



Installation und Einrichtung für Windows

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

This PDF was generated from <https://docs.netapp.com/de-de/workflow-automation/windows-install/concept-oncommand-workflow-automation-deployment-architecture.html> on April 19, 2024. Always check docs.netapp.com for the latest.

Inhalt

Installation und Einrichtung für Windows	1
Übersicht über OnCommand Workflow Automation	1
Systemanforderungen für die Installation von OnCommand Workflow Automation	4
Voraussetzungen für die Installation von Workflow Automation	6
Management von Hochverfügbarkeit	8
Einrichtung von OnCommand Workflow Automation	18
Upgrade von OnCommand Workflow Automation	36
Upgrade von Drittanbieterprodukten	38
Backup der OnCommand Workflow Automation-Datenbank	40
Wiederherstellen der OnCommand Workflow Automation-Datenbank	44
Setzt das bei der Installation erstellte Admin-Passwort zurück	48
Importieren Sie OnCommand Workflow Automation-Inhalte	49
Migrieren der OnCommand Workflow Automation Installation	51
Deinstallieren Sie OnCommand Workflow Automation	51
Verwalten des OnCommand Workflow Automation-SSL-Zertifikats	52
Verwalten von Perl- und Perl-Modulen	54
Fehlerbehebung bei Installations- und Konfigurationsproblemen	58
Zugehörige Dokumentation für OnCommand Workflow Automation	59

Installation und Einrichtung für Windows

Übersicht über OnCommand Workflow Automation

OnCommand Workflow Automation (WFA) ist eine Softwarelösung zur Automatisierung von Storage-Managementaufgaben, u. a. für Provisionierung, Migration, Ausmusterung, Datensicherung, Und Klonen-Storage. Mit WFA können Workflows zum Erstellen von Aufgaben erstellt werden, die von Ihren Prozessen festgelegt werden. WFA unterstützt sowohl ONTAP als auch Data ONTAP in 7-Mode.

Ein Workflow ist eine sich wiederholende und prozedurale Aufgabe, die aus sequenziellen Schritten besteht, einschließlich der folgenden Arten von Aufgaben:

- Bereitstellung, Migration oder Dekommissionierung von Storage für Datenbanken oder Dateisysteme
- Einrichtung einer neuen Virtualisierungsumgebung inklusive Storage Switches und Datastores
- Einrichtung von Storage für eine Applikation im Rahmen einer End-to-End-Orchestrierung

Storage-Architekten können Workflows definieren, um Best Practices einzuhalten und geschäftliche Anforderungen zu erfüllen. Beispiele dafür sind:

- Verwendung der erforderlichen Namenskonventionen
- Festlegen einzigartiger Optionen für Speicherobjekte
- Auswählen von Ressourcen
- Integration interner Konfigurationsmanagement-Datenbanken (CMDB) und Ticketapplikationen

WFA Funktionen herunter

- Workflow-Designportal zum Erstellen von Workflows

Das Workflow-Designportal enthält mehrere Bausteine, wie Befehle, Vorlagen, Suchgeräte, Filter, Und -Funktionen, die zum Erstellen von Workflows verwendet werden. Der Designer ermöglicht es Ihnen, erweiterte Funktionen in Workflows wie automatische Ressourcenauswahl, Zeilenwiederholung (Looping) und Freigabestellen zu integrieren.

Das Workflow-Designportal enthält auch Bausteine wie Wörterbucheinträge, Cache-Abfragen und Datenquellentypen zum Caching von Daten aus externen Systemen.

- Ausführungsportal zum Ausführen von Workflows, zum Überprüfen des Status der Workflow-Ausführung und der Zugriffsprotokolle
- Administrations-/Einstellungsoption für Aufgaben wie Einrichten von WFA, Verbinden mit Datenquellen und Konfigurieren von Benutzeranmeldeinformationen
- Web-Service-Schnittstellen zum Aufrufen von Workflows von externen Portalen und Orchestrierungssoftware für Datacenter
- Storage Automation Store zum Herunterladen der WFA Pakete. Das ONTAP 9.7.0 Paket wird mit WFA 5.1 ausgeliefert.

WFA Lizenzinformationen

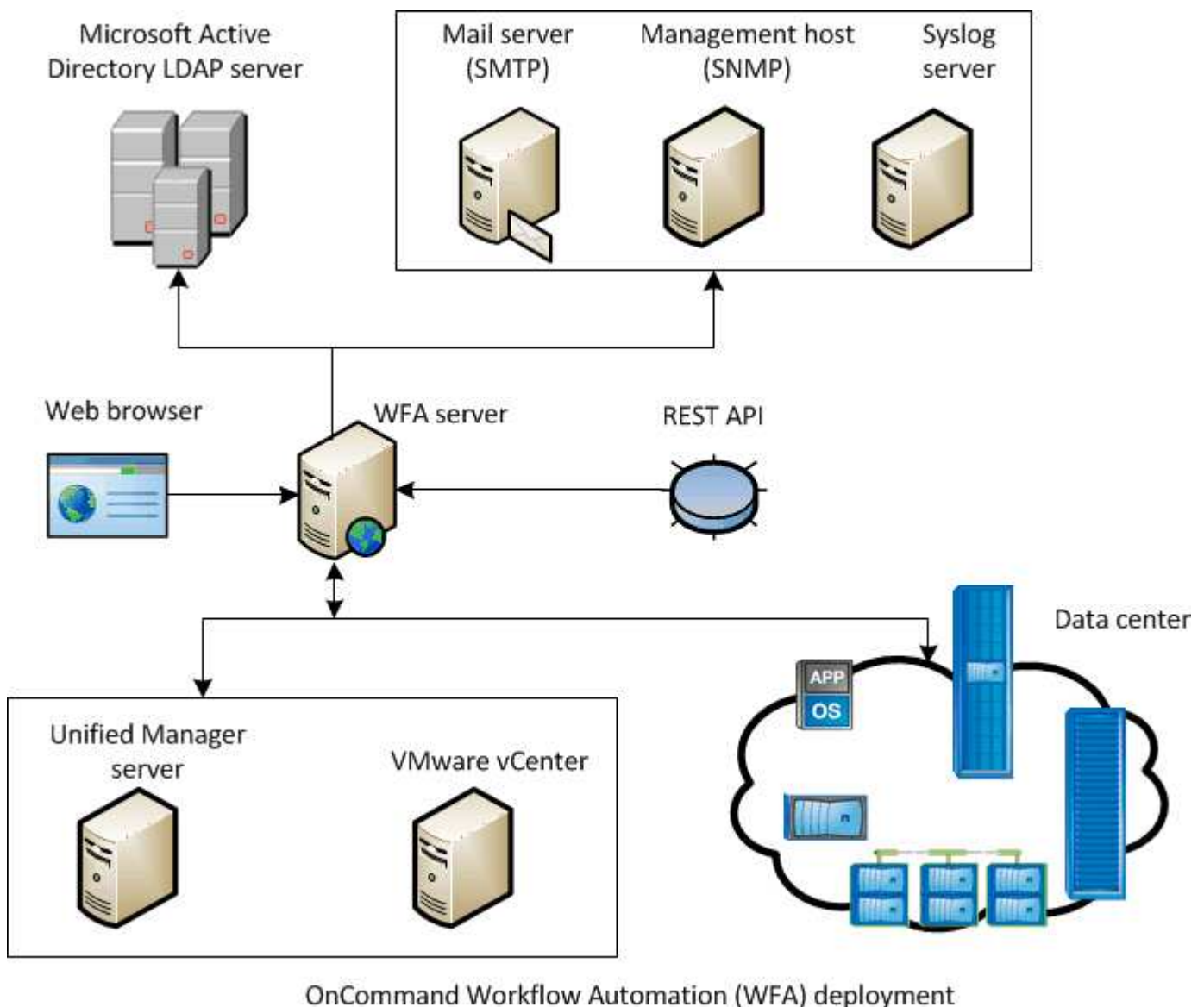
Für die Verwendung des OnCommand Workflow Automation-Servers ist keine Lizenz erforderlich.

Implementierungsarchitektur von OnCommand Workflow Automation

OnCommand Workflow Automation (WFA) Server ist installiert, um den Workflow-Betrieb über mehrere Datacenter hinweg zu koordinieren.

Sie können Ihre Automatisierungsumgebung zentral managen, indem Sie Ihren WFA Server mit mehreren Active IQ Unified Manager-Implementierungen und VMware vCenters verbinden.

Die folgende Abbildung zeigt ein Bereitstellungsbeispiel:

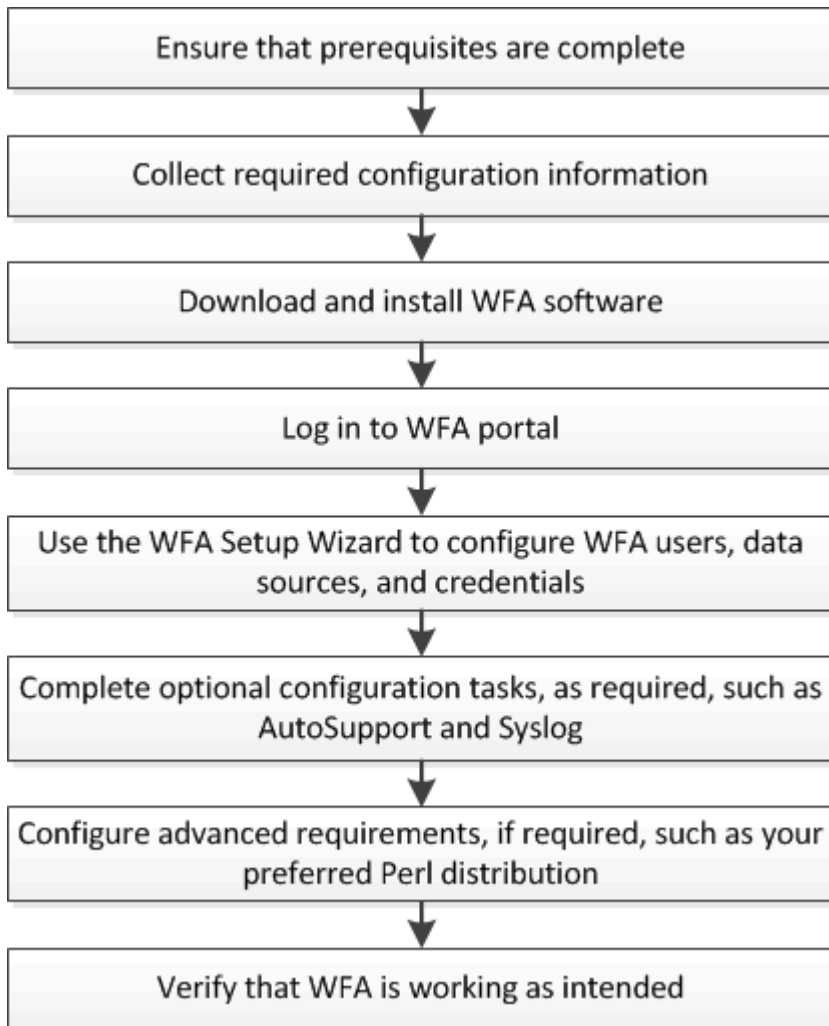


Übersicht über die OnCommand Workflow Automation-Installation und -Einrichtung

Bei der Installation von OnCommand Workflow Automation (WFA) werden beispielsweise

Aufgaben wie die Installationsvorbereitung, das WFA Installationsprogramm heruntergeladen und das Installationsprogramm ausgeführt. Nach Abschluss der Installation können Sie WFA Ihren Anforderungen konfigurieren.

Das folgende Flussdiagramm zeigt die Installations- und Konfigurationsaufgaben:



Bekannte Einschränkungen und Verbesserungen

OnCommand Workflow Automation (WFA) 5.1 umfasst einige Einschränkungen und nicht unterstützte Funktionen, auf die Sie vor dem Installieren und Konfigurieren von WFA achten sollten.

• Erstellen von Kategorienamen

- Wenn ein Bindestrich (-) in einem Kategorienamen verwendet wird, wird er nach dem Speichern der Kategorie durch ein Leerzeichen ersetzt. Wenn beispielsweise der Kategoriename "abc-xyz" angegeben wird, wird der Kategoriename als "abc xyz" gespeichert, wobei der Bindestrich entfernt wird. Um dieses Problem zu vermeiden, verwenden Sie keine Bindestriche in Kategorienamen.
- Wenn ein Doppelpunkt (:) in einem Kategorienamen verwendet wird, wird die Textzeichenfolge vor dem Doppelpunkt nach dem Speichern der Kategorie ignoriert. Wenn beispielsweise der Kategoriename "abc : xyz" angegeben wird, wird der Kategoriename als "xyz" gespeichert, wobei die "abc"-Zeichenfolge entfernt wird. Um dieses Problem zu vermeiden, verwenden Sie keine Doppelpunkte in

Kategorienamen.

- Es gibt keine Prüfung, um zu verhindern, dass zwei Kategorien denselben Namen haben. Dies führt jedoch zu einem Problem bei der Auswahl dieser Kategorien im Navigationsbereich. Um dieses Problem zu vermeiden, stellen Sie sicher, dass jeder Kategorienname eindeutig ist.

