Configurar o OnCommand Workflow Automation

OnCommand Workflow Automation 5.1

NetApp
October 22, 2024

Índice

Configurar o OnCommand Workflow Automation

Depois de concluir a instalação do OnCommand Workflow Automation (WFA), você deve concluir várias configurações. Você tem que acessar O WFA, configurar usuários, configurar fontes de dados, configurar credenciais e configurar O WFA.

Acesse o OnCommand Workflow Automation

Você pode acessar o OnCommand Workflow Automation (WFA) através de um navegador da Web a partir de qualquer sistema que tenha acesso ao servidor WFA.

Você deve ter instalado o Adobe Flash Player para o seu navegador.

Passos

1. Abra um navegador da Web e insira um dos seguintes na barra de endereços:
   - `https://wfa_server_ip`

     wfa_Server_ip é o endereço IP (endereço IPv4 ou IPv6) ou o nome de domínio totalmente qualificado (FQDN) do servidor WFA.

   - Se você estiver acessando O WFA no servidor WFA: `https://localhost/wfa` Se você tiver especificado uma porta não padrão para O WFA, você deve incluir o número da porta da seguinte forma:
   - `https://wfa_server_ip:port`
   - `https://localhost:port` Port é o número da porta TCP que você usou para o servidor WFA durante a instalação.
2. Na seção entrar, insira as credenciais do usuário administrativo que você inseriu durante a instalação.
3. No menu **Settings** > **Setup**, configure as credenciais e uma fonte de dados.
4. Marque a GUI da Web DO WFA para facilitar o acesso.

Fontes de dados do OnCommand Workflow Automation

A OnCommand Workflow Automation (WFA) opera com dados adquiridos a partir de fontes de dados. Várias versões do Active IQ Unified Manager e do VMware vCenter Server são fornecidas como tipos de fonte de dados predefinidos DO WFA. Você deve estar ciente dos tipos de fonte de dados predefinidos antes de configurar as fontes de dados para aquisição de dados.

Uma fonte de dados é uma estrutura de dados somente leitura que serve como uma conexão com o objeto fonte de dados de um tipo específico de fonte de dados. Por exemplo, uma fonte de dados pode ser uma conexão com um banco de dados Active IQ Unified Manager de um tipo de fonte de dados Active IQ Unified Manager 6,3. Você pode adicionar uma fonte de dados personalizada ao WFA depois de definir o tipo de fonte de dados necessário.

Para obter mais informações sobre os tipos de fonte de dados predefinidos, consulte a Matriz de interoperabilidade.

Informações relacionadas

"Ferramenta de Matriz de interoperabilidade do NetApp"

Configurando um usuário de banco de dados no DataFabric Manager

Você deve criar um usuário de banco de dados no Gerenciador DataFabric 5.x para configurar o acesso somente leitura do banco de dados do Gerenciador DataFabric 5.x ao OnCommand Workflow Automation.

Configure um usuário de banco de dados executando o ocsetup no Windows

Você pode executar o arquivo ocsetup no servidor DataFabric Manager 5.x para configurar o acesso somente leitura do banco de dados DataFabric Manager 5.x ao OnCommand Workflow Automation.

Passos

1. Faça o download do arquivo wfa_ocsetup.exe para um diretório no servidor DataFabric Manager 5.x do seguinte local: *Https*://WFA_Server_IP/download/WFA_ocsetup.exe.

   WFA_Server_IP é o endereço IP (endereço IPv4 ou IPv6) do seu SERVIDOR WFA.

   Se você tiver especificado uma porta não padrão para O WFA, você deve incluir o número da porta da seguinte forma: *Https*://wfa_Server_ip:port/download/wfa_ocsetup.exe.

   Port é o número da porta TCP que você usou para o servidor WFA durante a instalação.

   Se você estiver especificando um endereço IPv6, você deve incluí-lo com colchetes.

2. Clique duas vezes no arquivo wfa_ocsetup.exe.
3. Leia as informações no assistente de configuração e clique em **Next**.
4. Navegue ou digite o local do OpenJDK e clique em **Next**.
5. Introduza um nome de utilizador e uma palavra-passe para substituir as credenciais predefinidas.

   Uma nova conta de usuário de banco de dados é criada com acesso ao banco de dados DataFabric Manager 5.x.

   Se você não criar uma conta de usuário, as credenciais padrão serão usadas. Você deve criar uma conta de usuário para fins de segurança.

6. Clique em **seguinte** e reveja os resultados.
7. Clique em **Next** e, em seguida, clique em **Finish** para concluir o assistente.

