Einrichtung von OnCommand Workflow Automation

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

Inhalt

Einrichtung von OnCommand Workflow Automation . . . 1
Greifen Sie auf OnCommand Workflow Automation zu . . . 1
OnCommand Workflow Automation Datenquellen . . . 1
Erstellen Sie lokale Benutzer . . . 7
Konfigurieren Sie die Anmeldedaten eines Zielsystems . . . 8
OnCommand Workflow Automation wird konfiguriert . . . 9
Deaktivieren Sie die Standard-Passwortrichtlinie . . . 15
Ändern Sie die Standard-Passwortrichtlinie für Windows . . . 15
Aktivieren Sie Remote-Zugriff auf die OnCommand Workflow Automation-Datenbank unter Windows . . . 16
Zugriffsrechte von OnCommand Workflow Automation auf dem Host einschränken . . . 16
Ändern Sie die Einstellung für das Transaktions-Timeout von OnCommand Workflow Automation . . . 17
Konfigurieren Sie den Zeitüberschreitungswert für Workflow Automation . . . 18
Aktivieren von Chiffren und Hinzufügen neuer Chiffren . . . 18

Einrichtung von OnCommand Workflow Automation

Nach der Installation von OnCommand Workflow Automation (WFA) müssen Sie mehrere Konfigurationseinstellungen vornehmen. Sie müssen auf WFA zugreifen, Benutzer konfigurieren, Datenquellen einrichten, Anmeldedaten konfigurieren und WFA konfigurieren.

Greifen Sie auf OnCommand Workflow Automation zu

Sie können über einen Webbrowser von jedem System mit Zugriff auf den WFA Server auf OnCommand Workflow Automation (WFA) zugreifen.

Sie müssen Adobe Flash Player für Ihren Webbrowser installiert haben.

Schritte

1. Öffnen Sie einen Webbrowser, und geben Sie eine der folgenden Optionen in die Adressleiste ein:
   - `https://wfa_server_ip`

     wfa_Server_ip ist die IP-Adresse (IPv4- oder IPv6-Adresse) oder der vollständig qualifizierte Domain-Name (FQDN) des WFA-Servers.
   - Wenn Sie auf dem WFA Server auf WFA zugreifen: `https://localhost/wfa`Wenn Sie einen nicht-Standardport für WFA angegeben haben, müssen Sie die Portnummer wie folgt angeben:
   - `https://wfa_server_ip:port`
   - `https://localhost:port`Der Port ist die TCP-Portnummer, die Sie bei der Installation für den WFA-Server verwendet haben.
2. Geben Sie im Abschnitt Anmelden die Anmeldeinformationen des Admin-Benutzers ein, den Sie während der Installation eingegeben haben.
3. Richten Sie im Menü **Einstellungen** > **Setup** die Anmeldeinformationen und eine Datenquelle ein.
4. Erstellen Sie ein Lesezeichen für die WFA Web-GUI, um den Zugriff zu vereinfachen.

OnCommand Workflow Automation Datenquellen

OnCommand Workflow Automation (WFA) arbeitet auf Daten, die aus Datenquellen abgerufen werden. Verschiedene Versionen von Active IQ Unified Manager und VMware vCenter Server werden als vordefinierte WFA Datenquelltypen bereitgestellt. Sie müssen die vordefinierten Datenquelltypen kennen, bevor Sie die Datenquellen für die Datenerfassung einrichten.

Eine Datenquelle ist eine schreibgeschützte Datenstruktur, die als Verbindung zum Datenquellobjekt eines bestimmten Datenquelltyps dient. Beispielsweise kann eine Datenquelle eine Verbindung zu einer Active IQ Unified Manager-Datenbank eines Active IQ Unified Manager 6.3-Datenquelltyps sein. Sie können WFA eine benutzerdefinierte Datenquelle hinzufügen, nachdem Sie den erforderlichen Datenquelltyp definiert haben.

Weitere Informationen zu den vordefinierten Datenquelltypen finden Sie in der Interoperabilitäts-Matrix.

Verwandte Informationen

"NetApp Interoperabilitäts-Matrix-Tool"

Konfigurieren eines Datenbankbenutzers in DataFabric Manager

Sie müssen einen Datenbankbenutzer auf DataFabric Manager 5.x erstellen, um schreibgeschützten Zugriff auf die DataFabric Manager 5.x-Datenbank in OnCommand Workflow Automation zu konfigurieren.

Konfigurieren Sie einen Datenbankbenutzer, indem Sie ocsetup unter Windows ausführen

Sie können die ocSetup-Datei auf dem DataFabric Manager 5.x-Server ausführen, um schreibgeschützten Zugriff auf die DataFabric Manager 5.x-Datenbank in OnCommand Workflow Automation zu konfigurieren.

Schritte

1. Laden Sie die Datei wfa_ocsetup.exe von folgendem Speicherort in ein Verzeichnis des DataFabric Manager 5.x Servers herunter: *Https*://WFA_Server_IP/download/wfa_ocsetup.exe.

   WFA_Server_IP ist die IP-Adresse (IPv4 oder IPv6-Adresse) Ihres WFA Servers.

   Wenn Sie einen nicht standardmäßigen Port für WFA angegeben haben, müssen Sie die Portnummer wie folgt angeben: *Https*://wfa_Server_ip:Port/download/wfa_ocsetup.exe.

   Port ist die TCP-Portnummer, die Sie bei der Installation für den WFA Server verwendet haben.

   Wenn Sie eine IPv6-Adresse angeben, müssen Sie sie mit eckigen Klammern schließen.

