



Installation und Einrichtung für Linux

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

This PDF was generated from <https://docs.netapp.com/de-de/workflow-automation/rhel-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 Linux	1
Übersicht über OnCommand Workflow Automation.	1
Systemanforderungen für die Installation von OnCommand Workflow Automation	4
Voraussetzungen für die Installation von Workflow Automation.	7
Management von Hochverfügbarkeit	10
Einrichtung von OnCommand Workflow Automation	17
Upgrade von OnCommand Workflow Automation 3.1 oder höher	32
Upgrade von Drittanbieterprodukten	34
Backup der OnCommand Workflow Automation-Datenbank	35
Wiederherstellen der OnCommand Workflow Automation-Datenbank	39
Setzt das bei der Installation erstellte Admin-Passwort zurück	43
Importieren Sie OnCommand Workflow Automation-Inhalte	43
Migrieren der OnCommand Workflow Automation Installation.	45
Deinstallieren Sie OnCommand Workflow Automation	46
Verwalten des OnCommand Workflow Automation-SSL-Zertifikats.	46
Verwalten von Perl- und Perl-Modulen.	49
Fehlerbehebung bei Installations- und Konfigurationsproblemen	49
Zugehörige Dokumentation für OnCommand Workflow Automation	50

Installation und Einrichtung für Linux

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 ONTAP.

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

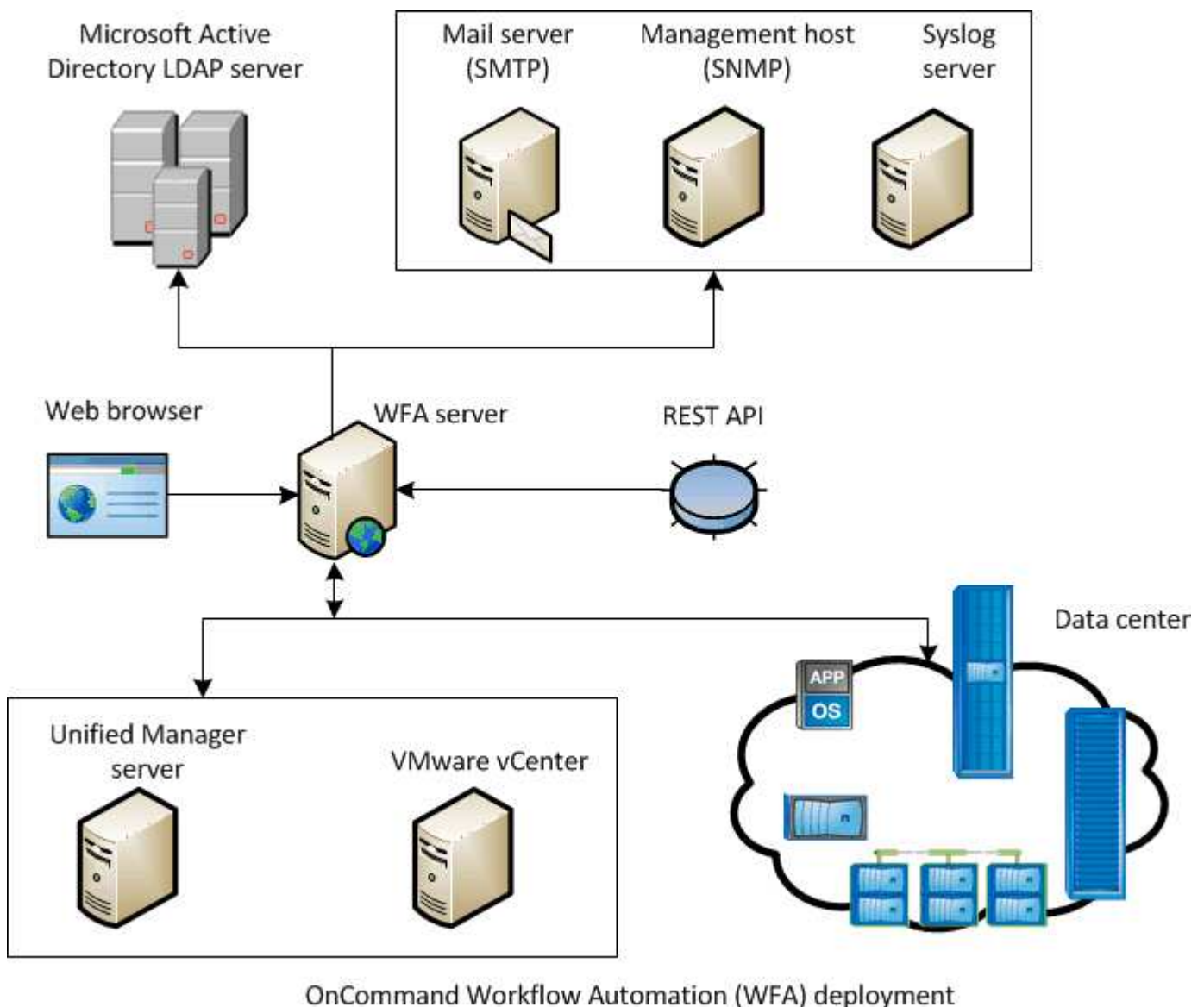
Für die Verwendung des OnCommand Workflow Automation-Servers ist keine Lizenz erforderlich.

