



Configurazione di OnCommand Workflow Automation

OnCommand Workflow Automation

NetApp
October 09, 2025

Sommario

Configurazione di OnCommand Workflow Automation	1
Accedere a OnCommand Workflow Automation	1
Origini dati OnCommand Workflow Automation	1
Configurazione di un utente di database su DataFabric Manager	2
Configurare un utente di database su Active IQ Unified Manager	4
Impostare un'origine dati	4
Aggiungere un server Unified Manager aggiornato come origine dati	6
Creare utenti locali	7
Configurare le credenziali di un sistema di destinazione	8
Configurazione di OnCommand Workflow Automation	9
Configurare AutoSupport	9
Configurare le impostazioni di autenticazione	10
Aggiungere gruppi Active Directory	11
Configurare le notifiche e-mail	11
Configurare SNMP	12
Configurare Syslog	14
Configurare i protocolli per la connessione ai sistemi remoti	14
Disattiva il criterio password predefinito	15
Modificare il criterio password predefinito per Windows	15
Abilitare l'accesso remoto al database OnCommand Workflow Automation su Windows	16
Limitare i diritti di accesso di OnCommand Workflow Automation sull'host	16
Modificare l'impostazione di timeout della transazione di OnCommand Workflow Automation	17
Configurare il valore di timeout per Workflow Automation	17
Abilitazione delle cifrazioni e aggiunta di nuove cifrazioni	18

Configurazione di OnCommand Workflow Automation

Una volta completata l'installazione di OnCommand Workflow Automation (Wfa), è necessario completare diverse impostazioni di configurazione. È necessario accedere a WFA, configurare gli utenti, configurare le origini dati, configurare le credenziali e configurare WFA.

Accedere a OnCommand Workflow Automation

È possibile accedere a OnCommand Workflow Automation (WFA) tramite un browser Web da qualsiasi sistema che abbia accesso al server WFA.

È necessario aver installato Adobe Flash Player per il browser Web.

Fasi

1. Aprire un browser Web e immettere una delle seguenti informazioni nella barra degli indirizzi:
 - ° `https://wfa_server_ip`
`wfa_server_ip` è l'indirizzo IP (indirizzo IPv4 o IPv6) o il nome di dominio completo (FQDN) del server WFA.
 - ° Se si accede a WFA sul server WFA: `https://localhost/wfa` Se è stata specificata una porta non predefinita per WFA, è necessario includere il numero della porta come segue:
 - ° `https://wfa_server_ip:port`
`https://localhost:port` Port (porta) è il numero della porta TCP utilizzato per il server WFA durante l'installazione.
2. Nella sezione Sign in (accesso), immettere le credenziali dell'utente amministratore immesse durante l'installazione.
3. Nel menu **Settings > Setup**, impostare le credenziali e un'origine dati.
4. Aggiungi ai preferiti l'interfaccia grafica Web WFA per un facile accesso.

Originи dati OnCommand Workflow Automation

OnCommand Workflow Automation (Wfa) opera sui dati acquisiti dalle origini dati. Sono disponibili varie versioni di Active IQ Unified Manager e VMware vCenter Server come tipi di origine dati WFA predefiniti. È necessario conoscere i tipi di origine dati predefiniti prima di impostare le origini dati per l'acquisizione.

Un'origine dati è una struttura di dati di sola lettura che funge da connessione all'oggetto origine dati di un tipo di origine dati specifico. Ad esempio, un'origine dati può essere una connessione a un database Active IQ Unified Manager di un tipo di origine dati Active IQ Unified Manager 6.3. È possibile aggiungere un'origine dati personalizzata a WFA dopo aver definito il tipo di origine dati richiesto.

Per ulteriori informazioni sui tipi di origine dati predefiniti, vedere la matrice di interoperabilità.

Informazioni correlate

"Tool di matrice di interoperabilità NetApp"

Configurazione di un utente di database su DataFabric Manager

Per configurare l'accesso in sola lettura del database DataFabric Manager 5.x a OnCommand Workflow Automation, è necessario creare un utente del database su DataFabric Manager 5.x.