2. Doppelklicken Sie auf die Datei wfa_ocsetup.exe.
3. Lesen Sie die Informationen im Setup-Assistenten und klicken Sie auf **Weiter**.
4. Suchen Sie nach OpenJDK, oder geben Sie die Position ein, und klicken Sie auf **Weiter**.
5. Geben Sie einen Benutzernamen und ein Kennwort ein, um die Standardanmeldeinformationen zu überschreiben.

   Ein neues Datenbank-Benutzerkonto wird mit Zugriff auf die DataFabric Manager 5.x Datenbank erstellt.

   > Wenn Sie kein Benutzerkonto erstellen, werden die Standardanmeldeinformationen verwendet. Aus Sicherheitsgründen müssen Sie ein Benutzerkonto erstellen.

6. Klicken Sie auf **Weiter** und sehen Sie sich die Ergebnisse an.
7. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**, um den Assistenten abzuschließen.

Konfigurieren Sie einen Datenbankbenutzer, indem Sie ocsetup unter Linux ausführen

Sie können die ocSetup-Datei auf dem DataFabric Manager 5.x-Server ausführen, um schreibgeschützten Zugriff auf die DataFabric Manager 5.x-Datenbank in OnCommand Workflow Automation zu konfigurieren.

Schritte

1. Laden Sie die wfa_ocsetup.sh-Datei mit dem folgenden Befehl im Terminal in Ihr Home-Verzeichnis auf dem DataFabric Manager 5.x Server herunter:

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

   WFA_Server_IP ist die IP-Adresse (IPv4 oder IPv6-Adresse) des WFA Servers.

   Wenn Sie einen nicht-Standardport für WFA angegeben haben, müssen Sie die Portnummer wie folgt angeben:

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

   Der Port ist die TCP-Portnummer, die Sie während der Installation für den WFA-Server verwendet haben.

   Wenn Sie eine IPv6-Adresse angeben, müssen Sie sie mit eckigen Klammern schließen.

2. Verwenden Sie den folgenden Befehl im Terminal, um die Datei wfa_ocsetup.sh in eine ausführbare Datei zu ändern: `chmod +x wfa_ocsetup.sh`
3. Führen Sie das Skript durch, indem Sie im Terminal Folgendes eingeben:

   ```
   ./wfa_ocsetup.sh OpenJDK_path
   ```

   OpenJDK_PATH ist der Pfad zu OpenJDK.

   /Opt/NTAPdfm/java

   Die folgende Ausgabe wird auf dem Terminal angezeigt, was auf eine erfolgreiche Einrichtung hinweist:

   ```
   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. Geben Sie einen Benutzernamen und ein Kennwort ein, um die Standardanmeldeinformationen zu überschreiben.

   Ein neues Datenbank-Benutzerkonto wird mit Zugriff auf die DataFabric Manager 5.x Datenbank erstellt.

   > Wenn Sie kein Benutzerkonto erstellen, werden die Standardanmeldeinformationen verwendet. Aus Sicherheitsgründen müssen Sie ein Benutzerkonto erstellen.

   Die folgende Ausgabe wird auf dem Terminal angezeigt, was auf eine erfolgreiche Einrichtung hinweist:

