Einrichtung von OnCommand Workflow Automation

OnCommand Workflow Automation 5.0

NetApp
April 19, 2024

This PDF was generated from https://docs.netapp.com/de-de/workflow-automation-50/windows-install/task-access-oncommand-workflow-automation.html on April 19, 2024. Always check docs.netapp.com for the latest.

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 . . . 14
Ändern Sie die Standard-Passwortrichtlinie für Windows . . . 14
Aktivieren Sie Remote-Zugriff auf die OnCommand Workflow Automation-Datenbank unter Windows . . . 15
Zugriffsrechte von OnCommand Workflow Automation auf dem Host einschränken . . . 16
Ändern Sie die Einstellung für das Transaktions-Timeout von OnCommand Workflow Automation . . . 16
Konfigurieren Sie den Zeitüberschreitungswert für Workflow Automation . . . 17

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.

Was Sie benötigen

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 vollqualifizierte Domain-Name (FQDN) des WFA-Servers.

   - Wenn Sie auf dem WFA Server auf WFA zugreifen: `https://localhost/wfa`+ Wenn Sie einen nicht standardmäßigen Port für WFA angegeben haben, müssen Sie wie folgt die Portnummer angeben:
   - `https://wfa_server_ip:port`
   - `https://localhost:port`+ *Port* ist die TCP-Portnummer, die Sie während 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. **Optional:** richten Sie im Menü **Einstellungen** > **Setup** die Anmeldeinformationen und eine Datenquelle ein.
4. **Optional:** Lesezeichen für die WFA Web GUI für einfachen Zugriff.

OnCommand Workflow Automation Datenquellen

OnCommand Workflow Automation (WFA) arbeitet auf Daten, die aus Datenquellen abgerufen werden. Verschiedene Versionen von Active IQ Data Center 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

Datacenter Manager-Datenbank eines Datenquelltyps des Active IQ Datacenter Manager 6.3 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 Active IQ Datacenter Manager

Sie müssen einen Datenbankbenutzer unter Active IQ Datacenter Manager Versionen vor 6.0 erstellen, um den schreibgeschützten Zugriff der Active IQ Datacenter Manager-Datenbank auf OnCommand Workflow Automation zu konfigurieren.

Konfigurieren Sie einen Datenbankbenutzer, indem Sie ocsetup unter Windows ausführen

Sie können die ausführen `ocsetup` Datei auf dem Active IQ Datacenter Manager-Server zum Konfigurieren des schreibgeschützten Zugriffs der Active IQ Datacenter Manager-Datenbank auf OnCommand Workflow Automation.

Schritte

1. Laden Sie die herunter `wfa_ocsetup.exe` Datei in ein Verzeichnis auf dem Active IQ-Rechenzentrumsmanager-Server von folgendem Speicherort aus: `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-Standardport 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 `wfa_ocsetup.exe` Datei:
3. Lesen Sie die Informationen im Setup-Assistenten und klicken Sie auf **Weiter**.
4. Durchsuchen Sie die JRE-Position, oder geben Sie sie ein, und klicken Sie auf **Weiter**.
5. Geben Sie einen Benutzernamen und ein Kennwort ein, um die Standardanmeldeinformationen zu überschreiben.

   Ein neues Datenbankbenutzerkonto wird mit Zugriff auf die Active IQ Data Center Manager 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 Active IQ Datacenter Manager-Server ausführen, um den schreibgeschützten Zugriff der Active IQ Datacenter Manager-Datenbank auf OnCommand Workflow Automation zu konfigurieren.

Schritte

1. Laden Sie die herunter `wfa_ocsetup.sh` Datei in Ihr Home-Verzeichnis auf dem Active IQ-Rechenzentrumsmanager-Server mit dem folgenden Befehl im Terminal: `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
   ```

   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. 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 JRE_path
   ```

   JRE_PATH ist der Pfad zum JRE.

   Beispiel

   ```
   /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 Datenbankbenutzerkonto wird mit Zugriff auf die Active IQ Data Center Manager 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 *****
```

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.

Was Sie benötigen

- Bei älteren Versionen als 6.0 von Active IQ Data Center Manager müssen Sie die neueste Version des ocsetup-Tools auf dem Data Center Manager-Server ausführen, um den schreibgeschützten Remote-Zugriff auf die Datenbank zu aktivieren und zu konfigurieren.
- Für Active IQ Data Center Manager6.0 und höher müssen Sie ein Datenbankbenutzerkonto auf dem Data Center Manager Server erstellt haben.

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

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

  Weitere Informationen finden Sie in der Dokumentation Ihrer Firewall.

  Dies sind die Standardnummern für TCP-Ports:

TCP-Portnummer	Serverversion des Data Center Manager	Beschreibung
2638	5.x	Sybase SQL Anywhere Datenbankserver
3306	6.x	MySQL-Datenbankserver

- Für Performance Advisor müssen Sie ein Active IQ Datacenter 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, den Datacenter 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.

