Executar tarefas de configuração e administrativas

Active IQ Unified Manager 9.16

NetApp
November 19, 2024

Índice

Executar tarefas de configuração e administrativas

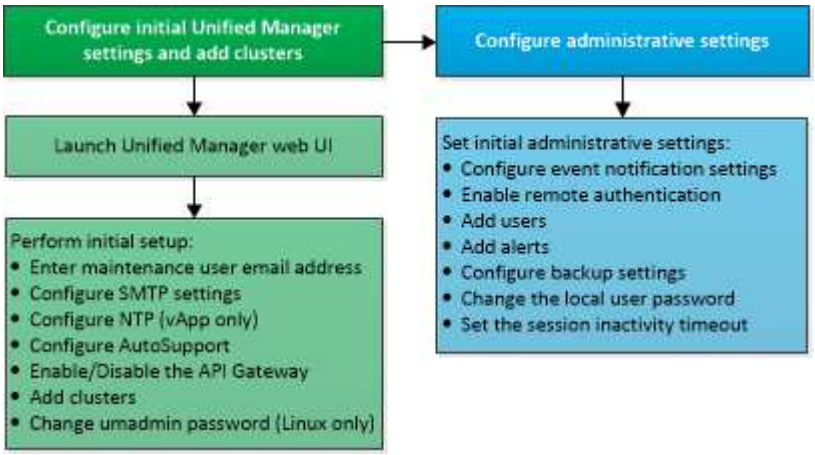
Configurando o Active IQ Unified Manager

Depois de instalar o Active IQ Unified Manager (antigo Gerenciador Unificado do OnCommand), você deve concluir a configuração inicial (também chamada de assistente de primeira experiência) para acessar a IU da Web. Depois, 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 instância do Unified Manager. Outros procedimentos são configurações recomendadas que são úteis para configurar em sua nova instância ou que são boas para saber antes de iniciar o monitoramento regular de seus sistemas ONTAP.

Descrição geral da sequência de configuração

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



Acessando a IU da Web do Unified Manager

Depois de instalar o Unified Manager, você pode acessar a IU da Web para configurar o Unified Manager para começar a monitorar seus sistemas ONTAP.

Antes de começar

- Se esta for a primeira vez que você estiver acessando a IU da Web, você deve fazer login como o usuário de manutenção (ou usuário umadmin para instalações Linux).
- Se você pretende permitir que os usuários acessem o Unified Manager usando o nome curto em vez de usar o nome de domínio totalmente qualificado (FQDN) ou o endereço IP, sua configuração de rede deve 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 IU da Web do Unified Manager a partir do navegador usando o URL exibido no final da instalação. O URL é o endereço IP ou o nome de domínio totalmente qualificado (FQDN) do servidor do Unified Manager.

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

2. Faça login na IU da Web do Unified Manager usando suas credenciais de usuário de manutenção.

> Se você fizer três tentativas consecutivas sem sucesso para fazer login na IU da Web dentro de uma hora, você será bloqueado para fora do sistema e precisará entrar em Contato com o administrador do sistema. Isto é aplicável apenas a utilizadores locais.

Executando a configuração inicial da IU da Web do Unified Manager

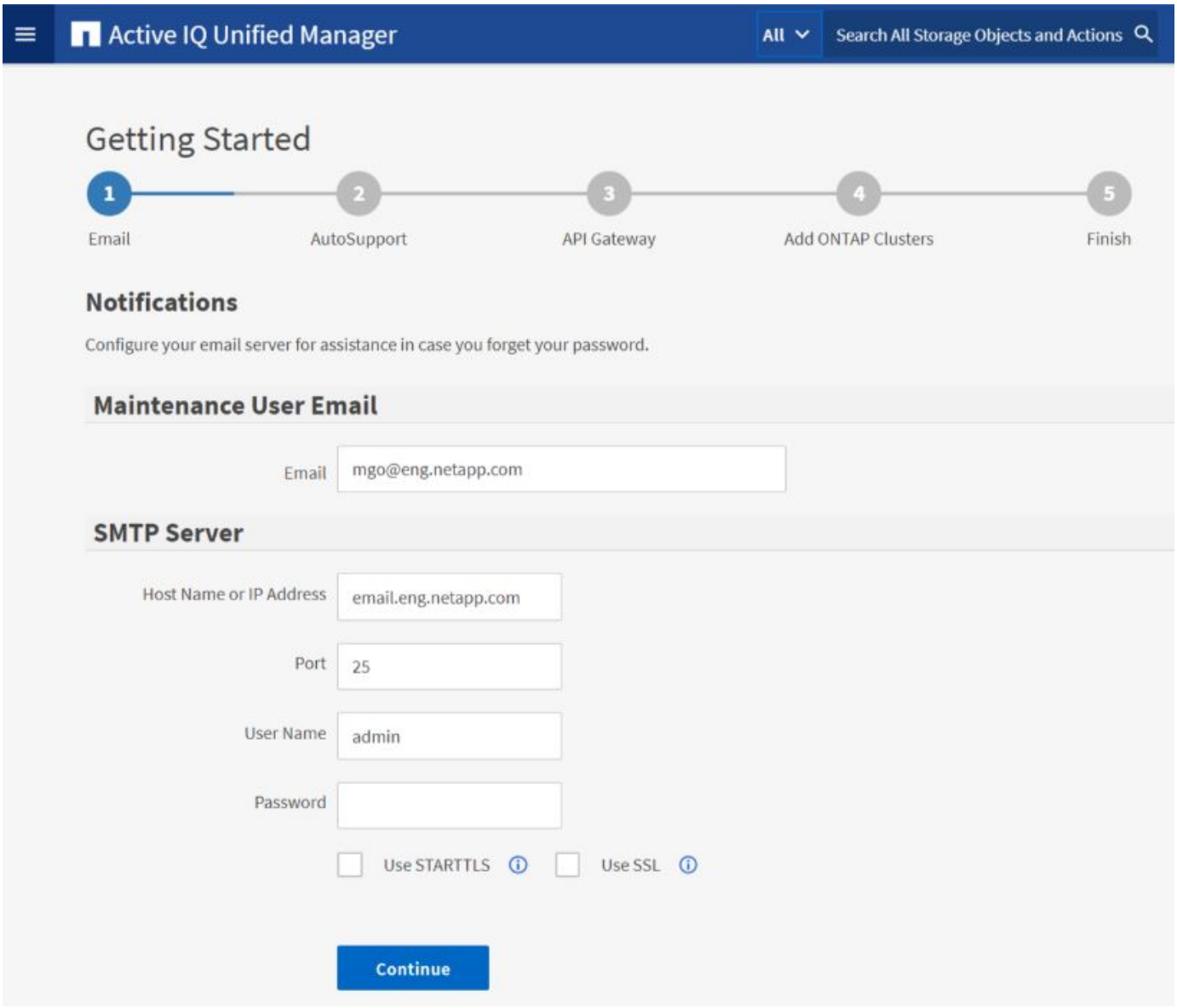
Para usar o Unified Manager, você deve primeiro configurar as opções de configuração inicial, incluindo o servidor NTP, o endereço de e-mail do usuário de manutenção, o host do servidor SMTP e a adição de clusters ONTAP.

Antes de começar

Você deve ter realizado as seguintes operações:

- Inicie a IU da Web do Unified Manager usando o URL fornecido após a instalação
- Logado usando o nome de usuário de manutenção e senha (usuário umadmin para instalações Linux) criados durante a instalação

A página Gerenciamento Unificado do Active IQ é exibida somente quando você acessa a IU da Web pela primeira vez. A página abaixo é de uma instalação na VMware.



Se você quiser alterar qualquer uma dessas opções posteriormente, selecione sua opção nas opções Gerais no painel de navegação esquerdo do Unified Manager. Observe que a configuração NTP é somente para instalações 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 adicionais de SMTP e o servidor NTP (somente instalações VMware). Em seguida, clique em **continuar**.

   Se você tiver selecionado a opção **Use STARTTLS** ou **Use SSL**, uma página de certificado será exibida após clicar no botão **Continue**. Verifique os detalhes do certificado e aceite o certificado para continuar com as configurações iniciais da IU da Web.

2. Na página AutoSupport, clique em **Concordo e continuar** para ativar o envio de mensagens do AutoSupport do Unified Manager para o NetAppactive IQ.

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

3. Nos sistemas Red Hat, altere a senha do usuário umadmin da cadeia padrão "'admin'" para uma cadeia personalizada.
4. Na página Configurar gateway de API, selecione se deseja usar o recurso de gateway de API que permite ao Gerenciador Unificado gerenciar os clusters do ONTAP que você está planejando monitorar usando APIs REST do ONTAP. Em seguida, clique em **continuar**.

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

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

   Este passo é opcional. Você pode adicionar clusters mais tarde na IU 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 fecha-se e a página Painel do Unified Manager é exibida.

Adição de clusters

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

Antes de começar

- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.
- Você deve ter as seguintes informações:
  - O Unified Manager dá suporte a clusters ONTAP on-premises, ONTAP Select, 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 conetar ao cluster. O nome do host deve ser resolvido para o endereço IP de gerenciamento de cluster.

    O endereço IP de gerenciamento de cluster deve ser o LIF de gerenciamento de cluster da máquina virtual de storage 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

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

  - O número da porta para se conetar ao cluster usando o protocolo HTTPS (normalmente a porta 443)
  - Você tem os certificados necessários:

    Certificado SSL (HTTPS): Este certificado pertence ao Unified Manager. Um certificado SSL (HTTPS)

autoassinado padrão é gerado com uma nova instalação do Unified Manager. A NetApp recomenda que você o atualize para um certificado assinado pela CA para obter uma melhor segurança. Se o certificado do servidor expirar, você deverá regenerá-lo e reiniciar o Unified Manager para que os serviços incorporem o novo certificado. Para obter mais informações sobre como regenerar o certificado SSL, "Gerando um certificado de segurança HTTPS"consulte .

Certificado EMS: Este certificado é de propriedade do Unified Manager. Ele 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 ativada 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 está ativada.