```
***** 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 *****
```

Konfigurieren Sie einen Datenbankbenutzer auf Active IQ Unified Manager

Sie müssen einen Datenbankbenutzer auf Active IQ Unified Manager erstellen, um schreibgeschützten Zugriff auf die Active IQ Unified Manager-Datenbank auf OnCommand Workflow Automation zu konfigurieren.

Schritte

1. Melden Sie sich mit Administratordaten bei Active IQ Unified Manager an.
2. Klicken Sie Auf **Einstellungen** > **Benutzer**.
3. Klicken Sie auf **Neuen Benutzer hinzufügen**.
4. Wählen Sie als Benutzertyp **Datenbankbenutzer** aus.

   Derselbe Benutzer sollte in OnCommand Workflow Automation verwendet werden, während Active IQ Unified Manager als Datenquelle in OnCommand Workflow Automation hinzugefügt wird.

Richten Sie eine Datenquelle ein

Sie müssen eine Verbindung mit einer Datenquelle in OnCommand Workflow Automation (WFA) einrichten, um Daten aus der Datenquelle zu erhalten.

- Für Active IQ Unified Manager 6.0 und höher müssen Sie auf dem Unified Manager-Server ein Datenbank-Benutzerkonto erstellt haben.

  Weitere Informationen finden Sie in der Online-Hilfe zum *OnCommand Unified Manager*.

- Der TCP-Port für eingehende Verbindungen auf dem Unified Manager-Server muss geöffnet sein.

  Weitere Informationen finden Sie in der Dokumentation Ihrer Firewall.

  Dies sind die Standardnummern für TCP-Ports:

TCP-Portnummer	Unified Manager Serverversion	Beschreibung
3306	6.x	MySQL-Datenbankserver

- Für Performance Advisor müssen Sie ein Active IQ Unified Manager-Benutzerkonto mit einer Mindestrolle

von GlobalRead erstellt haben.

Weitere Informationen finden Sie in der Online-Hilfe zum *OnCommand Unified Manager*.

- Für VMware vCenter Server müssen Sie ein Benutzerkonto auf dem vCenter Server erstellt haben.

  Details finden Sie in der Dokumentation zu VMware vCenter Server.

  > Sie müssen VMware PowerCLI installiert haben. Wenn Sie Workflows nur auf den Datenquellen von vCenter Server ausführen möchten, ist es nicht erforderlich, Unified Manager-Server als Datenquelle einzurichten.

- Der TCP-Port für eingehende Verbindungen auf dem VMware vCenter Server muss geöffnet sein.

  Die Standard-TCP-Portnummer lautet 443. Weitere Informationen finden Sie in der Dokumentation Ihrer Firewall.

Mit diesem Verfahren können Sie WFA mehrere Unified Manager-Serverdatenquellen hinzufügen. Sie dürfen dieses Verfahren jedoch nicht verwenden, wenn Sie Unified Manager Server 6.3 und höher mit WFA koppeln und die Schutzfunktion in Unified Manager Server verwenden möchten.

Weitere Informationen zum Pairing von WFA mit dem Unified Manager-Server 6.x finden Sie in der *OnCommand Unified Manager Online-Hilfe*.

> Beim Einrichten einer Datenquelle mit WFA müssen Sie beachten, dass die Datentypen in der WFA 6.0 4.0 Version von Active IQ Unified Manager 6.1 und 6.2 veraltet sind, und diese Datenquelltypen werden in zukünftigen Versionen nicht unterstützt.

Schritte

1. Zugriff auf WFA über einen Webbrowser
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Setup** auf **Datenquellen**.
3. Wählen Sie die entsprechende Aktion aus:

An…	Tun Sie das…
Erstellen einer neuen Datenquelle	Klicken Sie Auf In der Symbolleiste.
Bearbeiten Sie eine wiederhergestellte Datenquelle, wenn Sie WFA aktualisiert haben	Wählen Sie den vorhandenen Datenquelleneintrag aus, und klicken Sie auf In der Symbolleiste.

   Wenn Sie WFA eine Unified Manager-Serverdatenquelle hinzugefügt und die Version des Unified Manager-Servers aktualisiert haben, wird WFA die aktualisierte Version des Unified Manager-Servers nicht erkennen. Sie müssen die vorherige Version des Unified Manager-Servers löschen und dann WFA die aktualisierte Version des Unified Manager-Servers hinzufügen.

4. Wählen Sie im Dialogfeld Neue Datenquelle den erforderlichen Datenquellentyp aus, und geben Sie einen Namen für die Datenquelle und den Hostnamen ein.

   Auf der Grundlage des ausgewählten Datenquelltyps werden die Felder Port, Benutzername, Passwort und Timeout möglicherweise automatisch mit den Standarddaten ausgefüllt, sofern verfügbar. Sie können diese Einträge nach Bedarf bearbeiten.

5. Wählen Sie eine geeignete Aktion:

Für…	Tun Sie das…
Active IQ Unified Manager 6.3 und höher	Geben Sie die Anmeldeinformationen des Datenbankbenutzerkontos ein, das Sie auf dem Unified Manager-Server erstellt haben. Weitere Informationen zum Erstellen eines Datenbankbenutzerkontos finden Sie in der Online-Hilfe von *OnCommand Unified Manager*. Sie dürfen die Anmeldeinformationen eines Active IQ Unified Manager-Datenbankbenutzerkontos, das mit der Befehlszeilenschnittstelle oder dem ocsetup-Tool erstellt wurde, nicht bereitstellen.
VMware vCenter Server (nur für Windows)	(Nur für Windows) Geben Sie den Benutzernamen und das Passwort des Benutzers ein, den Sie auf dem VMware vCenter Server erstellt haben.

6. Klicken Sie Auf **Speichern**.
7. Wählen Sie in der Tabelle Datenquellen die Datenquelle aus, und klicken Sie auf In der Symbolleiste.
8. Überprüfen Sie den Status des Datenerfassungsprozesses.

Fügen Sie einen aktualisierten Unified Manager-Server als Datenquelle hinzu