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:

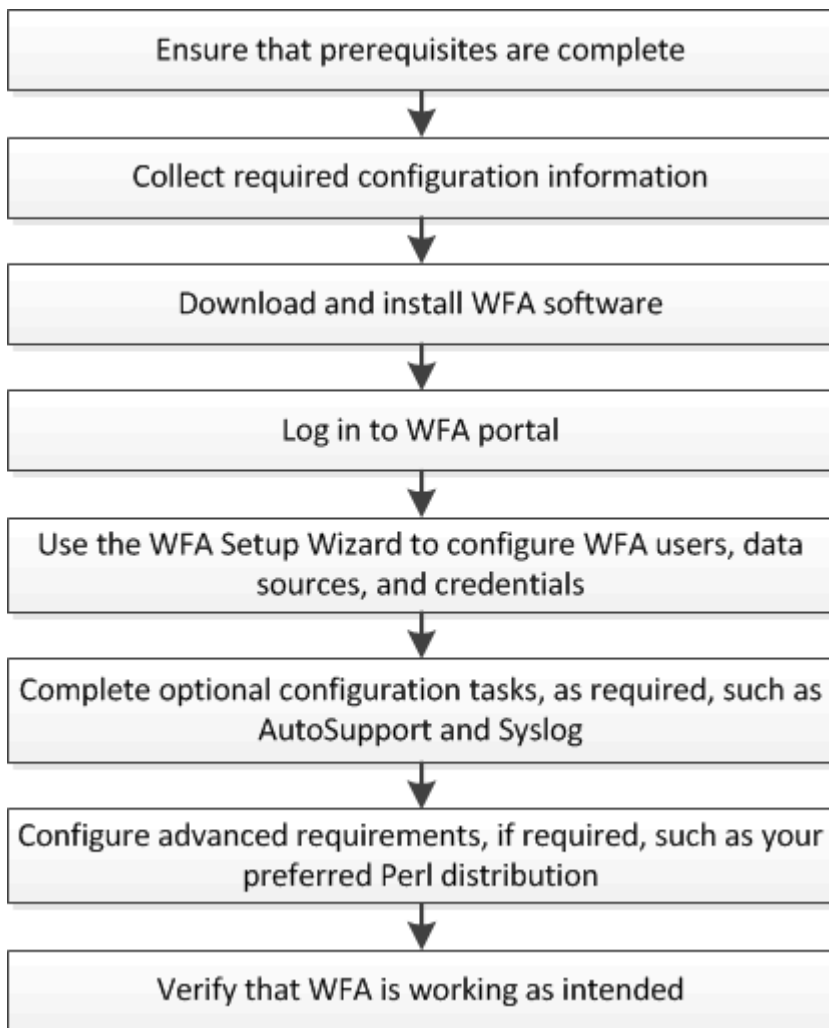


Übersicht über die OnCommand Workflow Automation-Installation und -Einrichtung

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 für OnCommand Workflow Automation

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.

- **LDAP-Authentifizierung**

- Sie können nur den LDAP-Server (Lightweight Directory Access Protocol) für die LDAP-Authentifizierung verwenden.
- Sie müssen Mitglied einer LDAP-Gruppe sein, um die LDAP-Authentifizierung verwenden zu können.
- Sie dürfen keinen LDAP-Benutzernamen verwenden, der Teil einer hierarchischen Struktur mehrerer Domänen zur Authentifizierung oder Benachrichtigung ist.



Microsoft Active Directory Lightweight Directory Services (AD LDS) wird nicht unterstützt.

• WFA Datenquellen Typen

OnCommand Unified Manager 6.0, 6.1 und 6.2 Datenquellen sind in der WFA 4.1 Version veraltet. Diese Datenquellen werden in zukünftigen Versionen nicht unterstützt.

• WFA installiert auf Linux

- Zertifizierte Inhalte von Data ONTAP 7-Mode sind im Moment nicht verfügbar.
- Befehle, die nur PowerShell Code enthalten, sind nicht mit Linux kompatibel.
- Zertifizierte Befehle für 7-Mode und VMware werden derzeit nicht auf Perl portiert und sind daher nicht mit Linux kompatibel.

• 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 Kategoriename 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

In der folgenden Tabelle sind alle mit dem WFA Server kompatiblen Betriebssystemversionen aufgeführt.

Betriebssystem	Version
Red Hat Enterprise Linux	7.0, 7.1, 7.2, 7.3, 7.4 7.5- und 7.6 64-Bit-Betriebssysteme
CentOS	Betriebssysteme 7.1, 7.2, 7.3, 7.4, 7.5 und 7.6 64-Bit



WFA sollte auf dedizierten physischen Computern oder VMs installiert werden. Sie dürfen keine anderen Anwendungen auf dem Server installieren, auf dem WFA ausgeführt wird.

- Einer der folgenden unterstützten Browser:
 - Mozilla Firefox
 - Microsoft Internet Explorer
 - Google Chrome
- Perl v5.x

Sie erhalten Informationen über die Perl-Module, die über die installiert werden sollen `./WFA-version_number.bin -l` Befehl.

Weitere Informationen finden Sie im ["Interoperabilitäts-Matrix-Tool"](#).



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

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
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




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

- Überprüfen, ob Perl v5.10.1 installiert ist

Erforderliche Konfigurationsinformationen

Einheit oder System	Details	Zweck
Arrays	<ul style="list-style-type: none"> • IP-Adresse • Benutzername und Passwort 	Betrieb auf Storage-Systemen durchführen  Anmeldedaten für das Root- oder Admin-Konto sind für den Speicher (Arrays) erforderlich.