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

- Você pode adicionar um cluster a partir da IU da Web e a autenticação baseada em certificado é ativada automaticamente.
- Você pode adicionar um cluster por meio da CLI do Unified Manager, a autenticação baseada em certificado não está habilitada por padrão. Se você adicionar um cluster usando a CLI do Unified Manager, será necessário editar o cluster usando a IU do Unified Manager. Você pode ver "Comandos de CLI do Unified Manager compatíveis" para adicionar um cluster usando a CLI do Unified Manager.
- Se a autenticação baseada em certificado estiver ativada para um cluster e você fizer o backup do Unified Manager de um servidor e restaurar para outro servidor do Unified Manager onde o nome de host ou o endereço IP forem alterados, o monitoramento do cluster poderá falhar. Para evitar a falha, edite e salve os detalhes do cluster. Para obter mais informações sobre como editar os detalhes do cluster, "Edição de clusters"consulte .

+ **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 deve regenerá-lo antes de adicionar o cluster. Para obter informações sobre a geração de certificados, consulte o artigo da base de conhecimento (KB) "Como renovar um certificado auto-assinado do ONTAP na interface do utilizador do System Manager" .

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

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

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração do cluster**.
2. Na página Configuração de cluster, clique em **Add**.
3. Na caixa de diálogo Adicionar cluster, especifique os valores necessários, como o nome do host ou o endereço IP do cluster, o nome do usuário, a senha e o 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 o próximo ciclo de monitoramento ser concluído.

4. Clique em **Enviar**.
5. Na caixa de diálogo autorizar host, clique em **Exibir certificado** para exibir as informações do certificado sobre o cluster.
6. Clique em **Sim**.

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

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

Depois que todos os objetos de um novo cluster forem descobertos, o Unified Manager começará a coletar dados históricos de desempenho dos 15 dias anteriores. Essas estatísticas são coletadas usando a funcionalidade de coleta de continuidade de dados. Esse recurso fornece mais de duas semanas de informações de desempenho para um cluster imediatamente após 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 dados de desempenho de 15 dias é intensiva em CPU, sugere-se que você alterne 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 de tempo em falta.

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

Informações relacionadas

"Instalando um certificado HTTPS assinado e retornado pela CA"

Configurando 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

Tem de ter a função Administrador de aplicações.

Depois de implantar o Unified Manager e concluir a configuração inicial, você deve considerar a configuração do ambiente para acionar alertas e gerar e-mails de notificação ou traps 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, configure um servidor SMTP e forneça um endereço de e-mail a partir 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. "Ativar autenticação remota".

   Se você quiser que os usuários remotos LDAP ou ative Directory acessem a instância do Unified Manager e recebam notificações de alerta, habilite 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 utilizadores".

   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 notificações, configurar as configurações de rede e configurar as opções SMTP e SNMP necessárias para o seu ambiente, você poderá atribuir alertas.

Configurar definições de notificação de eventos

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

Antes de começar

Você deve ter as seguintes informações:

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

  O endereço de e-mail aparece no campo "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 nome de usuário e senha para acessar o servidor
- Nome do host ou endereço IP para o host de destino de intercetação que receberá o trap SNMP, juntamente com a versão SNMP, porta de intercetação de saída, comunidade e outros valores de configuração SNMP necessários

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

todos os hosts da lista.

Tem de ter a função Administrador de aplicações 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 e-mail for pré-preenchido com o endereço "-ActiveIQUnifiedManager@localhost.com", você deve alterá-lo para um endereço de e-mail real e funcional para garantir que todas as notificações de 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 tiver selecionado a opção **Use STARTTLS** ou **Use SSL**, uma página de certificado será exibida após clicar no botão **Save**. 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 exibir 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 exibir um novo certificado.

Ativar 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 e dados de storage.

Antes de começar

Tem de ter a função Administrador de aplicações.

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

Você pode ativar a autenticação remota usando LDAP aberto ou ative Directory. Se a autenticação remota estiver desativada, os usuários remotos não poderão acessar o Unified Manager.

A autenticação remota é suportada por LDAP e LDAPS (Secure LDAP). O Unified Manager usa o 389 como a porta padrão para comunicação não segura e o 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…	Digite as seguintes informações…
Ative Directory	• Nome do administrador do servidor de autenticação em um dos seguintes formatos: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (Usando a notação LDAP apropriada) • Senha do administrador • Nome diferenciado base (usando a notação LDAP apropriada)
Abra o LDAP	• Vincular nome distinto (na notação LDAP apropriada) • Vincular senha • Nome diferenciado da base

Se a autenticação de um usuário do ative Directory demorar muito tempo ou tempo limite, o servidor de autenticação provavelmente levará muito tempo para responder. Desativar 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 SSL (Secure Sockets Layer).

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

Desativando grupos aninhados da autenticação remota

Se a autenticação remota estiver ativada, você poderá desativar a autenticação de grupo aninhado para que somente usuários individuais, e não membros de grupo, possam se autenticar remotamente no Unified Manager. Você pode desativar grupos aninhados quando quiser melhorar o tempo de resposta de autenticação do ative Directory.

Antes de começar

- Tem de ter a função Administrador de aplicações.
- A desativação de grupos aninhados só é aplicável ao usar o ative Directory.

Desativar o suporte para grupos aninhados no Unified Manager pode reduzir o tempo de autenticação. Se o suporte a grupos aninhados estiver desativado 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 grupos aninhados**.
3. Clique em **Salvar**.

Configurando serviços de autenticação

Os serviços de autenticação permitem a autenticação de usuários remotos ou grupos remotos em um servidor de autenticação antes de fornecer acesso ao Unified Manager. Você pode autenticar usuários usando serviços de autenticação predefinidos (como ative Directory ou OpenLDAP) ou configurando seu próprio mecanismo de autenticação.

Antes de começar

- Tem de ter ativado a autenticação remota.
- Tem de ter a função Administrador de aplicações.

Passos

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

Se selecionar…	Então faça isso…
Ative Directory	a. Introduza o nome e a palavra-passe do administrador. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for mais de ou@domain.com, então o nome distinto base é
OpenLDAP	a. Introduza o nome distinto de ligação e a palavra-passe de ligação. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for mais de ou@domain.com, então o nome distinto base é

Se selecionar…	Então faça isso…
Outros	a. Introduza o nome distinto de ligação e a palavra-passe de ligação. b. Especifique o nome distinto base do servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for mais de ou@domain.com, então o nome distinto base é c. Especifique a versão do protocolo LDAP suportada pelo servidor de autenticação. d. Introduza o nome de utilizador, a associação ao grupo, o grupo de utilizadores e os atributos de membro.

Se você quiser modificar o serviço de autenticação, você deve excluir quaisquer servidores de autenticação existentes e adicionar novos servidores de autenticação.

3. Clique em **Salvar**.

Adicionando servidores de autenticação

Você pode adicionar servidores de autenticação e ativar a autenticação remota no servidor de gerenciamento para que os usuários remotos no 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 o serviço de autenticação para que o servidor de gerenciamento possa autenticar usuários remotos ou grupos no servidor de autenticação.
- Tem de ter a função Administrador de aplicações.

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 de parceiro. Isso permite que o servidor de gerenciamento se comunique com o parceiro quando um dos servidores de autenticação está inacessível.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação remota**.
2. Ative ou desative a opção **Use secure Connection**:

Se você quiser…	Então faça isso…
Ative-o.	a. Selecione a opção **usar conexão segura**. b. Na área servidores de autenticação, clique em **Adicionar**. c. Na caixa de diálogo Adicionar servidor de autenticação, insira o nome de autenticação ou o endereço IP (IPv4 ou IPv6) do servidor. d. Na caixa de diálogo 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 **Yes**. Quando você ativa a opção **Use Secure Connection Authentication**, o Unified Manager se comunica com o servidor de autenticação e exibe o certificado. O Unified Manager usa o 636 como porta padrão para comunicação segura e o número de porta 389 para comunicação não segura.
Desative-o.	a. Desmarque a opção **Use Secure Connection**. 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 **Add**.

O servidor de autenticação adicionado é exibido na área servidores.

3. Execute uma autenticação de teste para confirmar que é possível autenticar usuários no servidor de autenticação que você adicionou.

Testando a configuração dos servidores de autenticação

Você pode validar a configuração de seus servidores de autenticação para garantir que o servidor de gerenciamento seja capaz de se comunicar com eles. É possível validar a configuração pesquisando um usuário remoto ou grupo remoto de seus servidores de autenticação e autenticando-os usando as configurações configuradas.

Antes de começar

- Você deve ter habilitado a autenticação remota e configurado o serviço de autenticação para que o servidor do Unified Manager possa autenticar o usuário remoto ou o grupo remoto.
- Você deve ter adicionado seus servidores de autenticação para que o servidor de gerenciamento possa pesquisar o usuário remoto ou grupo remoto desses servidores e autenticá-los.
- Tem de ter a função Administrador de aplicações.

Se o serviço de autenticação estiver definido como ative 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 de autenticação.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **Autenticação remota**.
2. Clique em **Test Authentication**.
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 **Teste**.

   Se estiver a autenticar um grupo remoto, não deve introduzir a palavra-passe.

Adicionar alertas

Você pode configurar alertas para notificá-lo quando um evento específico é 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 configurações de notificação, como endereço de e-mail do usuário, servidor SMTP e host de intercetação SNMP, para permitir que o servidor Active IQ Unified Manager use essas configurações para enviar notificações aos usuários quando um evento é gerado.
- Você deve saber os recursos e eventos para os quais deseja acionar o alerta e os nomes de usuário ou endereços de e-mail dos usuários que deseja notificar.
- Se você quiser que um script seja executado com base no evento, você deve ter adicionado o script ao Unified Manager usando a página Scripts.
- Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

Você pode criar um alerta diretamente da página de detalhes do evento depois de 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 cadeia de texto no campo **Name contains** para selecionar um grupo de recursos. Com base na cadeia de texto especificada, a lista de recursos disponíveis exibe

apenas os recursos que correspondem à regra de filtro. A cadeia de texto especificada é sensível a maiúsculas e minúsculas.