Configurare un utente di database eseguendo ocsetup su Windows

È possibile eseguire il file ocsetup sul server DataFabric Manager 5.x per configurare l'accesso in sola lettura del database DataFabric Manager 5.x su OnCommand Workflow Automation.

Fasi

1. Scaricare il file wfa_ocsetup.exe in una directory del server DataFabric Manager 5.x dal seguente percorso: *Https://Wfa_Server_IP/download/wfa_ocsetup.exe*.

WFA_Server_IP è l'indirizzo IP (indirizzo IPv4 o IPv6) del server WFA.

Se è stata specificata una porta non predefinita per WFA, è necessario includere il numero della porta nel modo seguente: *Https://wfa_server_ip:port/download/wfa_ocsetup.exe*.

Port è il numero di porta TCP utilizzato per il server WFA durante l'installazione.

Se si specifica un indirizzo IPv6, è necessario racchiuderlo tra parentesi quadre.

2. Fare doppio clic sul file wfa_ocsetup.exe.
3. Leggere le informazioni nella procedura di installazione guidata e fare clic su **Avanti**.
4. Cercare o digitare la posizione di OpenJDK e fare clic su **Avanti**.
5. Immettere un nome utente e una password per ignorare le credenziali predefinite.

Viene creato un nuovo account utente del database con accesso al database DataFabric Manager 5.x.



Se non si crea un account utente, vengono utilizzate le credenziali predefinite. Per motivi di sicurezza, è necessario creare un account utente.

6. Fare clic su **Avanti** e rivedere i risultati.
7. Fare clic su **Avanti**, quindi su **fine** per completare la procedura guidata.

Configurare un utente del database eseguendo ocsetup su Linux

È possibile eseguire il file ocsetup sul server DataFabric Manager 5.x per configurare l'accesso in sola lettura del database DataFabric Manager 5.x su OnCommand Workflow Automation.

Fasi

1. Scaricare il file wfa_ocsetup.sh nella home directory sul server DataFabric Manager 5.x utilizzando il

seguente comando nel terminale:

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

WFA_Server_IP è l'indirizzo IP (indirizzo IPv4 o IPv6) del server WFA.

Se è stata specificata una porta non predefinita per WFA, è necessario includere il numero della porta come segue:

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

Port (porta) è il numero di porta TCP utilizzato per il server WFA durante l'installazione.

Se si specifica un indirizzo IPv6, è necessario racchiuderlo tra parentesi quadre.

2. Utilizzare il seguente comando nel terminale per modificare il file wfa_ocsetup.sh in un eseguibile: chmod +x wfa_ocsetup.sh
3. Eseguire lo script inserendo quanto segue nel terminale:

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

OpenJDK_path è il percorso verso OpenJDK.

/Opt/NTAPdfm/java

Il seguente output viene visualizzato sul terminale, a indicare che la configurazione è stata eseguita correttamente:

```
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. Immettere un nome utente e una password per ignorare le credenziali predefinite.

Viene creato un nuovo account utente del database con accesso al database DataFabric Manager 5.x.



Se non si crea un account utente, vengono utilizzate le credenziali predefinite. Per motivi di sicurezza, è necessario creare un account utente.

Il seguente output viene visualizzato sul terminale, a indicare che la configurazione è stata eseguita correttamente:

```

***** 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 *****

```

Configurare un utente di database su Active IQ Unified Manager

È necessario creare un utente di database su Active IQ Unified Manager per configurare l'accesso in sola lettura del database Active IQ Unified Manager su OnCommand Workflow Automation.

Fasi

1. Accedere a Active IQ Unified Manager con le credenziali di amministratore.
2. Fare clic su **Impostazioni > utenti**.
3. Fare clic su **Aggiungi nuovo utente**.
4. Selezionare **Database User** come tipo di utente.

Lo stesso utente deve essere utilizzato in OnCommand Workflow Automation mentre si aggiunge Active IQ Unified Manager come origine dati in OnCommand Workflow Automation.

Impostare un'origine dati

Per acquisire i dati dall'origine dati, è necessario impostare una connessione con un'origine dati in OnCommand Workflow Automation (Wfa).

- Per Active IQ Unified Manager 6.0 e versioni successive, è necessario aver creato un account utente del database sul server Unified Manager.

Per ulteriori informazioni, consultare la *Guida in linea di Unified Manager OnCommand*.

- La porta TCP per le connessioni in entrata sul server Unified Manager deve essere aperta.

Per ulteriori informazioni, consultare la documentazione sul firewall.

Di seguito sono riportati i numeri di porta TCP predefiniti:

Numero della porta TCP	Versione del server Unified Manager	Descrizione
3306	6.x	Server di database MySQL

- Per Performance Advisor, è necessario aver creato un account utente Active IQ Unified Manager con un ruolo minimo di GlobalRead.

Per ulteriori informazioni, consultare la *Guida in linea di Unified Manager OnCommand*.

- Per VMware vCenter Server, è necessario aver creato un account utente su vCenter Server.

Per ulteriori informazioni, consultare la documentazione di VMware vCenter Server.



È necessario aver installato VMware PowerCLI. Se si desidera eseguire i flussi di lavoro solo sulle origini dati di vCenter Server, non è necessario configurare il server Unified Manager come origine dati.

- La porta TCP per le connessioni in entrata su VMware vCenter Server deve essere aperta.

Il numero di porta TCP predefinito è 443. Per ulteriori informazioni, consultare la documentazione sul firewall.

Questa procedura consente di aggiungere più origini dati del server Unified Manager a WFA. Tuttavia, non è necessario utilizzare questa procedura se si desidera associare Unified Manager Server 6.3 e versioni successive a WFA e utilizzare la funzionalità di protezione nel server Unified Manager.

Per ulteriori informazioni sull'associazione di WFA con Unified Manager Server 6.x, consultare la *Guida in linea di Unified Manager OnCommand*.



Durante la configurazione di un'origine dati con WFA, è necessario tenere presente che i tipi di origine dati Active IQ Unified Manager 6.0, 6.1 e 6.2 sono deprecati nella release WFA 4.0 e che questi tipi di origine dati non saranno supportati nelle versioni future.

Fasi

1. Accedere a WFA utilizzando un browser Web.
2. Fare clic su **Impostazioni** e sotto **Setup** fare clic su **origini dati**.
3. Scegliere l'azione appropriata:

Per...	Eseguire questa operazione...
Creare una nuova origine dati	Fare clic su sulla barra degli strumenti.
Modificare un'origine dati ripristinata se si è aggiornato Wfa	Selezionare la voce dell'origine dati esistente e fare clic su sulla barra degli strumenti.

Se è stata aggiunta un'origine dati del server Unified Manager a WFA e successivamente è stata aggiornata la versione del server Unified Manager, WFA non riconosce la versione aggiornata del server Unified Manager. È necessario eliminare la versione precedente del server Unified Manager e aggiungere la versione aggiornata del server Unified Manager a WFA.

4. Nella finestra di dialogo Nuova origine dati, selezionare il tipo di origine dati richiesto e immettere un nome per l'origine dati e il nome host.

In base al tipo di origine dati selezionato, i campi porta, nome utente, password e timeout potrebbero essere popolati automaticamente con i dati predefiniti, se disponibili. È possibile modificare queste voci in

base alle esigenze.

5. Scegliere un'azione appropriata:

Per...	Eseguire questa operazione...
Active IQ Unified Manager 6.3 e versioni successive	<p>Inserire le credenziali dell'account Database User creato sul server Unified Manager. Per ulteriori informazioni sulla creazione di un account utente per database, consultare la <i>Guida in linea di Unified Manager OnCommand</i>.</p> <p></p> <p>Non è necessario fornire le credenziali di un account utente database Active IQ Unified Manager creato utilizzando l'interfaccia della riga di comando o lo strumento ocsetup.</p>