Configure um usuário de banco de dados executando o ocsetup no Linux

Você pode executar o arquivo ocsetup no servidor DataFabric Manager 5.x para configurar o acesso somente leitura do banco de dados DataFabric Manager 5.x ao OnCommand Workflow Automation.

Passos

1. Faça o download do arquivo wfa_ocsetup.sh para seu diretório inicial no servidor DataFabric Manager 5.x usando o seguinte comando no terminal:

   `wget https://WFA_Server_IP/download/wfa_ocsetup.sh`

   WFA_Server_IP é o endereço IP (endereço IPv4 ou IPv6) do seu servidor WFA.

   Se você tiver especificado uma porta não padrão para O WFA, você deve incluir o número da porta da seguinte forma:

   `wget https://wfa_server_ip:port/download/wfa_ocsetup.sh`

   Port é o número da porta TCP que você usou para o servidor WFA durante a instalação.

   Se você estiver especificando um endereço IPv6, você deve incluí-lo com colchetes.

2. Use o seguinte comando no terminal para alterar o arquivo wfa_ocsetup.sh para um executável: `chmod +x wfa_ocsetup.sh`
3. Execute o script inserindo o seguinte no terminal:

   `./wfa_ocsetup.sh OpenJDK_path`

   OpenJDK_PATH é o caminho para o OpenJDK.

   /Opt/NTAPdfm/java

   A seguinte saída é exibida no terminal, indicando uma configuração bem-sucedida:

```
Verifying archive integrity... All good.
Uncompressing WFA OnCommand Setup.....
*** Welcome to OnCommand Setup Utility for Linux ***
    <Help information>
*** Please override the default credentials below ***
Override DB Username [wfa] :
```

4. Introduza um nome de utilizador e uma palavra-passe para substituir as credenciais predefinidas.

   Uma nova conta de usuário de banco de dados é criada com acesso ao banco de dados DataFabric Manager 5.x.

   > Se você não criar uma conta de usuário, as credenciais padrão serão usadas. Você deve criar uma conta de usuário para fins de segurança.

   A seguinte saída é exibida no terminal, indicando uma configuração bem-sucedida:

```
***** Start of response from the database *****
>>> Connecting to database
<<< Connected
*** Dropped existing 'wfa' user
=== Created user 'username'
>>> Granting access
<<< Granted access
***** End of response from the database *****
***** End of Setup *****
```

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

Você deve criar um usuário de banco de dados no Active IQ Unified Manager para configurar o acesso somente leitura do banco de dados do Active IQ Unified Manager para o OnCommand Workflow Automation.

Passos

1. Faça login no Active IQ Unified Manager com credenciais de administrador.
2. Clique em **Configurações** > **usuários**.
3. Clique em **Adicionar um novo usuário**.
4. Selecione **Database User** como o tipo de usuário.

   O mesmo usuário deve ser usado no OnCommand Workflow Automation ao adicionar o Active IQ Unified Manager como uma fonte de dados no OnCommand Workflow Automation.

Configure uma fonte de dados

Você deve configurar uma conexão com uma fonte de dados no OnCommand Workflow Automation (WFA) para adquirir dados da fonte de dados.

- Para o Active IQ Unified Manager 6,0 e posterior, você deve ter criado uma conta de usuário de banco de dados no servidor do Gerenciador Unificado.

  Consulte a Ajuda on-line do *OnCommand Unified Manager* para obter detalhes.

- A porta TCP para conexões de entrada no servidor do Unified Manager deve estar aberta.

  Consulte a documentação no firewall para obter detalhes.

  Os seguintes são os números de porta TCP padrão:

Número da porta TCP	Versão do servidor Unified Manager	Descrição
3306	6.x	Servidor de banco de dados MySQL

- Para o Consultor de desempenho, você deve ter criado uma conta de usuário do Active IQ Unified Manager com uma função mínima de GlobalRead.

  Consulte a Ajuda on-line do *OnCommand Unified Manager* para obter detalhes.

- Para o VMware vCenter Server, você deve ter criado uma conta de usuário no vCenter Server.

  Consulte a documentação do VMware vCenter Server para obter detalhes.

  Você deve ter instalado o VMware PowerCLI. Se você quiser executar fluxos de trabalho apenas em fontes de dados do vCenter Server, não é necessário configurar o servidor do Unified Manager como fonte de dados.

- A porta TCP para conexões de entrada no VMware vCenter Server deve estar aberta.

  O número da porta TCP padrão é 443. Consulte a documentação no firewall para obter detalhes.

Você pode adicionar várias fontes de dados de servidor do Unified Manager ao WFA usando este procedimento. No entanto, você não deve usar este procedimento se quiser emparelhar o servidor Unified Manager 6,3 e posterior com O WFA e usar a funcionalidade de proteção no servidor Unified Manager.