Se um recurso estiver em conformidade com as regras incluir e excluir que você especificou, a regra excluir terá precedência sobre a regra incluir 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 os quais deseja acionar um alerta.

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

6. Clique em **ações** e selecione os usuários que você deseja notificar, escolha a frequência de notificação, escolha se uma trap SNMP será enviada ao recetor de trap 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 será exibido em branco porque o endereço de e-mail modificado não será mais mapeado para o usuário selecionado anteriormente. Além disso, se você modificou 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 através de traps SNMP.

7. Clique em **Salvar**.

Exemplo de adição de um alerta

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

- Nome do alerta: HealthTest
- Recursos: Inclui todos os volumes cujo nome contém "abc" e exclui todos os volumes cujo nome contém "xyz"
- Eventos: Inclui todos os eventos críticos de saúde
- Ações: Inclui "sample@domain.com", um script "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 **Teste de integridade** 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'] na área recursos disponíveis e mova-o para a área recursos selecionados.
   c. Clique em **Excluir**, digite **xyz** no campo **Nome contém** e clique em **Adicionar**.
3. Clique em **Eventos** e selecione **Crítica** 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 digite **sample@domain.com** no campo alertar esses usuários.
6. Selecione **lembrar a cada 15 minutos** para notificar o usuário a cada 15 minutos.

   Você pode configurar um alerta para enviar repetidamente notificações aos destinatários por um tempo especificado. Você deve determinar a hora a partir da qual a notificação de evento está ativa para o alerta.

7. No menu Selecionar Script para execução, selecione **Test** script.
8. Clique em **Salvar**.

Alterar a palavra-passe do utilizador local

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

Antes de começar

Você deve estar conetado como um usuário local.

As senhas para o usuário de manutenção e para usuários remotos não podem ser alteradas usando estas etapas. Para alterar uma palavra-passe de utilizador remoto, contacte o administrador da palavra-passe. Para alterar a senha do usuário de manutenção, "Utilizar a consola de manutenção"consulte .

Passos

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

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

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

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

Definir o tempo limite de inatividade da sessão

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

Antes de começar

Tem de ter a função Administrador de aplicações.

Esta definição afeta todas as sessões de utilizador com sessão iniciada.

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

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Definições da funcionalidade**.

2. Na página **Configurações de recursos**, especifique o tempo limite de inatividade escolhendo uma das seguintes opções:

Se você quiser…	Então faça isso…
Não tenha tempo limite definido 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 o valor de tempo limite	No painel **tempo limite de inatividade**, mova o botão deslizante para a direita (ligado), especifique o valor de tempo limite de inatividade em minutos e clique em **aplicar**.

Alterando o nome do host do Unified Manager

Em algum momento, talvez você queira alterar o nome do host do sistema no qual você 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.

Alterando o nome do host do dispositivo 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, você também deve regenerar o certificado HTTPS.

Antes de começar

Você deve estar conetado ao Unified Manager como usuário de manutenção ou ter a função 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 IU da Web do Unified Manager. Se você configurou um endereço IP estático para sua rede durante a implantação, então você teria designado um nome para o host de rede. Se você configurou a rede usando DHCP, o nome do host deve ser retirado do DNS. Se o DHCP ou DNS não estiver configurado corretamente, o nome do host "'Unified Manager'" será atribuído automaticamente e associado ao certificado de segurança.

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

Se você acessar a IU da Web usando o endereço IP do servidor em vez do nome do host, não será necessário gerar um novo certificado se você alterar o nome do host. No entanto, é a melhor prática 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, será necessário atualizar manualmente o nome do host 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 reinicializada.

Passos

1. Gerar um certificado de segurança HTTPS

   Se você quiser usar o novo nome de host para acessar a IU da Web do Unified Manager, será necessário regenerar 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.

Gerando 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

Tem de ter a função Administrador de aplicações.

Pode haver vários motivos para regenerar o certificado, como se você quiser ter melhores valores para Nome distinto (DN) ou se quiser um tamanho de chave maior, ou um período de validade mais longo ou se o certificado atual expirou.

Se você não tiver acesso à IU da Web do Unified Manager, poderá regenerar 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 a `Reset Server Certificate` opção do console de manutenção, um novo certificado HTTPS será criado, 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 **Regenerate HTTPS Certificate**.

   A caixa de diálogo Regerate HTTPS Certificate (regenerar certificado HTTPS) é exibida.

3. Selecione uma das opções a seguir, dependendo de como você deseja gerar o certificado:

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

Se você quiser…	Faça isso…
Gerar o certificado usando valores diferentes	Clique na opção **Atualizar os atributos de certificado atuais**. 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 o E-MAil, EMPRESA, DEPARTAMENTO, cidade, estado e país, se quiser que esses valores sejam preenchidos no certificado. Você também pode selecionar a partir do TAMANHO DA CHAVE disponível (o algoritmo da chave é ""RSA"".) e 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 a no máximo 36500 dias. Embora seja permitido um período de validade de 36500 dias, recomenda-se que você use um período de validade não superior a 397 dias ou 13 meses. Porque se você selecionar um período de validade superior a 397 dias e Planejar exportar um CSR para este certificado e assiná-lo por uma CA bem 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, localhost)" se quiser remover as informações de identificação local do campo nomes alternativos no certificado. Quando esta caixa de verificação está selecionada, apenas o que introduzir no campo é utilizado no campo nomes alternativos. Quando deixado em branco, o certificado resultante não terá um campo de nomes alternativos.

4. Clique em **Yes** 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.

Reiniciando a máquina virtual do Unified Manager

Você pode reiniciar a máquina virtual a partir do console de manutenção do Unified Manager. Você deve reiniciar depois de 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 conetado ao console de manutenção como usuário de manutenção.

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

Passos

1. Aceda à consola de manutenção.
2. Selecione **Configuração do sistema** > **Reiniciar Máquina Virtual**.

Alteração do nome de 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 você 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 quando você listar suas máquinas Linux.

Antes de começar

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

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

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

Se você acessar a IU da Web usando o endereço IP do servidor em vez do nome do host, não será necessário gerar um novo certificado se você alterar o nome do host. No entanto, é a melhor prática atualizar o certificado, de modo que o nome do host no certificado corresponda ao nome do host real. O novo certificado não entra em vigor até que a máquina Linux seja reiniciada.

Se você alterar o nome do host no Unified Manager, será necessário atualizar manualmente o nome do host no OnCommand Workflow Automation (WFA). O nome do host não é atualizado automaticamente no WFA.

Passos

1. Faça login como usuário raiz no sistema Unified Manager que você deseja modificar.
2. Pare o software Unified Manager e o software MySQL associado digitando o seguinte comando:

   ```
   systemctl stop ocieau ocie mysqld
   ```

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

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. 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. Depois que o serviço for reiniciado, verifique se o novo nome de host é capaz de 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 original do host.

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

   ```
   systemctl start mysqld ocie ocieau
   ```

Ativar e desativar o gerenciamento de armazenamento baseado em políticas

A partir do Unified Manager 9,7, você pode provisionar workloads de storage (volumes e LUNs) nos clusters do ONTAP e gerenciar esses workloads com base em níveis de serviço de performance atribuídos. Essa funcionalidade é semelhante à criação de workloads no ONTAP System Manager e à inclusão de políticas de QoS, mas, quando aplicada usando o Unified Manager, você pode provisionar e gerenciar workloads em todos os clusters que sua instância do Unified Manager está monitorando.

Tem de ter a função Administrador de aplicações.

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

Quando ativada, esta opção fornece muitos itens novos na interface do utilizador:

Novo conteúdo	Localização
Uma página para provisionar novos workloads	Disponível em **Common Tasks** > **Provisioning**
Uma página para criar políticas de nível de serviço de desempenho	Disponível a partir de **Definições** > **políticas** > **níveis de Serviço de desempenho**
Uma página para criar políticas de eficiência de storage de performance	Disponível a partir de **Definições** > **políticas** > **eficiência de armazenamento**
Painéis que descrevem o desempenho atual de workload e o IOPS de workload	Disponível a partir do Dashboard

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

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Definições da funcionalidade**.
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 isso…
Desative o gerenciamento de storage baseado em políticas	No painel **Gerenciamento de armazenamento baseado em políticas**, mova o botão deslizante para a esquerda.
Habilite o gerenciamento de storage baseado em políticas	No painel **Gerenciamento de armazenamento baseado em políticas**, mova o botão deslizante para a direita.

Configuração do 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 no console de manutenção por meio.

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

Gerir definições de funcionalidades

A página Configurações de recursos permite ativar e desativar recursos específicos no Active IQ Unified Manager. Isso inclui criar e gerenciar objetos de armazenamento com base em políticas, ativar o gateway de API e o banner de login, fazer upload de scripts para gerenciar alertas, agendar uma sessão de IU da Web com base no tempo de inatividade e desativar o recebimento de eventos da plataforma Active IQ.

A página Configurações de recursos só está disponível para usuários com função Administrador de aplicativos.

Para obter informações sobre o carregamento de scripts, "Ativar e desativar o carregamento de scripts"consulte .

Habilitando o gerenciamento de storage baseado em políticas

A opção **Gerenciamento de armazenamento baseado em políticas** permite o gerenciamento de armazenamento com base nos objetivos de nível de serviço (SLOs). Esta opção está ativada por predefinição.

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

Pode optar por ativar ou desativar esta funcionalidade a partir de **Geral** > **Definições de funcionalidade** > **Gestão de armazenamento baseada em políticas**. Ao ativar este recurso, as seguintes páginas estão disponíveis para operação e monitoramento:

- Provisionamento (provisionamento de workload de storage)
- **Políticas** > **níveis de Serviço de desempenho**
- **Políticas** > **eficiência de armazenamento**
- Coluna cargas de trabalho gerenciadas pela coluna Performance Service Level (nível de Serviço de Performance) na página clusters Setup (Configuração dos clusters)
- Painel desempenho da carga de trabalho no **Dashboard**

Você pode usar as telas para criar níveis de Serviço de Performance e políticas de eficiência de storage e provisionar workloads de storage. Também é possível monitorar os workloads de storage que estão em conformidade com os níveis de Serviço de performance atribuídos e os que não estão em conformidade. O painel Performance de workload e Workload IOPS também permite avaliar a capacidade e a performance (IOPS) totais, disponíveis e usadas dos clusters no data center com base nos workloads de storage provisionados neles.