Systemanforderungen für die Installation von OnCommand Workflow Automation

Vor der Installation von WFA müssen Sie die Hardware- und Software-Anforderungen des OnCommand Workflow Automation (WFA) kennen.

Hardwareanforderungen für die Installation von WFA

In der folgenden Tabelle sind die Mindestanforderungen an die Hardware und die empfohlenen Hardwarespezifikationen für den WFA Server aufgeführt.

Komponente	Mindestanforderungen	Empfohlene Spezifikationen
CPU	2.27 GHz oder schneller, 4-Core, 64-Bit	2.27 GHz oder schneller, 4-Core, 64-Bit
RAM	4 GB	8 GB
Freier Speicherplatz	5 GB	20 GB

Wenn Sie WFA auf einer Virtual Machine (VM) installieren, sollten Sie den erforderlichen Arbeitsspeicher und die erforderliche CPU reservieren, damit die VM über ausreichende Ressourcen verfügt. Der Installer überprüft nicht die CPU-Geschwindigkeit.

Softwareanforderungen für die Installation von WFA

WFA ist auf einem 64-Bit Windows Betriebssystem ausgeführt und sollte auf dedizierten physischen Computern oder VMs installiert werden. Sie dürfen keine anderen Anwendungen auf dem Server installieren, auf dem WFA ausgeführt wird.

WFA läuft von Microsoft Windows Server 2012 Enterprise Edition zu Microsoft Windows Server 2016 (alle Editionen). Enterprise Edition ist das empfohlene Windows-Betriebssystem.

Für Windows 2012-Server muss .NET Framework Version 4.5.2 auf Ihrem Windows-System installiert sein. Wenn .NET Framework Version 4.5.2 nicht installiert ist, schlägt die Installation von WFA 5.1 fehl.

- Einer der folgenden unterstützten Browser:
 - Mozilla Firefox
 - Microsoft Internet Explorer
 - Google Chrome
- PowerShell 3.0
- VMware PowerCLI Version 5



Die PowerShell Extension für VMware APIs ist nur erforderlich, wenn Sie WFA zur Ausführung von Workflows auf VMware vSphere verwenden.



Antiviren-Applikationen verhindern möglicherweise, dass WFA Services gestartet werden.

Um dieses Problem zu vermeiden, konfigurieren Sie die Ausschlüsse für Virenschutzprüfungen für die folgenden WFA Verzeichnisse:

- Das Verzeichnis, in dem WFA installiert ist
- Das Verzeichnis, in dem Sie Perl installiert haben
- Das Verzeichnis, in dem Sie OpenJDK installiert haben
- Das MySQL-Datenverzeichnis

Weitere Informationen finden Sie im Interoperabilitäts-Matrix-Tool.

Verwandte Informationen

["NetApp Interoperabilitäts-Matrix-Tool"](#)

Für Workflow Automation erforderliche Ports

Wenn Sie eine Firewall verwenden, müssen Sie die erforderlichen Ports für Workflow Automation (WFA) kennen.

In diesem Abschnitt werden die Standard-Port-Nummern aufgeführt. Wenn Sie eine nicht standardmäßige Portnummer verwenden möchten, müssen Sie diesen Port zur Kommunikation öffnen. Weitere Informationen finden Sie in der Dokumentation zu Ihrer Firewall.

In der folgenden Tabelle sind die Standard-Ports aufgeführt, die auf dem WFA Server geöffnet sein sollen:

Port	Protokoll	Richtung	Zweck
80, 443	HTTP, HTTPS	Eingehend	WFA öffnen und sich anmelden
80, 443, 22	HTTP, HTTPS, SSH	Ausgehend	Befehlsausführung (ZAPI, PowerCLI)
445, 139, 389, 636	Microsoft-DS, NetBIOS-ssn, AD LDAP, AD LDAPS	Ausgehend	Microsoft Active Directory LDAP-Authentifizierung
161	SNMP	Ausgehend	Senden von SNMP-Meldungen zum Status von Workflows
3306	MySQL	Eingehend	Caching von schreibgeschützten Benutzern

Port	Protokoll	Richtung	Zweck
25	SMTP	Ausgehend	E-Mail-Benachrichtigung
80, 443, 25	HTTP, HTTPS, SMTP	Ausgehend	Senden von AutoSupport Meldungen
514	Syslog	Ausgehend	Senden von Protokollen an einen Syslog-Server

In der folgenden Tabelle sind die Standardports aufgeführt, die auf dem Unified Manager-Server geöffnet werden sollen:

Port	Protokoll	Richtung	Zweck
3306	MySQL	Eingehend	Caching von Daten aus Active IQ Unified Manager 6.0 und höher

In der folgenden Tabelle ist der Standardport aufgeführt, der auf VMware vCenter geöffnet werden soll:

Port	Protokoll	Richtung	Zweck
443	HTTPS	Eingehend	Caching von Daten aus VMware vCenter

In der folgenden Tabelle ist der Standardport aufgeführt, der auf dem SNMP-Hostcomputer geöffnet sein soll:

Port	Protokoll	Richtung	Zweck
162	SNMP	Eingehend	Empfangen von SNMP-Meldungen zum Status von Workflows

Voraussetzungen für die Installation von Workflow Automation

Vor der Installation von OnCommand Workflow Automation (WFA) müssen Sie sicherstellen, dass Sie über die erforderlichen Informationen verfügen und bestimmte Aufgaben abgeschlossen haben.

Bevor Sie WFA auf einem System installieren, müssen Sie die folgenden Aufgaben ausführen:

- Laden Sie die WFA Installationsdatei von der NetApp Support Site herunter und kopieren Sie die Datei auf den Server, auf dem WFA installiert werden soll



Zur Anmeldung auf der NetApp Support Site müssen Sie über gültige Zugangsdaten verfügen. Wenn Sie keine gültigen Zugangsdaten besitzen, können Sie sich auf der NetApp Support Site registrieren, um damit die entsprechenden Anmeldedaten zu erhalten.



- Überprüfen, ob das System ggf. Zugriff auf die folgenden Ressourcen hat:
 - Storage Controller
 - Active IQ Unified Manager
 - VMware vCenter




Wenn in Ihrer Umgebung der Zugriff auf Secure Shell (SSH) erforderlich ist, müssen Sie sicherstellen, dass SSH auf den Ziel-Controllern aktiviert ist.

- Es wird sichergestellt, dass PowerShell 3.0 oder höher installiert wird
- Sicherstellen, dass VMware Power CLI installiert ist, wenn Sie WFA zur Ausführung von Workflows auf VMware vSphere verwenden
- Erfassen der erforderlichen Konfigurationsinformationen
- Stellen Sie sicher, dass der MySQL .Net-Anschluss installiert ist, wenn Sie das Cmdlet "Invoke-MysqlQuery" verwenden

Erforderliche Konfigurationsinformationen

Einheit oder System	Details	Zweck
Arrays	<ul style="list-style-type: none">• IP-Adresse• Benutzername und Passwort	<p>Betrieb auf Storage-Systemen durchführen</p> <div><p>Anmeldedaten für das Root- oder Admin-Konto sind für den Speicher (Arrays) erforderlich.</p></div>
VSphere	<ul style="list-style-type: none">• IP-Adresse• Benutzername und Passwort eines Administrators für vCenter Server	<p>Erwerben von Daten, die mittels VMware-APIs ausgeführt werden</p> <div><p>Sie müssen VMware Power CLI installiert haben.</p></div>
Externe Repositorys wie OnCommand Balance und benutzerdefinierte Datenbanken	<ul style="list-style-type: none">• IP-Adresse• Benutzername und Passwort eines schreibgeschützten Benutzerkontos	<p>Anforderung Sie müssen die relevanten WFA Inhalte wie beispielsweise Wörterbucheinträge und Cacheabfragen für die externen Repositorys erstellen, um Daten aus den externen Repositorys zu erhalten.</p>

Einheit oder System	Details	Zweck
Mailserver	<ul style="list-style-type: none"> • IP-Adresse • Benutzername und Passwort <div>  <p>Benutzername und Passwort sind erforderlich, wenn Ihr Mailserver eine Authentifizierung erfordert.</p> </div>	WFA Benachrichtigungen erhalten Sie per E-Mail
AutoSupport Server	<ul style="list-style-type: none"> • Mail-Host 	Senden von AutoSupport-Meldungen über SMTP Falls Sie keinen E-Mail-Host konfiguriert haben, können Sie HTTP oder HTTPS zum Senden von AutoSupport-Meldungen verwenden.
Microsoft Active Directory (AD) LDAP-Server	<ul style="list-style-type: none"> • IP-Adresse • Benutzername und Passwort • Gruppenname 	Authentifizieren und autorisieren Sie mit AD-LDAP oder AD-LDAPS
SNMP-Managementapplikation	<ul style="list-style-type: none"> • IP-Adresse • Port 	WFA SNMP-Benachrichtigungen erhalten
Syslog-Server	<ul style="list-style-type: none"> • IP-Adresse 	Protokolldaten senden

Verwandte Informationen

["NetApp Support"](#)

Management von Hochverfügbarkeit

Sie können eine Hochverfügbarkeitskonfiguration konfigurieren, um Netzwerkvorgänge ständig zu unterstützen. Wenn eine der Komponenten ausfällt, übernimmt die gespiegelte Komponente in der Einrichtung den Betrieb und stellt unterbrechungsfreie Netzwerkressourcen bereit. Sie können auch ein Backup der WFA Datenbank und der unterstützten Konfigurationen erstellen, damit Sie die Daten bei einem Notfall wiederherstellen können.

Einrichtung von Workflow Automation in MSCS für hohe Verfügbarkeit

Sie können Workflow Automation (WFA) in einer Microsoft Cluster Service (MSCS) Umgebung installieren und konfigurieren, um Hochverfügbarkeit bereitzustellen und Failover bereitzustellen. Vor der Installation von WFA müssen Sie überprüfen, ob alle

erforderlichen Komponenten korrekt konfiguriert sind.

Ein hochverfügbares Setup unterstützt ständig die Applikationsprozesse. Wenn eine der Komponenten ausfällt, übernimmt die gespiegelte Komponente im Setup den Betrieb und stellt unterbrechungsfreie Netzwerkressourcen bereit.



MSCS ist die einzige Clustering-Lösung, die von WFA in Windows unterstützt wird.

Konfigurieren Sie MSCS zur Installation von Workflow Automation

Bevor Sie Workflow Automation (WFA) in Microsoft Cluster Server (MSCS) installieren, müssen Sie Ihre MSCS Umgebung konfigurieren.

- MSCS muss vom Servermanager installiert werden.
- Optional: SnapDrive für Windows muss installiert sein.

Die unterstützte Mindestversion ist Windows 2012.

- Dieselbe Version von WFA muss auf beiden Cluster-Nodes über denselben Pfad installiert werden.
- Beide Cluster-Knoten müssen der gleichen Domäne hinzugefügt werden.

Sie müssen diese Aufgabe mithilfe von Cluster Manager in der MSCS-Schnittstelle durchführen.

Schritte

1. Loggen Sie sich als Domänenadministrator bei Cluster Manager ein.
2. Stellen Sie mithilfe einer der folgenden Optionen sicher, dass auf die LUNs für beide Nodes zugegriffen werden kann:
 - Natives Verwalten der LUNs
 - Durch Verwendung von SnapDrive für Windows:
 - i. Installieren und konfigurieren Sie SnapDrive für Windows auf beiden Knoten.
 - ii. Erstellen Sie eine LUN mit SnapDrive für Windows, und konfigurieren Sie die LUN für beide Nodes.
3. Fügen Sie im Failover Cluster Manager die Festplatte dem Cluster hinzu.

Installieren Sie OnCommand Workflow Automation unter Windows

Sie können OnCommand Workflow Automation (WFA) installieren, um Storage-Workflows zu erstellen und anzupassen und um die in Ihrer Umgebung ausgeführten Storage-Aufgaben zu automatisieren.

- Sie müssen die Installationsvoraussetzungen überprüft haben.

Voraussetzungen für die Installation von Workflow Automation

- Wenn Sie WFA auf einem System installieren, auf dem WFA bereits installiert und dann deinstalliert wurde, müssen Sie sicherstellen, dass keine WFA Services auf diesem System vorhanden sind.
- Sie müssen das WFA Installationsprogramm von der NetApp Support Site heruntergeladen haben.
- Wenn Sie WFA auf einer virtuellen Maschine (VM) installieren, darf der Name der VM nicht das Unterstrich (_) Zeichen enthalten.

- ActiveState ActivePerl ist vor der Installation von WFA installiert.

Diese Installation hat keine Auswirkung auf andere Instanzen von ActivePerl, die Sie auf Ihrem WFA Server installiert haben.

- Bevor Sie WFA 4.2 oder höher neu installieren, müssen Sie das MySQL-Datenverzeichnis löschen, wenn Sie MySQL deinstalliert haben.