Para obter mais informações sobre como emparelhar O WFA com o servidor do Unified Manager 6.x, consulte a Ajuda on-line do *OnCommand Unified Manager*.

Ao configurar uma fonte de dados com O WFA, você deve estar ciente de que os tipos de fonte de dados do Active IQ Unified Manager 6,0, 6,1 e 6,2 estão obsoletos na versão DO WFA 4,0, e esses tipos de fonte de dados não serão suportados em versões futuras.

Passos

1. Acesse O WFA usando um navegador da Web.
2. Clique em **Configurações** e, em **Configuração**, clique em **fontes de dados**.
3. Escolha a ação apropriada:

Para…	**Faça isso…**
Crie uma nova fonte de dados	Clique na barra de ferramentas.
Edite uma fonte de dados restaurada se você atualizou O WFA	Selecione a entrada de origem de dados existente e clique na barra de ferramentas.

   Se você adicionou uma fonte de dados do servidor Unified Manager ao WFA e atualizou a versão do servidor Unified Manager, O WFA não reconhecerá a versão atualizada do servidor Unified Manager. Você deve excluir a versão anterior do servidor do Unified Manager e adicionar a versão atualizada do servidor do Unified Manager ao WFA.

4. Na caixa de diálogo Nova fonte de dados, selecione o tipo de fonte de dados necessária e insira um nome para a fonte de dados e o nome do host.

   Com base no tipo de fonte de dados selecionado, os campos porta, nome de usuário, senha e tempo limite podem ser preenchidos automaticamente com os dados padrão, se disponíveis. Você pode editar essas entradas conforme necessário.

5. Escolha uma ação apropriada:

Para…	Faça isso…
Active IQ Unified Manager 6,3 e posterior	Insira as credenciais da conta de usuário do banco de dados que você criou no servidor do Unified Manager. Consulte *Ajuda on-line do Gerenciador Unificado do OnCommand* para obter detalhes sobre como criar uma conta de usuário de banco de dados. Você não deve fornecer as credenciais de uma conta de usuário de banco de dados do Active IQ Unified Manager que foi criada usando a interface de linha de comando ou a ferramenta ocsetup.
VMware vCenter Server (somente para Windows)	(Apenas para Windows) Introduza o nome de utilizador e a palavra-passe do utilizador que criou no servidor VMware vCenter.

6. Clique em **Salvar**.
7. Na tabela fontes de dados, selecione a fonte de dados e clique na barra de ferramentas.
8. Verifique o estado do processo de aquisição de dados.

Adicione um servidor Unified Manager atualizado como uma fonte de dados

Se o servidor do Unified Manager (5.x ou 6.x) for adicionado como fonte de dados ao WFA e o servidor do Unified Manager for atualizado, você deverá adicionar o servidor do Unified Manager atualizado como fonte de dados porque os dados associados à versão atualizada não serão preenchidos NO WFA a menos que sejam adicionados manualmente como fonte de dados.

Passos

1. Faça login na GUI da Web DO WFA como administrador.
2. Clique em **Configurações** e em **Configuração**, clique em **fontes de dados**.
3. Clique na barra de ferramentas.
4. Na caixa de diálogo Nova fonte de dados, selecione o tipo de fonte de dados necessária e, em seguida, insira um nome para a fonte de dados e o nome do host.

   Com base no tipo de fonte de dados selecionado, os campos porta, nome de usuário, senha e tempo limite podem ser preenchidos automaticamente com os dados padrão, se disponíveis. Você pode editar essas entradas conforme necessário.

5. Clique em **Salvar**.
6. Selecione a versão anterior do servidor do Unified Manager e clique na barra de ferramentas.
7. Na caixa de diálogo Excluir tipo de fonte de dados, clique em **Sim**.

8. Na tabela fontes de dados, selecione a fonte de dados e, em seguida, clique na barra de ferramentas.
9. Verifique o estado da aquisição de dados na tabela Histórico.

Crie usuários locais

O OnCommand Workflow Automation (WFA) permite criar e gerenciar usuários locais DO WFA com permissões específicas para várias funções, como convidado, operador, aprovador, arquiteto, administrador e backup.

Você deve ter instalado O WFA e logado como administrador.

O WFA permite que você crie usuários para as seguintes funções:

- **Hóspede**

  Esse usuário pode visualizar o portal e o status de uma execução de fluxo de trabalho e pode ser notificado de uma alteração no status de uma execução de fluxo de trabalho.

- **Operador**

  Este usuário tem permissão para visualizar e executar fluxos de trabalho para os quais o usuário tem acesso.

- **Aprovador**

  Esse usuário tem permissão para visualizar, executar, aprovar e rejeitar fluxos de trabalho para os quais o usuário recebe acesso.