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

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

Ativando o 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 fazer login neles individualmente.

Você pode habilitar esse recurso nas páginas de configuração que aparecem quando você faz login no Unified Manager pela primeira vez. Alternativamente, você pode ativar ou desativar esse recurso de **Geral** > **Configurações de recursos** > **Gateway 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 com as APIs REST do Unified Manager. No entanto, se você tiver um requisito comercial específico para acessar as APIs do ONTAP para gerenciar recursos específicos que não sejam expostos ao Gerenciador Unificado, poderá ativar o recurso de gateway de API e executar as APIs do ONTAP. O gateway atua como um proxy para túnel as solicitações de API, mantendo as solicitações de cabeçalho e corpo no mesmo formato que nas APIs do ONTAP. Você pode usar suas credenciais do Unified Manager e executar APIs específicas para acessar e gerenciar os clusters do ONTAP sem passar credenciais de cluster individuais. O Unified Manager funciona como um ponto único de gerenciamento para executar as APIs nos clusters do ONTAP gerenciados pela sua instância do Unified Manager. A resposta retornada pelas APIs é a mesma que a resposta retornada pelas respetivas APIs REST do ONTAP executadas diretamente do ONTAP.

Depois de ativar esse recurso, você pode executar as APIs REST do Unified Manager a partir da categoria **barra de menus** > **botão Ajuda** > **Documentação da API** > **gateway**. Como alternativa, você pode inserir o nome do host ou o endereço IP e o URL para acessar a página REST API no formato `https://<hostname>/docs/api/`

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

Especificar o tempo limite de inatividade

Você pode especificar o valor de tempo limite de inatividade para o Active IQ Unified Manager. Após uma inatividade do tempo especificado, o aplicativo é desconetado automaticamente. Esta opção está ativada por predefinição.

Pode desativar esta funcionalidade ou modificar a hora a partir de **Geral** > **Definições da funcionalidade** > **tempo limite de inatividade**. Depois de ativar este recurso, você deve especificar o limite de tempo de inatividade (em minutos) no campo **LOGOUT AFTER**, após o qual o sistema faz logout automaticamente. O valor padrão é de 4320 minutos (72 horas).

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

Ativar eventos do portal Active IQ

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

Ao ativar esse recurso, o Active IQ Unified Manager exibe eventos descobertos pelo portal do Active IQ. Esses eventos são criados executando um conjunto de regras contra as mensagens do AutoSupport geradas a partir 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.

Pode optar por ativar ou desativar esta funcionalidade a partir de **Geral** > **Definições da funcionalidade** > **Eventos do Portal Active IQ**. Em sites sem acesso à rede externa, você deve carregar as regras manualmente de **Gerenciamento de armazenamento** > **Configuração do evento** > **regras de upload**.

Esta funcionalidade está ativada por predefinição. A desativação desse recurso impede que os eventos do

Active IQ sejam descobertos ou exibidos no Gerenciador Unificado. Quando desativado, a ativação desse recurso permite que o Gerenciador Unificado receba os eventos do Active IQ em um cluster em um horário predefinido de 00:15 para esse fuso horário do cluster.

Ativar e desativar as definições de segurança para conformidade

Usando o botão **Personalizar** no painel **Painel de Segurança** da página Configurações de recursos, você pode ativar ou desativar os parâmetros de segurança para monitoramento de conformidade no Unified Manager.

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

Somente usuários com função de administrador podem editar essas configurações.

Os critérios de segurança dos clusters do ONTAP, das máquinas virtuais de storage e dos volumes são avaliados em relação às recomendações definidas no "Guia de endurecimento de segurança para NetApp ONTAP 9". O painel Segurança no painel e na página Segurança exibe o status padrão de conformidade de segurança dos clusters, VMs de armazenamento e volumes. Os eventos de segurança também são gerados e as ações de gerenciamento habilitadas para os clusters e as VMs de storage que têm violações de segurança.

Personalizar as definições de segurança

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

Passos

1. Clique em **Geral > Definições de funcionalidades > Painel de segurança > Personalizar**. A janela pop-up **Personalizar definições do painel de segurança** é apresentada.

   Os parâmetros de conformidade de segurança que você ativa ou desativa podem afetar diretamente as exibições de segurança padrão, os relatórios e os relatórios programados nas telas clusters e VMs de armazenamento. Se você tiver carregado um relatório do excel a partir dessas telas antes de modificar os parâmetros de segurança, os relatórios do excel baixados podem estar com defeito.

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

Personalizar as definições de AutoSupport e autenticação

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

Na seção **Configurações de autenticação**, você pode habilitar alertas do Gerenciador Unificado para o

usuário administrador padrão do ONTAP.

Ativar e desativar o carregamento de scripts

A capacidade de carregar scripts para o Unified Manager e executá-los é ativada por padrão. Se a sua organização não quiser permitir esta atividade por motivos de segurança, pode desativar esta funcionalidade.

Antes de começar

Tem de ter a função Administrador de aplicações.

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Definições da funcionalidade**.
2. Na página **Configurações de recursos**, desative ou habilite o script escolhendo uma das seguintes opções:

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

Adicionando banner de login

Adicionar um banner de login permite que sua organização exiba qualquer informação, como, quem tem permissão de acesso ao sistema e os termos e condições de uso durante o login e logout.

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

Utilizar a consola de manutenção

Você pode usar o console de manutenção para configurar as 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 no sistema do 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 problemas com o dispositivo virtual, especialmente se a interface da Web do Unified Manager não estiver disponível
- Atualize para versões mais recentes do Unified Manager
- Gere pacotes de suporte para enviar ao suporte técnico
- Configure as definições de rede
- Altere a palavra-passe do utilizador de manutenção
- Conete-se a um provedor de dados externo para enviar estatísticas de desempenho
- Alterar a coleta de dados de desempenho interna
- Restaure o banco de dados e as configurações do Unified Manager a partir de uma versão com backup anterior.

O que o utilizador de manutenção faz

O usuário de manutenção é criado durante a instalação do Unified Manager em um sistema Red Hat Enterprise Linux. O nome de usuário de manutenção é o usuário "umadmin". O usuário de manutenção tem a função Administrador do aplicativo na IU da Web e esse usuário pode criar usuários subsequentes e atribuir-lhes funções.

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

Capacidades do utilizador de diagnóstico

O objetivo do acesso ao diagnóstico é habilitar o suporte técnico para ajudá-lo na solução de problemas e você só deve usá-lo quando direcionado pelo suporte técnico.

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

Aceder à consola de manutenção

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

Antes de começar

Você precisa ter instalado e configurado o Unified Manager.

Após 15 minutos de inatividade, o console de manutenção faz o logout.

Quando instalado no VMware, se você já fez login como usuário de manutenção pelo console VMware, não será possível fazer login simultaneamente usando o Secure Shell.

Passo

1. Siga estas etapas para acessar o console de manutenção:

Neste sistema operativo…	Siga estes passos…
VMware	a. Usando o Secure Shell, conete-se ao endereço IP ou ao nome de domínio totalmente qualificado do dispositivo virtual do Unified Manager. b. Inicie sessão na consola de manutenção utilizando o nome de utilizador e a palavra-passe de manutenção.
Linux	a. Usando o Secure Shell, conete-se ao endereço IP ou ao nome de domínio totalmente qualificado do sistema Unified Manager. b. Inicie sessão no sistema com o nome e a palavra-passe do utilizador de manutenção (umadmin). c. Digite o comando `maintenance_console` e pressione Enter.
Windows	a. Faça 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.

Acessando o console de manutenção usando o console vSphere VM

Se a interface de usuário do Unified Manager não estiver em operação ou se precisar executar funções que não estejam 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 ser ligado para acessar o console de manutenção.

Passos

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

   Após 15 minutos de inatividade, o console de manutenção faz o logout.

Menus da consola de manutenção

O console de manutenção consiste em diferentes menus que permitem manter e gerenciar recursos especiais e configurações 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. Repor certificado de servidor
  c. Fornecedor de dados externo
  d. Restauro de cópia de segurança
  e. Configuração do intervalo de polling de desempenho
  f. Desativar a autenticação SAML
  g. Exibir/alterar portas de aplicativos
  h. Configuração do registo de depuração
  i. Controle o acesso à porta MySQL 3306
  j. Saia

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

Menu Network Configuration (Configuração da rede)

O menu Network Configuration (Configuração de rede) permite gerir as definições de rede. Você deve usar esse menu quando a interface de usuário do Unified Manager não estiver disponível.

> Esse menu não estará disponível se o Unified Manager estiver instalado no Red Hat Enterprise Linux ou no Microsoft Windows.

Estão disponíveis as seguintes opções de menu.

- **Display IP Address Settings** (Exibir configurações de endereço IP)

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

- **Altere as configurações de endereço IP**

  Permite alterar qualquer uma das definições de rede para o dispositivo virtual, incluindo o endereço IP, máscara de rede, gateway ou servidores DNS. Se você mudar as configurações de rede de DHCP para redes estáticas usando o console de manutenção, não será possível editar o nome do host. Você deve selecionar **Commit Changes** para que as alterações ocorram.

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

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

- * Alterar configurações de pesquisa de nome de domínio*

  Permite alterar os nomes de domínio para os quais você deseja pesquisar ao resolver nomes de host. Você deve selecionar **Commit Changes** para que as alterações ocorram.

- **Exibir rotas estáticas**

  Apresenta as rotas de rede estáticas atuais.

- **Alterar rotas estáticas**

  Permite adicionar ou eliminar rotas de rede estáticas. Você deve selecionar **Commit Changes** para que as alterações ocorram.