Schritte

1. Melden Sie sich unter Windows mit einem Konto mit Administratorberechtigungen an.
2. Öffnen Sie den Windows Explorer, und navigieren Sie dann zum Verzeichnis, in dem sich die Installationsdatei befindet.
3. WFA installieren:
 - Interaktive Installation
 - i. Klicken Sie mit der rechten Maustaste, und führen Sie die ausführbare Datei des WFA Installer (.exe) als Admin-Benutzer aus.
 - ii. Klicken Sie Auf **Weiter**.
 - iii. Geben Sie die Anmeldeinformationen für den Standard-Admin-Benutzer ein, und klicken Sie dann auf **Weiter**.

Das standardmäßige Admin-Passwort muss die folgenden Kriterien erfüllen:

- Mindestens acht Zeichen
- Ein Großbuchstaben
- Ein Kleinbuchstaben
- Eine Ziffer
- Ein Sonderzeichen
- Die folgenden Sonderzeichen werden in einem Kennwort nicht unterstützt und führen zu Installationsfehlern:

`" ; < > , = & ^



Sie müssen die Anmeldedaten des Admin-Benutzers notieren.

- iv. Geben Sie einen Benutzernamen und ein Kennwort für die WFA-Dienstanmeldung ein. Für einen Domänenbenutzer geben Sie einen Benutzernamen im Format DOMAIN\USER an. Bei einem lokalen Systembenutzer ist das Format nur ein Benutzername. Der Standardbenutzername ist „wfa“.

Der WFA Installer erstellt einen lokalen Benutzer, wenn er nicht vorhanden ist. Wenn ein lokaler Benutzer existiert und das eingegebene Passwort sich von dem vorhandenen Passwort unterscheidet, aktualisiert WFA das Passwort.



Stellen Sie sicher, dass das Passwort der Kennwortrichtlinie entspricht, die für lokale Benutzer im System konfiguriert wurde. Wenn das Passwort nicht der Passwortrichtlinie entspricht, schlägt die Installation fehl.

- i. Wählen Sie die Ports für die WFA Konfiguration aus und klicken Sie dann auf **Weiter**.
- ii. Geben Sie einen Standortnamen und Ihren Firmennamen ein, und klicken Sie dann auf **Weiter**.

Der Standortname kann den Standort der WFA Installation enthalten, z. B. Pittsburgh, PA.

- iii. Wenn Sie den Standardinstallationsort ändern möchten, wählen Sie den Speicherort aus, an dem WFA installiert werden soll, und klicken Sie dann auf **Weiter**.
 - iv. Wenn Sie den Standard-Installationsort für Produkte von Drittanbietern ändern möchten, wählen Sie den Speicherort aus, an dem Sie Produkte von Drittanbietern installieren möchten, und klicken Sie dann auf **Weiter**.
 - v. Wenn Sie den Standardspeicherort der WFA-Datenbank nicht ändern möchten, klicken Sie auf **Weiter**.
 - vi. Klicken Sie auf **Installieren**, um mit der Installation fortzufahren.
 - vii. Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.
 - viii. Überprüfen Sie, ob WFA erfolgreich installiert wurde, indem Sie eine der folgenden Aktionen auswählen:
 - Zugriff auf WFA über einen Webbrowser
 - Überprüfen Sie mithilfe der Windows Services Konsole, ob der NetApp WFA Server Service und der NetApp WFA Database Service ausgeführt werden.
- Automatische Installation (über die Eingabeaufforderung):

```
WFA-version_number-build_number.exe /s
/v"WFA_ADMIN_USERNAME=wfa_username WFA_ADMIN_PASSWORD=password
WFA_ADMIN_CONFIRM_PASSWORD=confirm admin password /
WFA_MYSQL_PASS=password CONFIRM_WFA_MYSQL_PASS=confirm MySQL password
WFA_INSTALL_SITE=site WFA_INSTALL_ORGANIZATION=organization_name
WFA_HTTP_PORT=port WFA_HTTPS_PORT=port INSTALLDIR=install_directory
JDKINSTALLDIR=jdk_directory PerlDir=perl_directory
MySQLInstallDir=mysql_directory WFA_SERVICE_LOGON_USERNAME=wfa
service logon username WFA_SERVICE_LOGON_PASSWORD=wfa service logon
user password MYSQL_DATA_DIR= mysql data directory /qr /l*v
C:\install.log"
```

Beispiel


```
WFA-x64-V5.1.0.0.1-B5355278.exe /s /V„WFA_ADMIN_USERNAME=admin
WFA_ADMIN_PASSWORD=Unternehmen*123
WFA_ADMIN_CONFIRM_PASSWORD=Unternehmen*123 80 WFA_MYSQL_PASS=MySQL*123
BESTÄTIGEN_WFA_MYSQL_PASS=MySQL_PASS=123
WFA_INSTALL_SITE=NetApp_WFA_KNABENPROGRAMM\
WFA_443\WFA_MYSQL_Programm\WFA_Ilric\\ NetApp_Programm\WFA_Ilric\\\\ mitas_mitas\\\\
WFA_PROGRAMM\WFA_MITAS\\ WFA_MITAS\\WFA_1234\WFA_MITAS\WFA_WFA_MERG-
PROGRAMM\WFA_MITAS\ WFA_WFA_MWFA_MITAS WFA_WFA_NETAPP=
WFA_MWFA_MWFA_WFA_PROGRAMM WFA_MWFA_MWFA_MITAS
WFA_MWFA_MWFA_WFA_Programm
WFA_WFA_MWFA_MWFA_MWFA_MWFA_MWFA_MWFA_mitas
```



Die /qn Option wird von WFA nicht unterstützt.

Die Befehlsparameter sind wie folgt:

Parameter	Beschreibung
WFA_ADMIN_BENUTZERNAME	Admin-Benutzername Optionaler Parameter. Wenn Sie keinen Wert angeben, wird der Wert standardmäßig auf admin gesetzt.
WFA_ADMIN_PASSWORT	Passwort für Admin-Benutzer obligatorischer Parameter. Das standardmäßige Admin-Passwort muss die folgenden Kriterien erfüllen: <ul style="list-style-type: none">• Mindestens acht Zeichen• Ein Großbuchstaben• Ein Kleinbuchstaben• Eine Ziffer• Ein Sonderzeichen• Die folgenden Zeichen sind nicht zulässig und führen zum Fehlschlagen der Passwordeingabe: `" ; < > , = & ^
WFA_ADMIN_CONFIRM_PASSWORD	Passwort für Admin-Benutzer obligatorischer Parameter
WFA_MYSQL_PASS	MySQL-Benutzerpasswort obligatorischer Parameter
BESTÄTIGEN SIE_WFA_MYSQL_PASS	MySQL-Benutzerpasswort obligatorischer Parameter
WFA_INSTALL_SITE	Organisationseinheit, in der WFA installiert ist obligatorisch
WFA_INSTALL_ORGANISATION	Name des Unternehmens oder Unternehmens, in dem WFA installiert ist obligatorisch
WFA_HTTP_PORT	Optionaler HTTP-Port-Parameter. Wenn Sie keinen Wert angeben, wird der Wert standardmäßig auf 80 gesetzt.
WFA_HTTPS_PORT	Optionaler HTTPS-Port-Parameter. Wenn Sie keinen Wert angeben, wird der Wert standardmäßig auf 443 gesetzt.

Parameter	Beschreibung
INSTALLDIR	Installationverzeichnispfad Optionaler Parameter. Wenn Sie keinen Wert angeben, wird standardmäßig der Pfad „C:\Program Files\NetApp\WFA\“ verwendet.
JDKINSTALLDIR	Pfad des JDK-Installationsverzeichnisses Optionaler Parameter. Wenn Sie keinen Wert angeben, wird standardmäßig der Pfad „C:\Programme\NetApp\“ verwendet.
Stammverzeichnis	Perl-Installationspfad Optionaler Parameter. Wenn Sie keinen Wert angeben, wird der Pfad standardmäßig auf „C:\Perl64\“ gesetzt.
MySqlInstallDir	MySQL Installationsverzeichnis Pfad Optionaler Parameter. Wenn Sie keinen Wert angeben, wird der Pfad standardmäßig auf „C:\Programme\MySQL\“ gesetzt.
WFA_SERVICE_LOGIN_BENUTZERNAME	<p>Benutzername für WFA Service Logon Optionaler Parameter. Wenn Sie keinen Wert angeben, lautet der Standardbenutzername „wfa“.</p> <p>Für einen Domänenbenutzer geben Sie einen Benutzernamen im Format DOMAIN\USER an. Bei einem lokalen Systembenutzer ist das Format nur ein Benutzername.</p> <p>Der WFA Installer erstellt einen lokalen Benutzer, wenn er nicht vorhanden ist. Wenn ein lokaler Benutzer existiert und das eingegebene Passwort sich von dem vorhandenen Passwort unterscheidet, aktualisiert WFA das Passwort.</p> <div>  <p>Stellen Sie sicher, dass das Passwort der Kennwortrichtlinie entspricht, die für lokale Benutzer im System konfiguriert wurde. Wenn das Passwort nicht der Passwortrichtlinie entspricht, schlägt die Installation fehl.</p> </div>
WFA_SERVICE_LOGON_PASSWORD	Passwort für die Anmeldung des WFA-Dienstes obligatorisch

Parameter	Beschreibung
MYSQL_DATA_DIR	Verzeichnis für MYSQL-Daten Optionaler Parameter. Wenn Sie keinen Wert angeben, wird der Pfad standardmäßig auf „C:\ProgramData\MySQL\MySQLServerData“ gesetzt. Nur für Neuinstallation verfügbar.

Verwandte Informationen

["NetApp Support"](#)

Konfiguration der Workflow Automation mit MSCS

Nach der Installation von Workflow Automation (WFA) in Microsoft Cluster Server (MSCS) müssen Sie WFA mithilfe von Konfigurationsskripten für Hochverfügbarkeit in MSCS konfigurieren.

Sie müssen ein Backup von WFA erstellt haben.



Vergewissern Sie sich vor Beginn der Konfiguration, dass der WFA-Verschlüsselungsschlüssel auf beiden MSCS-Cluster-Knoten konsistent eingestellt ist. Wenn er nicht auf beiden Knoten festgelegt ist, können die Anmeldeinformationen nicht auf dem zweiten Knoten entschlüsselt werden, was zu Workflow-Ausfällen führt.

Schritte

1. Melden Sie sich beim ersten Node des MSCS-Clusters an, und führen Sie die folgenden Schritte aus:

Für...	Tun Sie das...
Windows 2012, Windows 2016, Windows 2019	<ol style="list-style-type: none"> a. Klicken Sie im Failover Cluster Manager mit der rechten Maustaste auf Service Roles. b. Wählen Sie Leere Service-Rolle erstellen aus, und benennen Sie die Rolle in „WFA“ um. c. Fügen Sie die IP-Adressressource zur neu erstellten „WFA“-Rolle hinzu: <ol style="list-style-type: none"> i. Klicken Sie im Failover Cluster Manager mit der rechten Maustaste auf die neu erstellte Rolle „WFA“. ii. Wählen Sie Ressource > Weitere Ressourcen > IP-Adresse. iii. Konfigurieren Sie die Cluster-IP-Adresse.

2. Bearbeiten Sie das `mscs_data_parameters.xml` Datei und legen Sie den relativen Pfad zum MySQL-Datenverzeichnis fest:


```
<dir>
  <description>Data directory</description>
  <srcpath>..\..\..\..\..\ProgramData\MySQL\MySQLServerData</srcpath>
  <destpath>wfa</destpath>
</dir>
```

3. Bearbeiten Sie das `mscs_resource_properties.xml` Datei und nehmen Sie folgende Aktualisierungen vor:

- Führen Sie einen Find/Replace für den aus `NA_WFA_DB` Servicename und aktualisieren Sie ihn in `MYSQL57`.
- Stellen Sie die ein `vip_res` `<prettyname>` So geben Sie den virtuellen IP-Adressennamen an:

```
<resource>
  <type>essential</type>
  <id>vip_res</id>
  <prettyname>WFA IP address</prettyname>
</resource>
```

- Stellen Sie die ein `data_res` `<prettyname>` Dem Festplattennamen, der der Ressource für die gemeinsame Festplatte zugewiesen ist:

```
<resource>
  <type>essential</type>
  <id>datadisk_res</id>
  <prettyname>Cluster Disk 2</prettyname>
</resource>
```

- Kopieren Sie die XML-Dateien vom ersten Knoten auf den zweiten Knoten:

```
copy "\\node1\D$\Program Files\NetApp\WFA\bin\ha\*.xml" "D:\Program
Files\NetApp\WFA\bin\ha"
```

- Führen Sie den Befehl aus, um dem zweiten Node dem Cluster beizutreten:

```
D:\Program Files\NetApp\WFA\bin\ha>perl ha_setup.pl --join -t mscs -f E:\
```

4. Führen Sie an der Eingabeaufforderung das `ha_setup.pl` Skript aus, um die WFA Daten an den gemeinsamen Speicherort zu verschieben und WFA für den Failover mit MSCS zu konfigurieren. Das Skript ist unter `WFA_install_location\WFA\bin\ha\` verfügbar.

```
perl ha_setup.pl --first [-t type_of_cluster_vcs] [-g cluster_group_name] [-i
IP_address_name] [-n cluster_name] [-k shared_disk_resource_name] [-f
shared_drive_path]
```

Das Skript `ha_setup.pl` erwartet einen Input unter Verwendung der IP-Adressressource für den MSCS-

Cluster. Bei der Installation auf MSCS 2016 muss die Ressource mit dem Namen und nicht mit der IP-Adresse hinzugefügt werden. WFA IP address. Beispiel:

```
perl ha_setup.pl --first -t mscs -g WFA -i "WFA IP address" -n wfa_cluster -k "Cluster Disk 2" -f E:\
```

5. Überprüfen Sie, ob die MSCS-Ressourcen erstellt werden, indem Sie auf die erfolgreich konfigurierte Meldung in der Ausgabe überprüfen.