  Recomenda-se fornecer o ID de e-mail do aprovador. Se houver vários aprovadores, você poderá fornecer um ID de e-mail do grupo no campo **e-mail**.

- **Arquiteto**

  Esse usuário tem acesso total para criar fluxos de trabalho, mas está impedido de modificar as configurações globais do SERVIDOR WFA.

- **Admin**

  Este utilizador tem acesso completo ao servidor WFA.

- **Backup**

  Este é o único usuário que pode gerar remotamente backups do SERVIDOR WFA. No entanto, o usuário está restrito a todos os outros acessos.

Passos

1. Clique em **Configurações** e, em **Gerenciamento**, clique em **usuários**.
2. Crie um novo usuário clicando na barra de ferramentas.
3. Introduza as informações necessárias na caixa de diálogo novo utilizador.
4. Clique em **Salvar**.

Configure as credenciais de um sistema de destino

Você pode configurar as credenciais de um sistema de destino no OnCommand Workflow Automation (WFA) e usar as credenciais para se conetar a esse sistema específico e executar comandos.

Após a aquisição de dados inicial, você deve configurar as credenciais para os arrays em que os comandos são executados. A conexão do controlador DO PowerShell WFA funciona em dois modos:

- Com credenciais

  O WFA tenta estabelecer uma conexão usando HTTPS primeiro e, em seguida, tenta usar HTTP. Você também pode usar a autenticação LDAP do Microsoft ative Directory para se conetar a arrays sem definir credenciais no WFA. Para usar o LDAP do ative Directory, você deve configurar o array para executar a autenticação com o mesmo servidor LDAP do ative Directory.

- Sem credenciais (para sistemas de storage operando no modo 7)

  O WFA tenta estabelecer uma conexão usando autenticação de domínio. Este modo utiliza o protocolo de chamada de procedimento remoto, que é protegido através do protocolo NTLM.

- O WFA verifica o certificado SSL (Secure Sockets Layer) para sistemas ONTAP. Os usuários podem ser solicitados a analisar e aceitar/negar a conexão com sistemas ONTAP se o certificado SSL não for confiável.
- Você deve reinserir as credenciais do ONTAP, NetApp Active IQ e LDAP (Lightweight Directory Access Protocol) depois de restaurar um backup ou concluir uma atualização no local.

Passos

1. Faça login NO WFA através de um navegador da Web como administrador.
2. Clique em **Configurações** e, em **Configuração**, clique em **credenciais**.
3. Clique na barra de ferramentas.
4. Na caixa de diálogo novas credenciais, selecione uma das seguintes opções na lista **Match**:
   - **Exato**

     Credenciais para um endereço IP específico ou nome de host

   - **Padrão**

     Credenciais para toda a sub-rede ou intervalo IP

   O uso de sintaxe de expressão regular não é suportado para esta opção.

5. Selecione o tipo de sistema remoto na lista **tipo**.
6. Digite o nome do host ou o endereço IPv4 ou IPv6 do recurso, o nome de usuário e a senha.

   O WFA 5,1 verifica os certificados SSL de todos os recursos adicionados ao WFA. Como a verificação de certificado pode solicitar que você aceite os certificados, o uso de curingas em credenciais não é suportado. Se você tiver vários clusters usando as mesmas credenciais, não poderá adicioná-los todos de uma só vez.

7. Teste a conetividade executando a seguinte ação:

Se você selecionou o seguinte tipo de correspondência…	Então…
Exato	Clique em **Teste**.
Padrão	Salve as credenciais e escolha uma das seguintes opções: • Selecione a credencial e clique na barra de ferramentas. • Clique com o botão direito do rato e selecione **testar conetividade**.

8. Clique em **Salvar**.

Configurando o OnCommand Workflow Automation

O OnCommand Workflow Automation (WFA) permite que você configure várias configurações - por exemplo, AutoSupport e notificações.

Ao configurar O WFA, você pode configurar uma ou mais das seguintes opções, conforme necessário:

- AutoSupport para enviar mensagens AutoSupport para suporte técnico
- Servidor LDAP (Lightweight Directory Access Protocol) do Microsoft ative Directory para autenticação LDAP e autorização para usuários WFA
- E-mail para notificações por e-mail sobre operações de fluxo de trabalho e envio de mensagens AutoSupport
- SNMP (Simple Network Management Protocol) para notificações sobre operações de fluxo de trabalho
- Syslog para registo de dados remoto

Configurar o AutoSupport

Você pode configurar várias configurações do AutoSupport, como a programação, o conteúdo das mensagens do AutoSupport e o servidor proxy. O AutoSupport envia logs semanais do conteúdo que você selecionou para o suporte técnico para arquivamento e análise de problemas.

