Configurando o Unified Manager

OnCommand Unified Manager 9.5

NetApp
October 23, 2024

Índice

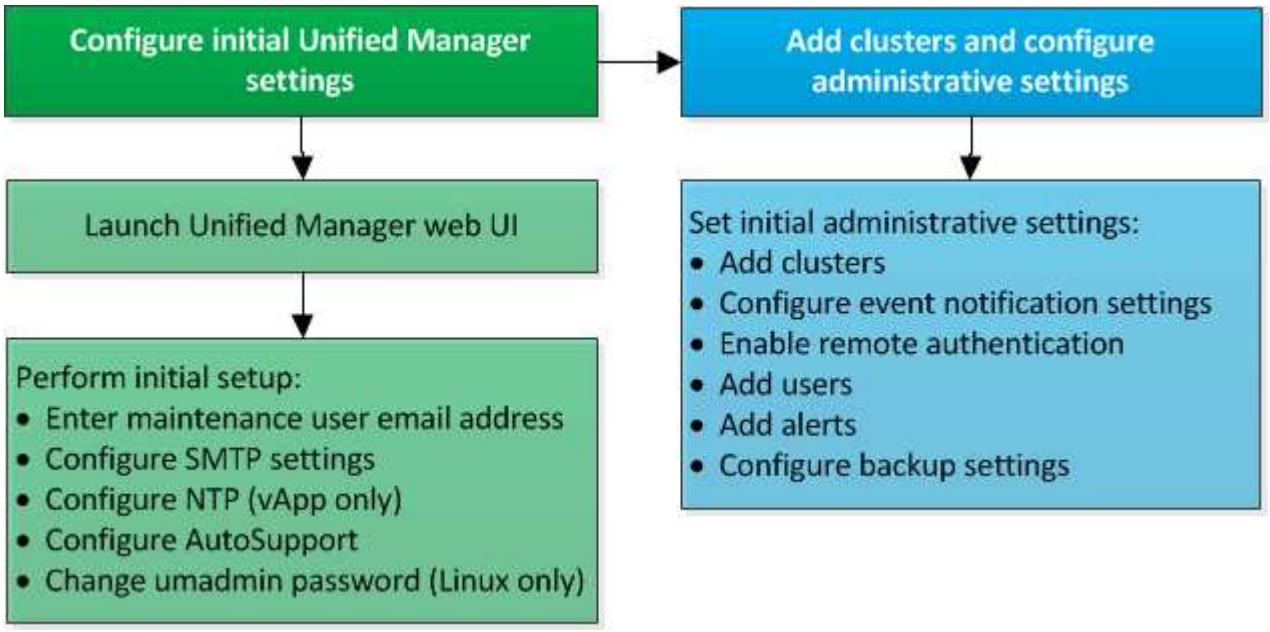
Configurando o Unified Manager

Depois de instalar o Unified Manager, 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.

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 e o nome e as opções do host do servidor SMTP.

