Antes de começar

- Você deve ter o URL e os metadados do IdP.
- Você deve ter acesso ao IdP.

O novo IdP pode ser configurado antes ou depois da configuração do 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 **Obter metadados do IdP** depois de inserir o URL do IdP para preencher o campo Metadados do IdP automaticamente.

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 o URI e os metadados do servidor do Unified Manager para concluir a configuração.

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

Atualizar as configurações de autenticação SAML após a alteração do certificado de segurança do 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 será atualizado se você renomear o sistema host, atribuir um novo endereço IP para o sistema host ou alterar manualmente o certificado de segurança do sistema.

Depois que o certificado de segurança for alterado e o servidor do Unified Manager for reiniciado, a autenticação SAML não funcionará e os usuários não poderão acessar a interface gráfica do Unified Manager. Você deve atualizar as configurações de autenticação SAML no servidor IdP e no servidor do Unified Manager para reativar o acesso à interface do usuário.

Passos

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

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

3. Inicie a interface do usuário do Unified Manager usando o FQDN ou endereço IP atualizado, aceite o certificado do servidor atualizado no seu navegador e efetue login usando as credenciais do usuário de manutenção.
4. Na página **Configuração/Autenticação**, selecione a aba **Autenticação SAML** e configure a conexão 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 é 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 seu servidor IdP e insira o URI e os metadados do servidor do Unified Manager para concluir a configuração.

Provedor de identidade	Etapas de configuração
ADFS	a. Exclua a entrada de confiança da parte confiável existente na GUI 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 reivindicação 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.
Shibboleth	a. Atualize o novo FQDN do servidor Unified Manager no `attribute-filter.xml` e `relying-party.xml` arquivos. b. Reinicie o servidor web Apache Tomcat e aguarde a porta 8005 ficar online.

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

Desativar autenticação SAML

Você pode desabilitar a autenticação SAML quando quiser parar de autenticar usuários remotos por meio de um provedor de identidade seguro (IdP) antes que eles possam efetuar login na interface da Web do Unified Manager. Quando a autenticação SAML está desabilitada, os provedores de serviços de diretório configurados, como Active Directory ou LDAP, executam a autenticação de logon.

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

Você também pode desabilitar a autenticação SAML usando o console de manutenção do Unified Manager se não tiver acesso à interface gráfica do usuário.

O Unified Manager é reiniciado automaticamente após a autenticação SAML ser desabilitada.

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 é 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 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 e os metadados do servidor do Unified Manager.

Desabilitar a autenticação SAML no console de manutenção

Pode ser necessário desabilitar a autenticação SAML no console de manutenção quando não houver acesso à GUI do Unified Manager. Isso pode acontecer em casos de configuração incorreta ou se o IdP não estiver acessível.

Antes de começar

Você deve ter acesso ao console de manutenção como usuário de manutenção.

Quando a autenticação SAML está desabilitada, os provedores de serviços de diretório configurados, como Active Directory ou LDAP, executam a autenticação de logon. Usuários locais e usuários de manutenção poderão acessar a interface gráfica do usuário, além dos usuários remotos configurados.

Você também pode desabilitar a autenticação SAML na página Configuração/Autenticação na interface do usuário.

O Unified Manager é reiniciado automaticamente após a autenticação SAML ser desabilitada.

Passos

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

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

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

Na próxima vez que 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.

Se necessário, acesse seu IdP e exclua o URL e os metadados do servidor do Unified Manager.

Página de autenticação SAML

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

- Você deve ter a função de Administrador de Aplicativos para criar ou modificar a configuração SAML.
- Você deve ter configurado a autenticação remota.
- Você deve ter configurado pelo menos um usuário remoto ou grupo remoto.

Após a autenticação remota e os usuários remotos terem sido configurados, você pode marcar a caixa de seleção Habilitar autenticação SAML para habilitar a autenticação usando um provedor de identidade seguro.

- **URI do IdP**

  O URI para acessar o IdP do servidor do Unified Manager. Exemplos de URIs estão listados abaixo.

  URI de exemplo do ADFS:

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

  Exemplo de URI Shibboleth:

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

- **Metadados IdP**

  Os metadados do IdP em formato XML.

  Se o URL do IdP estiver acessível no servidor do Unified Manager, você poderá 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**

  Metadados do sistema host em formato XML.

Gerenciar autenticação

Você pode habilitar a autenticação usando LDAP ou Active Directory no servidor do Unified Manager e configurá-lo para funcionar com seus servidores para autenticar usuários remotos.

Para habilitar a autenticação remota, configurar serviços de autenticação e adicionar servidores de autenticação, consulte a seção anterior sobre **Configurando o Unified Manager para enviar notificações de alerta**.