Passos

1. Faça login NO WFA através de um navegador da Web como administrador.
2. Clique em **Configurações** e, em **Configuração**, clique em **AutoSupport**.
3. Certifique-se de que a caixa **Enable AutoSupport** está selecionada.
4. Introduza as informações necessárias.
5. Selecione uma das seguintes opções na lista **Content**:

Se você quiser incluir…	Em seguida, escolha esta opção…
Apenas detalhes de configuração, como usuários, fluxos de trabalho e comandos de sua instalação DO WFA	`send only configuration data`
Detalhes de configuração DO WFA e dados em tabelas de cache DO WFA, como o esquema	`send configuration and cache data` (predefinição)
Detalhes de configuração DO WFA, dados em tabelas de cache DO WFA e dados no diretório de instalação	`send configuration and cache extended data`

A senha de qualquer usuário DO WFA é *não* incluída nos dados do AutoSupport.

6. Teste se você pode baixar uma mensagem do AutoSupport:
   a. Clique em **Download**.
   b. Na caixa de diálogo que se abre, selecione o local para guardar o ficheiro .7z.
7. Teste o envio de uma mensagem AutoSupport para o destino especificado clicando em **Enviar agora**.
8. Clique em **Salvar**.

Configure as definições de autenticação

Você pode configurar o OnCommand Workflow Automation (WFA) para usar um servidor LDAP (Lightweight Directory Access Protocol) do Microsoft ative Directory (AD) para autenticação e autorização.

Você deve ter configurado um servidor LDAP do Microsoft AD em seu ambiente.

Apenas a autenticação LDAP do Microsoft AD é suportada para O WFA. Você não pode usar outros métodos de autenticação LDAP, incluindo o Microsoft AD Lightweight Directory Services (AD LDS) ou o Catálogo Global da Microsoft.

Durante a comunicação, o LDAP envia o nome de utilizador e a palavra-passe em texto simples. No entanto, a comunicação LDAPS (LDAP Secure) é criptografada e segura.

Passos

1. Faça login NO WFA através de um navegador da Web como administrador.
2. Clique em **Configurações** e, em **Configuração**, clique em **Autenticação**.
3. Marque a caixa de seleção **Ativar ative Directory** .
4. Introduza as informações necessárias nos campos:
   a. Se você quiser usar o formato de domínio para usuários de domínio, substitua sAMAccountName por userPrincipalName no campo **User name attribute**.
   b. Se forem necessários valores exclusivos para o seu ambiente, edite os campos obrigatórios.
   c. Introduza o URI do servidor AD da seguinte forma:

`ldap://active_directory_server_address\[:port\]`

LDAP://NB-T01.example.com[:389]

Se tiver ativado o LDAP sobre SSL, pode utilizar o seguinte formato URI: `ldaps://active_directory_server_address\[:port\]`

a. Adicione uma lista de nomes de grupos AD as funções necessárias.

Você pode adicionar uma lista de nomes de grupos do AD às funções necessárias na janela grupos do ative Directory.

5. Clique em **Salvar**.
6. Se for necessária conetividade LDAP a uma matriz, configure o serviço WFA para efetuar logon como o usuário de domínio necessário:
   a. Abra o console de serviços do Windows usando services.msc.
   b. Clique duas vezes no serviço **servidor WFA NetApp**.
   c. Na caixa de diálogo Propriedades do servidor NetApp WFA, clique na guia **Log on** e selecione **this account**.
   d. Introduza o nome de utilizador e a palavra-passe do domínio e, em seguida, clique em **OK**.

Adicionar grupos do ative Directory

Você pode adicionar grupos do ative Directory no OnCommand Workflow Automation (WFA).

Passos

1. Faça login NO WFA através de um navegador da Web como administrador.
2. Clique em **Configurações** e em **Gerenciamento**, clique em **grupos do ative Directory**.
3. Na janela grupos do ative Directory, clique no ícone **novo**.
4. Na caixa de diálogo novo grupo do ative Directory, insira as informações necessárias.

   Se você selecionar **Aprovador** na lista suspensa **função**, é recomendável fornecer o ID de e-mail do aprovador. Se houver vários aprovadores, você poderá fornecer um ID de e-mail do grupo no campo **e-mail**. Selecione os diferentes eventos do fluxo de trabalho para os quais a notificação deve ser enviada para o grupo específico do ative Directory.

5. Clique em **Salvar**.

Configurar notificações por e-mail

Você pode configurar o OnCommand Workflow Automation (WFA) para enviar notificações por e-mail sobre operações de fluxo de trabalho - por exemplo, fluxo de trabalho iniciado ou falha no fluxo de trabalho.