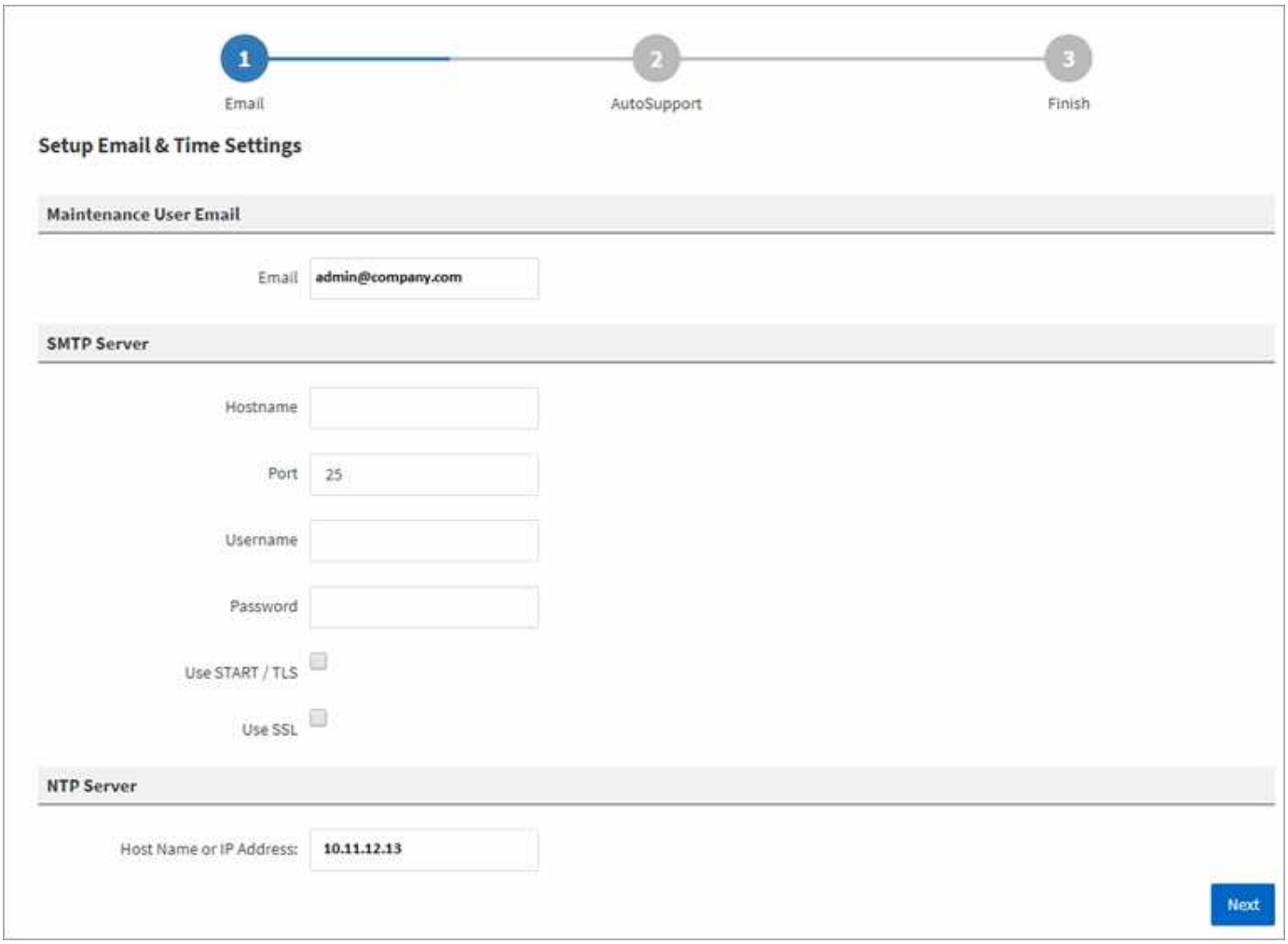
Antes de começar

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

Sobre esta tarefa

A página Configuração inicial do Gerenciador Unificado do OnCommand é exibida somente quando você acessa pela primeira vez a IU da Web. A página abaixo é de uma instalação na VMware.



Se você quiser alterar qualquer uma dessas opções posteriormente, use as opções Administração, que podem ser acessadas clicando no na barra de ferramentas do Unified Manager.

Passos

1. Na janela **Configuração inicial do Gerenciador Unificado do OnCommand**, 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 **seguinte**.
2. Na página **AutoSupport**, clique em **Concordo e continue** para ativar o AutoSupport.

   Se você precisar designar um proxy para fornecer acesso à Internet para enviar conteúdo do AutoSupport para suporte, ou se quiser desativar o AutoSupport, use as opções Administração.

3. Nos sistemas Red Hat e CentOS, você pode optar por alterar a senha do usuário umadmin da cadeia de carateres padrão "'admin'" para uma cadeia de carateres personalizada.

Resultados

A janela Configuração inicial é fechada e a IU da Web do Unified Manager é exibida. A página Configuration/Cluster Data Sources (fontes de dados de configuração/cluster) é exibida para que você possa adicionar clusters ao sistema.

Adição de clusters

É possível adicionar um cluster ao Gerenciador Unificado do OnCommand 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

- Você deve ter a função Administrador do OnCommand ou Administrador do armazenamento.
- Você deve ter as seguintes informações:
  - 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.

  - Nome de usuário e senha do administrador do Data ONTAP

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

  - Tipo de protocolo (HTTP ou HTTPS) que pode ser configurado no cluster e o número da porta usado para se conetar ao cluster

    Você pode adicionar clusters que estão por trás de um NAT/firewall usando o endereço IP NAT do Unified Manager. Qualquer sistema de automação do fluxo de trabalho conetado ou SnapProtect também deve estar atrás do NAT/firewall, e as chamadas da API SnapProtect devem usar o endereço IP NAT para identificar o cluster.