  - **Adicionar rota**

    Permite adicionar uma rota estática.

  - **Eliminar rota**

    Permite eliminar uma rota estática.

  - * Voltar*

    Leva-o de volta ao **Menu Principal**.

  - **Saída**

    Sai da consola de manutenção.

- * Desativar a interface de rede*

  Desativa todas as interfaces de rede disponíveis. Se apenas uma interface de rede estiver disponível, não é possível desativá-la. Você deve selecionar **Commit Changes** para que as alterações ocorram.

- **Ativar interface de rede**

  Permite interfaces de rede disponíveis. Você deve selecionar **Commit Changes** para que as alterações ocorram.

- **Commit Changes**

  Aplica quaisquer alterações efetuadas às definições de rede para o dispositivo virtual. Você deve selecionar essa opção para realizar quaisquer alterações feitas ou as alterações não ocorrem.

- **Ping um anfitrião**

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

- **Restaurar para as configurações padrão**

  Repõe todas as definições para as predefinições de fábrica. Você deve selecionar **Commit Changes** para

que as alterações ocorram.

- * Voltar*

  Leva-o de volta ao **Menu Principal**.

- **Saída**

  Sai da consola de manutenção.

Menu System Configuration (Configuração do sistema)

O menu System Configuration (Configuração do sistema) permite-lhe gerir o seu dispositivo virtual, fornecendo várias opções, tais como a visualização do estado do servidor e a reinicialização e encerramento da máquina virtual.

Quando o Unified Manager é instalado em um sistema Linux ou Microsoft Windows, somente a opção ""Restaurar a partir de um backup do Unified Manager"" está disponível neste menu.

Estão disponíveis as seguintes opções de menu:

- **Estado do servidor de visualização**

  Exibe o status atual do servidor. As opções de status incluem Running (Corrida) e Not Running (não corrida).

  Se o servidor não estiver em execução, talvez seja necessário entrar em Contato com o suporte técnico.

- **Reboot Virtual Machine**

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

- **Desligue a máquina virtual**

  Desliga a máquina virtual, parando todos os serviços.

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

- * Alterar senha de usuário *

  Altera a palavra-passe do utilizador que está atualmente ligado, que só pode ser o utilizador de manutenção.

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

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

- **Aumente o tamanho do disco de troca**

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

- **Alterar fuso horário**

Altera o fuso horário para a sua localização.

- **Altere o servidor NTP**

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

- **Altere o serviço NTP**

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

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

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

- **Redefinir certificado de servidor**

  Redefine o certificado de segurança do servidor.

- **Altere o nome de host**

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

- * Voltar*

  Sai do menu System Configuration (Configuração do sistema) e regressa ao menu Main (Menu principal).

- **Saída**

  Sai do menu da consola de manutenção.

Menu suporte e Diagnóstico

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

Estão disponíveis as seguintes opções de menu:

- **Gerar Pacote de suporte leve**

  Permite produzir um pacote de suporte leve que contém apenas 30 dias de Registros e Registros de banco de dados de configuração — exclui dados de desempenho, arquivos de gravação de aquisição e despejo de heap do servidor.

- **Gerar Pacote de suporte**

  Permite criar um pacote de suporte completo (arquivo 7-Zip) contendo informações de diagnóstico no diretório inicial do usuário de diagnóstico. Se o seu sistema estiver ligado à Internet, também pode 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 Gerenciador Unificado, dados detalhados sobre os componentes internos do servidor do Gerenciador Unificado e logs de nível detalhado não incluídos normalmente nas mensagens do AutoSupport ou no pacote de suporte leve.

Opções de menu adicionais

As opções de menu a seguir permitem executar várias tarefas administrativas no servidor do Unified Manager.

Estão disponíveis as seguintes opções de menu:

- **Redefinir certificado de servidor**

  Regenera o certificado do servidor HTTPS.

  Você pode regenerar o certificado do servidor na GUI do Unified Manager clicando em **Geral** > **certificados HTTPS** > **Regenerate HTTPS Certificate**.

- * Desativar 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. Essa opção de console geralmente é usada quando um problema com o servidor IDP ou a configuração SAML impede que os usuários acessem a GUI do Unified Manager.

- **Fornecedor de dados Externo**

  Fornece opções para conetar o Unified Manager a um provedor de dados externo. Depois de estabelecer a conexão, os dados de desempenho são enviados para um servidor externo para que os especialistas em desempenho de storage possam traçar as métricas de desempenho usando software de terceiros. São apresentadas as seguintes opções:

  - **Configuração do servidor de exibição**--exibe as configurações atuais de conexão e configuração para 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.

    Depois que a conexão é excluída, o Unified Manager perde sua conexão com o servidor externo.

- **Backup Restore**

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

- **Configuração do intervalo de polling de desempenho**

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

  Você pode alterar esse intervalo para 10 ou 15 minutos se descobrir que coleções de clusters grandes não estão sendo concluídas no tempo.

- **Exibir/alterar portas de aplicativos**

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

- * Controle o acesso à porta MySQL 3306*

  Controla o acesso do host à porta MySQL padrão 3306. Por razões de segurança, o acesso por meio dessa porta é restrito apenas ao localhost durante uma nova instalação do Unified Manager em sistemas Linux, Windows e VMware vSphere. Essa opção permite alternar a visibilidade dessa porta entre o localhost e os hosts remotos, ou seja, se ela estiver habilitada para localhost somente em seu ambiente, você também poderá disponibilizar essa porta para hosts remotos. Como alternativa, quando ativado para todos os hosts, você pode restringir o acesso desta porta apenas ao localhost. Se o acesso foi ativado em hosts remotos anteriormente, a configuração é mantida em um cenário de atualização. Você deve verificar as configurações de firewall em sistemas Windows depois de alternar a visibilidade da porta e desativar as configurações de firewall se as configurações estiverem configuradas para restringir o acesso à porta MySQL 3306.

- **Saída**

  Sai do menu da consola de manutenção.

Alterar a palavra-passe do utilizador 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 IU da Web do Unified Manager, clique em **Esqueceu a senha**.

   É apresentada uma página que solicita o nome do utilizador cuja palavra-passe pretende repor.

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 **RESET password** no e-mail e defina a nova senha.
4. Retorne à IU da Web e faça login no Unified Manager usando a nova senha.

Alterar a senha 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 mais tarde.

Antes de começar

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

Passos

1. Faça login como usuário raiz no sistema Linux no qual o Unified Manager está sendo executado.
2. Altere a senha 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 protocolos HTTP e HTTPS

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

Antes de começar

Você deve ter uma ID de usuário e senha autorizados para fazer 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 o navegador antes de atribuir um novo número de porta para o tráfego HTTP e HTTPS. Selecionar uma porta insegura pode tornar o sistema inacessível, o que exigiria que você entre em Contato com o suporte ao cliente para obter uma resolução.

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

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

   Os prompts do console do Unified Managermaintenance são exibidos.

2. Digite o número da opção de menu chamada **Exibir/alterar portas do 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 solicitado a alterar as portas e reiniciar o Unified Manager agora.

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

Após essa alteração, os usuários devem incluir o novo número de porta no URL para acessar a interface da Web do Gerenciador Unificado, por exemplo, https://host.company.com:1234+, https://12.13.14.15:1122+, ou https://[2001:db8:0:1]:2123+.

Adicionando 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 vSphere, selecione **Configuração do sistema** > **Reboot Operating System**.

   Após a reinicialização, o console de manutenção pode detetar a interface de rede recém-adicionada.

2. Aceda à consola de manutenção.
3. Selecione **Configuração de rede** > **Ativar Interface de rede**.
4. Selecione a nova interface de rede e pressione **Enter**.

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

5. Digite **y** para ativar a interface de rede.
6. Introduza as definições de rede.

   É-lhe pedido que introduza as definições de rede se estiver a utilizar uma interface estática ou se o DHCP não for detetado.

   Depois de introduzir as definições de rede, regressa automaticamente ao menu **Configuração de rede**.

7. Selecione **Commit Changes**.

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

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

O diretório do 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 de clusters depois que o diretório atinge 95% cheio.

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.

Adicionando espaço ao diretório de dados do host Linux

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

Antes de começar

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

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

Passos

1. Faça login como usuário 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 diretório atual `/opt/netapp/data`.
4. Copie o conteúdo e a configuração de privilégios do diretório existente `/opt/netapp/data` para o diretório de dados de backup:

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

5. Se o se Linux estiver ativado:

   a. Obtenha o tipo se Linux para pastas na pasta existente `/opt/netapp/data`:

      ```
      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. Expanda o tamanho `/opt/netapp/data` do diretório para um mínimo de 150 GB por meio de comandos LVM ou adicionando discos extras.

   > Se você criou `/opt/netapp/data` a partir de um disco, 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, `resize` como e `extend` podem não funcionar como esperado.

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

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

O sistema retorna uma confirmação semelhante à seguinte:

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

9. Se o se Linux estiver ativado, confirme que o contexto `/opt/netapp/data` do 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 de banco de dados no futuro.
11. Copie o conteúdo dos dados de backup de volta para o diretório expandido `/opt/netapp/data`:

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

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

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

13. Inicie o serviço MySQL:

```
systemctl start mysqld
```

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

```
systemctl start ocie ocieau
```

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

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

Adicionando espaço ao disco de dados da máquina virtual VMware

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

- Tem de ter as credenciais do utilizador de manutenção.

Recomendamos que você faça backup de 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 da VMware para obter detalhes.

   Em alguns casos raros, a implantação do Unified Manager usa o disco rígido 2 para o disco de dados em vez do disco rígido 3. Se isso tiver ocorrido em sua implantação, aumente o espaço de qualquer disco maior. O disco de dados sempre terá mais espaço do que o outro disco.

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

Adicionando espaço à unidade lógica do servidor Microsoft Windows

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

Antes de começar

Você deve ter o Privileges administrador do Windows.