Einheit oder System	Details	Zweck
Externe Repositories wie OnCommand Balance und benutzerdefinierte Datenbanken	<ul style="list-style-type: none"> • IP-Adresse • Benutzername und Passwort eines schreibgeschützten Benutzerkontos 	Anforderung Sie müssen die relevanten WFA Inhalte wie beispielsweise Wörterbucheinträge und Cacheabfragen für die externen Repositories erstellen, um Daten aus den externen Repositories zu erhalten.
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"](#)

Perl-Module auf CentOS und RHEL installieren

Einige Perl-Module sind standardmäßig nicht mit dem Perl-Paket für Linux enthalten.

Während der WFA Installation überprüft der WFA Installer, ob alle Perl-Module im System verfügbar sind, und führt diese weiter aus, wenn diese Anforderung erfüllt ist. Vor der Installation von OnCommand Workflow Automation (WFA) müssen die Perl-Module installiert werden.



Der WFA Installer versucht, die Perl-Module automatisch zu installieren, wenn die Perl-Module in den yum-Repositorys verfügbar sind, die auf dem System konfiguriert sind. Wenn die Perl-Module nicht verfügbar sind, fordert das Installationsprogramm den Benutzer auf, die Perl-Module manuell zu installieren. Die eine Ausnahme ist das „Perl-Core“-Modul. Dieses Modul wird nicht automatisch auf dem System installiert, auch wenn es in den im System konfigurierten yum-Repositorys verfügbar ist. Dies ist ein bekanntes Problem.

Perl-Modul	NAME des RPM-Pakets
Perl-Kernmodule	perl-Core
DBI	perl-DBI
XML::DOM	perl-XML-DOM
Begriff::ReadKey	perl-TermReadKey
HTTP::Anfrage	perl-libwww-perl
XML::LibXML Perl-XML-LibXML	perl-XML-LibXML
DBD::mysql	perl-DBD-MySQL
URI::URL	perl-URI
HTTP::Antwort	perl-libwww-perl
HTTP::Headers	perl-libwww-perl
Netto::SSLeay	perl-Net-SSLeay
URI::Escape	perl-URI
LWP::Protokoll::https Perl-LWP-Protocol-https	perl-LWP-Protocol-https
XML::Parser	perl-XML-Parser
LWP::UserAgent	perl-libwww-perl
NET: LDAP	perl-LDAP
Datum::Kalk	perl-Date-CalcXML

Schritte

1. Melden Sie sich beim Linux-Server als an `root` Benutzer:

2. Überprüfen Sie, ob alle für WFA erforderlichen Perl Module auf dem System installiert sind:

```
./WFA-4.2.0.0.0.bin -l
```

3. Wenn keine Perl-Module erkannt werden, prüfen Sie, ob sie im konfigurierten Repository verfügbar sind:

```
yum search Perl-module-name
```

Wenn das DBD::mysql-Modul nicht erkannt wird:

```
yum search perl-DBD-MySQL
```

4. Wenn sich keine Perl-Module im Repository befinden, konfigurieren Sie das Repository, das das Perl-Modul enthält, oder laden Sie das Perl-Modul aus dem Internet herunter.

5. Installieren Sie fehlende Perl-Module aus dem konfigurierten Repository:

```
yum -y install Perl-module-name
```

Installieren Sie das DBD:mysql-Modul aus dem konfigurierten Repository:

```
yum -y install perl-DBD-MySQL
```

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 VCS für hohe Verfügbarkeit

Sie müssen Workflow Automation (WFA) in einer Veritas Cluster Server (VCS) Umgebung installieren und konfigurieren, um Hochverfügbarkeit einzurichten und Failover zu ermöglichen. 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.



VCS ist die einzige Clustering-Lösung, die von WFA unter Linux unterstützt wird.

VCS zur Installation von OnCommand Workflow Automation konfigurieren

Bevor Sie OnCommand Workflow Automation (WFA) in Veritas Cluster Server (VCS) installieren, müssen Sie sicherstellen, dass die Cluster-Knoten zur Unterstützung von WFA ordnungsgemäß konfiguriert sind.

- VCS muss auf beiden Knoten des Clusters gemäß den Anweisungen im *Veritas Cluster Server 6.1.1 Installation Guide* installiert werden.
- Um Benachrichtigungen über Cluster-Ereignisse zu erhalten, muss die VCS-Software gemäß den Anweisungen im *Veritas Cluster Server Administrator's Guide* für SNMP und SMTP konfiguriert werden.
- Alle Anforderungen und Richtlinien für die Konfiguration von Cluster-Servern müssen gemäß VCS-Dokumentation erfüllt werden.
- SnapDrive für UNIX muss installiert sein, wenn Sie LUNs mit SnapDrive für UNIX erstellen möchten.
- Auf beiden Cluster-Nodes muss eine unterstützte Version des Betriebssystems ausgeführt werden.

Die mindestens unterstützten Betriebssysteme sind Red hat Enterprise Linux 7.0 und VCS 6.1.1.

- Dieselbe Version von WFA muss auf beiden Cluster-Nodes über denselben Pfad installiert werden.
- Der WFA Server muss über Fibre Channel (FC) oder iSCSI mit dem Storage-System verbunden sein.
- Die Latenz muss zwischen dem WFA Server und dem Storage-System mindestens betragen.
- Der FC-Link muss aktiv sein, und die erstellten LUNs müssen beiden Cluster-Nodes zugänglich sein.
- Auf jedem System müssen mindestens zwei Netzwerkschnittstellen eingerichtet sein: Eine für die Node-zu-Node-Kommunikation und die andere für die Node-to-Client-Kommunikation.
- Der Name der für die Node-to-Client-Kommunikation verwendeten Netzwerkschnittstelle sollte auf beiden Systemen identisch sein.
- Zwischen den Cluster-Nodes muss eine separate Heartbeat-Verbindung hergestellt werden. Andernfalls wird die Netzwerkschnittstelle für die Kommunikation zwischen den Cluster-Nodes verwendet.
- Um hohe Verfügbarkeit zu gewährleisten, muss ein gemeinsamer Speicherort erstellt werden.