- O FQDN do Gerenciador Unificado deve ser capaz de fazer ping no sistema ONTAP.

  Você pode verificar isso usando o seguinte comando ONTAP: `ping -node node_name -destination Unified_Manager_FQDN`.

- 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.

Sobre esta tarefa

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

Você pode monitorar um único cluster por duas instâncias do Unified Manager desde que tenha configurado um segundo LIF de gerenciamento de cluster no cluster para que cada instância do Unified Manager se conete por meio de um LIF diferente.

Passos

1. No painel de navegação à esquerda, clique em **Configuração** > **fontes de dados do Cluster**.
2. Na página **Configuration/Cluster Data Sources** (fontes de dados de configuração/cluster), clique em **Add** (Adicionar).
3. Na caixa de diálogo **Adicionar cluster**, especifique os valores necessários, como o nome do host ou o endereço IP do cluster, nome de usuário, senha, protocolo de comunicação e número da porta.

   Por padrão, o protocolo HTTPS e a porta 443 são selecionados.

   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. Se o HTTPS estiver selecionado, execute as seguintes etapas:

   a. Na caixa de diálogo **autorizar Host**, clique em **Exibir certificado** para exibir as informações do certificado sobre o cluster.

   b. Clique em **Sim**.

      O Unified Manager verifica o certificado somente quando o cluster é adicionado inicialmente. O Unified Manager não verifica o certificado de cada chamada de API para o ONTAP.

   Se o certificado expirou, não é possível adicionar um novo cluster. Você deve primeiro renovar o certificado SSL e depois adicionar o cluster.

Resultados

Depois que todos os objetos de um novo cluster forem descobertos (cerca de 15 minutos), o Unified Manager começa a coletar dados históricos de desempenho dos 15 dias anteriores. Essas estatísticas são coletadas usando a funcionalidade de coleta de continuidade de dados. Esse recurso fornece 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 receber uma mensagem de erro que não pode adicionar o cluster, verifique se existem os seguintes problemas:

- Se os relógios nos dois sistemas não estiverem sincronizados e a data de início do certificado HTTPS do Unified Manager for posterior à data no cluster. Você deve garantir que os relógios são sincronizados usando NTP ou um serviço similar.
- Se o cluster tiver atingido o número máximo de destinos de notificação EMS, o endereço do Unified Manager não poderá ser adicionado. Por predefinição, apenas podem ser definidos 20 destinos de notificação EMS no cluster.

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 de Administrador do OnCommand.

Sobre esta tarefa

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
- Versão SNMP, endereço IP do host de destino de trap, porta de trap de saída e a comunidade para configurar a trap SNMP

Você deve ter a função Administrador do OnCommand ou Administrador do armazenamento.

Passos

1. Na barra de ferramentas, clique em  e, em seguida, clique em **notificações** no menu Configuração à esquerda.
2. Na página **Configuração/notificações**, configure as configurações apropriadas e clique em **Salvar**.

   Notas:

   - Se o Endereço de for preenchido com o endereço “OnCommand@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.

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 de Administrador do OnCommand.

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).

Sobre esta tarefa

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. Na barra de ferramentas, clique em e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.
2. Na página **Configuração/Autenticação**, selecione **Ativar autenticação remota**.
3. No campo **Authentication Service** (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. Adicione servidores de autenticação e teste a autenticação.
5. Clique em **Salvar e fechar**.

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 de Administrador do OnCommand.
- A desativação de grupos aninhados só é aplicável ao usar o ative Directory.

Sobre esta tarefa

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. Na barra de ferramentas, clique em e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.
2. Na página **Configuração/Autenticação**, marque a caixa **Desativar pesquisa de grupo aninhado**.
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 de Administrador do OnCommand.

Sobre esta tarefa

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. Na barra de ferramentas, clique em e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.
2. Na página **Configuração/Autenticação**, clique em **servidor de gerenciamento** > **Autenticação**.
3. Ative ou desative a opção **Use secure Connection Authentication**:

Se você quiser…	Então faça isso…
Ative-o.	a. Na caixa de verificação Ativar autenticação remota, selecione a opção **utilizar ligação 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.