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

Passos

1. Inicie sessão como administrador no servidor Windows no qual pretende adicionar espaço em disco.
2. Siga a etapa 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 do Unified Manager está instalado.	Siga as etapas no tópico da Microsoft: "Estender um volume básico"
Em um servidor físico, adicione uma unidade de disco rígido.	Siga as etapas no tópico da Microsoft: "Adicionar unidades de disco rígido"
Em uma máquina virtual, aumente o tamanho de uma partição de disco.	Siga as etapas no tópico VMware: "Aumentando o tamanho de uma partição de disco"

Gerenciando o 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 recursos podem gerenciar os objetos no Unified Manager.

Adicionando usuários

Você pode adicionar usuários locais ou usuários de banco de dados usando a página usuários. Você também pode adicionar usuários remotos ou grupos que pertencem a um servidor de autenticação. Você pode atribuir funções a esses usuários e, com base no Privileges das funções, os usuários podem gerenciar os objetos de storage e dados com o Unified Manager, ou exibir os dados em um banco de dados.

Antes de começar

- Tem de ter a função Administrador de aplicações.
- Para adicionar um utilizador ou grupo remoto, tem de ter ativado a autenticação remota e configurado o servidor de autenticação.
- Se você planeja configurar a autenticação SAML para que um provedor de identidade (IDP) autentique usuários acessando a interface gráfica, certifique-se de que esses usuários sejam definidos como usuários "remode".

  O acesso à IU não é permitido para usuários do tipo "local" ou "Manutenção" quando a autenticação SAML está ativada.

Se você adicionar um grupo do Windows ative Directory, todos os membros diretos e subgrupos aninhados poderão se autenticar no Unified Manager, a menos que os subgrupos aninhados estejam desativados. Se você adicionar um grupo do OpenLDAP ou de outros serviços de autenticação, somente os membros diretos desse grupo poderão se autenticar no Unified Manager.

Passos

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

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

4. Clique em **Add**.

Criando um usuário de banco de dados

Para oferecer suporte a uma conexão entre o Workflow Automation e o Unified Manager, ou para acessar exibições de banco de dados, primeiro é necessário criar um usuário de banco de dados com a função Esquema de integração ou Esquema de Relatório na IU da Web do Unified Manager.

Antes de começar

Tem de ter a função Administrador de aplicações.

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

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **usuários**.
2. Na página usuários, clique em **Adicionar**.
3. Na caixa de diálogo Adicionar usuário, selecione **Usuário de 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 **Role**, selecione a função apropriada.

Se você é…	Escolha esta função
Conetando o Unified Manager ao Workflow Automation	Esquema de integração
Acessando relatórios e outras exibições de banco de dados	Esquema Relatório

6. Clique em **Add**.

Editar as definições do utilizador

Você pode editar as configurações do usuário - como o endereço de e-mail e a função - que são especificadas cada usuário. Por exemplo, talvez você queira alterar a função de um usuário que é um operador de armazenamento e atribuir Privileges ao usuário do administrador de armazenamento.

Antes de começar

Tem de ter a função Administrador de aplicações.

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

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

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **usuários**.
2. Na página usuários, selecione o usuário para o qual 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**.

Visualização de usuários

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

Antes de começar

Tem de ter a função Administrador de aplicações.

Passo

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

Eliminar utilizadores ou grupos

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

Antes de começar

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

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

- Tem de ter a função Administrador de aplicações.

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 **Yes** para confirmar a exclusão.

O que é RBAC

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

Que controle de acesso baseado em função faz

O controle de acesso baseado em função (RBAC) permite que os administradores gerenciem grupos de usuários definindo funções. Se você precisar restringir o acesso para funcionalidades específicas aos administradores selecionados, você deverá configurar contas de administrador para eles. Se você quiser restringir as informações que os administradores podem exibir e as operações que podem executar, você deve aplicar funções às contas de administrador criadas.

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

Quando você inicia uma operação que requer Privileges específico, o servidor de gerenciamento solicita que você faça login. Por exemplo, para criar contas de administrador, você deve fazer login com acesso à conta de Administrador de aplicativos.

Definições dos tipos de utilizador

Um tipo de usuário especifica o tipo de conta que o usuário detém 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 usuário do Unified Manager são os seguintes:

- **Usuário de manutenção**

  Criado durante a configuração inicial do Unified Manager. O usuário de manutenção cria usuários adicionais e atribui funções. O utilizador de manutenção é também o único utilizador com acesso à consola 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 IU do Unified Manager e executa funções com base na função dada pelo usuário de manutenção ou por um usuário com a função Administrador de aplicativos.

- **Grupo remoto**

  Um grupo de usuários que acessam a IU 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 do grupo remoto têm acesso à IU do Unified Manager usando suas credenciais de usuário individuais. Os grupos remotos podem executar funções de acordo com suas funções atribuídas.

- **Utilizador remoto**

  Acessa a IU do Unified Manager usando as credenciais armazenadas no servidor de autenticação. Um usuário remoto executa funções com base na função dada pelo usuário de manutenção ou um usuário com a função Administrador de aplicativos.

- **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 nem ao console de manutenção e não pode executar chamadas de API.

Definições de funções de utilizador

O usuário de manutenção ou o administrador de aplicativos atribui uma função a cada usuário. Cada função contém determinados Privileges. O escopo das atividades que

você pode executar no Unified Manager depende da função atribuída e de qual Privileges a função contém.

O Unified Manager inclui as seguintes funções de usuário predefinidas:

- **Operador**

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

- **Administrador de armazenamento**

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

- **Administrador de aplicação**

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

  Quando o Unified Manager é instalado em sistemas Linux, o usuário inicial com a função Application Administrator é automaticamente chamado de "umadmin".

- **Esquema de integração**

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

- **Esquema Relatório**

  Essa função permite o 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_performance
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - scalemonitor

Funções e recursos de usuário do Unified Manager

Com base na função de usuário atribuída, você pode determinar quais operações podem ser executadas no Unified Manager.

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

Função	Operador	Administrador de armazenamento	Administrador de aplicativos	Esquema de integração	Esquema Relatório
Ver informações do sistema de armazenamento	•	•	•	•	•
Veja outros dados, como históricos e tendências de capacidade	•	•	•	•	•
Exibir, atribuir e resolver eventos	•	•	•		
Visualize objetos do serviço de storage, como associações de SVM e pools de recursos	•	•	•		
Exibir políticas de limite	•	•	•		
Gerenciar objetos de serviço de storage, como associações de SVM e pools de recursos		•	•		
Definir alertas		•	•		
Gerenciar opções de gerenciamento de storage		•	•		
Gerenciar políticas de gerenciamento de storage		•	•		
Gerenciar usuários			•		

Função	Operador	Administrador de armazenamento	Administrador de aplicativos	Esquema de integração	Esquema Relatório
Gerenciar opções administrativas			•		
Definir políticas de limite			•		
Gerenciar acesso ao banco de dados			•		
Gerencie a integração com O WFA e forneça acesso às visualizações do banco de dados				•	
Programe e salve relatórios		•	•		
Execute as operações "Fix it" a partir de ações de gerenciamento		•	•		
Forneça acesso somente leitura às exibições do banco de dados					•

Gerenciando configurações de autenticação SAML

Depois de configurar as configurações de autenticação remota, é possível ativar a autenticação SAML (Security Assertion Markup Language) para que os usuários remotos sejam autenticados por um provedor de identidade seguro (IDP) antes que eles possam acessar a IU da Web do Unified Manager.

Observe que somente usuários remotos terão acesso à interface gráfica do usuário do Unified Manager depois que a autenticação SAML for ativada. Os utilizadores locais e os utilizadores de manutenção não poderão aceder à IU. Essa 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.

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

Padrões de criptografia suportados

- AES (Advanced Encryption Standard): AES-128 e AES-256
- Algoritmo Hash seguro (SHA): SHA-1 e SHA-256

Provedores de identidade validados

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

Requisitos de configuração ADFS

- Você deve definir três regras de reivindicação na ordem a seguir, necessárias para que o Unified Manager analise respostas ADFS SAML para essa entrada confiável de parte confiável.

Regra de reclamação	Valor
Nome da conta SAM	ID do nome
Nome da conta SAM	urna:oid:0.9.2342.19200300.100.1.1
Grupos de token — Nome não qualificado	urna:oid: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 podem receber um erro ao fazer logout do Unified Manager . Siga estes passos:
  a. Abra o Console de Gerenciamento ADFS.
  b. Clique na pasta Authentication Policies (políticas de autenticação) no modo de exibição de 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 da "Autenticação do Windows" padrão.
- Em alguns casos, o login pelo IDP é rejeitado quando o certificado de segurança do Unified Manager é assinado pela CA. Existem duas soluções alternativas para resolver este problema:
  - Siga as instruções identificadas no link para desativar a verificação de revogação no servidor ADFS para a entidade dependente associada a cert AC encadeada:

    "Desativar Verificação de revogação por confiança de parte dependente"

◦ Peça que o servidor da CA resida no servidor ADFS para assinar a solicitação de cert do servidor do Unified Manager.

Outros requisitos de configuração

- O desvio do relógio do Unified Manager é definido para 5 minutos, portanto, a diferença de tempo entre o servidor IDP e o servidor do Unified Manager não pode ser superior a 5 minutos ou a autenticação falhará.

Habilitando a autenticação SAML

Você pode ativar a autenticação SAML (Security Assertion Markup Language) para que os usuários remotos sejam autenticados por um provedor de identidade seguro (IDP) antes que eles possam acessar a IU 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 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 ativar 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 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 ativada. Os utilizadores locais e os utilizadores de manutenção não poderão aceder à IU. Essa configuração não afeta os usuários que acessam o console de manutenção, os comandos do Unified Manager ou ZAPIs.

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

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação SAML**.
2. Marque a caixa de seleção **Enable SAML Authentication** (Ativar autenticação SAML*).

   São apresentados os campos necessários para configurar a ligação IDP.

3. Insira o URI de IDP e os metadados de IDP necessários para conetar o servidor do Unified Manager ao servidor de IDP.

   Se o servidor IDP estiver acessível diretamente a partir do servidor do Unified Manager, você poderá clicar no botão **obter metadados IDP** depois de inserir o URI IDP para preencher o campo metadados 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.