Successfully configured MSCS cluster resources on this node

6. Stoppen Sie die WFA Services vom Failover Cluster Manager:

Für...	Tun Sie das...
Windows 2012, Windows 2016, Windows 2019	<p>a. Wählen Sie Service-Rollen aus, und wählen Sie dann die neu erstellte „WFA“-Rolle aus.</p> <p>b. Klicken Sie im Ressourcenfenster mit der rechten Maustaste auf MYSQL57 und wählen Sie dann Offline nehmen aus.</p> <p>c. Klicken Sie im Bereich Ressourcen mit der rechten Maustaste auf NA_WFA_SRV, und wählen Sie dann Offline nehmen aus.</p>

Der WFA Datenbankservice und der WFA Serverservice müssen offline geschaltet werden. WFA Services dürfen nicht aus den Windows Services angehalten werden.

1. Verschieben Sie WFA Ressourcen manuell zum sekundären Node.
2. Vergewissern Sie sich, dass vom zweiten Node auf die freigegebene Festplatte zugegriffen werden kann.
3. Führen Sie an der Eingabeaufforderung das Skript ha_setup.pl auf dem sekundären Node des Clusters aus, um WFA zur Verwendung der Daten vom gemeinsam genutzten Speicherort zu konfigurieren:

```
perl ha_setup.pl --join [-t type_of_cluster_mscs] [-f shared_drive_path]
```

Das Skript ha_setup.pl ist unter WFA_install_location\WFA\bin\ha\ verfügbar.

```
perl ha_setup.pl --join -t mscs -f E:\
```

4. Stellen Sie im Failover Cluster Manager die WFA Ressourcen online:

Für...	Tun Sie das...
Windows 2012, Windows 2016, Windows 2019	<p>a. Klicken Sie mit der rechten Maustaste auf die neu erstellte „WFA“-Rolle, und wählen Sie dann Start-Rolle aus. Die Rolle muss sich im Status „läuft“ befinden, und die einzelnen Ressourcen müssen sich im Status „Online“ befinden.</p>

5. Manuelles Umschalten auf den zweiten Knoten des MSCS-Clusters.
6. Überprüfen Sie, ob die WFA Services auf dem zweiten Node des Clusters ordnungsgemäß starten.

Konfigurieren Sie frühere OnCommand Workflow Automation-Versionen, um Hochverfügbarkeit zu erzielen

Sie können OnCommand Workflow Automation (WFA) Versionen vor 3.1 konfigurieren, um Hochverfügbarkeit zu erhalten.

Schritte

1. Aktualisieren Sie die bestehende Version von WFA auf die neueste verfügbare Version von WFA.

Upgrade von WFA

Diese aktualisierte Version von WFA ist der primäre Node des Clusters.

2. Erstellen eines Backups der WFA Datenbank.

"Backup der WFA Datenbank"

Wenn einer der Parameter manuell geändert wurde, müssen Sie ein Backup der WFA Datenbank erstellen, die bestehende WFA Installation deinstallieren, die neueste verfügbare Version von WFA installieren, das Backup wiederherstellen und dann mit der Microsoft Cluster Service (MSCS) Konfiguration fortfahren.

3. Konfigurieren Sie MSCS zur Installation von WFA auf dem primären Node.

"Konfigurieren Sie MSCS zur Installation von WFA"

4. Installieren Sie die neueste verfügbare Version von WFA auf dem sekundären Node.

"WFA installieren"

5. Konfigurieren Sie WFA in MSCS.

"Konfigurieren Sie WFA in MSCS"

Der WFA Server ist für Hochverfügbarkeit konfiguriert.

Deinstallieren Sie Workflow Automation in einer MSCS-Umgebung

Sie können Workflow Automation (WFA) von einem Cluster deinstallieren, indem Sie alle WFA Services von den Cluster-Nodes löschen.

Diese Aufgabe gilt für Windows Server 2012.

Schritte

1. Versetzen Sie die Dienste mit Failover Cluster Manager in den Offline-Modus:
 - a. Klicken Sie mit der rechten Maustaste auf die Rolle.
 - b. Wählen Sie **Rolle Stoppen**.
2. Deinstallieren Sie WFA auf dem ersten Node und deinstallieren Sie WFA auf dem zweiten Node.

"Deinstallieren Sie OnCommand Workflow Automation"

3. Löschen Sie die Cluster-Ressourcen aus Failover Cluster Manager:
 - a. Klicken Sie mit der rechten Maustaste auf die Rolle.
 - b. Wählen Sie **Entfernen**.
4. Löschen Sie die Daten manuell am freigegebenen Speicherort.

Sichern Sie die OnCommand Workflow Automation-Datenbank und -Konfigurationen unter Windows und stellen Sie sie wieder her

Sie können eine Backup- und Restore-Erstellung für die OnCommand Workflow Automation (WFA) Datenbank und unterstützte Konfigurationen erstellen, damit Sie die Daten bei einem Ausfall wiederherstellen können. Zu den unterstützten Konfigurationen gehören Datenzugriff, HTTP Timeout und SSL-Zertifikate.

Sie müssen über Administratorrechte oder Anmeldedaten zum Erstellen verfügen.

Sie müssen das Backup an einem sicheren Ort erstellen, da die Wiederherstellung des Backups Zugriff auf alle Storage-Systeme bietet, auf die WFA zugegriffen hat.



Im Disaster Recovery können nur die CLI-Befehle oder REST-APIs für umfassende Backup- und Restore-Vorgänge verwendet werden. Die Web-Benutzeroberfläche kann nicht zum Erstellen eines Backups während der Disaster Recovery in einer Umgebung mit hoher Verfügbarkeit verwendet werden.

Schritte

1. Backup der bestehenden Datenbanken und Konfigurationen

"Backup der OnCommand Workflow Automation-Datenbank"

2. Stellen Sie ein vorheriges Backup Ihrer Datenbanken und Konfigurationen wieder her.

"Wiederherstellen der OnCommand Workflow Automation-Datenbank"

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 Datenquellentypen bereitgestellt. Sie müssen die vordefinierten Datenquellentypen kennen, bevor Sie die Datenquellen für die Datenerfassung einrichten.

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

Weitere Informationen zu den vordefinierten Datenquellentypen 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 Datenquellentypen 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 Datenquellentyps 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	<p>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 <i>OnCommand Unified Manager</i>.</p> <div><p>Sie dürfen die Anmeldeinformationen eines Active IQ Unified Manager-Datenbankbenutzerkontos, das mit der Befehlszeilenschnittstelle oder dem ocsetup-Tool erstellt wurde, nicht bereitstellen.</p></div>
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 Datenquellentyps 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 Datenquellentyp 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	<p>Speichern Sie die Anmeldeinformationen, und wählen Sie eine der folgenden Optionen:</p> <ul style="list-style-type: none"> • 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 **Versions** 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	<ol style="list-style-type: none">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	<ol style="list-style-type: none">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;whitespaceChar=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	<code>.\wfa --db-access=public --restart</code>
Deaktivieren des Remote-Zugriffs	<code>.\wfa --db-access=default --restart</code>

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"/>

```

Upgrade von OnCommand Workflow Automation

Wenn Sie eine ältere Version von OnCommand Workflow Automation (WFA) installiert haben, können Sie ein Upgrade auf die aktuelle Version von WFA durchführen, um die neuen Funktionen und Verbesserungen zu nutzen.

- Sie können nur von WFA 5.0 oder 4.2 ein Upgrade auf WFA 5.1 durchführen.

Wenn WFA 4.1 oder ältere Versionen von WFA ausgeführt werden, müssen Sie zuerst ein Upgrade auf WFA 5.0 oder 4.2 durchführen und dann auf WFA 5.1 upgraden.

- Sie können ein Backup von WFA 5.0 oder 4.2 unter WFA 5.1 wiederherstellen. Ein Backup von WFA Datenbanken kann nur auf einem System wiederhergestellt werden, auf dem dieselbe oder eine höhere Version von WFA ausgeführt wird.

Wenn Sie beispielsweise ein Backup auf einem System erstellt haben, auf dem WFA 4.2 ausgeführt wird, kann das Backup nur auf Systemen wiederhergestellt werden, auf denen WFA 4.2 oder höher ausgeführt wird.

- Sie können MySQL nicht eigenständig installieren, wenn Sie ein Upgrade von Versionen vor WFA 4.2 durchführen.

Sie können MySQL jedoch selbst installieren:

- Während einer Neuinstallation von WFA 4.2 und höher oder

- Wenn Sie ein Upgrade von WFA 4.2 auf neuere Versionen von WFA durchführen.
 - i. Sichern Sie die WFA Datenbank mit einer der folgenden Optionen:
- WFA Webportal
- PowerShell-Skript Wenn Sie dieselbe Version von WFA wiederherstellen möchten, können Sie das von Ihnen erstellte Backup zum Wiederherstellen der WFA-Datenbank verwenden.
 - i. Deinstallieren Sie die vorhandene Version von WFA.
 - ii. Installieren der neuesten Version von WFA
 - iii. WFA Datenbank wiederherstellen.

Sie können den wiederhergestellten Inhalt auf Vollständigkeit in der Funktionalität prüfen, z. B. können Sie die Funktion Ihrer benutzerdefinierten Workflows überprüfen.

Upgrade von OnCommand Workflow Automation 3.1 oder höheren Versionen

Sie können ein Upgrade von OnCommand Workflow Automation (WFA) 3.1 oder höheren Versionen auf die aktuellen Versionen von WFA durchführen, um die neuen Funktionen und Verbesserungen zu nutzen.

Sie müssen die .exe-Binärdatei von der NetApp Support Site auf die WFA Host Machine heruntergeladen haben.

Die WFA 5.1-Cluster-Verbindung muss das SSL-Zertifikat akzeptieren. Beim Update von einer früheren Version von WFA auf WFA 5.1 müssen Sie die Cluster-Verbindung zertifizieren. Speichern Sie nach dem vorhandenen Upgrade die Cluster-Verbindungsdetails für die Cluster-Zertifizierung.

Sie können MySQL beim Upgrade von älteren WFA Versionen nicht eigenständig installieren. Sie können MySQL jedoch selbst installieren:

- Während einer Neuinstallation von WFA 4.2 und höher oder
- Wenn Sie ein Upgrade von WFA 4.2 auf neuere Versionen von WFA durchführen.

Schritt

1. Upgrade von WFA 3.1 oder höheren Versionen durch Auswahl einer der folgenden Methoden:

- Interaktive Installation
 - i. Navigieren Sie zur .exe-Binärdatei auf dem WFA-Hostcomputer und führen Sie die Datei aus.
 - ii. Befolgen Sie die Anweisungen auf dem Bildschirm im Assistenten, um die Aktualisierung abzuschließen.
- Automatische Installation

Geben Sie an der Eingabeaufforderung Folgendes ein:

```
WFA-version_number-build_number.exe /s /v"WFA_ADMIN_USERNAME_UP=wfa username
WFA_ADMIN_PASSWORD_UP=password /qr /l*v C:\upgrade.log"
```

▪ Beispiel*:

```
WFA-x64-v4.2.0.0.0-B2973881.exe /s /v"WFA_ADMIN_USERNAME_UP=admin
WFA_ADMIN_PASSWORD_UP=password*123 /qr /l*v C:\upgrade.log"
```



Die /qn Option wird von WFA nicht unterstützt.

Wenn Sie ein unbeaufsichtigte Upgrade durchführen möchten, müssen Sie Werte für alle Befehlsparameter enthalten:

- WFA_ADMIN_USERNAME_UP ist der Benutzername eines WFA Benutzers, der über die Berechtigung zum Erstellen eines WFA Datenbank-Backups verfügt.
- WFA_ADMIN_PASSWORD_UP ist das Passwort des Benutzers.

Pack-Identifizierung während des Upgrades

Während des Upgrade-Prozesses identifiziert und klassifiziert OnCommand Workflow Automation (WFA) die Einheiten in ein Paket. Wenn Sie eine Einheit eines Pakets vor dem Upgrade gelöscht haben, wird das Paket während des Upgrades nicht identifiziert.

Während des Upgrades vergleicht WFA die Pakete in der Datenbank mit der Liste der im Storage Automation Store veröffentlichten Pakete, um die vor dem Upgrade installierten Pakete zu identifizieren. Die Pack-Identifizierung klassifiziert somit vorhandene Packungen in der Datenbank.

WFA führt die folgenden Prozesse zur Identifizierung und Klassifizierung von Paketen durch:

- Unterhält eine Liste der im Storage Automation Store freigegebenen Pakete, um die vor dem Upgrade installierten Pakete zu vergleichen und zu identifizieren.
- Klassifiziert die Einheiten in einem Paket als Teil der Synchronisierung des Storage Automation Store, wenn Storage Automation Store aktiviert ist.
- Klassifiziert die Einheiten in Packungen unter Verwendung der aktualisierten Liste.

Die Identifikation von Packs ist nur für von NetApp zertifizierte Pakete anwendbar, die im Storage Automation Store heruntergeladen wurden.

Wenn ein Paket während des Upgrades nicht erkannt wird, können Sie es erneut importieren, um es in WFA zu identifizieren. Die wfa.log Dateien enthalten Details zu den Einheiten, die während des Upgrades nicht als Paket identifiziert wurden.

Upgrade von Drittanbieterprodukten

Kunden können ein Upgrade von Drittanbieterprodukten auf OnCommand Workflow Automation (WFA) wie OpenJDK, MySQL und ActiveState Perl in Windows durchführen. Bei Produkten von Drittanbietern wie Open JDK, MYSQL usw. werden Sicherheitslücken aufweisen. Mit dieser Version von WFA können Sie nun selbstständig Upgrades für Drittanbieterprodukte durchführen.

Upgrade von OpenJDK

Oracle JRE wird nicht mehr in OnCommand Workflow Automation unterstützt. In dieser Version ersetzt OpenJDK Oracle JRE für Windows. Neue Versionen von OpenJDK for OnCommand Workflow Automation (WFA) können auf dem Windows-Server aktualisiert werden. Sie können ein Upgrade auf eine neuere Version von OpenJDK durchführen, um auf dem Windows-Server Sicherheitslücken zu finden.

Sie müssen auf dem WFA Server über Windows-Administratorrechte verfügen.

Sie können OpenJDK-Versionen innerhalb von Versionsfamilien aktualisieren. Sie können beispielsweise ein Upgrade von OpenJDK 11.0.1 auf OpenJDK 11.0 durchführen, aber Sie können nicht direkt von OpenJDK 11 auf OpenJDK 12 aktualisieren.

Schritte

1. Melden Sie sich als Admin-Benutzer auf der WFA Host Machine an.
2. Laden Sie die neueste Version von OpenJDK 11 (64-Bit) auf das Zielsystem herunter.
3. Verwenden Sie die Windows Services-Konsole, um den WFA-Server und die WFA-Datenbankdienste zu beenden.
4. Extrahieren Sie die heruntergeladene Version von OpenJDK 11 in den Ordner, in dem Sie JDK installiert haben.
5. Verwenden Sie die Windows Services-Konsole, um die WFA-Services zu starten.

MySQL aktualisieren

Sie können neue Versionen von MySQL für OnCommand Workflow Automation (WFA) auf dem Windows Server aktualisieren. Sie können ein Upgrade auf eine neuere Version von MySQL durchführen, um auf dem Windows-Server Sicherheitslücken zu finden.

Sie müssen über die Administratorrechte für Windows und das Passwort für DEN MYSQL Root-Benutzer auf dem WFA Server verfügen.



Vor der Neuinstallation von WFA 4.2 oder neuer müssen Sie das MySQL-Datenverzeichnis gelöscht haben, wenn Sie MySQL deinstalliert haben.

Sie sollten die folgenden Einschränkungen beachten:

- Sie können ein Upgrade in einer beliebigen Version von MySQL 5.7 durchführen.
Sie können beispielsweise ein Upgrade von MySQL 5.7.1 auf MySQL 5.7 durchführen.
- Sie können kein Upgrade von MySQL 5.7 auf MySQL 5.8 durchführen

Schritte

1. Melden Sie sich als Admin-Benutzer auf der WFA Host Machine an.
2. Laden Sie die entsprechende Version von MySQL auf das Zielsystem herunter.
3. Verwenden Sie die Windows Services-Konsole, um die folgenden WFA-Services zu beenden:
 - NetApp WFA Database oder MYSQL57
 - NetApp WFA Server
4. Klicken Sie auf DAS MYSQL msi Paket, um das Upgrade von MySQL aufzurufen.
5. Befolgen Sie die Anweisungen auf dem Bildschirm, um die MySQL-Installation abzuschließen.
6. Starten Sie die WFA Services über die Windows Services Konsole.

ActiveState Perl aktualisieren

OnCommand Workflow Automation (WFA) arbeitet mit der Enterprise Edition von ActiveState Perl unter Windows. Sie können ein Upgrade auf eine neuere Version von ActiveState Perl durchführen, um auf dem Windows-Server die Behebung von Sicherheitsschwachstellen zu erhalten.

Sie müssen auf dem WFA Server über Windows-Administratorrechte verfügen. ActiveState Perl unterstützt keine Upgrades von "in-Place".

WFA 5.1 nutzt die Enterprise Edition von ActiveState Perl.

Sie können ein Upgrade von ActiveState Perl 5.26.3 auf spätere Builds durchführen. Sie können kein Upgrade auf eine Hauptversion von ActiveState Perl durchführen.

Schritte

1. Melden Sie sich als Admin-Benutzer auf der WFA Host Machine an.
2. Laden Sie die aktuelle Version von 64-Bit ActiveState Enterprise Edition 5.26.3 auf das Zielsystem herunter.
3. Verwenden Sie die Windows Services-Konsole, um die folgenden WFA-Services zu beenden:
 - WFA Database oder MYSQL57
 - WFA Server
4. Deinstallieren Sie die aktuelle Version von ActiveState Perl auf dem Zielsystem über das Bedienfeld.
5. Führen Sie eine Sicherung des Ordners C:\Perl64\Site\lib durch.
6. Installieren Sie die neue ActiveState Enterprise Edition auf dem Zielcomputer.
7. Stellen Sie den Ordner \Site\lib von ActiveState Enterprise Edition wieder her, dessen Backup Sie in Schritt 5 erstellt haben.
8. Starten Sie die WFA Services über die Windows Services Konsole neu.

Backup der OnCommand Workflow Automation-Datenbank

Ein Backup der OnCommand Workflow Automation Datenbank (WFA) umfasst die Systemkonfigurationseinstellungen und Cacheinformationen, einschließlich der Playground-Datenbank. Sie können das Backup für Wiederherstellungszwecke auf demselben System oder auf einem anderen System verwenden.

Ein automatisches Backup der Datenbank wird täglich um 2 Uhr erstellt. Sie wird als ZIP-Datei an folgendem Speicherort gespeichert: `wfa_install_location\WFA-Backups`.

WFA speichert bis zu fünf Backups im WFA-Backup-Verzeichnis und ersetzt das älteste Backup durch das neueste Backup. Das Verzeichnis WFA-Backups wird bei der Deinstallation von WFA nicht gelöscht. Sie können das automatisch erstellte Backup zur Wiederherstellung verwenden, wenn Sie kein Backup der WFA Datenbank erstellt haben, während Sie WFA deinstallieren.

Sie können die WFA-Datenbank auch manuell sichern, wenn Sie spezifische Änderungen für die Wiederherstellung speichern müssen, beispielsweise wenn Sie vor dem automatischen Backup die von Ihnen vorgenommenen Änderungen sichern möchten.



- Sie können ein Backup einer WFA Datenbank nur auf einem System wiederherstellen, auf dem dieselbe oder eine höhere Version von WFA ausgeführt wird.

Wenn Sie beispielsweise ein Backup auf einem System erstellt haben, auf dem WFA 4.2 ausgeführt wird, kann das Backup nur auf Systemen wiederhergestellt werden, auf denen WFA 4.2 oder höher ausgeführt wird.

- Es ist nicht möglich, das Backup der WFA Datenbank während einer Disaster Recovery in einer Hochverfügbarkeitseinrichtung über die Web-Benutzeroberfläche zu verwenden.

Backup und Wiederherstellung der Benutzeranmeldeinformationen

Zum Backup der WFA Datenbank sind die WFA Benutzeranmeldeinformationen enthalten.



Die WFA Datenbank ist ebenfalls in den AutoSupport-Daten enthalten, das Passwort eines WFA Benutzers ist jedoch nicht in den AutoSupport-Daten enthalten.

Wenn eine WFA Datenbank aus einem Backup wiederhergestellt wird, sind folgende Elemente erhalten:

- Die bei der aktuellen WFA Installation erstellten Admin-Benutzer-Anmeldedaten.
- Wenn ein Benutzer mit anderen Administratorrechten als der standardmäßige Admin-Benutzer die Datenbank wiederherstellt, werden die Anmeldeinformationen der beiden Admin-Benutzer wiederhergestellt.
- Alle anderen Anmeldedaten der aktuellen WFA Installation werden durch die vom Backup bereitgestellten Anmeldedaten ersetzt.

Erstellen Sie Backups der WFA Datenbank vom Webportal

Sie können ein Backup der OnCommand Workflow Automation (WFA) Datenbank über das Web-Portal erstellen und die Backup-Datei für Recovery-Zwecke verwenden. Sie können kein vollständiges Backup über das Web-Portal durchführen.

Sie müssen über Administrator- oder Architektur-Anmeldeinformationen verfügen, um diese Aufgabe ausführen zu können.

Ein WFA Benutzer mit einer Backup-Rolle kann sich zum Durchführen eines Backups nicht im Web-Portal anmelden. WFA Benutzer mit Backup-Rolle können nur Remote- oder skriptbasierte Backups ausführen.

Schritte

1. Melden Sie sich als Administrator bei der WFA Web-GUI an.
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Wartung** auf **Sicherung & Wiederherstellung**.
3. Klicken Sie Auf **Backup**.
4. Wählen Sie im Dialogfeld, das geöffnet wird, einen Speicherort aus, und speichern Sie die Datei.

Sichern Sie die WFA Datenbank mit dem PowerShell Skript

Wenn Sie häufig ein Backup der OnCommand Workflow Automation (WFA) Datenbank erstellen möchten, können Sie das PowerShell Skript verwenden, das im WFA Installationspaket enthalten ist.

Sie müssen über Anmeldedaten für Admin-Benutzer, Anmeldeinformationen für Architektur oder Sicherungsb Benutzer verfügen.

Weitere Informationen finden Sie in DER REST-Dokumentation.

Schritte

1. Öffnen Sie Windows PowerShell als Admin-Benutzer und sichern Sie anschließend die WFA Datenbank:

```
<WFA_install_location\WFA\bin\Backup.ps1> -User user_name -Password password  
-Path backup_file_path
```

- WFA_install_location ist das WFA Installationsverzeichnis.
- User_Name ist der Benutzername des Admin-Benutzers, des Architekten oder des Backup-Benutzers.
- Das Passwort ist das Passwort des Admin-Benutzers, des Architekten oder des Backup-Benutzers.
- Backup_file_path ist der vollständige Verzeichnispfad für die Sicherungsdatei.



Die Sicherungsdatei ist eine ZIP-Datei mit dem Namen im folgenden Format:
wfa_backup_servername_.zip

- wfa_Backup_ ist ein fester Teil des Dateinamens, der der Name des Backup-Servers ist.
- Servername wird aus der Umgebung des Windows-Servers extrahiert.
- _.zip ist ein fester Teil des Dateinamens. C:\Program Files\NetApp\WFA\bin\Backup.ps1 -User backup -Password MyPassword123 -Path C:\WFA_backups\backup_10_08_12

Nach Abschluss des Backups wird die folgende Ausgabe angezeigt:

C:\WFA_Backups\Backup_1008_12\wfa_backup_myserver.zip . Vergewissern Sie sich, dass die Sicherungsdatei am angegebenen Speicherort erstellt wurde.

Sichern der WFA Datenbank mit der CLI

Wenn Sie die OnCommand Workflow Automation (WFA) Datenbank häufig sichern möchten, können Sie die WFA Befehlszeilenschnittstelle (CLI) verwenden, die Sie beim WFA Installationspaket erhalten haben.

Es gibt zwei Backup-Typen:

- Vollständiges Backup
- Regelmäßige Sicherung

Sichern Sie die WFA Datenbank mithilfe der CLI (vollständig)

Sie können ein vollständiges Backup der WFA-Datenbank (OnCommand Workflow Automation) über die WFA-Befehlszeilenschnittstelle (CLI) durchführen. In einem vollständigen Backup werden die WFA Datenbank, die WFA Konfiguration und der Schlüssel gesichert.

Sie müssen über Anmeldedaten für Admin-Benutzer oder Systemarchitekten verfügen.

In einer Hochverfügbarkeitsumgebung sollten geplante Backups mithilfe VON REST APIs erstellt werden. Sie können keine Backups über die CLI erstellen, wenn WFA sich im Failover-Modus befindet.

Weitere Informationen finden Sie in DER REST-Dokumentation.

Schritte

1. Navigieren Sie an der Shell-Eingabeaufforderung zum folgenden Verzeichnis auf dem WFA Server:
`WFA_install_location\WFA\bin.`

`WFA_install_location` ist das WFA Installationsverzeichnis.

2. Backup der WFA Datenbank:

```
.\wfa --backup --user=USER [--password=PASS] [--location=PATH] [--full]
```

- Benutzer ist der Benutzername des Backup-Benutzers.
- Passwort ist das Passwort des Backup-Benutzers.

Falls Sie kein Passwort angegeben haben, müssen Sie das Passwort eingeben, wenn Sie dazu aufgefordert werden.

- Der Pfad ist der vollständige Verzeichnispfad zur Sicherungsdatei.

3. Vergewissern Sie sich, dass die Sicherungsdatei am angegebenen Speicherort erstellt wurde.

Sichern Sie die WFA Datenbank mithilfe der CLI (regelmäßig)

Sie können ein regelmäßiges Backup der OnCommand Workflow Automation (WFA) Datenbank mithilfe der WFA Befehlszeilenschnittstelle (CLI) durchführen. In einem regelmäßigen Backup wird nur die WFA Datenbank gesichert.

Sie müssen über Anmeldedaten für Admin-Benutzer, Anmeldeinformationen für Architektur oder Sicherungsbutzer verfügen.

In einer Hochverfügbarkeitsumgebung sollten geplante Backups mithilfe VON REST APIs erstellt werden. Sie können keine Backups über die CLI erstellen, wenn WFA sich im Failover-Modus befindet.

Weitere Informationen finden Sie in DER REST-Dokumentation.

Schritte

1. Navigieren Sie an der Shell-Eingabeaufforderung zum folgenden Verzeichnis auf dem WFA Server:
`WFA_install_location\WFA\bin.`

`WFA_install_location` ist das WFA Installationsverzeichnis.

2. Backup der WFA Datenbank:

```
.\wfa --backup --user=USER [--password=PASS] [--location=PATH]
```

- Benutzer ist der Benutzername des Backup-Benutzers.
- Passwort ist das Passwort des Backup-Benutzers.

Falls Sie kein Passwort angegeben haben, müssen Sie das Passwort eingeben, wenn Sie dazu aufgefordert werden.

- Der Pfad ist der vollständige Verzeichnispfad zur Sicherungsdatei.

3. Vergewissern Sie sich, dass die Sicherungsdatei am angegebenen Speicherort erstellt wurde.

Sichern der WFA Datenbank mithilfe VON REST-APIs

Sie können ein Backup der OnCommand Workflow Automation (WFA) Datenbank mithilfe der REST-APIs erstellen. Wenn WFA in einem Failover-Modus in einer hochverfügbaren Umgebung ist, können Sie mithilfe der REST-APIs geplante Backups erstellen. Sie können die Befehlszeilenschnittstelle (CLI) nicht verwenden, um Backups während eines Failover zu erstellen.

Es gibt zwei Backup-Typen:

- Vollständiges Backup
- Regelmäßige Sicherung

Durchführen eines vollständigen Backups der WFA Datenbank mithilfe VON REST-APIs

Sie können mithilfe der REST-APIs ein vollständiges Backup der WFA Datenbank (OnCommand Workflow Automation) durchführen. In einem vollständigen Backup werden die WFA Datenbank, die WFA Konfiguration und der Schlüssel gesichert.

Sie müssen über Administrator- oder Architekturdaten verfügen.

Schritt

1. Geben Sie die folgende URL in Ihren Webbrowser ein: `https://IP address of the WFA server/rest/backups?full=true`

Weitere Informationen finden Sie in DER REST-Dokumentation.

Führen Sie mithilfe VON REST-APIs ein regelmäßiges Backup der WFA Datenbank durch

Sie können mithilfe der REST-APIs ein regelmäßiges Backup der WFA Datenbank (OnCommand Workflow Automation) durchführen. In einem regelmäßigen Backup wird nur die WFA Datenbank gesichert.

Sie benötigen Admin-, Architect- oder Backup-Anmeldedaten.

Schritt

1. Geben Sie die folgende URL in Ihren Webbrowser ein: `https://IP address of the WFA server/rest/backups`

Weitere Informationen finden Sie in DER REST-Dokumentation.

Wiederherstellen der OnCommand Workflow Automation-Datenbank

Zur Wiederherstellung der OnCommand Workflow Automation Datenbank (WFA) gehören auch die Wiederherstellung der Systemkonfigurationseinstellungen und der

Cacheinformationen, einschließlich der Playground-Datenbank.

- Durch Wiederherstellen einer WFA Datenbank wird die aktuelle WFA Datenbank gelöscht.
- Sie können ein Backup einer WFA Datenbank nur auf einem System wiederherstellen, auf dem dieselbe oder eine höhere Version von WFA ausgeführt wird.

Wenn Sie beispielsweise ein Backup auf einem System erstellt haben, auf dem WFA 4.2 ausgeführt wird, kann das Backup nur auf Systemen wiederhergestellt werden, auf denen WFA 4.2 oder höher ausgeführt wird.

- Nach Abschluss des Wiederherstellungsvorgangs wird das WFA SSL-Zertifikat durch das SSL-Zertifikat in der Backup-Datei ersetzt.



- Während der Disaster Recovery ist ein umfassender Restore von WFA Datenbanken und Konfigurationen erforderlich und kann sowohl in Standalone- als auch in Hochverfügbarkeitsumgebungen eingesetzt werden.
- Ein umfassendes Backup kann nicht über die Web UI erstellt werden.

Sie können die WFA Datenbank während des Disaster Recovery nur mit den CLI-Befehlen oder REST-APIs sichern und wiederherstellen.

WFA Datenbank wiederherstellen

Sie können die zuvor gesicherte OnCommand Workflow Automation-Datenbank (WFA) wiederherstellen.

- Sie müssen ein Backup der WFA Datenbank erstellt haben.
- Sie müssen über Administrator- oder Architekturdaten verfügen.
- Durch Wiederherstellen einer WFA Datenbank wird die aktuelle Datenbank gelöscht.
- Sie können ein WFA Datenbank-Backup nur auf einem System wiederherstellen, auf dem dieselbe oder eine neuere Version von OnCommand Workflow Automation ausgeführt wird.

Wenn Sie beispielsweise ein Backup auf einem System mit OnCommand Workflow Automation 4.2 erstellt haben, kann das Backup nur auf Systemen mit OnCommand Workflow Automation 4.2 oder höher wiederhergestellt werden.

Schritte

1. Melden Sie sich als Administrator bei der WFA Web-GUI an.
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Wartung** auf **Sicherung & Wiederherstellung**.
3. Klicken Sie auf **Datei auswählen**.
4. Wählen Sie im daraufhin angezeigten Dialogfeld die WFA Backup-Datei aus und klicken Sie auf **Öffnen**.
5. Klicken Sie Auf **Wiederherstellen**.

Sie können den wiederhergestellten Inhalt auf Vollständigkeit in der Funktionalität prüfen, z. B. die Funktion Ihrer benutzerdefinierten Workflows.

Wiederherstellen der WFA Datenbank über die CLI

Bei einem Ausfall können Sie die OnCommand Workflow Automation (WFA) Datenbank und die unterstützten Konfigurationen wiederherstellen, die Sie zuvor über die Befehlszeilenschnittstelle (CLI) gesichert haben. Zu den unterstützten Konfigurationen gehören Datenzugriff, HTTP Timeout und SSL-Zertifikate.

Die folgenden zwei Arten der Wiederherstellung:

- Vollständige Wiederherstellung
- Regelmäßige Wiederherstellung

Stellen Sie mithilfe der CLI eine (vollständige) WFA Datenbank wieder her

Sie können die OnCommand Workflow Automation (WFA) Datenbank mit der Befehlszeilenschnittstelle (CLI) wiederherstellen. In einer vollständigen Wiederherstellung können Sie die WFA Datenbank, die WFA Konfiguration und den Schlüssel wiederherstellen.

- Sie müssen ein Backup der WFA Datenbank erstellt haben.
- Sie müssen über Administrator- oder Architekturdaten verfügen.

Schritte

1. Navigieren Sie an der Shell-Eingabeaufforderung zum folgenden Verzeichnis auf dem WFA Server:
WFA_install_location\WFA\bin

wfa_install_location ist das WFA Installationsverzeichnis.

2. Führen Sie den Wiederherstellungsvorgang aus:

```
wfa.cmd --restore --full --user=user_name [--password=password] [--location=path] --restart
```

- User_Name ist der Benutzername des Admin- oder Architect-Benutzers.
- Passwort ist das Passwort des Benutzers.

Falls Sie kein Passwort angegeben haben, müssen Sie das Passwort eingeben, wenn Sie dazu aufgefordert werden.

- Der Pfad ist der vollständige Verzeichnispfad zur Wiederherstellungsdatei.

3. Vergewissern Sie sich, dass der Wiederherstellungsvorgang erfolgreich ist und WFA zugänglich ist.

Stellen Sie mithilfe der CLI eine (normale) WFA Datenbank wieder her

Sie können die OnCommand Workflow Automation (WFA) Datenbank regelmäßig wiederherstellen, indem Sie die REST-APIs verwenden. In einer normalen Wiederherstellung kann nur eine Sicherung der WFA Datenbank durchgeführt werden.

- Sie müssen ein Backup der WFA Datenbank erstellt haben.

- Sie müssen über Administratoranmeldeinformationen, Anmeldedaten für den Systemarchitekten oder Anmeldedaten für den Backup-Benutzer verfügen.

Schritte

1. Navigieren Sie an der Shell-Eingabeaufforderung zum folgenden Verzeichnis auf dem WFA Server:
WFA_install_location\WFA\bin

wfa_install_location ist das WFA Installationsverzeichnis.

2. Führen Sie den Wiederherstellungsvorgang aus:

```
wfa.cmd --restore --user=user_name [--password=password] [--location=path]
```

- User_Name ist der Benutzername des Admin- oder Architect-Benutzers.
- Passwort ist das Passwort des Benutzers.

Falls Sie kein Passwort angegeben haben, müssen Sie das Passwort eingeben, wenn Sie dazu aufgefordert werden.

- Der Pfad ist der vollständige Verzeichnispfad zur Wiederherstellungsdatei.

3. Vergewissern Sie sich, dass der Wiederherstellungsvorgang erfolgreich ist und WFA zugänglich ist.

Wiederherstellung der WFA Datenbank mithilfe VON REST-APIs

Sie können die OnCommand Workflow Automation (WFA) Datenbank mithilfe VON REST-APIs wiederherstellen. Sie können die Befehlszeilenschnittstelle (CLI) nicht verwenden, um während eines Failover die WFA Datenbank wiederherzustellen.

Die folgenden zwei Arten der Wiederherstellung:

- Vollständige Wiederherstellung
- Regelmäßige Wiederherstellung

Stellen Sie die WFA Datenbank mithilfe VON REST-APIs wieder her (vollständig)

Sie können die OnCommand Workflow Automation (WFA) Datenbank mithilfe VON REST-APIs wiederherstellen. In einer vollständigen Wiederherstellung können Sie die WFA Datenbank, die WFA Konfiguration und den Schlüssel wiederherstellen.

- Sie müssen eine ZIP-Sicherung der WFA Datenbank erstellt haben.
- Sie müssen über Administrator- oder Architekturdaten verfügen.
- Wenn Sie die Datenbank im Rahmen des Migrationsvorgangs wiederherstellen, müssen Sie eine vollständige Wiederherstellung durchführen.

Schritte

1. Geben Sie in den Browser DES REST-Clients die folgende URL ein: `https://IP address of WFA server/rest/backups?full=true`
2. Wählen Sie im Backup-Fenster die Methode **POST** aus.
3. Wählen Sie in der Dropdown-Liste **Teil** die Option **mehrteiligem Körper** aus.

4. Geben Sie im Feld **Datei** die folgenden Informationen ein:
 - a. Wählen Sie in der Dropdown-Liste **Inhaltstyp** die Option **mehrteilige/Formulardaten** aus.
 - b. Wählen Sie in der Dropdown-Liste **Charset** die Option **ISO-8859-1** aus.
 - c. Geben Sie im Feld **Dateiname** den Namen der Sicherungsdatei ein, die Sie erstellt haben und die Sie wiederherstellen möchten.
 - d. Klicken Sie Auf **Durchsuchen**.
 - e. Wählen Sie den Speicherort der ZIP-Sicherungsdatei aus.
5. Navigieren Sie zum Verzeichnis WFA_install_location\wfa\bin und starten Sie die WFA Services neu:
6. Starten Sie den Service **NetApp WFA Database** und **NetApp WFA Server** neu:

```
wfa --restart
```

7. Vergewissern Sie sich, dass der Wiederherstellungsvorgang erfolgreich ist und WFA zugänglich ist.

Stellen Sie die WFA Datenbank mithilfe VON REST-APIs wieder her (regelmäßig)

Sie können die WFA-Datenbank (OnCommand Workflow Automation) regelmäßig wiederherstellen, indem SIE REST-APIs verwenden. In einer normalen Wiederherstellung ist es nur möglich, die WFA Datenbank wiederherzustellen.

- Sie müssen eine ZIP-Sicherung der WFA Datenbank erstellt haben.
- Sie müssen über Administrator- oder Architekturdaten verfügen.
- Wenn Sie die Datenbank im Rahmen des Migrationsvorgangs wiederherstellen, müssen Sie eine vollständige Wiederherstellung durchführen.

Schritte

1. Geben Sie in den Browser DES REST-Clients die folgende URL ein: `https://IP address of WFA server/rest/backups`
2. Wählen Sie im Backup-Fenster die Methode **POST** aus.
3. Wählen Sie in der Dropdown-Liste **Teil** die Option **mehrteiligem Körper** aus.
4. Geben Sie im Feld **Datei** die folgenden Informationen ein:
 - a. Wählen Sie in der Dropdown-Liste **Inhaltstyp** die Option **mehrteilige/Formulardaten** aus.
 - b. Wählen Sie in der Dropdown-Liste **Charset** die Option **ISO-8859-1** aus.
 - c. Geben Sie im Feld **Dateiname** den Namen der Sicherungsdatei als Backupdatei ein.
 - d. Klicken Sie Auf **Durchsuchen**.
 - e. Wählen Sie den Speicherort der ZIP-Sicherungsdatei aus.
5. Navigieren Sie zum Verzeichnis WFA_install_location\wfa\bin und starten Sie die WFA Services neu:
6. Vergewissern Sie sich, dass der Wiederherstellungsvorgang erfolgreich ist und WFA zugänglich ist.

Setzt das bei der Installation erstellte Admin-Passwort zurück

Falls Sie das Passwort des Admin-Benutzers vergessen haben, den Sie bei der

Installation des OnCommand Workflow Automation-Servers (WFA) erstellt haben, können Sie das Passwort zurücksetzen.

- Sie müssen über Administratorrechte für das Windows System verfügen, auf dem WFA installiert ist.
- Die WFA Services müssen ausgeführt werden.
- Bei diesem Verfahren wird nur das Passwort des Admin-Benutzers zurückgesetzt, der während der WFA Installation erstellt wurde.

Sie können das Passwort anderer WFA Admin-Benutzer, die Sie nach der WFA Installation erstellt haben, nicht zurücksetzen.

- Durch diese Vorgehensweise wird die Passwortrichtlinie, die Sie konfiguriert haben, nicht durchgesetzt.

Sie müssen entweder ein Passwort eingeben, das zu Ihrer Passwortrichtlinie entspricht, oder das Passwort von der WFA Benutzeroberfläche ändern, nachdem Sie das Passwort zurückgesetzt haben.

Schritte

1. Öffnen Sie eine Eingabeaufforderung, und navigieren Sie zum folgenden Verzeichnis:

```
WFA_install_location\WFA\bin\
```

2. Geben Sie den folgenden Befehl ein:

```
wfa --admin-password [--password=PASS]
```

Wenn Sie das Passwort im Befehl nicht angeben, müssen Sie bei der entsprechenden Eingabeaufforderung das Passwort eingeben.

3. Befolgen Sie an der Eingabeaufforderung die Anweisungen auf dem Bildschirm, um das Admin-Passwort zurückzusetzen.

Importieren Sie OnCommand Workflow Automation-Inhalte

Sie können WFA Inhalte (User-created OnCommand Workflow Automation) wie Workflows, Finder und Befehle importieren. Sie können auch Inhalte importieren, die von einer anderen WFA Installation exportiert werden, Inhalte, die aus dem Storage Automation Store oder der WFA Community heruntergeladen werden, sowie Pakete einschließlich Data ONTAP PowerShell Toolkits und Perl NMSDK Toolkits.

- Sie benötigen Zugriff auf den WFA Inhalt, den Sie importieren möchten.
- Der zu importierende Inhalt muss auf einem System erstellt worden sein, das dieselbe oder eine frühere Version von WFA ausführt.

Wenn beispielsweise WFA 2.2 ausgeführt wird, können Sie keine Inhalte importieren, die mit WFA 3.0 erstellt wurden.

- Sie können in N-2-Versionen von WFA entwickelte Inhalte nur in WFA 5.1 importieren.
- Wenn die .dar-Datei auf NetApp zertifizierte Inhalte verweist, müssen die NetApp-zertifizierten Content-Packs importiert werden.

Die NetApp zertifizierten Content Packs können im Storage Automation Store heruntergeladen werden. Überprüfen Sie in der Dokumentation des Pakets, ob alle Anforderungen erfüllt sind.

Schritte

1. Melden Sie sich über einen Webbrowser bei WFA an.
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Wartung** auf **Workflows importieren**.
3. Klicken Sie auf **Datei**, um die .dar-Datei auszuwählen, die Sie importieren möchten, und klicken Sie dann auf **Import**.
4. Klicken Sie im Dialogfeld Erfolg importieren auf **OK**.

Verwandte Informationen

["NetApp Community: OnCommand Workflow Automation"](#)

Überlegungen beim Importieren von OnCommand Workflow Automation-Inhalten

Beachten Sie beim Importieren benutzererstellter Inhalte, Inhalte, die aus einer anderen OnCommand Workflow Automation-Installation (WFA) exportiert werden, oder Inhalte, die aus dem Storage Automation Store oder der WFA Community heruntergeladen werden.

- WFA Inhalte werden als .dar-Datei gespeichert und können den gesamten vom Benutzer erstellten Inhalt von einem anderen System oder bestimmte Elemente wie Workflows, Finder, Befehle und Wörterbuchbegriffe enthalten.
- Wenn eine vorhandene Kategorie aus einer .dar-Datei importiert wird, wird der importierte Inhalt mit dem vorhandenen Inhalt in der Kategorie zusammengeführt.

Nehmen wir beispielsweise im WFA Server zwei Workflows für WF1 und WF2 in Kategorie A vor. Werden Workflows WF3 und WF4 in Kategorie A auf den WFA Server importiert, enthält Kategorie A nach dem Import Workflows WF1, WF2, WF3 und WF4.

- Wenn die .dar-Datei Wörterbucheinträge enthält, werden die den Wörterbucheinträgen entsprechenden Cache-Tabellen automatisch aktualisiert.

Wenn die Cache-Tabellen nicht automatisch aktualisiert werden, wird eine Fehlermeldung in der Datei wfa.log protokolliert.

- Beim Import einer .dar-Datei, die eine Abhängigkeit von einem Paket hat, das nicht im WFA-Server vorhanden ist, versucht WFA zu identifizieren, ob alle Abhängigkeiten von den Entitäten erfüllt werden.
 - Wenn eine oder mehrere Entitäten fehlen oder eine niedrigere Version einer Entität gefunden wird, schlägt der Import fehl und eine Fehlermeldung wird angezeigt.

Die Fehlermeldung enthält Details zu den Paketen, die installiert werden sollten, um die Abhängigkeiten zu erfüllen.

- Wenn eine höhere Version einer Entität gefunden wird oder sich die Zertifizierung geändert hat, wird ein generisches Dialogfeld über die nicht übereinstimmende Version angezeigt und der Import abgeschlossen.

Die Details zur Versionsabweichung werden in einer Datei mit wfa.log protokolliert.

- Fragen und Support-Anfragen für folgende müssen an die WFA Community gerichtet sein:
 - Alle Inhalte werden von der WFA Community heruntergeladen
 - Sie haben benutzerdefinierte WFA Inhalte erstellt

- Sie haben WFA Inhalte geändert

Migrieren der OnCommand Workflow Automation Installation

Sie können eine Installation von OnCommand Workflow Automation (WFA) migrieren, um den eindeutigen WFA Datenbankschlüssel zu erhalten, der während der WFA Installation installiert ist. Sie können beispielsweise die WFA Installation von einem Windows 2012 Server zu einem Windows 2016 Server migrieren.

- Sie müssen diese Vorgehensweise nur durchführen, wenn Sie eine WFA Installation, die den WFA Datenbankschlüssel enthält, auf einen anderen Server migrieren möchten.
- Beim Wiederherstellen einer WFA Datenbank wird der WFA Schlüssel nicht migriert.
- Die Migration einer WFA Installation führt keine Migration der SSL-Zertifikate durch.
- 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. Zugriff auf WFA über einen Webbrowser als Administrator
2. Sichern der WFA Datenbank
3. Öffnen Sie eine Eingabeaufforderung auf dem WFA-Server, und ändern Sie die Verzeichnisse an den folgenden Speicherort: `c:\Program Files\NetApp\WFA\bin`
4. Geben Sie an der Eingabeaufforderung Folgendes ein, um den Datenbankschlüssel abzurufen:

```
wfa.cmd -key
```

5. Notieren Sie den angezeigten Datenbankschlüssel.
6. WFA deinstallieren.
7. Installation von WFA auf dem erforderlichen System
8. Öffnen Sie die Eingabeaufforderung auf dem neuen WFA-Server, und ändern Sie die Verzeichnisse an den folgenden Speicherort: `c:\Program Files\NetApp\WFA\bin`
9. Geben Sie an der Eingabeaufforderung Folgendes ein, um den Datenbankschlüssel zu installieren:

```
wfa.cmd -key=yourdatabasekey
```

Yourdatabasekey ist der Schlüssel, den Sie in der früheren WFA Installation angegeben haben.

10. Stellen Sie die WFA Datenbank aus dem von Ihnen erstellten Backup wieder her.

Deinstallieren Sie OnCommand Workflow Automation

Sie können OnCommand Workflow Automation (WFA) mit Microsoft Windows Programme and Features deinstallieren.

Schritte

1. Melden Sie sich unter Windows mit einem Konto mit Administratorrechten an.
2. Klicken Sie auf **Alle Programme > Systemsteuerung > Systemsteuerung > Programme und Funktionen**.
3. Deinstallieren Sie WFA, indem Sie eine der folgenden Optionen auswählen:
 - Wählen Sie **NetApp WFA** und klicken Sie auf **Deinstallieren**.
 - Klicken Sie mit der rechten Maustaste **NetApp WFA** und wählen Sie **Deinstallieren**.
4. Wenn der Deinstallationsprozess nicht mehr reagiert, bevor er abgeschlossen ist, beenden Sie den **NetApp WFA Database**-Dienst von der Windows Services-Konsole aus und versuchen Sie erneut, die Deinstallation durchzuführen.

Verwalten des OnCommand Workflow Automation-SSL-Zertifikats

Sie können das WFA OnCommand Workflow Automation SSL-Standardzertifikat durch ein selbstsigniertes Zertifikat oder ein Zertifikat ersetzen, das von einer Zertifizierungsstelle (CA) signiert ist.

Bei der Installation von WFA wird das selbstsignierte WFA SSL-Zertifikat generiert. Wenn Sie ein Upgrade durchführen, wird das Zertifikat für die vorherige Installation durch das neue Zertifikat ersetzt. Wenn Sie ein nicht standardmäßiges selbstsigniertes Zertifikat oder ein von einer CA signiertes Zertifikat verwenden, müssen Sie das Standard-WFA SSL-Zertifikat durch Ihr Zertifikat ersetzen.

Ersetzen Sie das Standard-SSL-Zertifikat der Workflow Automation

Sie können das Standard-SSL-Zertifikat der Workflow Automation (WFA) ersetzen, wenn das Zertifikat abgelaufen ist oder Sie die Gültigkeitsdauer des Zertifikats erhöhen möchten.

Sie müssen auf dem WFA Server über Windows-Administratorrechte verfügen.

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. Melden Sie sich als Admin-Benutzer auf der WFA Host Machine an.
2. Verwenden Sie die Windows Services-Konsole, um die folgenden WFA-Services zu beenden:
 - NetApp WFA Datenbank
 - NetApp WFA Server
3. Löschen Sie die datei wfa.keystore von folgendem Speicherort:

```
<WFA_install_location>\WFA\jboss\standalone\configuration\keystore
```

4. Öffnen Sie eine Eingabeaufforderung auf dem WFA-Server, und ändern Sie das Verzeichnis in den folgenden Speicherort:<OpenJDK_install_location>\bin
5. Erhalten Sie den Datenbankschlüssel:

```
keytool -keysize 2048 -genkey -alias "ssl keystore" -keyalg RSA -keystore  
"<WFA_install_location>\WFA\jboss\standalone\configuration\keystore\wfa.keysto  
re" -validity xxxx
```

Xxxx ist die Anzahl der Tage für die Gültigkeit des neuen Zertifikats.

6. Geben Sie bei der entsprechenden Aufforderung das Kennwort ein (Standard oder neu).

Das Standardpasswort ist ein zufällig generiertes verschlüsseltes Passwort.

Um das Standardpasswort zu erhalten und zu entschlüsseln, befolgen Sie die Schritte im Knowledge Base-Artikel ["Verlängern des selbstsignierten Zertifikats bei WFA 5.1.1.0.4"](#)

Um ein neues Passwort zu verwenden, befolgen Sie die Schritte im Knowledge Base-Artikel ["So aktualisieren Sie ein neues Passwort für den Schlüsselspeicher in WFA."](#)

7. Geben Sie die erforderlichen Details für das Zertifikat ein.
8. Überprüfen Sie die angezeigten Informationen, und geben Sie ein Yes.
9. Drücken Sie **Enter**, wenn Sie dazu aufgefordert werden: Geben Sie das Schlüsselpasswort für <SSL keystore> <ZURÜCK, wenn das gleiche wie das Schlüsselspeicherkennwort> ein.
10. Starten Sie die WFA Services über die Windows Services Konsole neu.

Erstellen Sie eine Anfrage zum Signieren eines Zertifikats für Workflow Automation

Sie können in Windows eine Zertifikatsignierungsanforderung (CSR) erstellen, sodass Sie das SSL-Zertifikat verwenden können, das von einer Zertifizierungsstelle (CA) anstelle des Standard-SSL-Zertifikats für Workflow Automation (WFA) signiert ist.

- Sie müssen auf dem WFA Server über Windows-Administratorrechte verfügen.
- Sie müssen das von WFA bereitgestellte Standard-SSL-Zertifikat ersetzt haben.

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

Schritte

1. Melden Sie sich als Admin-Benutzer auf der WFA Host Machine an.
2. Öffnen Sie eine Eingabeaufforderung auf dem WFA-Server, und ändern Sie dann das Verzeichnis in den folgenden Speicherort: + <OpenJDK_install_location>\bin
3. CSR erstellen:

```
keytool -certreq -keystore  
WFA_install_location\WFA\jboss\standalone\configuration\keystore\wfa.keystore  
-alias "ssl keystore" -file C:\file_name.csr
```

File_Name ist der Name der CSR-Datei.

4. Geben Sie bei der entsprechenden Aufforderung das Kennwort ein (Standard oder neu).

Das Standardpasswort ist ein zufällig generiertes verschlüsseltes Passwort.

Um das Standardpasswort zu erhalten und zu entschlüsseln, befolgen Sie die Schritte im Knowledge

Base-Artikel ["Verlängern des selbstsignierten Zertifikats bei WFA 5.1.1.0.4"](#)

Um ein neues Passwort zu verwenden, befolgen Sie die Schritte im Knowledge Base-Artikel ["So aktualisieren Sie ein neues Passwort für den Schlüsselspeicher in WFA."](#)

5. Senden Sie die Datei file_Name.csr an die CA, um ein signiertes Zertifikat zu erhalten.

Weitere Informationen finden Sie auf der CA-Website.

6. Laden Sie ein Kettenzertifikat von der CA herunter, und importieren Sie dann das Kettenzertifikat in Ihren Schlüsselspeicher: `keytool -import -alias "ssl keystore CA certificate" -keystore "WFA_install_location\WFA\jboss\standalone\configuration\keystore\wfa.keystore" -trustcacerts -file C:\chain_cert.cer`

C:\Chain_cert.cer ist die von der CA empfangene Kettenzertifikat-Datei. Die Datei muss im X.509-Format vorliegen.

7. Importieren Sie das signierte Zertifikat, das Sie von der CA erhalten haben:

```
keytool -import -alias "ssl keystore" -keystore
"WFA_install_location\WFA\jboss\standalone\configuration\keystore\wfa.keystore"
-file C:\certificate.cer
```

C:\Certificate.cer ist die von der CA empfangene Kettenzertifikat-Datei.

8. Starten Sie die folgenden WFA Services:

- NetApp WFA Datenbank
- NetApp WFA Server

Verwalten von Perl- und Perl-Modulen

OnCommand Workflow Automation (WFA) unterstützt Perl-Befehle für Workflow-Vorgänge. ActivePerl 5.26.3 wird bei der Installation von WFA auf dem WFA Server installiert und konfiguriert. Sie können Ihre bevorzugten Perl-Verteilung und Perl-Module installieren und konfigurieren.

Neben ActivePerl sind auch die erforderlichen Perl-Module aus dem NetApp Manageability SDK installiert, wenn Sie WFA installieren. Für die erfolgreiche Ausführung von Perl-Befehlen sind die NetApp Manageability SDK Perl-Module erforderlich.

Konfigurieren Sie Ihre bevorzugte Perl-Verteilung

Standardmäßig ist ActivePerl mit OnCommand Workflow Automation (WFA) installiert. Wenn Sie eine andere Perl-Verteilung verwenden möchten, können Sie Ihre bevorzugte Perl-Distribution für die Verwendung mit WFA konfigurieren.

Sie müssen die erforderliche Perl Verteilung auf dem WFA Server installiert haben.

Sie dürfen die Standard-ActivePerl-Installation nicht deinstallieren oder überschreiben. Sie müssen Ihre bevorzugte Perl-Distribution an einem separaten Speicherort installieren.

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 CustomPerl -PerlPath CustomPerlPath
```

```
Set-WfaConfig -Name CustomPerl -PerlPath C:\myperl\perl.exe
```

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

Standortspezifische Perl-Module verwalten

Sie können den ActiveState Perl Package Manager (PPM) verwenden, um Ihre standortspezifischen Perl-Module zu verwalten. Sie müssen Ihre standortspezifischen Perl-Module außerhalb des WFA Installationsverzeichnis (OnCommand Workflow Automation) installieren, um das Löschen Ihrer Perl-Module während eines WFA Upgrades zu vermeiden.

Mithilfe der Umgebungsvariable PERL5LIB können Sie den Perl-Interpreter konfigurieren, der auf dem WFA Server installiert ist, um Ihre Perl-Module zu verwenden.

Die Installation des Try-Tiny Perl Moduls im Benutzerbereich bei c:\Perl wird in diesem Verfahren als Beispiel verwendet. Dieser Benutzerbereich wird bei der Deinstallation von WFA nicht gelöscht, und Sie können den Bereich nach der Neuinstalliert oder einem Upgrade von WFA wiederverwenden.

Schritte

1. Stellen Sie die Umgebungsvariable PERL5LIB auf den Speicherort ein, an dem Sie Ihre Perl-Module installieren möchten.

```
c:\>echo %PERL5LIB% c:\Perl
```

2. Vergewissern Sie sich, dass der Perl-Modulbereich nicht mit initialisiert wurde ppm area list.

```
c:\Program Files\NetApp\WFA\Perl64\bin>ppm area list
```

name	pkgs	lib
(user)	n/a	C:/Perl
site*	0	C:/Program Files/NetApp/WFA/Perl64/site/lib
perl	229	C:/Program Files/NetAPP/WFA/Perl64/lib

3. Initialisieren Sie den Perl-Modulbereich mithilfe von `ppm area init user`.

```
c:\Program Files\NetApp\WFA\Perl64\bin>ppm area init user
```

```
Syncing user PPM database with .packlists...done
```

4. Überprüfen Sie, ob der Perl-Modulbereich mit initialisiert wird `ppm area list`.

```
c:\Program Files\NetApp\WFA\Perl64\bin>ppm area list
```

name	pkgs	lib
user	0	C:/Perl
site*	0	C:/Program Files/NetApp/WFA/Perl64/site/lib
perl	229	C:/Program Files/NetAPP/WFA/Perl64/lib

5. Fügen Sie die erforderlichen Repositories hinzu und installieren Sie die erforderlichen Pakete.

- a. Fügen Sie das erforderliche Repository mit hinzu `ppm repo add`.

```
c:\Program Files\NetApp\WFA\Perl64\bin>ppm repo add
http://ppm4.activestate.com/MSWin32-x64/5.16/1600/package.xml
```

```
Downloading ppm4.activestate.com packlist...done
Updating ppm4.activestate.com database...done
Repo 1 added.
```

- b. Überprüfen Sie, ob das erforderliche Repository mit hinzugefügt wird `ppm repo list`.

```
c:\Program Files\NetApp\WFA\Perl64\bin>ppm repo list
```

id	pkgs	name
1	17180	ppmr.activestate.com

(1 enabled repository)

- c. Installieren Sie das erforderliche Perl-Modul mithilfe von `ppm install`.

```
c:\Program Files\NetApp\WFA\Perl64\bin>ppm install Try-Tiny --area user
```

```
Downloading ppm4.activestate.com packlist...done
Updating ppm4.activestate.com database...done
Downloading Try-Tiny-0.18...done
Unpacking Try-Tiny-0.18...done
Generating HTML for Try-Tiny-0.18...done
Updating files in user area...done
  2 files installed
```

- d. Überprüfen Sie, ob das erforderliche Perl-Modul mithilfe von `ppm area list` installiert ist.

```
c:\Program Files\NetApp\WFA\Perl64\bin>ppm area list
```

name	pkgs	lib
user	1	C:/Perl
site*	0	C:/Program Files/NetApp/WFA/Perl64/site/lib
perl	229	C:/Program Files/NetAPP/WFA/Perl64/lib

Reparieren Sie die ActivePerl-Installation

ActiveState ActivePerl wird bei der Installation von WFA auf dem OnCommand Workflow

Automation (WFA) Server installiert. ActivePerl ist für die Ausführung von Perl-Befehlen erforderlich. Wenn Sie ActivePerl versehentlich vom WFA Server deinstallieren oder die ActivePerl-Installation beschädigt ist, können Sie die ActivePerl-Installation manuell reparieren.

Schritte

1. Sichern Sie die WFA Datenbank mit einer der folgenden Optionen:
 - WFA Webportal
 - PowerShell Skript
2. WFA deinstallieren.
3. Installieren Sie die Version von WFA, die Sie deinstalliert haben.

ActivePerl ist bei der Installation von WFA installiert.

4. WFA Datenbank wiederherstellen.

Sie können den wiederhergestellten Inhalt auf Vollständigkeit in der Funktionalität prüfen, z. B. die Funktion Ihrer benutzerdefinierten Workflows.

Fehlerbehebung bei Installations- und Konfigurationsproblemen

Sie können Probleme beheben, die bei der Installation und Konfiguration von OnCommand Workflow Automation (WFA) auftreten können.

Die Anmeldeseite für OnCommand Workflow Automation kann nicht geöffnet werden

Wenn Sie .Net 3.5 installiert haben, wird die Internet Information Services (IIS) mit ihr installiert. Der IIS belegt Port 80, der von WFA verwendet wird.

Stellen Sie sicher, dass entweder die IIS-Rolle entfernt oder IIS im WFA Server deaktiviert ist.

Performance Advisor Daten in WFA können nicht angezeigt werden

Wenn Performance Advisor Daten in WFA nicht angezeigt werden können oder der Datenerfassungsprozess aus der Performance Advisor Datenquelle ausfällt, sollten Sie bestimmte Aktionen durchführen, um das Problem zu beheben.

- Vergewissern Sie sich, dass Sie die Anmeldedaten eines Active IQ Unified Manager-Benutzers mit einer Mindestrolle von GlobalRead angegeben haben, wenn Sie Performance Advisor als Datenquelle in WFA konfigurieren.
- Vergewissern Sie sich, dass Sie den richtigen Port angegeben haben, wenn Sie Performance Advisor als Datenquelle in WFA konfigurieren.

Standardmäßig verwendet Active IQ Unified Manager Port 8088 für eine HTTP-Verbindung und Port 8488 für eine HTTPS-Verbindung.

- Stellen Sie sicher, dass Leistungsdaten vom Active IQ Unified Manager-Server erfasst werden.

OnCommand Workflow Automation (WFA) zeigt eine leere Seite unter Windows 2012 an

Wenn Sie Adobe Flash Player separat von der Adobe-Website heruntergeladen und installiert haben, wird möglicherweise eine leere Seite angezeigt. Sie dürfen den Flash Player nicht separat herunterladen und installieren, da er in Windows 2012 im Paket mit Internet Explorer enthalten ist. Updates für den Flash Player werden über Windows-Updates installiert.

Wenn Sie den Flash Player separat heruntergeladen und installiert haben, müssen Sie die folgenden Schritte durchführen:

Schritte

1. Deinstallieren Sie den Flash Player, den Sie bereits installiert haben.
2. Öffnen Sie unter Windows **Server Manager > lokaler Server > ROLLEN UND FUNKTIONEN > AUFGABEN** und wählen Sie **Rollen und Funktionen hinzufügen**.
3. Klicken Sie im Assistenten zum Hinzufügen von Rollen und Funktionen auf **Funktionen > Benutzeroberfläche und Infrastruktur**, wählen Sie **Desktop Experience** und schließen Sie das Hinzufügen der Funktion ab.

Hinzufügen von Desktop Experience fügt den Flash Player zu Windows hinzu.

4. Starten Sie Windows Neu.

Zugehörige Dokumentation für OnCommand Workflow Automation

Sie erhalten zusätzliche Dokumente und Tools, mit denen Sie die erweiterte Konfiguration Ihres OnCommand Workflow Automation (WFA) Servers vornehmen können.

Andere Referenzen

Der Workflow Automation Speicherplatz in der NetApp Community bietet zusätzliche Schulungsressourcen, darunter:

- **NetApp Community**

["NetApp Community: Workflow Automation \(WFA\)"](#)

Werkzeugreferenzen

- **Interoperabilitätsmatrix**

Listet die unterstützten Kombinationen von Hardware-Komponenten und Software-Versionen auf.

["Interoperabilitätsmatrix"](#)

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 IRGEND EINER 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.