Wenn Unified Manager-Server (5.x oder 6.x) als Datenquelle zu WFA hinzugefügt wird und dann der Unified Manager-Server aktualisiert wird, Sie müssen den aktualisierten Unified Manager-Server als Datenquelle hinzufügen, da die Daten, die mit der aktualisierten Version verknüpft sind, nicht in WFA gefüllt werden, es sei denn, er wird manuell als Datenquelle hinzugefügt.

Schritte

1. Melden Sie sich als Administrator bei der WFA Web-GUI an.
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Setup** auf **Datenquellen**.
3. Klicken Sie Auf In der Symbolleiste.
4. Wählen Sie im Dialogfeld Neue Datenquelle den erforderlichen Datenquellentyp aus, und geben Sie anschließend einen Namen für die Datenquelle und den Hostnamen ein.

   Auf der Grundlage des ausgewählten Datenquelltyps werden die Felder Port, Benutzername, Passwort und Timeout möglicherweise automatisch mit den Standarddaten ausgefüllt, sofern verfügbar. Sie können diese Einträge nach Bedarf bearbeiten.

5. Klicken Sie Auf **Speichern**.
6. Wählen Sie die vorherige Version des Unified Manager-Servers aus, und klicken Sie auf In der Symbolleiste.

7. Klicken Sie im Bestätigungsdialogfeld Datenquelltyp löschen auf **Ja**.
8. Wählen Sie in der Tabelle Datenquellen die Datenquelle aus, und klicken Sie dann auf In der Symbolleiste.
9. Überprüfen Sie den Datenerfassungsstatus in der Tabelle Verlauf.

Erstellen Sie lokale Benutzer

Mit OnCommand Workflow Automation (WFA) können Sie lokale WFA Benutzer mit spezifischen Berechtigungen für verschiedene Rollen wie Gast, Operator, Genehmiger, Architekt, Admin und Backup.

Sie müssen WFA installiert und als Administrator angemeldet haben.

WFA ermöglicht Ihnen das Erstellen von Benutzern für die folgenden Rollen:

- **Gast**

  Dieser Benutzer kann das Portal und den Status einer Workflow-Ausführung anzeigen und über eine Änderung des Status einer Workflow-Ausführung informiert werden.

- **Betreiber**

  Dieser Benutzer darf Workflows anzeigen und ausführen, für die der Benutzer Zugriff erhält.

- **Genehmiger**

  Dieser Benutzer kann Workflows anzeigen, ausführen, genehmigen und ablehnen, für die der Benutzer Zugriff erhält.

  > Es wird empfohlen, die E-Mail-ID des Genehmigers anzugeben. Wenn es mehrere Genehmiger gibt, können Sie im Feld **E-Mail** eine Gruppen-E-Mail-ID angeben.

- * Architekt*

  Dieser Benutzer hat vollen Zugriff auf die Erstellung von Workflows, kann aber aufgrund der Änderung globaler WFA Servereinstellungen eingeschränkt werden.

- **Admin**

  Dieser Benutzer hat vollständigen Zugriff auf den WFA Server.

- **Backup**

  Dieser ist der einzige Benutzer, der im Remote-Zugriff Backups des WFA Servers generieren kann. Der Benutzer ist jedoch von allen anderen Zugriffsrechten eingeschränkt.

Schritte

1. Klicken Sie auf **Einstellungen** und klicken Sie unter **Verwaltung** auf **Benutzer**.
2. Erstellen Sie einen neuen Benutzer, indem Sie auf klicken In der Symbolleiste.
3. Geben Sie die erforderlichen Informationen im Dialogfeld Neuer Benutzer ein.

4. Klicken Sie Auf **Speichern**.

Konfigurieren Sie die Anmeldedaten eines Zielsystems

In OnCommand Workflow Automation (WFA) können Sie die Anmeldedaten für ein Zielsystem konfigurieren und über die Anmeldeinformationen eine Verbindung zum spezifischen System herstellen und Befehle ausführen.

Nach der ersten Datenerfassung müssen Sie die Anmeldeinformationen für die Arrays konfigurieren, auf denen die Befehle ausgeführt werden. PowerShell WFA Controller-Verbindung funktioniert in zwei Modi:

- Mit Anmeldedaten

  WFA versucht zuerst eine Verbindung mit HTTPS herzustellen, und versucht dann mit HTTP. Sie können auch die LDAP-Authentifizierung von Microsoft Active Directory verwenden, um eine Verbindung zu Arrays herzustellen, ohne dass in WFA Anmeldedaten definiert werden. Um Active Directory LDAP verwenden zu können, müssen Sie das Array so konfigurieren, dass die Authentifizierung mit demselben Active Directory LDAP-Server durchgeführt wird.

- Ohne Zugangsdaten (für Storage-Systeme im 7-Mode)

  WFA versucht, eine Verbindung über eine Domänenauthentifizierung herzustellen. In diesem Modus wird das Anrufprotokoll für die Remote-Prozedur verwendet, das mit dem NTLM-Protokoll gesichert wird.

- WFA überprüft das SSL-Zertifikat (Secure Sockets Layer) für ONTAP Systeme. Benutzer werden möglicherweise aufgefordert, die Verbindung zu ONTAP-Systemen zu überprüfen und zu akzeptieren/abzulehnen, wenn das SSL-Zertifikat nicht vertrauenswürdig ist.
- Sie müssen die Zugangsdaten für ONTAP, NetApp Active IQ und LDAP (Lightweight Directory Access Protocol) erneut eingeben, nachdem Sie ein Backup wiederhergestellt oder ein Upgrade durchgeführt haben.

Schritte

1. Melden Sie sich über einen Webbrowser als Administrator bei WFA an.
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Setup** auf **Anmeldeinformationen**.
3. Klicken Sie Auf In der Symbolleiste.
4. Wählen Sie im Dialogfeld Neue Anmeldeinformationen eine der folgenden Optionen aus der Liste **Match** aus:

   - **Exakt**

     Anmeldeinformationen für eine bestimmte IP-Adresse oder einen bestimmten Hostnamen

   - **Muster**

     Zugangsdaten für den gesamten Subnetz oder IP-Bereich