Neste momento, você pode configurar o servidor IDP com essas informações.

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 **Confirm and Logout** (confirmar e terminar sessão) e o Unified Manager é reiniciado.

Da próxima vez que os 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 estiver 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 provedor de identidade, a GUI do Unified Manager não honra 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 da função** > **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 à esquerda, clique em **Geral** > **Autenticação SAML**.
2. Insira o novo URI de IDP e os metadados de IDP necessários para conetar o servidor do Unified Manager ao IDP.

   Se o IDP estiver acessível diretamente a partir do servidor do Unified Manager, você poderá clicar no botão **obter metadados IDP** depois de inserir o URL IDP para preencher o campo metadados IDP automaticamente.

3. Copie o URI de metadados do Unified Manager ou salve os metadados em um arquivo de texto XML.
4. Clique em **Save Configuration** (Guardar configuração).

   É apresentada uma caixa de mensagem para confirmar que pretende 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.

Da próxima vez que os 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.

Atualizando as configurações de autenticação SAML após a alteração do certificado de segurança do Unified Manager

Qualquer alteração ao certificado de segurança HTTPS instalado no servidor do Unified Manager requer que você atualize as configurações de autenticação SAML. O certificado é 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 Unified Manager para reativar o acesso à interface do usuário.

Passos

1. Inicie sessão na consola de manutenção.
2. No **Menu Principal**, insira o número da opção **Desativar autenticação SAML**.

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

3. Inicie a interface de usuário do Unified Manager usando o FQDN ou o endereço IP atualizado, aceite o certificado de servidor atualizado no navegador e faça login usando as credenciais de usuário de manutenção.
4. Na página **Configuração/Autenticação**, selecione a guia **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 **Confirm and Logout** (confirmar e terminar sessão) e o Unified Manager é reiniciado.
8. Acesse seu servidor IDP e insira o URI e os metadados do servidor Unified Manager para concluir a configuração.

Provedor de identidade	Etapas de configuração
ADFS	a. Exclua a entrada confiável de parte confiável existente na GUI de gerenciamento ADFS. b. Adicione uma nova entrada confiável de 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 respostas ADFS SAML para essa entrada confiável de parte confiável. d. Reinicie o serviço ADFS Windows.

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

9. Faça login no Unified Manager e verifique se a autenticação SAML funciona como esperado por meio do IDP.

Desativando a autenticação SAML

Você pode desativar a autenticação SAML quando quiser parar de autenticar usuários remotos por meio de um provedor de identidade seguro (IDP) antes que eles possam fazer login na IU da Web do Unified Manager. Quando a autenticação SAML está desativada, os provedores de serviços de diretório configurados, como o ative Directory ou LDAP, executam a autenticação de logon.

Depois de desativar a autenticação SAML, os utilizadores locais e os utilizadores de manutenção poderão aceder à interface gráfica do utilizador, além dos utilizadores remotos configurados.

Você também pode desativar 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 desativada.

Passos

1. No painel de navegação à esquerda, clique em **Geral** > **Autenticação SAML**.
2. Desmarque a caixa de seleção **Enable SAML Authentication** (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 **Confirm and Logout** (confirmar e terminar sessão) e o Unified Manager é reiniciado.

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

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

Desativar a autenticação SAML a partir do console de manutenção

Talvez seja necessário desativar a autenticação SAML do console de manutenção quando não houver acesso à GUI do Unified Manager. Isso pode acontecer em casos de má configuração 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 desativada, os provedores de serviços de diretório configurados, como o ative Directory ou LDAP, executam a autenticação de logon. Usuários locais e usuários de manutenção poderão acessar a interface gráfica do usuário além de usuários remotos configurados.

Você também pode desativar a autenticação SAML na página Configuração/Autenticação na IU.

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

Passos

1. Inicie sessão na consola de manutenção.
2. No **Menu Principal**, insira o número da opção **Desativar autenticação SAML**.

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

3. Digite **y** e pressione Enter e o Unified Manager será reiniciado.

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

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

Página 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 IU da Web do Unified Manager.

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

Depois que a autenticação remota e os usuários remotos tiverem sido configurados, você poderá selecionar a caixa de seleção Habilitar autenticação SAML para habilitar a autenticação usando um provedor de identidade seguro.

- * IDP URI*

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

  Exemplo de URI de ADFS:

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

  Exemplo de Shibboleth URI:

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

- **Metadados IDP**

  Os metadados IDP em formato XML.

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

- **Sistema anfitrião (FQDN)**

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

- * Host URI*

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

- **Metadados do host**

  Os metadados do sistema anfitrião em formato XML.

Gerenciamento da autenticação

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

Para ativar a autenticação remota, configurar serviços de autenticação e adicionar severs de autenticação, consulte a seção anterior em **Configurando o Unified Manager para enviar notificações de alerta**.

Editando servidores de autenticação

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

Antes de começar

Tem de ter a função Administrador de aplicações.

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 deseja editar e clique em **Editar**.
4. Na caixa de diálogo **Editar servidor de autenticação**, edite os detalhes da porta.
5. Clique em **Salvar**.

Eliminar 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

pretender alterar um servidor de autenticação com o qual o servidor de gestão está a comunicar, pode eliminar o servidor de autenticação e adicionar um novo servidor de autenticação.

Antes de começar

Tem de ter a função Administrador de aplicações.

Quando você exclui um servidor de autenticação, usuários remotos ou grupos 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 **Yes** para confirmar a solicitação de exclusão.

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

Autenticação com ative Directory ou OpenLDAP

Você pode ativar a autenticação remota no servidor de gerenciamento e configurar o servidor de gerenciamento para se comunicar com seus servidores de autenticação para que os usuários 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:

- Microsoft ative Directory

  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 os usuários remotos no servidor de autenticação acessem o Unified Manager. As credenciais para usuários remotos ou grupos são mantidas pelo servidor de autenticação. O servidor de gerenciamento usa o LDAP (Lightweight Directory Access Protocol) para autenticar usuários remotos no servidor de autenticação configurado.

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

Registo de auditoria

Você pode detetar se os logs de auditoria foram comprometidos com o uso de logs de auditoria. Todas as atividades realizadas por um utilizador são monitorizadas e registadas nos registos de auditoria. As auditorias são realizadas para todas as interfaces de usuário e funcionalidades do Active IQ Unified Manager das APIs expostas

publicamente.

Você pode usar o **Registro de auditoria: Exibição de arquivo** para exibir e acessar todos os arquivos de log de auditoria disponíveis no Active IQ Unified Manager. Os arquivos no Audit Log: File View são listados com base em sua data de criação. Esta vista apresenta informações de todo o registo de auditoria que são capturados da instalação ou atualização para o presente no sistema. Sempre que você executa uma ação no Unified Manager, as informações são atualizadas e estão disponíveis nos logs. O status de cada arquivo de log é capturado usando o atributo "Status de integridade de arquivo" que é monitorado ativamente para detetar adulteração ou exclusão do arquivo de log. Os logs de auditoria podem ter um dos seguintes estados quando os logs de auditoria estão disponíveis no sistema:

Estado	Descrição
ATIVO	Ficheiro no qual os registos estão a ser registados atualmente.
NORMAL	Ficheiro inativo, comprimido e armazenado no sistema.
ADULTERADO	Arquivo que foi comprometido por um usuário que editou manualmente o arquivo.
MANUAL_DELETE	Arquivo que foi excluído por um usuário autorizado.
ROLLOVER_DELETE	Ficheiro que foi eliminado devido à implementação com base na política de configuração contínua.
UNEXPECTED_DELETE	Arquivo que foi excluído devido a razões desconhecidas.

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

- Configurar
- Eliminar
- Transferir

O botão **DELETE** permite excluir 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 juntamente com o nome do usuário que realizou a operação de exclusão.

A exclusão de um arquivo de log causará a exclusão do arquivo do sistema, mas a entrada na tabela DB 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 "ADULTERADO" são baixados em um formato compactado `.gzip`.

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 registos de auditoria arquivados não estão incluídos.

Configurando logs de auditoria

Você pode usar o botão **Configurar** na seção Logs de auditoria para configurar a política de rolagem para arquivos de log de auditoria e também ativar o log remoto para os Logs de auditoria.

Você pode definir os valores nos DIAS DE RETENÇÃO DO REGISTRO **MAX** e **DIAS DE RETENÇÃO DO LOG DE AUDITORIA** de acordo com a quantidade e a frequência desejadas dos dados que deseja armazenar no sistema. O valor no campo **TAMANHO TOTAL DO LOG DE AUDITORIA** é o tamanho dos dados totais do log de auditoria presentes no sistema. A política de rolagem é determinada pelos valores no campo **DIAS DE RETENÇÃO DO LOG DE AUDITORIA**, **TAMANHO DO ARQUIVO MAX** 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 de arquivo continua disponível no banco de dados e é marcada como "Rollover Delete". O valor **AUDIT LOG RETENT DAYS** 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 é rolado.

Passos

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

   Se pretender ativar o registo remoto, deve selecionar **Ativar registo remoto**.

Ativar o registo remoto de registos de auditoria

Pode selecionar a caixa de verificação **Ativar registo remoto** na caixa de diálogo Configurar registos de auditoria para ativar o registo de auditoria remota. Você pode usar esse recurso para transferir logs de auditoria para um servidor Syslog remoto. Isso permitirá que você gerencie seus logs de auditoria quando houver restrições de espaço.

O Registro remoto de logs de auditoria fornece um backup à prova de violação no caso de os arquivos de log de auditoria no servidor Active IQ Unified Manager serem adulterados.

Passos

1. Na caixa de diálogo **Configurar registos de auditoria**, selecione a caixa de verificação **Ativar registo remoto**.

   São apresentados campos adicionais para configurar o registo remoto.

2. Introduza **HOSTNAME** e **PORT** do servidor remoto ao qual pretende ligar.
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` formato. Este certificado deve ser obtido a partir do servidor Syslog de destino e não deve ter expirado. O certificado deve conter o nome do host selecionado como parte do `SubjectAltName` atributo (SAN).