Sie können SnapDrive für UNIX verwenden, um den freigegebenen Speicherort zu erstellen.

Sie können die LUNs auch über SnapDrive oder über die Befehlszeilenschnittstelle des Storage-Systems verwalten. Weitere Informationen finden Sie in der Kompatibilitätsmatrix für SnapDrive für UNIX.

Schritte

1. Überprüfen Sie, ob VCS ordnungsgemäß installiert ist: `hastatus -summary`

Beide Knoten müssen online sein und der VCS Service muss auf beiden Knoten ausgeführt werden.

2. Stellen Sie mithilfe einer der folgenden Optionen sicher, dass auf die LUNs für beide Nodes zugegriffen werden kann:
 - Natives Managen der LUNs
 - Verwenden Sie SnapDrive für UNIX:
 - i. Installieren Sie SnapDrive für UNIX auf beiden Knoten.
 - ii. Konfigurieren Sie SnapDrive für UNIX auf beiden Knoten.
 - iii. Führen Sie auf dem ersten Knoten den aus `snapdrive storage create` Befehl zum Erstellen einer LUN.
 - iv. Vergewissern Sie sich, dass die auf dem ersten Node erstellte LUN auf dem zweiten Node sichtbar ist, indem Sie den ausführen `snapdrive storage show -all` Befehl.

Installieren Sie OnCommand Workflow Automation unter Linux

Sie können OnCommand Workflow Automation (WFA) über die Befehlszeilenschnittstelle (CLI) installieren.

- Sie müssen die Installationsvoraussetzungen überprüft haben.

Installationsvoraussetzungen

- 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.

Sie können den Standardinstallationsort an der Shell-Eingabeaufforderung ändern: `./WFA-version_number.bin [-i WFA_install_directory] [-d mysql_data_directory]`

Wenn Sie den Standardspeicherort für die Installation ändern, wird das MySQL-Datenverzeichnis bei der Deinstallation von WFA nicht gelöscht. Sie müssen das Verzeichnis manuell löschen.



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

Schritte

1. Melden Sie sich beim Linux-Server als `root` Benutzer:
2. Navigieren Sie zum Verzeichnis, in dem sich die ausführbare `.bin`-Datei befindet.
3. Installation von WFA durch Auswahl einer der folgenden Methoden:
 - Interaktive Installation
 - i. Starten Sie die interaktive Sitzung: `./WFA-version_number.bin`
 - ii. Geben Sie die Anmeldeinformationen für den standardmäßigen Administratorbenutzer ein, und drücken Sie dann die Eingabetaste.

Sie müssen die Anmeldedaten für den Admin-Benutzer notieren und sicherstellen, dass das Passwort die folgenden Kriterien erfüllt:

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

``" ; < > , = & ^`

- iii. Akzeptieren Sie die Standard-Ports für die WFA-Konfiguration oder stellen Sie benutzerdefinierte Ports bereit, und drücken Sie dann die Eingabetaste.
- iv. Geben Sie Ihren Firmennamen und einen Standortnamen an, und drücken Sie anschließend die

Eingabetaste.

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

v. Überprüfen Sie, ob WFA erfolgreich installiert ist, indem Sie eine der folgenden Aktionen auswählen:

- Zugriff auf WFA über einen Webbrowser
- Überprüfen Sie, ob der NetApp WFA Server Service und der NetApp WFA Database Service ausgeführt werden:

```
service wfa-server status
service wfa-db status
```

◦ Automatische Installation

An der Shell-Eingabeaufforderung:

```
./WFA-version_number.bin [-u admin_user_name] [-p admin_user_password] [-m
https_port] [-n http_port] [-c company_name] [-s site_name] [-i
install_directory] [-d mysql_data_directory] [-y] [-b]
```

Wenn Sie eine automatische Installation ausführen möchten, müssen Sie Werte für alle Befehlsoptionen angeben. Folgende Befehlsoptionen stehen zur Verfügung:

Option	Beschreibung
-Y	Option zum überspringen überspringt die Installationsbestätigung
-B	Option zum überspringen von Überspringen, um während eines Upgrades ein Backup der WFA Datenbank zu erstellen
-U	Admin-Benutzername

Option	Beschreibung
-P	<p>Admin-Benutzer-Passwort das Admin-Benutzerpasswort muss die folgenden Kriterien erfüllen:</p> <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 Passworteingabe: `" ; < > , = & ^
-M	HTTPS-Port
-N	HTTP-Port
-S	Standortname
-C	Name des Unternehmens
-i	Pfad für das Installationsverzeichnis
-D	MySQL-Datenverzeichnis
-H	Mit dieser Option wird die Hilfe angezeigt

Verwandte Informationen

["NetApp Support"](#)

Konfigurieren Sie Workflow Automation in VCS

Nach der Installation von Workflow Automation (WFA) in VCS müssen WFA in VCS mithilfe von Konfigurationsskripten konfiguriert werden, um hohe Verfügbarkeit zu gewährleisten.

- Sie müssen dieselbe Version von WFA auf beiden Cluster-Nodes installiert haben.
- Sie müssen den gleichen Installationspfad für beide Nodes aufweisen.
- Sie müssen ein Backup von WFA erstellen.