     Die Verwendung der Syntax für reguläre Ausdrücke wird für diese Option nicht unterstützt.

5. Wählen Sie den Remote-Systemtyp aus der Liste **Typ** aus.
6. Geben Sie entweder den Hostnamen oder die IPv4- oder IPv6-Adresse der Ressource, den Benutzernamen und das Passwort ein.

WFA 5.1 überprüft die SSL-Zertifikate aller zu WFA hinzugefügten Ressourcen. Da Sie möglicherweise zur Zertifikatverifizierung aufgefordert werden, die Zertifikate zu akzeptieren, wird die Verwendung von Platzhalter in den Anmeldeinformationen nicht unterstützt. Wenn mehrere Cluster mit denselben Anmeldedaten verwendet werden, können Sie sie nicht alle gleichzeitig hinzufügen.

7. Testen Sie die Verbindung, indem Sie die folgende Aktion ausführen:

Wenn Sie den folgenden Match-Typ ausgewählt haben…	Dann…
Exakt	Klicken Sie Auf **Test**.
Muster	Speichern Sie die Anmeldeinformationen, und wählen Sie eine der folgenden Optionen: • Wählen Sie die Anmeldeinformationen aus, und klicken Sie auf In der Symbolleiste. • Klicken Sie mit der rechten Maustaste, und wählen Sie **Konnektivität testen**.

8. Klicken Sie Auf **Speichern**.

OnCommand Workflow Automation wird konfiguriert

Mit OnCommand Workflow Automation (WFA) können Sie verschiedene Einstellungen konfigurieren, beispielsweise AutoSupport und Benachrichtigungen.

Bei der Konfiguration von WFA können Sie je nach Bedarf eine oder mehrere der folgenden Optionen einrichten:

- AutoSupport zum Senden von AutoSupport Meldungen an den technischen Support
- Microsoft Active Directory Lightweight Directory Access Protocol (LDAP)-Server für die LDAP-Authentifizierung und -Autorisierung für WFA Benutzer
- E-Mail für E-Mail-Benachrichtigungen über Workflow-Vorgänge und das Senden von AutoSupport-Nachrichten
- Simple Network Management Protocol (SNMP) für Benachrichtigungen über Workflow-Vorgänge
- Syslog für Remote-Datenprotokollierung

Konfigurieren Sie AutoSupport

Sie können mehrere AutoSupport-Einstellungen konfigurieren, z. B. Zeitplan, Inhalt der AutoSupport-Meldungen und Proxyserver. AutoSupport sendet wöchentliche Protokolle der Inhalte, die Sie ausgewählt haben, an den technischen Support, um sie zu archivieren und Probleme zu analysieren.

Schritte

1. Melden Sie sich über einen Webbrowser als Administrator bei WFA an.

2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Einstellungen** auf **AutoSupport**.
3. Vergewissern Sie sich, dass das Feld **AutoSupport** aktivieren ausgewählt ist.
4. Geben Sie die erforderlichen Informationen ein.
5. Wählen Sie eine der folgenden Optionen aus der Liste * Content* aus:

Wenn Sie Folgendes einschließen möchten:	Wählen Sie dann diese Option…
Nur Konfigurationsdetails, wie Benutzer, Workflows und Befehle Ihrer WFA Installation	`send only configuration data`
Details zur WFA Konfiguration sowie Daten in WFA Cache-Tabellen wie z. B. dem Schema	`send configuration and cache data` (Standard)
Details zur WFA Konfiguration, Daten in WFA Cache-Tabellen und Daten im Installationsverzeichnis	`send configuration and cache extended data`

Das Passwort eines WFA Benutzers ist in den AutoSupport-Daten „*Not*“ enthalten.

6. Testen, dass Sie eine AutoSupport Nachricht herunterladen können:
   a. Klicken Sie Auf **Download**.
   b. Wählen Sie im Dialogfeld, das geöffnet wird, den Speicherort für die .7z-Datei aus.
7. Testen Sie das Senden einer AutoSupport-Nachricht an das angegebene Ziel, indem Sie auf **Jetzt senden** klicken.
8. Klicken Sie Auf **Speichern**.

Konfigurieren Sie die Authentifizierungseinstellungen

Sie können OnCommand Workflow Automation (WFA) konfigurieren, um einen Microsoft Active Directory (AD) LDAP-Server (Lightweight Directory Access Protocol) zur Authentifizierung und Autorisierung zu verwenden.

Sie müssen einen Microsoft AD LDAP-Server in Ihrer Umgebung konfiguriert haben.

Für WFA wird nur die Microsoft AD-LDAP-Authentifizierung unterstützt. Sie können keine anderen LDAP-Authentifizierungsmethoden verwenden, einschließlich Microsoft AD Lightweight Directory Services (AD LDS) oder Microsoft Global Catalog.

Während der Kommunikation sendet LDAP den Benutzernamen und das Passwort im Klartext. Allerdings ist die Kommunikation mit LDAPS (LDAP Secure) verschlüsselt und sicher.

Schritte

1. Melden Sie sich über einen Webbrowser als Administrator bei WFA an.
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Setup** auf **Authentifizierung**.
3. Aktivieren Sie das Kontrollkästchen * Active Directory aktivieren*.
4. Geben Sie die erforderlichen Informationen in die folgenden Felder ein:

a. Wenn Sie das Domain-Format des Benutzers@für Domain-Benutzer verwenden möchten, ersetzen Sie sAMAccountName im Feld **User Name attribut** durch userPrincipalName.

b. Wenn für Ihre Umgebung eindeutige Werte erforderlich sind, bearbeiten Sie die erforderlichen Felder.

c. Geben Sie die URI des AD-Servers wie folgt ein:
`ldap://active_directory_server_address\[:port\]`

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

Wenn Sie LDAP über SSL aktiviert haben, können Sie das folgende URI-Format verwenden:
`ldaps://active_directory_server_address\[:port\]`

a. Fügen Sie eine Liste mit AD-Gruppennamen der erforderlichen Rollen hinzu.