Editar servidores de autenticação

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

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Passos

1. No painel de navegação esquerdo, 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

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 você quiser alterar um servidor de autenticação com o qual o servidor de gerenciamento está se comunicando, você pode excluir o servidor de autenticação e adicionar um novo servidor de autenticação.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

Quando você exclui um servidor de autenticação, usuários ou grupos remotos do servidor de autenticação não poderão mais acessar o Unified Manager.

Passos

1. No painel de navegação esquerdo, 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 habilitada, os certificados associados ao servidor de autenticação serão excluídos junto com o servidor de autenticação.

Autenticação com Active Directory ou OpenLDAP

Você pode habilitar a autenticação remota no servidor de gerenciamento e configurá-lo para se comunicar com seus servidores de autenticação para que os usuários dentro dos 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:

- Diretório Ativo da Microsoft

  Você não pode usar o Microsoft Lightweight Directory Services.

- OpenLDAP

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

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

Registro de auditoria

Você pode detectar se os logs de auditoria foram comprometidos usando 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 do usuário e das APIs expostas publicamente do Active IQ Unified Manager.

Você pode usar o **Registro de auditoria: Visualização de arquivo** para visualizar e acessar todos os arquivos de log de auditoria disponíveis no seu Active IQ Unified Manager. Os arquivos no Log de auditoria: Exibição de arquivos são listados com base na data de criação. Esta exibição exibe informações de todos os logs de auditoria capturados desde a instalação ou atualização até o presente 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 que está inativo, compactado e armazenado no sistema.
VIOLADO	Arquivo que foi comprometido por um usuário que editou o arquivo manualmente.
EXCLUSÃO_MANUAL	Arquivo que foi excluído por um usuário autorizado.
ROLLOVER_DELETE	Arquivo que foi excluído devido à descontinuação com base na Política de configuração de descontinuação.

Estado	Descrição
EXCLUSÃO_INESPERADA	Arquivo que foi excluído por motivos desconhecidos.

A página Log de Auditoria inclui os seguintes botões de comando:

- Configurar
- Excluir
- Download

O botão **EXCLUIR** permite que você exclua qualquer um dos logs de auditoria listados na exibição Logs de Auditoria. Você pode excluir um log de auditoria e, opcionalmente, fornecer um motivo para excluir o arquivo, o que ajudará no futuro a determinar uma exclusão válida. A coluna MOTIVO lista o motivo junto com o nome do usuário que executou a operação de exclusão.

A exclusão de um arquivo de log causará a exclusão do arquivo do sistema, mas a entrada na tabela do banco de dados não será excluída.

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

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

Configurar logs de auditoria

Você pode usar o botão **Configurar** na seção Logs de Auditoria para configurar a política contínua para arquivos de Log de Auditoria e também habilitar o registro remoto para os Logs de Auditoria.

Você pode definir os valores em **TAMANHO MÁXIMO DO ARQUIVO** e **DIAS DE RETENÇÃO DO LOG DE AUDITORIA** de acordo com a quantidade e a frequência desejadas de dados que você deseja armazenar no sistema. O valor no campo **TAMANHO TOTAL DO LOG DE AUDITORIA** é o tamanho total dos dados do log de auditoria presentes no sistema. A política de rollover é determinada pelos valores no campo **DIAS DE RETENÇÃO DO LOG DE AUDITORIA**, **TAMANHO MÁXIMO DO ARQUIVO** e **TAMANHO TOTAL DO LOG DE AUDITORIA**. Quando o tamanho do backup do log de auditoria atinge o valor configurado em **TAMANHO TOTAL DO LOG DE AUDITORIA**, 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 **DIAS DE RETENÇÃO DO LOG DE AUDITORIA** é para o número de dias em que os arquivos de log de auditoria são preservados. Qualquer arquivo mais antigo que o valor definido neste campo será substituído.

Passos

1. Clique em **Registros 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.

Se você quiser habilitar o registro remoto, selecione **Habilitar registro remoto**. /// 2025-6-11, OUTRODOC-133

Habilitar registro remoto de logs de auditoria

Você pode selecionar a caixa de seleção **Habilitar registro remoto** na caixa de diálogo Configurar registros de auditoria para habilitar o registro de auditoria remota. Você pode usar este 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 de logs de auditoria fornece um backup à prova de violação 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**, marque a caixa de seleção **Habilitar registro remoto**.

   Campos adicionais para configurar o registro remoto são exibidos.

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

   O certificado deve ser carregado em `.pem` formatar. Este certificado deve ser obtido do servidor Syslog de destino e não deve ter expirado. O certificado deve conter o “hostname” selecionado como parte do `SubjectAltName` Atributo (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. Marque a caixa de seleção **Habilitar autenticação do cliente** se o servidor Syslog de destino exigir autenticação baseada em certificado.