Schritte

1. Melden Sie sich beim ersten Node des Clusters an.
2. Verwenden Sie Cluster Manager, um zu überprüfen, ob der HA-Status beider Nodes ausgeführt wird.
3. Führen Sie an der Shell Eingabeaufforderung das `ha_setup.pl` Skript aus, um die WFA Daten an den gemeinsamen Speicherort zu verschieben und WFA mit VCS für Failover zu konfigurieren: `perl ha_setup.pl --first [-t type_of_cluster_vcs] [-g cluster_group_name] [-e NIC_card_name] [-i IP_address] [-m Netmask] [-n cluster_name] [-f mount_point_of_shared_LUN] [-v name_of_logical_volume] [-d disk_group_name] [-l install_directory]`

Das Skript ist beim Standardinstallationsverzeichnis unter `/opt/netapp/wfa/bin/ha/` verfügbar.

```
perl ha_setup.pl --first -t vcs -g WFA -e eth0 -i 10.238.170.3 -m
255.255.255.0 -n wfa_cluster -f /mnt/wfa_mount/ -v lun_volume -d lun_dg -l
/opt/netapp/wfa
```

4. Überprüfen Sie mit Cluster Manager, ob WFA Services, Bereitstellungspunkt, virtuelle IP, NIC und Volume-Gruppe der Cluster-Gruppe hinzugefügt werden.
5. Verwenden Sie Cluster Manager, um WFA Ressourcen zum sekundären Node zu verschieben:
 - a. Wählen Sie die Cluster-Gruppe aus, und klicken Sie mit der rechten Maustaste darauf.
 - b. Wählen Sie **Wechseln Zu > Sekundärer Knoten**.
6. Stellen Sie sicher, dass sich Datenmontierung, virtuelle IP-, Volume- und NIC-Karten auf dem zweiten Node des Clusters befinden.
7. Versetzen Sie die WFA Services offline, indem Sie Cluster Manager verwenden:
 - a. Wählen Sie **WFA > Applikation > wfa-Server** aus.
 - b. Klicken Sie mit der rechten Maustaste, und wählen Sie **Offline**.
 - c. Wählen Sie **WFA > Applikation > wfa-db** aus.
 - d. Klicken Sie mit der rechten Maustaste, und wählen Sie **Offline**.
8. Führen Sie an der Shell 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_vcs] [-f mount_point_of_shared_LUN]`

Das Skript ist beim Standardinstallationsverzeichnis unter `/opt/netapp/wfa/bin/ha/` verfügbar.

```
perl ha_setup.pl --join -t vcs -f /mnt/wfa_mount/
```

9. Gehen Sie zu Cluster Manager und klicken Sie auf **Clustergruppe > Online > Server**.

Es kann eine Weile dauern, bis Cluster Manager zeigt, dass die Anwendungsressourcen online sind. Sie können auch mit der rechten Maustaste auf die Anwendungsressourcen klicken und überprüfen, ob die Ressourcen online sind.

10. Stellen Sie sicher, dass WFA über die während dieser Konfiguration verwendete IP-Adresse zugänglich ist.

Konfiguration einer früheren Version von OnCommand Workflow Automation für Hochverfügbarkeit

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 Veritas Cluster Server Konfiguration (VCS) fortfahren.

3. VCS konfigurieren, um WFA auf dem primären Node zu installieren.

"VCS zur Installation von WFA konfigurieren"

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

"WFA installieren"

5. Konfigurieren Sie WFA in VCS.

"Konfigurieren Sie WFA in VCS"

Der WFA Server ist für Hochverfügbarkeit konfiguriert.

Deinstallieren Sie Workflow Automation in einer VCS-Umgebung

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

Schritte

1. Versetzen Sie die Services in den Offline-Modus, indem Sie Cluster Manager verwenden:
 - a. Klicken Sie mit der rechten Maustaste auf die Cluster-Gruppe.
 - b. Wählen Sie **Offline** und dann den Knoten aus.
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 Cluster Manager:
 - a. Klicken Sie mit der rechten Maustaste auf die Cluster-Gruppe.
 - b. Wählen Sie **Löschen**.
4. Löschen Sie die Daten manuell am freigegebenen Speicherort.

Sichern Sie die OnCommand Workflow Automation-Datenbank und -Konfigurationen unter Linux 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.



- Während der Disaster Recovery ist ein umfassendes Backup von WFA Datenbanken und Konfigurationen erforderlich und kann sowohl in Standalone- als auch in Hochverfügbarkeitsumgebungen eingesetzt werden.
- Im Disaster Recovery können nur die CLI-Befehle oder REST-APIs für umfassende Backup- und Restore-Vorgänge verwendet werden.

Sie können die Web-Benutzeroberfläche nicht zum Sichern oder Wiederherstellen der WFA Datenbank während eines Disaster Recovery verwenden.

Schritte

1. Sichern der OnCommand Workflow Automation-Datenbank.

["Backup der OnCommand Workflow Automation-Datenbank"](#)

2. Wiederherstellen eines früheren Backups der OnCommand Workflow Automation-Datenbank.

["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-Standardport für WFA angegeben haben, müssen Sie die Portnummer wie folgt angeben:

`https://wfa_server_ip:port/download/wfa_ocsetup.exe.`

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

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

2. Doppelklicken Sie auf 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) Ihres WFA Servers.

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

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

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

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

2. Verwenden Sie den folgenden Befehl im Terminal, um die Datei `wfa_ocsetup.sh` in eine ausführbare Datei zu ändern:

```
chmod +x wfa_ocsetup.sh
```

3. Führen Sie das Skript durch, indem Sie im Terminal Folgendes eingeben:

```
./wfa_ocsetup.sh 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 *****
```

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 ein Datenbankbenutzerkonto auf dem Unified Manager Server 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*.