Se você quiser…	Então faça isso…
Desative-o.	a. Na caixa de verificação Ativar autenticação remota, desmarque a opção **usar conexão segura**. b. Na área servidores de autenticação, clique em **Adicionar**. c. Na caixa de diálogo Adicionar servidor de autenticação, especifique o nome do host ou o endereço IP (IPv4 ou IPv6) do servidor e os detalhes da porta. d. Clique em **Add**.

O servidor de autenticação adicionado é exibido na área servidores.

4. 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 de Administrador do OnCommand.

Sobre esta tarefa

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. Na barra de ferramentas, clique em e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.
2. Na página **Configuração/Autenticação**, clique em **Autenticação de teste**.
3. Na caixa de diálogo **Test User**, especifique o nome de usuário e a senha do usuário remoto ou o nome de usuário do grupo remoto e clique em **Test**.

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

Adicionando usuários

Você pode adicionar usuários locais ou usuários de banco de dados usando a página Gerenciamento/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 de Administrador do OnCommand.
- 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.

Sobre esta tarefa

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. Na barra de ferramentas, clique em  e, em seguida, clique em **Users** (usuários) no menu Left Management (Gerenciamento à esquerda).
2. Na página **Gerenciamento/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**.

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 do 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.
- Para que um script seja executado com base no evento, você deve ter adicionado o script ao Unified Manager usando a página Gerenciamento/Scripts.
- Você deve ter a função Administrador do OnCommand ou Administrador do armazenamento.

Sobre esta tarefa

Você pode criar um alerta diretamente da página de detalhes do evento depois de receber um evento, além de criar um alerta da página Configuração/alertas, conforme descrito aqui.

Passos

1. No painel de navegação esquerdo, clique em **Configuration** > **Alerting**.
2. Na página **Configuração/alertas**, clique em **Adicionar**.
3. Na caixa de diálogo **Adicionar alerta**, clique em **Nome** e insira um nome e uma descrição para o alerta.
4. Clique em **recursos** e selecione os recursos 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 Gerenciamento/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 "ample@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:

1. Clique em **Nome** e insira `HealthTest` no campo **Nome** do alerta.
2. Clique em **recursos** e, na guia incluir, selecione **volumes** na lista suspensa.
   a. Digite `abc` o campo **Name contains** para exibir os volumes cujo nome contém "'abc'".
   b. Selecione * todos os volumes cujo nome contenha 'abc'>>* na área recursos disponíveis e mova-o para a área recursos selecionados.
   c. Clique em **Excluir**, digite `xyz` o 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 insira `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**.

Eventos EMS que são adicionados automaticamente ao Unified Manager

Ao usar o software Unified Manager 9,4 ou superior, os seguintes eventos do ONTAP EMS são adicionados automaticamente ao Unified Manager. Esses eventos serão gerados quando acionados em qualquer cluster que o Unified Manager esteja monitorando.

Os eventos EMS a seguir estão disponíveis ao monitorar clusters executando o software ONTAP 9.5 ou superior:

Nome do evento do Unified Manager	Nome do evento EMS	Recurso afetado	Gravidade do ONTAP
Acesso ao armazenamento de objetos negado para realocação agregada	arl.netra.ca.check.failed	Agregado	Erro
Acesso ao armazenamento de objetos negado para realocação de agregados durante o failover do storage	gb.netra.ca.check.failed	Agregado	Erro
Espaço FabricPool quase cheio	FabricPool.quase.full	Cluster	Erro
Período de carência do NVMe-of iniciado	nvmf.graceperiod.start	Cluster	Aviso
Período de carência NVMe-of Ativo	nvmf.graceperiod.active	Cluster	Aviso
O período de carência do NVMe-of expirou	nvmf.graceperiod.expired	Cluster	Aviso
LUN destruído	lun.destroy	LUN	Informações
Nuvem AWS MetaDataConnFail	Cloud.AWS.metadataConnFail	Nó	Erro
Cloud AWS IAMCredsExpired	Cloud.AWS.iamCredsExpired	Nó	Erro
Nuvem AWS IAMCredsInvalid	Cloud.AWS.iamCredsInvalid	Nó	Erro
Cloud AWS IAMCredsNotFound	Cloud.AWS.iamCredsNotFound	Nó	Erro
Cloud AWS IAMCredsNotInitialized	Cloud.AWS.iamNotInitialized	Nó	Informações
Nuvem AWS IAMRoleInvalid	Cloud.AWS.iamRoleInvalid	Nó	Erro