Você deve ter configurado um host de e-mail em seu ambiente.

Passos

1. Faça login NO WFA através de um navegador da Web como administrador.
2. Clique em **Configurações** e, em **Configuração**, clique em **Mail**.
3. Introduza as informações necessárias nos campos.
4. Teste as configurações de e-mail executando as seguintes etapas:
   a. Clique em **Enviar e-mail de teste**.
   b. Na caixa de diálogo testar conexão, digite o endereço de e-mail para o qual você deseja enviar o e-mail.
   c. Clique em **Teste**.
5. Clique em **Salvar**.

Configurar o SNMP

Você pode configurar o OnCommand Workflow Automation (WFA) para enviar traps SNMP (Simple Network Management Protocol) sobre o status das operações de fluxo de trabalho.

O WFA agora suporta protocolos SNMP v1 e SNMP v3. O SNMP v3 fornece recursos de segurança adicionais.

O arquivo .mib WFA fornece informações sobre as armadilhas que são enviadas pelo servidor WFA. O arquivo .mib está localizado no diretório <WFA_install_location> no servidor WFA.

O servidor WFA envia todas as notificações de trap com um identificador de objeto genérico (1,3.6,1.4,1.789,1.1.12.0).

Você não pode usar strings de comunidade SNMP, como Community_string_SNMP_host para configuração SNMP.

Configurar SNMP versão 1

Passos

1. Faça login NO WFA através de um navegador da Web como usuário admin e, em seguida, acesse o servidor WFA.
2. Clique em **Configurações** e, em **Configuração**, clique em **SNMP**.
3. Marque a caixa de seleção **Enable SNMP** (Ativar VRF*).
4. Na lista suspensa **Version**, selecione **Version 1**.
5. Insira um endereço IPv4 ou IPv6 ou o nome do host e o número da porta do host de gerenciamento.

   O WFA envia traps SNMP para o número de porta especificado. O número da porta padrão é 162.

6. Na seção notificar ligado , marque uma ou mais das seguintes caixas de seleção:
   - Execução do fluxo de trabalho iniciada
   - Execução do fluxo de trabalho concluída com êxito
   - A execução do fluxo de trabalho falhou/foi parcialmente bem-sucedida
   - Execução do fluxo de trabalho a aguardar aprovação

◦ Falha na aquisição

7. Clique em **Enviar notificação de teste** para verificar as configurações.
8. Clique em **Salvar**.

Configurar SNMP versão 3

Você também pode configurar o OnCommand Workflow Automation (WFA) para enviar traps de protocolo de gerenciamento de rede simples (SNMP) versão 3 sobre o status das operações de fluxo de trabalho.

A versão 3 oferece duas opções de segurança adicionais:

- Versão 3 com autenticação

  As armadilhas são enviadas sem criptografia pela rede. Os aplicativos de gerenciamento SNMP, que são configurados pelos mesmos parâmetros de autenticação que as mensagens de intercetação SNMP, podem receber traps.

- Versão 3 com autenticação e criptografia

  As armadilhas são enviadas criptografadas pela rede. Para receber e descriptografar esses traps, você deve configurar aplicativos de gerenciamento SNMP com os mesmos parâmetros de autenticação e chave de criptografia que os traps SNMP.

Passos

1. Faça login NO WFA através de um navegador da Web como usuário admin e, em seguida, acesse o servidor WFA.
2. Clique em **Configurações** e, em **Configuração**, clique em **SNMP**.
3. Marque a caixa de seleção **Enable SNMP** (Ativar VRF*).
4. Na lista suspensa **Version**, selecione uma das seguintes opções:
   ◦ Versão 3
   ◦ Versão 3 com autenticação
   ◦ Versão 3 com autenticação e criptografia
5. Selecione as opções de configuração SNMP que correspondem à opção específica do SNMP versão 3 que escolheu no passo 4.
6. Insira um endereço IPv4 ou IPv6 ou o nome do host e o número da porta do host de gerenciamento. O WFA envia traps SNMP para o número de porta especificado. O número da porta padrão é 162.
7. Na seção notificar ligado , marque uma ou mais das seguintes caixas de seleção:
   ◦ Planeamento do fluxo de trabalho iniciado/falhou/concluído
   ◦ Execução do fluxo de trabalho iniciada
   ◦ Execução do fluxo de trabalho concluída com êxito
   ◦ Execução do fluxo de trabalho falhou/ parcialmente bem-sucedida
   ◦ Execução do fluxo de trabalho a aguardar aprovação
   ◦ Falha na aquisição
8. Clique em **Enviar notificação de teste** para verificar as configurações.