- 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>

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 Bestätigungsdiaologfeld 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	Speichern Sie die Anmeldeinformationen, und wählen Sie eine der folgenden Optionen: <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	Nur Konfigurationsdaten senden
Details zur WFA Konfiguration sowie Daten in WFA Cache-Tabellen wie z. B. dem Schema	Senden von Konfigurations- und Cache-Daten (Standard)
Details zur WFA Konfiguration, Daten in WFA Cache-Tabellen und Daten im Installationsverzeichnis	Senden von Konfigurations- und Zwischenspeichern erweiterter Daten



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

6. Testen, dass Sie eine AutoSupport Nachricht herunterladen können:
 - a. Klicken Sie Auf **Download**.
 - b. Wählen Sie im Dialogfeld, das geöffnet wird, den Speicherort 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. Fügen Sie den erforderlichen Rollen eine Liste mit Active Directory-Gruppennamen hinzu.



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

3. Klicken Sie auf **Administration > WFA Konfiguration**.
4. Klicken Sie im Dialogfeld WFA Configuration auf die Registerkarte **Authentifizierung** und aktivieren Sie dann das Kontrollkästchen **Active Directory aktivieren**.
5. 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.
6. Klicken Sie auf **Hinzufügen**, um das Active Directory in der Tabelle Active Directory Servers mit einem URI-Format hinzuzufügen: 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\[:port\]

7. Geben Sie die Anmeldeinformationen an, um den LDAP-Server und den Basis-DN zu binden.
8. Testen Sie die Authentifizierung des angegebenen Benutzers:
 - a. Geben Sie den Benutzernamen und das Kennwort ein.
 - b. Klicken Sie Auf **Authentifizierung Testen**.



Sie müssen die Active Directory-Gruppe hinzugefügt haben, um die Authentifizierung des angegebenen Benutzers in WFA zu testen.

9. Klicken Sie Auf **Speichern**.

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.

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 sich als Root-Benutzer beim WFA Host-System angemeldet haben.

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. Navigieren Sie an der Shell-Eingabeaufforderung zum folgenden Verzeichnis auf dem WFA Server:
WFA_install_location/wfa/bin/
2. Geben Sie den folgenden Befehl ein:

```
./wfa --password-policy=none --restart=WFA
```

Ändern Sie die Standard-Kennwortrichtlinie

OnCommand Workflow Automation (WFA) ist so konfiguriert, dass eine Passwortrichtlinie für lokale Benutzer durchgesetzt wird. Sie können die Standard-Passwortrichtlinie ändern.

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

- In diesem Verfahren wird der WFA Standardinstallationspfad verwendet.

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

- Der Befehl für die Standard-Passwortrichtlinie ist `./wfa --password-Policy=default`.

Der Standardwert ist

`"minLength=true,8;specialChar=true,1;digitalChar=true,1;lowercaseChar=true,1;uppercaseChar=true,1;whitespaceChar=false"`. Dies bedeutet, dass die Standard-Passwortrichtlinie eine Mindestlänge von acht Zeichen haben muss und mindestens 1 Sonderzeichen, 1 Ziffer, 1 Kleinbuchstaben, 1 Großbuchstaben und keine Leerzeichen enthalten muss.

Schritte

1. Navigieren Sie an der Shell-Eingabeaufforderung zum folgenden Verzeichnis auf dem WFA Server:
`WFA_install_location/wfa/bin/`
2. Ändern Sie die Standard-Passwortrichtlinie durch Eingabe des folgenden Befehls:

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

Aktivieren oder deaktivieren Sie den Remote-Zugriff auf die OnCommand Workflow Automation-Datenbank

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

- Sie müssen sich als Root-Benutzer beim WFA Host-System angemeldet haben.
- Falls eine Firewall auf dem WFA Host-System installiert ist, müssen Sie Ihre Firewall-Einstellungen so konfiguriert haben, dass der Zugriff auf den MySQL Port (3306) vom Remote-System aus möglich ist.

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. Wechseln Sie zum folgenden Verzeichnis auf dem WFA Server: `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>

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 sich als Root-Benutzer beim WFA Host-System angemeldet haben.

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. Navigieren Sie an der Shell-Eingabeaufforderung zum folgenden Verzeichnis auf dem WFA Server:
WFA_install_location/wfa/bin/
2. Geben Sie den folgenden Befehl ein:

```
./wfa --txn-timeout[=TIMEOUT] --restart=WFA
```

```
./wfa --txn-timeout=1000 --restart=WFA
```

Konfigurieren Sie den Zeitüberschreitungswert für Workflow Automation

Sie können den Zeitüberschreitungswert für die Web-GUI (WFA) konfigurieren, anstatt den Standardwert für eine Zeitüberschreitung von 180 Sekunden zu verwenden.

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. Sie können den Zeitüberschreitungswert nicht über die WFA Web GUI einstellen.

Schritte

1. Melden Sie sich als Root-Benutzer auf der WFA Host Machine 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 3.1 oder höher

Sie können ein Upgrade von OnCommand Workflow Automation (WFA) 3.1 oder höher auf die neueste verfügbare Version von WFA durchführen, um die neuen Funktionen und Verbesserungen zu nutzen.

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

Sie können nur von WFA 5.0 oder 4.2 aus auf 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.