   Você precisará baixar o certificado de autenticação do cliente e enviá-lo ao servidor Syslog antes de salvar a configuração do Log de Auditoria, caso contrário, a conexão falhará. Dependendo do tipo de servidor Syslog, pode ser necessário criar um hash do certificado de autenticação do cliente.

   Exemplo: syslog-ng requer que um <hash> do certificado seja criado usando o comando `openssl x509 -noout -hash -in cert.pem` , e então você deve vincular simbolicamente o certificado de autenticação do cliente a um arquivo nomeado após <hash> .0.

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

   Você será redirecionado para a página Logs de Auditoria.

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

Página de autenticação remota

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

Você deve ter a função de Administrador de Aplicativos ou Administrador de Armazenamento.

Depois de marcar a caixa de seleção Habilitar autenticação remota, você pode 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 Active Directory, OpenLDAP, ou especifique seu próprio mecanismo de autenticação. Você pode especificar um serviço de autenticação somente se tiver habilitado a autenticação remota.

  - **Diretório Ativo**
    - 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 distinto base será **cn=ou,dc=domain,dc=com**.

    - Desativar pesquisa de grupo aninhado

      Especifica se a opção de pesquisa de grupo aninhado deve ser habilitada ou desabilitada. Por padrão, esta opção está desabilitada. Se você usar o Active Directory, poderá acelerar a autenticação desabilitando o suporte para grupos aninhados.

    - Usar conexão segura

      Especifica o serviço de autenticação usado para comunicação com servidores de autenticação.

  - **OpenLDAP**
    - Vincular nome distinto

      Especifica o nome distinto de vinculação que é usado junto com o nome distinto base para localizar usuários remotos no servidor de autenticação.

- Senha de vinculação

  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 distinto base será **cn=ou,dc=domain,dc=com**.

- Usar conexão segura

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

◦ **Outros**

- Vincular nome distinto

  Especifica o nome distinto de vinculação que é usado junto com o nome distinto base para localizar usuários remotos no servidor de autenticação que você configurou.

- Senha de vinculação

  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 distinto 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 nomes de login de usuário a serem autenticados pelo servidor de gerenciamento.

- Atributo de Associação de Grupo

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

- UGID

  Se os usuários remotos forem incluídos como membros de um objeto GroupOfUniqueNames no servidor de autenticação, esta opção permitirá que você atribua a associação de grupo do servidor de gerenciamento aos usuários remotos com base em um atributo especificado nesse objeto GroupOfUniqueNames.

- Desativar pesquisa de grupo aninhado

Especifica se a opção de pesquisa de grupo aninhado deve ser habilitada ou desabilitada. Por padrão, esta opção está desabilitada. Se você usar o Active Directory, poderá acelerar a autenticação desabilitando o suporte para grupos aninhados.

- Membro

  Especifica o nome do atributo que 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 remota.

> Os valores inseridos para os atributos *Membro*, *Classe de Objeto de Usuário* e *Classe de Objeto de Grupo* devem ser os mesmos adicionados nas configurações do Active Directory, OpenLDAP e LDAP. Caso contrário, a autenticação poderá falhar.

- Usar conexão segura

  Especifica o serviço de autenticação usado para comunicação 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 para usuários ou grupos remotos são mantidas pelo servidor de autenticação.

- **Botões de comando**

  Permite adicionar, editar ou excluir servidores de autenticação.

  - Adicionar

    Permite que você adicione 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 do 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 autenticando um usuário ou grupo remoto.

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

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

Gerenciar certificados de segurança

Você pode configurar HTTPS no servidor do Unified Manager para monitorar e gerenciar seus clusters por meio de uma conexão segura.

Visualizar o certificado de segurança HTTPS

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

Antes de começar

Você deve ter a função de Operador, Administrador de Aplicativos ou Administrador de Armazenamento.

Visualizar o certificado permite que você verifique o conteúdo de um certificado regenerado ou visualize os Nomes Alt 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 no topo da página

Se precisar visualizar informações mais detalhadas sobre o certificado de segurança do que as exibidas na página Certificado HTTPS, você poderá visualizar o certificado de conexão no seu navegador.

Baixe uma solicitação de assinatura de certificado HTTPS

Você pode baixar uma solicitação de assinatura de certificação para o certificado de segurança HTTPS atual para que você possa fornecer o arquivo para uma Autoridade de Certificação assinar. Um certificado assinado por uma CA ajuda a evitar ataques do tipo man-in-the-middle e fornece melhor proteção de segurança do que um certificado

autoassinado.

Antes de começar

Você deve ter a função de Administrador do Aplicativo.

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 para uma Autoridade de Certificação assinar e depois instalar o certificado assinado.