Nome do evento do Unified Manager	Nome do evento EMS	Recurso afetado	Gravidade do ONTAP
Nuvem AWS IAMRoleNotFound	Cloud.AWS.iamRoleNotFound	Nó	Erro
Objstore Host não resolvível	objstore.host.unresolvable	Nó	Erro
InterClusterLifDown	objstore.interclusterlifDown	Nó	Erro
Solicitar assinatura de armazenamento de objetos incompatível	osc.signatureMismatch	Nó	Erro
Uma das NFSv4 piscinas esgotada	Nblade.nfsV4PoolExhaust	Nó	Crítico
Memória do monitor QoS maximizada	qos.monitor.memory.maxed	Nó	Erro
Memória do monitor QoS interrompida	qos.monitor.memory.abated	Nó	Informações
NVMeNS Destroy	NVMeNS.destroy	Namespace	Informações
NVMeNS Online	NVMeNS.offline	Namespace	Informações
NVMeNS Offline	NVMeNS.online	Namespace	Informações
NVMeNS fora do espaço	NVMeNS.out.of.space	Namespace	Aviso
Replicação síncrona fora de sincronização	sms.status.out.of.sync	Relação de SnapMirror	Aviso
Replicação síncrona restaurada	sms.status.in.sync	Relação de SnapMirror	Informações
Falha na ressincronização automática de replicação síncrona	sms.resync.tentativa.falhou	Relação de SnapMirror	Erro
Muitas conexões CIFS	Nblade.cifsManyAuths	SVM	Erro
Conexão CIFS máx. Excedida	Nblade.cifsMaxOpenSameFile	SVM	Erro

Nome do evento do Unified Manager	Nome do evento EMS	Recurso afetado	Gravidade do ONTAP
Número máximo de ligação CIFS por utilizador excedido	Nblade.cifsMaxSessPerUsrConn	SVM	Erro
Conflito de nomes NetBIOS CIFS	Nblade.cifsNbNameConflict	SVM	Erro
Tentativas de conetar compartilhamento CIFS inexistente	Nblade.cifsNoPrivShare	SVM	Crítico
Falha na operação de cópia sombra CIFS	cifs.shadowcopy.failure	SVM	Erro
Vírus encontrado por AV Server	Nblade.vscanVirusDetected	SVM	Erro
Nenhuma conexão do servidor AV para verificação de vírus	Nblade.vscanNoScannerConn	SVM	Crítico
Nenhum servidor AV registado	Nblade.vscanNoRegdScanner	SVM	Erro
Nenhuma conexão responsiva do servidor AV	Nblade.vscanConnInactive	SVM	Informações
Servidor AV demasiado ocupado para aceitar novo pedido de digitalização	Nblade.vscanConnBackPressure	SVM	Erro
Tentativa de usuário não autorizado para o servidor AV	Nblade.vscanBadUserPrivAccess	SVM	Erro
Os constituintes do FlexGroup têm problemas de espaço	FlexGroup.constituintes.have.space.issues	Volume	Erro
Estado do espaço dos constituintes do FlexGroup tudo OK	FlexGroup.constituintes.space.status.all.ok	Volume	Informações

Nome do evento do Unified Manager	Nome do evento EMS	Recurso afetado	Gravidade do ONTAP
Os constituintes do FlexGroup têm problemas inodes	FlexGroup.constituents.have.inodes.issues	Volume	Erro
FlexGroup constituintes inodes Status tudo OK	FlexGroup.constituents.inodes.status.all.ok	Volume	Informações
Volume Logical Space quase cheio	Monitor.vol.nearFull	Volume	Aviso
Volume espaço lógico cheio	monitor.vol.full	Volume	Erro
Volume lógico espaço normal	monitor.vol.one.ok	Volume	Informações
Falha na seleção automática do volume do WAFL	WAFL.vol.autoSize.fail	Volume	Erro
WAFL volume AutoSize Done (tamanho automático do volume)	WAFL.vol.autoSize.done	Volume	Informações

Subscrever eventos ONTAP EMS

Você pode se inscrever para receber eventos do sistema de Gerenciamento de Eventos (EMS) gerados por sistemas instalados com o software ONTAP. Um subconjunto de eventos EMS é relatado automaticamente ao Unified Manager, mas eventos EMS adicionais são relatados somente se você se inscreveu nesses eventos.