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 selbst installieren:

- Wenn Sie ein Upgrade von WFA 4.2 auf neuere Versionen von WFA durchführen.
- Upgrade von WFA 3.1 oder höher durch Auswahl einer der folgenden Methoden:
 - Interaktive Installation
 - i. Navigieren Sie auf dem WFA Host Machine zur .bin-Binärdatei und führen Sie die Datei anschließend aus.
 - ii. Befolgen Sie die Anweisungen auf dem Bildschirm, um die Aktualisierung abzuschließen.
 - Automatische Installation

An der Shell-Eingabeaufforderung:

```
./WFA-version_number-build_number.bin [-y] [-u admin_user_name] [-p
admin_user_password]
```

Beispiel:

```
./WFA-3.1-Z3234343435.bin -y -u admin -p Company*234
```

Während der automatischen Aktualisierung müssen Sie Werte für alle der folgenden Befehlsoptionen enthalten:

- -y Überspringt die Installationsbestätigung.
- -u Gibt den Admin-Benutzernamen an.
- -p Gibt das Admin-Benutzerpasswort an.

Wenn Sie das Admin-Benutzerpasswort nicht angegeben haben, müssen Sie bei der entsprechenden Eingabeaufforderung das Passwort eingeben.

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 Workflow Automation (WFA) wie OpenJDK und MySQL in Linux durchführen.

Upgrade von OpenJDK

Oracle JRE wird nicht mehr in OnCommand Workflow Automation unterstützt. In dieser Version ersetzt OpenJDK Oracle JRE für Linux. Sie können auf eine neuere Version von OpenJDK auf dem Linux-Server, auf dem OnCommand Workflow Automation installiert ist, aktualisieren, um Fehlerbehebungen für Sicherheitslücken zu erhalten.

Sie müssen Root-Rechte für das Linux System besitzen, auf dem WFA installiert ist.

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 Root-Benutzer auf der WFA Host Machine an.
2. Installieren Sie die neueste Version von OpenJDK 11 aus dem yum-Repository auf dem Zielsystem.
3. Beenden Sie an der Shell-Eingabeaufforderung den WFA Server.
4. Starten Sie den WFA Server neu.

Aktualisieren Sie MySQL auf Linux

Sie können auf eine neuere Version von MySQL auf dem Linux-Server aktualisieren, auf dem OnCommand Workflow Automation installiert ist, um die Behebung von Sicherheitslücken zu erhalten.

Sie müssen Root-Rechte für das Linux System besitzen, auf dem WFA installiert ist.



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

Sie können nur ein Upgrade auf kleinere Updates von MySQL 5.7 durchführen, z. B. 5.7.22 auf 5.7.26. Sie können kein Upgrade auf die Hauptversionen von MySQL durchführen, z. B. Version 5.8.

Schritte

1. Melden Sie sich als Root-Benutzer auf der WFA Host Machine an.
2. Laden Sie das neueste MySQL Community Server .rpm Paket auf dem Zielsystem herunter.
3. Enttar das Paket in ein Verzeichnis auf dem Zielsystem.
4. Sie erhalten nach dem Entwerfen des Bundles mehrere .rpm Pakete im Verzeichnis, WFA benötigt jedoch nur die folgenden rpm-Pakete:

- mysql-Community-Client-5.7.x
- mysql-Community-libs-5.7.x
- mysql-Community-Server-5.7.x
- mysql-Community-common-5.7.x
- mysql-Community-libs-compat-5.7.x Löschen Sie alle anderen .rpm-Pakete. Die Installation aller Pakete in einem rpm-Paket verursacht keine Probleme.

5. Beenden Sie an der Shell-Eingabeaufforderung die WFA-Datenbank und die Server-Services:

```
service wfa-db stop
```

```
service wfa-server stop
```

6. Rufen Sie das Upgrade von MySQL mit dem folgenden Befehl auf:

```
rpm -uvh *.rpm
```

*.rpm Bezieht sich auf die .rpm-Pakete im Verzeichnis, in dem Sie die neuere Version von MySQL heruntergeladen haben.

7. Starten Sie die WFA Services:

```
service wfa-db start
```

```
service wfa-server start
```

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 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 Sicherungsbenuzer 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 die WFA Datenbank mithilfe der CLI wieder her (vollständig)

Sie können die OnCommand Workflow Automation (WFA) Datenbank und die unterstützten Konfigurationen wiederherstellen, die Sie zuvor über die Befehlszeilenschnittstelle (CLI) gesichert haben. 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. Wiederherstellen der WFA Datenbank:

```
wfa --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 die WFA Datenbank mithilfe der CLI wieder her (regelmäßig)

Sie können die OnCommand Workflow Automation (WFA) Datenbank, die Sie zuvor mit Hilfe der Befehlszeilenschnittstelle (CLI) gesichert haben, regelmäßig wiederherstellen. In einer normalen Wiederherstellung ist es nur möglich, die WFA Datenbank wiederherzustellen.

- 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. Wiederherstellen der WFA Datenbank:

```
wfa --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 `/opt/netapp/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 `/opt/netapp/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, den Sie beim Installieren des OnCommand Workflow Automation (WFA) Servers erstellt haben, vergessen haben, können Sie ihn zurücksetzen.

- Sie müssen Root-Rechte für das Linux-System besitzen, auf dem WFA installiert ist.
- Die WFA Services müssen ausgeführt werden.
- Bei diesem Verfahren wird nur das Passwort des während der WFA Installation erstellten Admin-Benutzers zurückgesetzt.

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.