9. Clique em **Salvar**.

Configurar Syslog

Você pode configurar o OnCommand Workflow Automation (WFA) para enviar dados de log para um servidor Syslog específico para fins como Registro de eventos e análise de informações de log.

Você deve ter configurado o servidor Syslog para aceitar dados do SERVIDOR WFA.

Passos

1. Faça login NO WFA através de um navegador da Web como administrador.
2. Clique em **Configurações** e, em **Manutenção**, clique em **Syslog**.
3. Marque a caixa de seleção **Enable Syslog** (Ativar Syslog*).
4. Introduza o nome do anfitrião Syslog e selecione o nível de registo Syslog.
5. Clique em **Salvar**.

Configurar protocolos para conexão a sistemas remotos

Pode configurar o protocolo utilizado pelo OnCommand Workflow Automation (WFA) para ligar a sistemas remotos. Pode configurar o protocolo com base nos requisitos de segurança da sua organização e no protocolo suportado pelo sistema remoto.

Passos

1. Faça login NO WFA através de um navegador da Web como administrador.
2. Clique em **Data Source Design** > **Remote System Types**.
3. Execute uma das seguintes ações:

Se você quiser…	Faça isso…
Configurar um protocolo para um novo sistema remoto	a. Clique em . b. Na caixa de diálogo novo tipo de sistema remoto, especifique os detalhes, como nome, descrição e versão.
Modifique a configuração do protocolo de um sistema remoto existente	a. Selecione e faça duplo clique no sistema remoto que pretende modificar. b. Clique em .

4. Na lista Connection Protocol (Protocolo de ligação), selecione uma das seguintes opções:
   - HTTPS com fallback para HTTP (padrão)
   - Apenas HTTPS
   - Apenas HTTP
   - Personalizado
5. Especifique os detalhes do protocolo, da porta padrão e do tempo limite padrão.

6. Clique em **Salvar**.

Desative a política de senha padrão

O OnCommand Workflow Automation (WFA) está configurado para impor uma política de senha para usuários locais. Se não pretender utilizar a política de palavra-passe, pode desativá-la.

Você deve ter feito login no sistema host DO WFA como administrador.

O caminho de instalação padrão DO WFA é usado neste procedimento. Se você alterou o local padrão durante a instalação, você deve usar o caminho de instalação alterado DO WFA.

Passos

1. Abra o Windows Explorer e navegue até o seguinte diretório: `WFA_install_location\WFA\bin\.`
2. Clique duas vezes no arquivo PS.cmd.

   Um prompt de interface de linha de comando (CLI) do PowerShell é aberto com os módulos ONTAP e WFA carregados nele.

3. No prompt, digite o seguinte:

   ```
   Set-WfaConfig -Name PasswordPolicy -Enable $false
   ```

4. Quando solicitado, reinicie os serviços DO WFA.

Modifique a política de senha padrão para o Windows

O OnCommand Workflow Automation (WFA) aplica uma política de senha para usuários locais. Você pode modificar a política de senha padrão para definir uma senha de acordo com sua exigência.

Você deve estar conetado ao sistema host WFA como um usuário root.

- O caminho de instalação padrão DO WFA é usado neste procedimento.

  Se você alterou o local padrão durante a instalação, você deve usar o caminho de instalação personalizado DO WFA.

- O comando para modificar a política de senha padrão é .

  A configuração padrão é "minLength true,8;specialChar true,1;digitalChar true,1;lowcase Char true,1;uppercasChar true,1;whitespaceChar false". De acordo com essa configuração para a política de senha padrão, a senha deve ter um comprimento mínimo de oito carateres, deve conter pelo menos um caractere especial, um dígito, um caractere minúsculo e um caractere maiúsculo, e não deve conter espaços.

Passos

1. No prompt de comando, navegue para o seguinte diretório no servidor WFA:

   ```
   WFA_install_location/wfa/bin/
   ```

2. Modificar a política de palavra-passe predefinida:

```
.\wfa --password-policy=PasswordPolicyString --restart=WFA
```

Ative o acesso remoto ao banco de dados do OnCommand Workflow Automation no Windows

Por padrão, o banco de dados OnCommand Workflow Automation (WFA) pode ser acessado apenas por clientes que estão sendo executados no sistema host WFA. Pode alterar as predefinições se pretender aceder à base de dados WFA a partir de um sistema remoto.

- Você deve ter feito login no sistema host WFA como um usuário admin.
- Se um firewall estiver instalado no sistema anfitrião WFA, tem de ter configurado as definições da firewall para permitir o acesso a partir do sistema remoto.

O caminho de instalação padrão DO WFA é usado neste procedimento. Se você alterou o local padrão durante a instalação, você deve usar o caminho de instalação personalizado DO WFA.