4. Insira os valores para os seguintes campos: **CHARSET**, **TEMPO LIMITE DE CONEXÃO**, **ATRASO DE CONEXÃO**.

   Os valores devem estar em milissegundos para esses campos.

5. Selecione o formato Syslog e a versão do protocolo TLS necessários nos campos **FORMAT** e **PROTOCOL**.
6. Marque a caixa de seleção **Ativar 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 para o servidor Syslog antes de salvar a configuração do Log de auditoria, caso contrário a conexão falhará. Dependendo do tipo de servidor Syslog, talvez seja necessário criar um hash do certificado de autenticação do cliente.

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

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

   Você será redirecionado para a página Logs de auditoria.

> ⓘ O valor **tempo limite da conexão** pode afetar a configuração. Se a configuração demorar mais tempo a responder do que o valor definido, pode resultar em falha de configuração devido a um erro de conexão. Para estabelecer uma conexão bem-sucedida, aumente o valor **tempo limite da conexão** e tente a configuração novamente.

Página Autenticação remota

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

Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

Depois de selecionar a caixa de verificação Ativar autenticação remota, pode ativar a autenticação remota utilizando um servidor de autenticação.

- **Serviço de autenticação**

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

  - **Ative Directory**
    - Nome do administrador

      Especifica o nome de administrador do servidor de autenticação.

- Palavra-passe

  Especifica a senha para acessar o servidor de autenticação.

- Nome diferenciado base

  Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for mais de ou@domain.com, então o nome distinto base é

- Desative a Pesquisa de grupos aninhados

  Especifica se deseja ativar ou desativar a opção de pesquisa de grupo aninhado. Por predefinição, esta opção está desativada. Se você usar o ative Directory, poderá acelerar a autenticação desativando o suporte para grupos aninhados.

- Utilize a ligação segura

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

◦ **OpenLDAP**

- Vincular Nome distinto

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

- Vincular senha

  Especifica a senha para acessar o servidor de autenticação.

- Nome diferenciado base

  Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for mais de ou@domain.com, então o nome distinto base é

- Utilize a ligação segura

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

◦ **Outros**

- Vincular Nome distinto

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

- Vincular senha

  Especifica a senha para acessar o servidor de autenticação.

- Nome diferenciado base

  Especifica a localização dos usuários remotos no servidor de autenticação. Por exemplo, se o nome de domínio do servidor de autenticação for mais de ou@domain.com, então o nome distinto

base é

- Versão do protocolo

  Especifica a versão LDAP (Lightweight Directory Access Protocol) suportada pelo servidor de autenticação. Pode especificar se a versão do protocolo tem de ser detetada automaticamente ou definir a versão para 2 ou 3.

- Atributo Nome Utilizador

  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 especificado no servidor de autenticação do usuário.

- UGID

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

- Desative a Pesquisa de grupos aninhados

  Especifica se deseja ativar ou desativar a opção de pesquisa de grupo aninhado. Por predefinição, esta opção está desativada. Se você usar o ative Directory, poderá acelerar a autenticação desativando o suporte para grupos aninhados.

- Membro

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

- Classe Objeto Utilizador

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

- Classe Objeto Grupo

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

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

- Utilize a ligação segura

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

> Se pretender modificar o serviço de autenticação, certifique-se de que elimina quaisquer servidores de autenticação existentes e adiciona novos servidores de autenticação.

Área 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 remotos ou grupos são mantidas pelo servidor de autenticação.

- **Botões de comando**

  Permite adicionar, editar ou excluir servidores de autenticação.

  - Adicionar

    Permite adicionar um servidor de autenticação.

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

  - Editar

    Permite editar as definições de um servidor de autenticação selecionado.

  - Eliminar

    Exclui os servidores de autenticação selecionados.

- **Nome ou endereço IP**

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

- **Porto**

  Exibe o número da porta do servidor de autenticação.

- * Teste de Autenticação*

  Este botão valida a configuração do servidor de autenticação autenticando um usuário ou grupo remoto.

  Durante o teste, se você especificar apenas o nome de usuário, o servidor de gerenciamento pesquisará o usuário remoto no servidor de autenticação, mas não autenticará o usuário. Se especificar o nome de utilizador e a palavra-passe, o servidor de gestão procura e autentica o utilizador remoto.

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

Gerenciamento de certificados de segurança

Você pode configurar o HTTPS no servidor do Unified Manager para monitorar e gerenciar seus clusters em uma conexão segura.

Exibindo o certificado de segurança HTTPS

Você pode comparar os detalhes do certificado HTTPS com o certificado recuperado em

seu navegador para garantir que a conexão criptografada do navegador com o Unified Manager não esteja sendo intercetada.

Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

A exibição do certificado permite verificar o conteúdo de um certificado regenerado ou exibir nomes Alt de assunto (SAN) a partir dos quais você pode acessar o Unified Manager.

Passo

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

   O certificado HTTPS é exibido na parte superior da página

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

Transferir 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 a uma autoridade de certificação para assinar. Um certificado assinado pela CA ajuda a evitar ataques man-in-the-middle e fornece melhor proteção de segurança do que um certificado autoassinado.

Antes de começar

Tem de ter a função Administrador de aplicações.

Passos

1. No painel de navegação esquerdo, clique em **Geral** > **certificado HTTPS**.
2. Clique em **Download de solicitação de assinatura de certificado HTTPS**.
3. Salve o `<hostname>.csr` arquivo.

Você pode fornecer o arquivo a uma autoridade de certificação para assinar e, em seguida, instalar o certificado assinado.

Instalando um certificado HTTPS assinado e retornado pela CA

Você pode fazer o upload e instalar um certificado de segurança depois que uma Autoridade de certificação o tiver assinado e retornado. O arquivo que você carregar e instalar deve ser uma versão assinada do certificado autoassinado existente. Um certificado assinado pela CA ajuda a evitar ataques 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:

- Fez o download do arquivo de solicitação de assinatura de certificado e o assinou por uma Autoridade de Certificação

- Salva a cadeia de certificados no formato PEM
- Incluídos todos os certificados na cadeia, desde o certificado do servidor Unified Manager até o certificado de assinatura raiz, incluindo quaisquer certificados intermediários presentes

Tem de ter a função Administrador de aplicações.

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 **escolha arquivo…** para localizar o arquivo a ser carregado.
4. Selecione o arquivo e clique em **Instalar** para instalar o arquivo.

   Para obter informações, "Instalar um certificado HTTPS gerado usando ferramentas externas"consulte .

Exemplo de cadeia de certificados

O exemplo a seguir mostra como o arquivo de 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 que são autoassinados ou CA assinados e são 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 gerados externamente pelo par de chaves público-privadas. Os algoritmos de par 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 carregar deve estar no seguinte formato de entrada.

1. Chave privada do servidor que pertence ao host 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 usados para assinar o certificado acima

Formato para carregar um certificado com um par de chaves EC

As curvas permitidas são "prime256v1" e "ecp384r1". Amostra 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 pertencentes 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-----
```

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

Verifica durante o carregamento de certificados gerados externamente

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

- A chave privada na entrada é validada com base no certificado do host na entrada.
- O Nome Comum (CN) no certificado de host é verificado em relação ao FQDN do host.
- O Nome Comum (CN) do certificado de anfitrião não deve estar vazio ou em branco e não deve ser definido como localhost.
- A data de início da validade não deve ser futura e a data de validade do certificado não deve ser anterior.
- Se houver CA ou CA intermediária, a data de início de validade do certificado não deve ser no futuro e a data de 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): "O ActiveIQ Unified Manager não instala um certificado gerado externamente"

Descrições de páginas para gerenciamento de certificados

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

Página certificado HTTPS

A página certificado HTTPS permite exibir o certificado de segurança atual, fazer download de uma solicitação de assinatura de certificado, gerar um novo certificado HTTPS autoassinado ou instalar um novo certificado HTTPS.

Se não tiver gerado um novo certificado HTTPS auto-assinado, o certificado que aparece nesta página é o certificado que foi gerado durante a instalação.

Botões de comando

Os botões de comando permitem executar as seguintes operações:

- * Faça o download do pedido de assinatura de certificado HTTPS*

  Transfere uma solicitação de certificação para o certificado HTTPS atualmente instalado. O navegador solicita que você salve o arquivo <hostname>.csr para que você possa fornecer o arquivo a uma autoridade de certificação para assinar.

- **Instalar certificado HTTPS**

  Permite que você carregue e instale um certificado de segurança depois que uma autoridade de certificação o tiver assinado e devolvido. O novo certificado entra em vigor após reiniciar o servidor de gerenciamento.

- **Regenerate HTTPS Certificate**

  Permite gerar um novo certificado HTTPS autoassinado, que substitui o certificado de segurança atual. O novo certificado entrará em vigor após a reinicialização do Unified Manager.

Caixa de diálogo regenerar certificado HTTPS

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

As informações atuais do certificado são exibidas 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.

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

- **Email**

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

- **Empresa**

  Opcional. Normalmente, o nome incorporado da sua empresa.

- **Departamento**

  Opcional. O nome do departamento em sua empresa.

- **Cidade**

  Opcional. A localização da cidade da sua empresa.

- **Estado**

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

- **País**

  Opcional. A localização do país da sua empresa. Este é normalmente um código ISO de duas letras do país.

- **Nomes alternativos**

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

  Marque a caixa de seleção "'Excluir informações de identificação local (por exemplo, localhost)" se quiser remover as informações de identificação local do campo nomes alternativos no certificado. Quando esta caixa de verificação está selecionada, apenas o que introduzir no campo é utilizado no campo nomes alternativos. Quando deixado em branco, o certificado resultante não terá um campo de nomes alternativos.

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

  O algoritmo de chave é definido como RSA. Você pode selecionar um dos tamanhos de chave: 2048, 3072 ou 4096 bits. O tamanho da chave padrão é definido para 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 obter mais informações, "Gerando certificados HTTPS"consulte .

Informações sobre direitos autorais

Informações sobre marcas comerciais