



OnCommand Workflow Automation wird konfiguriert

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

Inhalt

- OnCommand Workflow Automation wird konfiguriert. 1
 - Konfigurieren Sie AutoSupport. 1
 - Konfigurieren Sie die Authentifizierungseinstellungen 2
 - Fügen Sie Active Directory-Gruppen hinzu 3
 - Konfigurieren Sie E-Mail-Benachrichtigungen 3
 - Konfigurieren Sie SNMP 4
 - Syslog Konfigurieren 5
 - Konfigurieren von Protokollen zum Anschluss an Remote-Systeme 6

OnCommand Workflow Automation wird konfiguriert

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

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

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

Konfigurieren Sie AutoSupport

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

Schritte

1. Melden Sie sich über einen Webbrowser als Administrator bei WFA an.
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Einstellungen** auf **AutoSupport**.
3. Vergewissern Sie sich, dass das Feld **AutoSupport** aktivieren ausgewählt ist.
4. Geben Sie die erforderlichen Informationen ein.
5. Wählen Sie eine der folgenden Optionen aus der Liste * Content* aus:

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



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

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

Konfigurieren Sie die Authentifizierungseinstellungen

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

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

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



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

Schritte

1. Melden Sie sich über einen Webbrowser als Administrator bei WFA an.
2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Setup** auf **Authentifizierung**.
3. Aktivieren Sie das Kontrollkästchen * Active Directory aktivieren*.
4. Geben Sie die erforderlichen Informationen in die folgenden Felder ein:
 - a. Wenn Sie das Domain-Format des Benutzers@für Domain-Benutzer verwenden möchten, ersetzen Sie sAMAccountName im Feld **User Name attribut** durch userPrincipalName.
 - b. Wenn für Ihre Umgebung eindeutige Werte erforderlich sind, bearbeiten Sie die erforderlichen Felder.
 - c. Geben Sie die URI des AD-Servers wie folgt ein:
`ldap://active_directory_server_address\[[:port\]`

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

Wenn Sie LDAP über SSL aktiviert haben, können Sie das folgende URI-Format verwenden:

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

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



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

5. Klicken Sie Auf **Speichern**.
6. Wenn eine LDAP-Konnektivität zu einem Array erforderlich ist, konfigurieren Sie den WFA Service zur Anmeldung als erforderlicher Domänenbenutzer:

- a. Öffnen Sie die Windows Services-Konsole über Services.msc.
- b. Doppelklicken Sie auf den **NetApp WFA Server Service**.
- c. Klicken Sie im Dialogfeld Eigenschaften von NetApp WFA Server auf die Registerkarte **Anmelden** und wählen Sie dann **Dieses Konto** aus.
- d. Geben Sie den Benutzernamen und das Kennwort der Domäne ein, und klicken Sie dann auf **OK**.

Fügen Sie Active Directory-Gruppen hinzu

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

Schritte

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

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

5. Klicken Sie Auf **Speichern**.

Konfigurieren Sie E-Mail-Benachrichtigungen

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

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

Schritte

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

Konfigurieren Sie SNMP

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

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

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



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

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

Konfigurieren Sie SNMP-Version 1

Schritte

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

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

6. Wählen Sie im Abschnitt Benachrichtigen auf ein oder mehrere der folgenden Kontrollkästchen aus:
 - Workflow-Ausführung gestartet
 - Workflow-Ausführung erfolgreich abgeschlossen
 - Ausführung des Workflows fehlgeschlagen/teilweise erfolgreich
 - Workflow-Ausführung wartet auf Genehmigung
 - Erfassungsfehler
7. Klicken Sie auf **Testbenachrichtigung senden**, um die Einstellungen zu überprüfen.
8. Klicken Sie Auf **Speichern**.

Konfigurieren Sie SNMP-Version 3

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

Version 3 bietet zwei zusätzliche Sicherheitsoptionen:

- Version 3 mit Authentifizierung

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

- Version 3 mit Authentifizierung und Verschlüsselung

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

Schritte

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

Syslog Konfigurieren

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

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

Schritte

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



2. Klicken Sie auf **Einstellungen** und klicken Sie unter **Wartung** auf **Syslog**.
3. Aktivieren Sie das Kontrollkästchen **Syslog** aktivieren.
4. Geben Sie den Syslog-Host-Namen ein, und wählen Sie die Syslog-Ebene.
5. Klicken Sie Auf **Speichern**.

Konfigurieren von Protokollen zum Anschluss an Remote-Systeme

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

Schritte

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

Ihr Ziel ist	Tun Sie das...
Konfigurieren eines Protokolls für ein neues Remote-System	<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**.

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.