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

Schritte

1. Melden Sie sich als Root-Benutzer beim Linux-System an, auf dem WFA installiert ist.
2. Navigieren Sie an der Shell-Eingabeaufforderung zum folgenden Verzeichnis auf dem WFA Server:
`WFA_install_location/wfa/bin/`
3. Geben Sie den folgenden Befehl ein:

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

Falls Sie kein Passwort angegeben haben, müssen Sie das Passwort bei der entsprechenden Eingabeaufforderung eingeben.

4. Folgen Sie an der Shell-Eingabeaufforderung den Anweisungen auf dem Bildschirm.

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 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 Shell-Eingabeaufforderung auf dem WFA-Server, und ändern Sie das Verzeichnis in den folgenden Speicherort: WFA_install_location/wfa/bin/
4. Geben Sie an der Shell-Eingabeaufforderung Folgendes ein, um den Datenbankschlüssel zu erhalten:

```
./wfa -key
```

5. Notieren Sie den angezeigten Datenbankschlüssel.
6. WFA deinstallieren.
7. Installation von WFA auf dem erforderlichen System
8. Öffnen Sie eine Shell-Eingabeaufforderung auf dem WFA-Server, und ändern Sie das Verzeichnis in den folgenden Speicherort: WFA_install_location/wfa/bin/

9. Installieren Sie an der Shell-Eingabeaufforderung den Datenbankschlüssel, indem Sie den folgenden Befehl eingeben:

```
./wfa -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 einem einzigen Befehl von Ihrem Red hat Enterprise Linux Computer deinstallieren.

Sie müssen Root-Benutzerzugriff auf den Red hat Enterprise Linux-Rechner haben, von dem aus WFA deinstalliert werden soll.

Schritte

1. Melden Sie sich als Root-Benutzer an der Red hat Enterprise Linux-Maschine an, von der aus WFA deinstalliert werden soll.
2. Geben Sie an der Shell-Eingabeaufforderung den folgenden Befehl ein:

```
rpm -e wfa
```

Wenn sich der Standardspeicherort für die Installation geändert hat, wird das MySQL-Datenverzeichnis bei der Deinstallation von WFA nicht gelöscht. Sie müssen das Verzeichnis manuell löschen.

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 Root-Rechte für das Linux-System besitzen, auf dem WFA installiert 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. Melden Sie sich als Root-Benutzer auf der WFA Host Machine an.
2. Navigieren Sie an der Shell-Eingabeaufforderung zum folgenden Verzeichnis auf dem WFA Server:
WFA_install_location/wfa/bin
3. Stoppen Sie die WFA Datenbank- und Serverdienste:

```
./wfa --stop=WFA
```

```
./wfa --stop=DB
```

4. Löschen Sie die datei wfa.keystore aus dem folgenden Verzeichnis:
WFA_install_location/wfa/jboss/Standalone/Configuration/keystore.
5. Öffnen Sie eine Shell-Eingabeaufforderung auf dem WFA-Server, und ändern Sie dann das Verzeichnis in den folgenden Speicherort: <OpenJDK_install_Location>/bin
6. Erhalten Sie den Datenbankschlüssel:

```
keytool -keysize 2048 -genkey -alias "ssl keystore" -keyalg RSA -keystore  
"WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore"  
-validity xxxx
```

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

7. 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."](#)

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

```
./wfa --start=DB
```

```
./wfa --start=WFA
```

Erstellen Sie eine Anfrage zum Signieren eines Zertifikats für Workflow Automation

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

- Sie müssen Root-Rechte für das Linux-System besitzen, auf dem WFA installiert ist.

- 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 Root-Benutzer auf der WFA Host Machine an.
2. Öffnen Sie eine Shell-Eingabeaufforderung auf dem WFA-Server, und ändern Sie dann das Verzeichnis in den folgenden Speicherort: <OpenJDK_install_Location>/bin
3. CSR-Datei erstellen:

```
keytool -certreq -keystore
WFA_install_location/wfa/jboss/standalone/configuration/keystore/wfa.keystore
-alias "ssl keystore" -file /root/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 chain_cert.cer
```

chain_cert.cer Ist die von der Zertifizierungsstelle empfangene Datei für die Kette. 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"
-trustcacerts -file certificate.cer
```

certificate.cer Ist die von der Zertifizierungsstelle empfangene Datei für die Kette.

8. Starten Sie die WFA Services:

```
./wfa --start=DB
```

```
./wfa --start=WFA
```

Verwalten von Perl- und Perl-Modulen

OnCommand Workflow Automation (WFA) unterstützt Perl-Befehle für Workflow-Vorgänge. Sie können Ihre bevorzugten Perl-Verteilung und Perl-Module installieren und konfigurieren.

Die erforderlichen Perl-Module des NetApp Manageability SDK sind ebenfalls bei der Installation von WFA installiert. Für die erfolgreiche Ausführung von Perl-Befehlen sind die NetApp Manageability SDK Perl-Module erforderlich.

Sie können bei Bedarf zusätzliche Perl-Module aus den Red hat-Paketarchiven oder aus den CPAN-Repositories installieren.

Konfigurieren Sie Ihre bevorzugte Perl-Verteilung

Das Perl-Paket, das auf Ihrem System installiert ist, wird von OnCommand Workflow Automation verwendet. 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.

Schritte

1. Navigieren Sie an der Shell-Eingabeaufforderung zum folgenden Verzeichnis auf dem WFA Server:
WFA_install_location/wfa/bin/
2. Geben Sie den folgenden Befehl ein:

```
/wfa --custom-perl[=PERL_PATH] --restart=WFA
```

```
/wfa --custom-perl=/usr/local/perl5-11/bin/perl --restart=WFA
```

Fehlerbehebung bei Installations- und Konfigurationsproblemen

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

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.

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.