> Im Fenster „Active Directory Groups“ können Sie den erforderlichen Rollen eine Liste mit AD-Gruppennamen hinzufügen.

5. Klicken Sie Auf **Speichern**.
6. Wenn eine LDAP-Konnektivität zu einem Array erforderlich ist, konfigurieren Sie den WFA Service zur Anmeldung als erforderlicher Domänenbenutzer:
   a. Öffnen Sie die Windows Services-Konsole über Services.msc.
   b. Doppelklicken Sie auf den **NetApp WFA Server** Service.
   c. Klicken Sie im Dialogfeld Eigenschaften von NetApp WFA Server auf die Registerkarte **Anmelden** und wählen Sie dann **Dieses Konto** aus.
   d. Geben Sie den Benutzernamen und das Kennwort der Domäne ein, und klicken Sie dann auf **OK**.

Fügen Sie Active Directory-Gruppen hinzu

Sie können Active Directory-Gruppen in OnCommand Workflow Automation (WFA) hinzufügen.

Schritte

1. Melden Sie sich über einen Webbrowser als Administrator bei WFA an.
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Verwaltung** auf **Active Directory Groups**.
3. Klicken Sie im Fenster Active Directory Groups auf das Symbol **New**.
4. Geben Sie im Dialogfeld Neue Active Directory-Gruppe die erforderlichen Informationen ein.

   Wenn Sie in der Dropdown-Liste **Rolle Genehmiger** die Option **Genehmiger** wählen, wird empfohlen, die E-Mail-ID des Genehmigers anzugeben. Wenn es mehrere Genehmiger gibt, können Sie im Feld **E-Mail** eine Gruppen-E-Mail-ID angeben. Wählen Sie die verschiedenen Ereignisse des Workflows aus, für den die Benachrichtigung an die bestimmte Active Directory-Gruppe gesendet werden soll.

5. Klicken Sie Auf **Speichern**.

Konfigurieren Sie E-Mail-Benachrichtigungen

Zudem können Sie OnCommand Workflow Automation (WFA) so konfigurieren, dass Sie E-Mail-Benachrichtigungen zu Workflow-Vorgängen senden – beispielsweise gestartete Workflows oder fehlgeschlagener Workflow.

Sie müssen einen Mail-Host in Ihrer Umgebung konfiguriert haben.

Schritte

1. Melden Sie sich über einen Webbrowser als Administrator bei WFA an.
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Setup** auf **Mail**.
3. Geben Sie die erforderlichen Informationen in die Felder ein.
4. Testen Sie die E-Mail-Einstellungen wie folgt:
   a. Klicken Sie auf **Testmail senden**.
   b. Geben Sie im Dialogfeld Verbindung testen die E-Mail-Adresse ein, an die Sie die E-Mail senden möchten.
   c. Klicken Sie Auf **Test**.
5. Klicken Sie Auf **Speichern**.

Konfigurieren Sie SNMP

Sie können OnCommand Workflow Automation (WFA) konfigurieren, um SNMP-Traps (Simple Network Management Protocol) zum Status von Workflow-Vorgängen zu senden.

WFA unterstützt jetzt SNMP v1- und SNMP v3-Protokolle. SNMP v3 bietet zusätzliche Sicherheitsfunktionen.

Die WFA .mib-Datei bietet Informationen zu den Traps die vom WFA Server gesendet werden. Die mib-Datei befindet sich im Verzeichnis <WFA_install_location>\wfa\bin\wfa.mib auf dem WFA Server.

> Der WFA Server sendet alle Trap-Benachrichtigungen über eine generische Objektkennung (1.3.6.1.4.1.789.1.1.12.0).

Sie können SNMP-Community-Strings wie Community_string@SNMP_Host nicht für die SNMP-Konfiguration verwenden.

Konfigurieren Sie SNMP-Version 1

Schritte

1. Melden Sie sich bei WFA über einen Webbrowser als Admin-Benutzer an und greifen Sie dann auf den WFA Server zu.
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Setup** auf **SNMP**.
3. Aktivieren Sie das Kontrollkästchen **SNMP aktivieren**.
4. Wählen Sie in der Dropdown-Liste **Version**die Option **Version 1** aus.
5. Geben Sie eine IPv4- oder IPv6-Adresse oder den Hostnamen und die Portnummer des Management-Hosts ein.

   WFA sendet SNMP-Traps an die angegebene Portnummer. Die Standardanschlussnummer ist 162.

6. Wählen Sie im Abschnitt Benachrichtigen auf ein oder mehrere der folgenden Kontrollkästchen aus:
   - Workflow-Ausführung gestartet
   - Workflow-Ausführung erfolgreich abgeschlossen
   - Ausführung des Workflows fehlgeschlagen/teilweise erfolgreich

- Workflow-Ausführung wartet auf Genehmigung
- Erfassungsfehler

7. Klicken Sie auf **Testbenachrichtigung senden**, um die Einstellungen zu überprüfen.
8. Klicken Sie Auf **Speichern**.

Konfigurieren Sie SNMP-Version 3

Sie können auch OnCommand Workflow Automation (WFA) konfigurieren, um SNMP-Traps (Simple Network Management Protocol) Version 3 über den Status von Workflow-Operationen zu senden.

Version 3 bietet zwei zusätzliche Sicherheitsoptionen:

- Version 3 mit Authentifizierung

  Traps werden unverschlüsselt über das Netzwerk gesendet. SNMP-Verwaltungsanwendungen, die mit denselben Authentifizierungsparametern wie SNMP-Trap-Nachrichten konfiguriert sind, können Traps empfangen.

- Version 3 mit Authentifizierung und Verschlüsselung

  Traps werden über das Netzwerk verschlüsselt gesendet. Um diese Traps zu empfangen und zu entschlüsseln, müssen Sie SNMP-Verwaltungsanwendungen mit denselben Authentifizierungsparametern und Verschlüsselungsschlüsseln wie die SNMP-Traps konfigurieren.

Schritte

1. Melden Sie sich bei WFA über einen Webbrowser als Admin-Benutzer an und greifen Sie dann auf den WFA Server zu.
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Setup** auf **SNMP**.
3. Aktivieren Sie das Kontrollkästchen **SNMP aktivieren**.