Instalar um certificado HTTPS assinado e retornado pela CA

Você pode carregar e instalar um certificado de segurança depois que uma Autoridade Certificadora o assinar e devolver. O arquivo que você carrega e instala deve ser uma versão assinada do certificado autoassinado existente. Um certificado assinado por uma CA ajuda a evitar ataques do tipo man-in-the-middle e fornece 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 assinou com uma autoridade de certificação
- Salvou a cadeia de certificados no formato PEM
- Incluiu todos os certificados na cadeia, desde o certificado do servidor do Unified Manager até o certificado de assinatura raiz, incluindo quaisquer certificados intermediários presentes

Você deve ter a função de Administrador do Aplicativo.

Se a validade do certificado para o qual um CSR foi criado for superior a 397 dias, a validade será reduzida para 397 dias pela CA 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 exibida, clique em **Escolher arquivo…** para localizar o arquivo a ser carregado.
4. Selecione o arquivo e clique em **Instalar** para instalar o arquivo.

   Para obter informações, consulte"Instalando um certificado HTTPS gerado usando 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-----
```

Instalar um certificado HTTPS gerado usando ferramentas externas

Você pode instalar certificados autoassinados ou assinados por 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 pares de chaves pública-privada gerados externamente. Os algoritmos de pares de chaves permitidos são “RSA” e “EC”. A opção **Instalar certificado HTTPS** está disponível na página Certificados HTTPS, na seção Geral. 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. Certificado das CAs em sentido inverso até a raiz, que são usadas 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 deve reiniciar a instância do Active IQ Unified Manager para que as alterações entrem em vigor.

Verificações durante o upload de certificados gerados externamente

O sistema realiza verificações ao carregar um certificado gerado usando ferramentas externas. Se alguma das verificações falhar, o certificado será rejeitado. Também há validação incluída para os certificados gerados a partir do CSR dentro do produto e para certificados gerados usando ferramentas externas.

- A chave privada na entrada é validada em relação ao certificado do host na entrada.
- O Nome Comum (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 ser no futuro e a data de expiração da validade do certificado não deve ser no passado.
- Se existir uma CA intermediária ou CA, a data de início da validade do certificado não deve ser no futuro e a data de expiração da validade não deve ser no passado.

A chave privada na entrada não deve ser 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):https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["O ActiveIQ Unified Manager falha ao instalar um certificado gerado externamente"^]

Descrições de páginas para gerenciamento de certificados

Você pode usar a página Certificado HTTPS para visualizar os certificados de segurança atuais e gerar novos certificados HTTPS.

Página do certificado HTTPS

A página Certificado HTTPS permite que você visualize o certificado de segurança atual, baixe uma solicitação de assinatura de certificado, gere um novo certificado HTTPS autoassinado ou instale um novo certificado HTTPS.

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

Botões de comando

Os botões de comando permitem que você execute as seguintes operações:

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

  Baixa uma solicitação de certificação para o certificado HTTPS instalado no momento. Seu navegador solicita que você salve o arquivo <hostname>.csr para que você possa fornecê-lo a uma Autoridade de Certificação para assinatura.

- **Instalar certificado HTTPS**

  Permite que você carregue e instale um certificado de segurança depois que uma Autoridade de Certificação o assinar e devolver. O novo certificado entra em vigor após você reiniciar o servidor de gerenciamento.

- **Regenerar certificado HTTPS**

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

Caixa de diálogo Regenerar certificado HTTPS

A caixa de diálogo Regenerar certificado HTTPS permite que você personalize as informações de segurança e, em seguida, gere um novo certificado HTTPS com essas informações.

As informações atuais do certificado aparecem nesta página.

A seleção “Regenerar usando atributos de certificado atuais” e "Atualizar os atributos de certificado atuais`" permite que você regenere o certificado com as informações atuais ou gere 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 entrar em contato com sua organização; normalmente o endereço de e-mail do administrador do certificado ou do departamento de TI.

- **Empresa**

  Opcional. Normalmente, o nome incorporado da sua empresa.

- **Departamento**

  Opcional. O nome do departamento da sua empresa.

- **Cidade**

  Opcional. A localização da sua empresa na cidade.

- **Estado**

  Opcional. Localização do estado ou província, não abreviada, da sua empresa.

- **País**

  Opcional. A localização da sua empresa no país. Normalmente, este é 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 host local existente ou outros endereços de rede. Separe cada nome alternativo com uma vírgula.

  Marque a caixa de seleção “Excluir informações de identificação local (por exemplo, host local)” se desejar 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 deixado em branco, o certificado resultante não terá nenhum campo Nomes Alternativos.

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

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

- **PERÍODO DE VALIDADE**

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

Para mais informações, consulte "Gerando certificados HTTPS".

Informações sobre direitos autorais

Informações sobre marcas comerciais