Passos

1. Abra o Explorador do Windows e navegue para o seguinte diretório: WFA_install_location
2. Execute uma das seguintes ações:

Para…	Digite o seguinte comando…
Ativar o acesso remoto	`.\wfa --db-access=public --restart`
Desativar o acesso remoto	`.\wfa --db-access=default --restart`

Restringir os direitos de acesso do OnCommand Workflow Automation no host

Por padrão, o OnCommand Workflow Automation (WFA) executa os fluxos de trabalho como o administrador do sistema host. Você pode restringir os direitos DO WFA no sistema host alterando as configurações padrão.

Você deve ter feito login no sistema host DO WFA como administrador.

Passos

1. Crie uma nova conta de usuário do Windows com permissões para abrir sockets e gravar no diretório home DO WFA.
2. Abra o console de serviços do Windows usando services.msc e clique duas vezes em **NetApp WFA Database**.
3. Clique no separador **Iniciar sessão**.
4. Selecione **esta conta** e insira as credenciais do novo usuário que você criou e clique em **OK**.

5. Clique duas vezes em **servidor WFA NetApp**.
6. Clique no separador **Iniciar sessão**.
7. Selecione **esta conta** e insira as credenciais do novo usuário que você criou e clique em **OK**.
8. Reinicie o **Banco de dados WFA do NetApp** e os serviços **servidor WFA do NetApp**.

Modifique a configuração de tempo limite da transação do OnCommand Workflow Automation

Por padrão, a transação do banco de dados OnCommand Workflow Automation (WFA) expira em 300 segundos. Você pode aumentar a duração do tempo limite padrão ao restaurar um banco de dados WFA de grande porte a partir de um backup para evitar possíveis falhas na restauração do banco de dados.

Você deve ter feito login no sistema host DO WFA como administrador.

O caminho de instalação padrão DO WFA é usado neste procedimento. Se você alterou o local padrão durante a instalação, você deve usar o caminho de instalação alterado DO WFA.

Passos

1. Abra o Windows Explorer e navegue até o seguinte diretório:

   ```
   WFA_install_location\WFA\bin
   ```

2. Clique duas vezes no arquivo PS.cmd.

   Um prompt de interface de linha de comando (CLI) do PowerShell é aberto com os módulos ONTAP e WFA carregados nele.

3. No prompt, digite o seguinte:

   ```
   Set-WfaConfig -Name TransactionTimeOut -Seconds NumericValue
   ```

   ```
   Set-WfaConfig -Name TransactionTimeOut -Seconds 1000
   ```

4. Quando solicitado, reinicie os serviços DO WFA.

Configure o valor de tempo limite para o Workflow Automation

Você pode configurar o valor de tempo limite para a GUI da Web do Workflow Automation (WFA), em vez de usar o valor de tempo limite padrão.

O valor de tempo limite padrão para a GUI da Web DO WFA é de 180 minutos. Você pode configurar o valor de tempo limite para atender aos seus requisitos por meio da CLI. Não é possível definir o valor de tempo limite da GUI da Web DO WFA.

O valor de tempo limite definido é um tempo limite absoluto em vez de um tempo limite relacionado à inatividade. Por exemplo, se você definir este valor para 30 minutos, então você será desconetado após 30 minutos, mesmo que esteja ativo no final desse tempo.

Passos

1. Faça login como administrador na máquina host DO WFA.
2. Defina o valor de tempo limite:

```
installdir bin/wfa -S=timeout value in minutes
```

Ativar cifras e adicionar novas cifras

O OnCommand Workflow Automation 5,1 suporta vários cifras fora da caixa. Além disso, você pode adicionar cifras adicionais, conforme necessário.

As seguintes cifras podem ser ativadas fora da caixa:

```
enabled-cipher-suites=
"TLS_DHE_DSS_WITH_AES_128_GCM_SHA256,TLS_DHE_DSS_WITH_AES_256_GCM_SHA384,T
LS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA25
6,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA38
4,TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384,TLS_ECDH_RSA_WITH_AES_128_GCM_SHA25
6,TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384"
```

Cifras adicionais podem ser adicionadas a esta configuração no `standalone-full.xml` arquivo. Este ficheiro está localizado em: `<installdir>/jboss/standalone/configuration/standalone-full.xml`.

O arquivo pode ser modificado para suportar cifras adicionais da seguinte forma:

```
<https-listener name="https" socket-binding="https" max-post-
size="1073741824" security-realm="SSLRealm"
enabled-cipher-suites="**< --- add additional ciphers here ---\>**
enabled-protocols="TLSv1.1,TLSv1.2"/>
```

Informações sobre direitos autorais

Informações sobre marcas comerciais