4. Wählen Sie in der Dropdown-Liste **Version** eine der folgenden Optionen aus:
   - Version 3
   - Version 3 mit Authentifizierung
   - Version 3 mit Authentifizierung und Verschlüsselung
5. Wählen Sie die SNMP-Konfigurationsoptionen aus, die der spezifischen SNMP-Version 3 entsprechen, die Sie in Schritt 4 gewählt haben.
6. Geben Sie eine IPv4- oder IPv6-Adresse oder den Hostnamen und die Portnummer des Management-Hosts ein. WFA sendet SNMP-Traps an die angegebene Portnummer. Die Standardanschlussnummer ist 162.
7. Wählen Sie im Abschnitt Benachrichtigen auf ein oder mehrere der folgenden Kontrollkästchen aus:
   - Workflow-Planung gestartet/fehlgeschlagen/abgeschlossen
   - Workflow-Ausführung gestartet
   - Workflow-Ausführung erfolgreich abgeschlossen
   - Ausführung des Workflows fehlgeschlagen/teilweise erfolgreich
   - Workflow-Ausführung wartet auf Genehmigung

- Erfassungsfehler

8. Klicken Sie auf **Testbenachrichtigung senden**, um die Einstellungen zu überprüfen.
9. Klicken Sie Auf **Speichern**.

Syslog Konfigurieren

Sie können OnCommand Workflow Automation (WFA) konfigurieren, um Protokolldaten für Zwecke wie Ereignisprotokollierung und die Analyse von Protokollinformationen an einen bestimmten Syslog-Server zu senden.

Sie müssen den Syslog-Server konfiguriert haben, um Daten vom WFA-Server zu akzeptieren.

Schritte

1. Melden Sie sich über einen Webbrowser als Administrator bei WFA an.
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Wartung** auf **Syslog**.
3. Aktivieren Sie das Kontrollkästchen **Syslog** aktivieren.
4. Geben Sie den Syslog-Host-Namen ein, und wählen Sie die Syslog-Ebene.
5. Klicken Sie Auf **Speichern**.

Konfigurieren von Protokollen zum Anschluss an Remote-Systeme

Sie können das von OnCommand Workflow Automation (WFA) verwendete Protokoll konfigurieren, um eine Verbindung zu Remote-Systemen herzustellen. Sie können das Protokoll auf Grundlage der Sicherheitsanforderungen Ihres Unternehmens und des vom Remote-System unterstützten Protokolls konfigurieren.

Schritte

1. Melden Sie sich über einen Webbrowser als Administrator bei WFA an.
2. Klicken Sie Auf **Datenquellendesign** > **Remote-Systemtypen**.
3. Führen Sie eine der folgenden Aktionen aus:

Ihr Ziel ist	Tun Sie das…
Konfigurieren eines Protokolls für ein neues Remote-System	a. Klicken Sie Auf . b. Geben Sie im Dialogfeld Neuer Remote-Systemtyp die Details wie Name, Beschreibung und Version an.
Ändern Sie die Protokollkonfiguration eines vorhandenen Remote-Systems	a. Wählen Sie das zu ändernde Remote-System aus, und doppelklicken Sie darauf. b. Klicken Sie Auf .

4. Wählen Sie aus der Liste Connection Protocol eine der folgenden Optionen aus:
   - HTTPS mit Fallback zu HTTP (Standard)
   - Nur HTTPS

    - Nur HTTP
    - Individuell
5. Geben Sie Details für das Protokoll, den Standardport und das Standard-Timeout an.
6. Klicken Sie Auf **Speichern**.

Deaktivieren Sie die Standard-Passwortrichtlinie

OnCommand Workflow Automation (WFA) ist so konfiguriert, dass eine Passwortrichtlinie für lokale Benutzer durchgesetzt wird. Wenn Sie die Passwortrichtlinie nicht verwenden möchten, können Sie sie deaktivieren.

Sie müssen als Administrator beim WFA Host-System angemeldet sein.

In diesem Verfahren wird der WFA Standardinstallationspfad verwendet. Wenn Sie während der Installation den Standardspeicherort geändert haben, müssen Sie den geänderten WFA Installationspfad verwenden.

Schritte

1. Öffnen Sie Windows Explorer und navigieren Sie zum folgenden Verzeichnis: `WFA_install_location\WFA\bin\.`
2. Doppelklicken Sie auf die Datei ps.cmd.

   Es wird eine PowerShell Eingabeaufforderung für die Befehlszeilenschnittstelle (CLI) geöffnet, wobei ONTAP- und WFA-Module enthalten sind.

3. Geben Sie an der Eingabeaufforderung Folgendes ein:

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

4. Starten Sie die WFA Services nach der entsprechenden Aufforderung neu.

Ändern Sie die Standard-Passwortrichtlinie für Windows

OnCommand Workflow Automation (WFA) erzwingt lokale Benutzer durch ein Passwort. Sie können die Standard-Passwortrichtlinie ändern, um ein Kennwort gemäß Ihrer Anforderung festzulegen.

Sie müssen als Root-Benutzer beim WFA Host-System angemeldet sein.

- In diesem Verfahren wird der WFA Standardinstallationspfad verwendet.

  Wenn Sie während der Installation den Standardspeicherort geändert haben, müssen Sie auch den benutzerdefinierten WFA Installationspfad verwenden.

- Der Befehl zum Ändern der Standard-Passwortrichtlinie ist .\wfa --password-Policy=default.

  Die Standardeinstellung ist “minLength=true,8;specialChar=true,1;digitalChar=true,1;lowercaseChar=true,1;uppercaseChar=true,1;whespaceChar=false”. Gemäß dieser Einstellung für die Standard-Passwortrichtlinie muss das Passwort eine Mindestlänge von acht Zeichen aufweisen, mindestens ein Sonderzeichen, eine Ziffer, ein Kleinbuchstaben und ein Großbuchstaben enthalten und darf keine Leerzeichen enthalten.

Schritte

1. Navigieren Sie an der Eingabeaufforderung zum folgenden Verzeichnis auf dem WFA Server:

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

2. Ändern Sie die Standard-Passwortrichtlinie:

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

Aktivieren Sie Remote-Zugriff auf die OnCommand Workflow Automation-Datenbank unter Windows

Standardmäßig ist der Zugriff auf die OnCommand Workflow Automation (WFA) Datenbank nur von Clients möglich, die auf dem WFA Host-System ausgeführt werden. Sie können die Standardeinstellungen ändern, wenn Sie von einem Remote-System aus auf die WFA Datenbank zugreifen möchten.

- Sie müssen sich als Admin-Benutzer beim WFA Host-System angemeldet haben.
- Falls auf dem WFA Host-System eine Firewall installiert ist, müssen Sie Ihre Firewall-Einstellungen so konfiguriert haben, dass der Zugriff über das Remote-System möglich ist.

In diesem Verfahren wird der WFA Standardinstallationspfad verwendet. Wenn Sie während der Installation den Standardspeicherort geändert haben, müssen Sie auch den benutzerdefinierten WFA Installationspfad verwenden.

Schritte

1. Öffnen Sie den Windows Explorer, und navigieren Sie zum folgenden Verzeichnis: WFA_install_location\WFA\bin
2. Führen Sie eine der folgenden Aktionen aus:

An…	Geben Sie den folgenden Befehl ein…
Remote-Zugriff aktivieren	`.\wfa --db-access=public --restart`
Deaktivieren des Remote-Zugriffs	`.\wfa --db-access=default --restart`

Zugriffsrechte von OnCommand Workflow Automation auf dem Host einschränken

Standardmäßig führt OnCommand Workflow Automation (WFA) die Workflows als Administrator des Host-Systems aus. Sie können die WFA Rechte auf dem Hostsystem einschränken, indem Sie die Standardeinstellungen ändern.

Sie müssen als Administrator beim WFA Host-System angemeldet sein.

Schritte

1. Erstellen Sie ein neues Windows Benutzerkonto mit Rechten zum Öffnen von Sockets und zum Schreiben in das WFA Home Directory.
2. Öffnen Sie die Windows Services-Konsole über Services.msc und doppelklicken Sie auf **NetApp WFA Database**.
3. Klicken Sie auf die Registerkarte **Anmelden**.
4. Wählen Sie **This Account** aus, und geben Sie die Anmeldeinformationen des neuen Benutzers ein, den Sie erstellt haben, und klicken Sie dann auf **OK**.
5. Doppelklicken Sie auf **NetApp WFA Server**.
6. Klicken Sie auf die Registerkarte **Anmelden**.
7. Wählen Sie **This Account** aus, und geben Sie die Anmeldeinformationen des neuen Benutzers ein, den Sie erstellt haben, und klicken Sie dann auf **OK**.
8. Starten Sie die Services **NetApp WFA Database** und **NetApp WFA Server** neu.

Ändern Sie die Einstellung für das Transaktions-Timeout von OnCommand Workflow Automation

Die Transaktionszeiten der OnCommand Workflow Automation (WFA) Datenbank liegen standardmäßig in 300 Sekunden vor. Sie können die Standard-Zeitdauer beim Wiederherstellen einer großen WFA Datenbank aus einem Backup erhöhen, um einen potenziellen Ausfall der Datenbankwiederherstellung zu vermeiden.

Sie müssen als Administrator beim WFA Host-System angemeldet sein.

In diesem Verfahren wird der WFA Standardinstallationspfad verwendet. Wenn Sie während der Installation den Standardspeicherort geändert haben, müssen Sie den geänderten WFA Installationspfad verwenden.

Schritte

1. Öffnen Sie Windows Explorer und navigieren Sie zum folgenden Verzeichnis:

   ```
   WFA_install_location\WFA\bin
   ```

2. Doppelklicken Sie auf die Datei ps.cmd.

   Es wird eine PowerShell Eingabeaufforderung für die Befehlszeilenschnittstelle (CLI) geöffnet, wobei ONTAP- und WFA-Module enthalten sind.

3. Geben Sie an der Eingabeaufforderung Folgendes ein:

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

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

4. Starten Sie die WFA Services nach der entsprechenden Aufforderung neu.

Konfigurieren Sie den Zeitüberschreitungswert für Workflow Automation

Sie können den Zeitüberschreitungswert für die Web-GUI (WFA) für Workflow Automation konfigurieren, anstatt den standardmäßigen Timeout-Wert zu verwenden.

Der Standardwert für die WFA Web GUI ist 180 Minuten. Sie können den Zeitüberschreitungswert konfigurieren, um Ihre Anforderungen über CLI zu erfüllen. Sie können den Zeitüberschreitungswert nicht über die WFA Web GUI einstellen.

> Der von Ihnen eingestellte Timeout-Wert ist ein absolutes Timeout und nicht ein Timeout im Zusammenhang mit Inaktivität. Wenn Sie diesen Wert z. B. auf 30 Minuten setzen, werden Sie nach 30 Minuten abgemeldet, auch wenn Sie am Ende dieser Zeit aktiv sind.

Schritte

1. Melden Sie sich als Administrator auf der WFA Host-Maschine an.
2. Legen Sie den Zeitüberschreitungswert fest:

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

Aktivieren von Chiffren und Hinzufügen neuer Chiffren

OnCommand Workflow Automation 5.1 unterstützt eine Reihe von Chiffren Out-of-the-Box. Außerdem können Sie nach Bedarf weitere Chiffren hinzufügen.

Die folgenden Chiffren können sofort aktiviert werden:

```
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"
```

Zu dieser Konfiguration können im weitere Chiffren hinzugefügt werden `standalone-full.xml` Datei: Diese Datei befindet sich unter: `<installdir>/jboss/standalone/configuration/standalone-full.xml`.

Die Datei kann wie folgt geändert werden, um weitere Chiffren zu unterstützen:

```
<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"/>
```