Antes de começar

Não assine eventos EMS que já foram adicionados ao Unified Manager automaticamente, pois isso pode causar confusão ao receber dois eventos para o mesmo problema.

Sobre esta tarefa

Você pode se inscrever em qualquer número de eventos EMS. Todos os eventos aos quais você se inscreve são validados e somente os eventos validados são aplicados aos clusters que você está monitorando no Unified Manager. O *Catálogo de Eventos do ONTAP 9 EMS* fornece informações detalhadas para todas as mensagens do EMS para a versão especificada do software ONTAP 9. Localize a versão apropriada do Catálogo de Eventos *EMS* na página Documentação do produto da ONTAP 9 para obter uma lista dos eventos aplicáveis.

"Biblioteca de produtos ONTAP 9"

Você pode configurar alertas para os eventos do ONTAP EMS aos quais você se inscreve e criar scripts personalizados para serem executados para esses eventos.

Se você não receber os eventos do ONTAP EMS aos quais você se inscreveu, pode haver um problema com a configuração DNS do cluster que está impedindo que o cluster chegue ao servidor do Unified Manager. Para resolver esse problema, o administrador do cluster deve corrigir a configuração DNS do cluster e reiniciar o Unified Manager. Isso irá liberar os eventos EMS pendentes para o servidor do Unified Manager.

Passos

1. No painel de navegação esquerdo, clique em **Configuração** > **Gerenciar eventos**.
2. Na página **Configuração/gerir eventos**, clique no botão **Subscrever a eventos EMS**.
3. Na caixa de diálogo **Inscrever-se para eventos EMS**, insira o nome do evento ONTAP EMS ao qual deseja se inscrever.

   Para ver os nomes dos eventos EMS aos quais você pode assinar, a partir do shell do cluster ONTAP, você pode usar o `event route show` comando (antes do ONTAP 9) ou o `event catalog show` comando (ONTAP 9 ou posterior).

   "Como configurar assinaturas de eventos do ONTAP EMS no Gerenciador Unificado / Active IQ Unified Manager da OnCommand"

4. Clique em **Add**.

   O evento EMS é adicionado à lista de eventos EMS subscritos, mas a coluna aplicável ao cluster exibe o status como ""desconhecido"" para o evento EMS que você adicionou.

5. Clique em **Salvar e fechar** para Registrar a assinatura do evento EMS no cluster.
6. Clique em **Inscrever-se para eventos EMS** novamente.

   O status "'Sim'" aparece na coluna aplicável ao cluster para o evento EMS que você adicionou.

   Se o status não for "Sim", verifique a ortografia do nome do evento ONTAP EMS. Se o nome for inserido incorretamente, você deve remover o evento incorreto e adicionar o evento novamente.

Depois de terminar

Quando o evento EMS do ONTAP ocorre, o evento é exibido na página Eventos. Pode selecionar o evento para ver detalhes sobre o evento EMS na página de detalhes do evento. Você também pode gerenciar a disposição do evento ou criar alertas para o evento.

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 ao usar o Internet Explorer. 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:

http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/

- 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.
- Quando os usuários tentam acessar o Unified Manager usando o Internet Explorer, eles podem ver a mensagem **o site não pode exibir a página**. Se isso ocorrer, certifique-se de que esses usuários desmarque a opção "Mostrar mensagens de erro HTTP amigáveis" em **Ferramentas** > **Opções da Internet** > **Avançado**.

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 OnCommand.
- 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.

Sobre esta tarefa

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. Na barra de ferramentas, clique em e, em seguida, clique em **Autenticação** no menu Configuração à esquerda.

2. Na página **Configuração/Autenticação**, selecione a guia **Autenticação SAML**.
3. Marque a caixa de seleção **Enable SAML Authentication** (Ativar autenticação SAML*).

   São apresentados os campos necessários para configurar a ligação IDP.

4. 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.

5. 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.

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.

Resultados

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.

