Configurando o Active IQ Unified Manager

Active IQ Unified Manager 9.16

NetApp
November 19, 2024

Índice

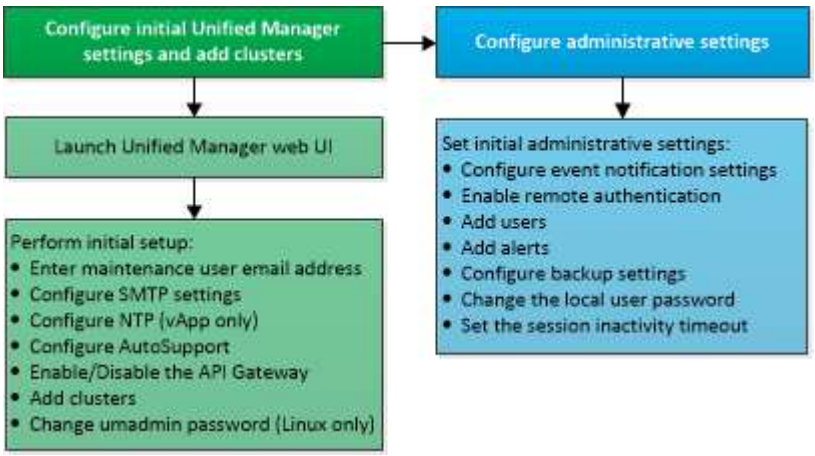
Configurando o Active IQ Unified Manager

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

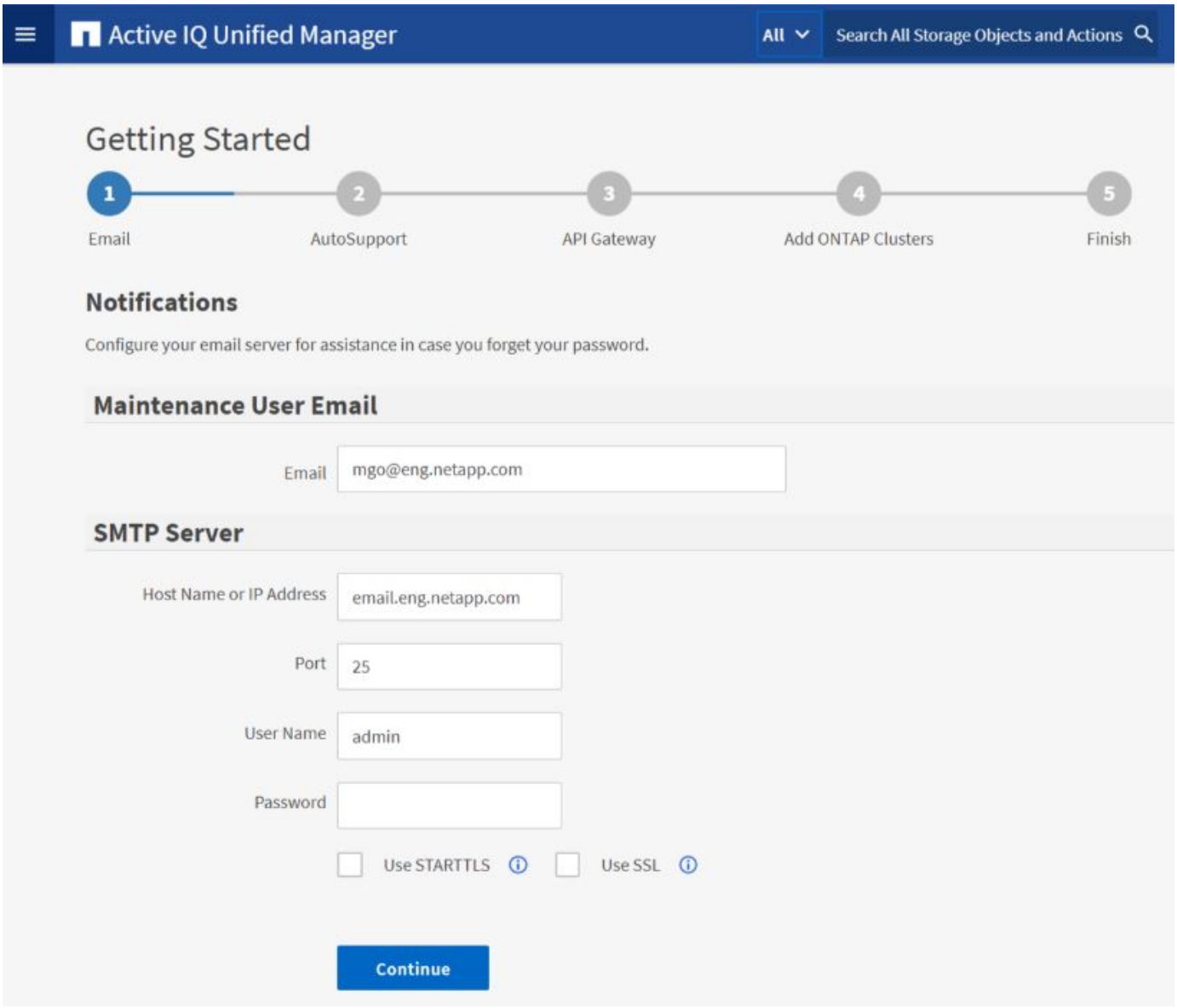
Para usar o Unified Manager, você deve primeiro configurar as opções de configuração inicial, incluindo o servidor NTP, o endereço de e-mail do usuário de manutenção, o host do servidor SMTP e a adição de clusters ONTAP.

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.

Informações sobre direitos autorais

Informações sobre marcas comerciais