Über diese Aufgabe

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

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

> Beim Einrichten einer Datenquelle mit WFA, müssen Sie beachten, dass Active IQ Data Center Manager 6.0, 6.1 und 6.2 Datentypen in der WFA 4.0 Version veraltet sind, und diese Datenquellen 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 Datacenter Manager-Serverdatenquelle hinzugefügt und dann die Version des Data Center Manager-Servers aktualisiert haben, erkennt WFA die aktualisierte Version des Datacenter Manager-Servers nicht. Sie müssen die vorherige Version des Data Center Manager-Servers löschen und dann WFA die aktualisierte Version des Data Center 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 Data Center Manager Versionen vor 6.0	Geben Sie den Benutzernamen und das Kennwort ein, die Sie beim Ausführen von ocsetup verwendet haben, um die Standardanmeldeinformationen zu überschreiben.
Active IQ Datacenter Manager 6.3 und höher	Geben Sie die Anmeldeinformationen des Datenbankbenutzerkontos ein, das Sie auf dem Datacenter Manager-Server erstellt haben. Weitere Informationen zum Erstellen eines Datenbankbenutzerkontos finden Sie in der Online-Hilfe von *OnCommand Unified Manager*.
Performance Advisor für (Active IQ Datacenter Manager Versionen vor 6.0)	Geben Sie die Anmeldeinformationen für einen Benutzer von Active IQ-Rechenzentrumsmanager mit einer Mindestrolle von GlobalRead ein. Sie dürfen die Anmeldeinformationen eines Active IQ Data Center Manager-Datenbankbenutzerkontos, das mit der Befehlszeilenschnittstelle oder dem occsetup-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. **Optional:** 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 Datacenter Manager-Server als Datenquelle hinzu

Wenn Datacenter Manager-Server (5.x oder 6.x) als Datenquelle zu WFA hinzugefügt und dann der Datacenter Manager-Server aktualisiert wird, Sie müssen den aktualisierten Datacenter 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 dann 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 Data Center Manager-Servers aus, und klicken Sie auf In der Symbolleiste.
7. Klicken Sie im Bestätigungsdialogfeld **Datenquellentyp löschen** auf **Ja**.
8. **Optional:** 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.

Was Sie benötigen

Sie müssen WFA installiert und als Administrator angemeldet haben.

Über diese Aufgabe

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.

Über diese Aufgabe

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.

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

Sie können die Syntax für reguläre Ausdrücke für diese Option verwenden.

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.
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 (ASUP) für das Senden von ASUP 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 zu Workflow-Vorgängen und Senden von ASUP Meldungen
- 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	Nur Konfigurationsdaten senden
Details zur WFA Konfiguration sowie Daten in WFA Cache-Tabellen wie z. B. dem Schema	Senden von Konfigurations- und Cache-Daten (Standard)
Details zur WFA Konfiguration, Daten in WFA Cache-Tabellen und Daten im Installationsverzeichnis	Senden von Konfigurations- und Zwischenspeichern erweiterter Daten

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 aus, der gespeichert werden soll `.7z` Datei:
7. **Optional:** 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.

Was Sie benötigen

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

Über diese Aufgabe

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. **Optional:** Wenn Sie das Format *user@Domain* für Domain-Benutzer verwenden möchten, ersetzen Sie `sAMAccountName` Mit `userPrincipalName` Im Feld * Benutzername Attribut*.

   b. **Optional:** 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]`

      Beispiel

      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. **Optional:** Wenn eine LDAP-Verbindung zu einem Array erforderlich ist, konfigurieren Sie den WFA-Service so, dass Sie sich als erforderlicher Domänenbenutzer anmelden:

   a. Öffnen Sie die Windows Services-Konsole mit `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.

Was Sie benötigen

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. **Optional:** Testen Sie die E-Mail-Einstellungen, indem Sie die folgenden Schritte durchführen:
   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.

Über diese Aufgabe

WFA `.mib` Datei bietet Informationen zu den vom WFA Server gesendeten Traps. Der `.mib` Die Datei befindet sich im `<WFA_install_location>\wfa\bin\wfa.mib` Verzeichnis 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.

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. 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.

5. Wählen Sie im Abschnitt **Benachrichtigen bei** 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
6. Klicken Sie auf **Testbenachrichtigung senden**, um die Einstellungen zu überprüfen.
7. 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.

Was Sie benötigen

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 **Designer** > **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.

Ihr Ziel ist	Tun Sie das…
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.

Was Sie benötigen

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

Über diese Aufgabe

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 `ps.cmd` Datei:

   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.

Was Sie benötigen

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

Über diese Aufgabe

- 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 lautet `.\wfa --password-policy=default`.

  Die Standardeinstellung ist "minLength=true,6;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 sechs 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.

Was Sie benötigen

- 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.

Über diese Aufgabe

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.

1. Öffnen Sie 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.

Was Sie benötigen

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 mit `services.msc` 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.

Was Sie benötigen

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

Über diese Aufgabe

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 `ps.cmd` Datei:

   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
   ```

   Beispiel

   ```
   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.

Über diese Aufgabe

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
   ```

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.