Depois de terminar

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. Quando o Unified Manager é implantado no Windows, Red Hat ou CentOS, é possível alterar o tempo limite da sessão da GUI usando o seguinte comando da CLI do Unified Manager: `um option set absolute.session.timeout=00:15:00`Este comando define o tempo limite da sessão da GUI do Unified Manager para 15 minutos.

Configurar definições de cópia de segurança da base de dados

Você pode configurar as configurações de backup do banco de dados do Unified Manager para definir o caminho do backup do banco de dados, a contagem de retenção e as programações de backup. Você pode ativar backups programados diários ou semanais. Por padrão, backups programados são desativados.

Antes de começar

- Você deve ter a função Operador, Administrador OnCommand ou Administrador de armazenamento.
- Você deve ter um mínimo de 150 GB de espaço disponível no local que você definir como caminho de backup.

  É recomendável usar um local remoto externo ao sistema host do Unified Manager.

- Quando o Unified Manager estiver instalado em um sistema Linux, verifique se o usuário "jboss" tem permissões de gravação no diretório de backup.
- Você não deve agendar operações de backup para que ocorram imediatamente após a adição de um novo cluster enquanto o Unified Manager estiver coletando 15 dias de dados históricos de desempenho.

Sobre esta tarefa

Mais tempo é necessário na primeira vez que um backup é executado do que para backups subsequentes, porque o primeiro backup é um backup completo. Um backup completo pode ter mais de 1 GB e pode levar de três a quatro horas. Backups subsequentes são incrementais e exigem menos tempo.

Passos

1. Na barra de ferramentas, clique em  e, em seguida, clique em **Gestão** > **cópia de segurança da base de dados**.
2. Na página **Backup de gerenciamento/banco de dados**, clique em **ações** > **Configurações de backup de banco de dados**.
3. Configure os valores apropriados para um caminho de backup e contagem de retenção.

   O valor padrão para a contagem de retenção é 10; você pode usar 0 para criar backups ilimitados.

4. Na seção **frequência de programação**, marque a caixa de seleção **Ativar** e especifique um horário diário ou semanal.
   - **Diária**

     Se selecionar esta opção, tem de introduzir uma hora no formato de 24 horas para criar a cópia de segurança. Por exemplo, se você especificar 18:30, um backup será criado diariamente às 6:30:00.

   - **Semanal**

     Se selecionar esta opção, tem de especificar a hora e o dia para a criação da cópia de segurança. Por exemplo, se você especificar o dia como segunda-feira e hora como 16:30, um backup semanal será criado todas as segundas-feiras às 4:30:00.

5. Clique em **Salvar e fechar**.

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.

Sobre esta tarefa

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 **Change Password** (alterar palavra-passe), introduza a palavra-passe atual e a nova palavra-passe.
4. Clique em **Salvar**.

Depois de terminar

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.

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 ou CentOS 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 do OnCommand atribuída a você para executar essas tarefas.

Sobre esta tarefa

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 "'OnCommand'" 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

Você pode gerar um novo certificado de segurança HTTPS por vários motivos, incluindo se deseja assinar com uma autoridade de certificação diferente ou se o certificado de segurança atual expirou. O novo certificado substitui o certificado existente.

Antes de começar

Tem de ter a função de Administrador do OnCommand.

Sobre esta tarefa

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.

Passos

1. Na barra de ferramentas, clique em  e, em seguida, clique em **certificado HTTPS** no menu **Configuração**.
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**.
Gerar o certificado usando valores diferentes	`Click the *Update the Current Certificate Attributes* option. Os campos Nome Comum e nomes alternativos usarão os valores do certificado existente se você não inserir novos valores. Os outros campos não requerem valores, mas você pode inserir valores, por exemplo, para a Cidade, Estado e país, se quiser que esses valores sejam preenchidos no certificado.` 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. E

4. Clique em **Yes** para regenerar o certificado.
5. Reinicie o servidor do Unified Manager para que o novo certificado entre em vigor.

Depois de terminar

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.

Sobre esta tarefa

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, é possível alterar o nome do host da máquina Red Hat Enterprise Linux ou CentOS 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.

Sobre esta tarefa

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 os seguintes comandos na ordem mostrada:

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: `service network restart`
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 inserindo os seguintes comandos na ordem mostrada:

Informações sobre direitos autorais

Informações sobre marcas comerciais