VMware vCenter Server (solo per Windows)	<p>(Solo per Windows) inserire il nome utente e la password dell'utente creato sul server VMware vCenter.</p>

6. Fare clic su **Save** (Salva).

7. Nella tabella origini dati, selezionare l'origine dati e fare clic su  sulla barra degli strumenti.

8. Verificare lo stato del processo di acquisizione dei dati.

Aggiungere un server Unified Manager aggiornato come origine dati

Se il server Unified Manager (5.x o 6.x) viene aggiunto come origine dati a WFA e il server Unified Manager viene aggiornato, È necessario aggiungere il server Unified Manager aggiornato come origine dati perché i dati associati alla versione aggiornata non vengono popolati in WFA, a meno che non venga aggiunto manualmente come origine dati.

Fasi

1. Accedere alla GUI Web di WFA come amministratore.
2. Fare clic su **Impostazioni** e in **Setup**, fare clic su **origini dati**.
3. Fare clic su  sulla barra degli strumenti.
4. Nella finestra di dialogo Nuova origine dati, selezionare il tipo di origine dati richiesto, quindi immettere un nome per l'origine dati e il nome host.

In base al tipo di origine dati selezionato, i campi porta, nome utente, password e timeout potrebbero essere popolati automaticamente con i dati predefiniti, se disponibili. È possibile modificare queste voci in base alle esigenze.

5. Fare clic su **Save** (Salva).
6. Selezionare la versione precedente del server Unified Manager e fare clic su  sulla barra degli strumenti.

7. Nella finestra di dialogo di conferma dell'eliminazione del tipo di origine dati, fare clic su **Sì**.
8. Nella tabella origini dati, selezionare l'origine dati, quindi fare clic su  sulla barra degli strumenti.
9. Verificare lo stato di acquisizione dei dati nella tabella History (Cronologia).

Creare utenti locali

OnCommand Workflow Automation (WFA) consente di creare e gestire utenti WFA locali con autorizzazioni specifiche per diversi ruoli, ad esempio guest, operatore, approvatore, architetto, admin e backup.

È necessario aver installato WFA e aver effettuato l'accesso come amministratore.

WFA consente di creare utenti per i seguenti ruoli:

- **Ospite**

Questo utente può visualizzare il portale e lo stato dell'esecuzione di un flusso di lavoro e può essere informato di una modifica dello stato dell'esecuzione di un flusso di lavoro.

- **Operatore**

A questo utente è consentito visualizzare in anteprima ed eseguire i flussi di lavoro per i quali l'utente ha accesso.

- **Approvatore**

A questo utente è consentito visualizzare in anteprima, eseguire, approvare e rifiutare i flussi di lavoro per i quali l'utente ha accesso.



Si consiglia di fornire l'ID email del responsabile dell'approvazione. Se sono presenti più responsabili dell'approvazione, è possibile fornire un ID e-mail di gruppo nel campo **e-mail**.

- **Architetto**

Questo utente ha pieno accesso alla creazione di flussi di lavoro, ma non può modificare le impostazioni globali del server WFA.

- **Amministratore**

Questo utente ha accesso completo al server WFA.

- **Backup**

Si tratta dell'unico utente in grado di generare in remoto i backup del server WFA. Tuttavia, l'utente non può accedere ad altri tipi di accesso.

Fasi

1. Fare clic su **Impostazioni** e in **Gestione** fare clic su **utenti**.
2. Creare un nuovo utente facendo clic su  sulla barra degli strumenti.
3. Inserire le informazioni richieste nella finestra di dialogo nuovo utente.

4. Fare clic su **Save** (Salva).

Configurare le credenziali di un sistema di destinazione

È possibile configurare le credenziali di un sistema di destinazione in OnCommand Workflow Automation (Wfa) e utilizzare le credenziali per connettersi a quel sistema specifico ed eseguire i comandi.

Dopo l'acquisizione iniziale dei dati, è necessario configurare le credenziali per gli array su cui vengono eseguiti i comandi. La connessione del controller PowerShell WFA funziona in due modalità:

- Con credenziali

WFA tenta prima di stabilire una connessione utilizzando HTTPS, quindi tenta di utilizzare HTTP. È inoltre possibile utilizzare l'autenticazione LDAP di Microsoft Active Directory per connettersi agli array senza definire le credenziali in WFA. Per utilizzare Active Directory LDAP, è necessario configurare l'array in modo che esegua l'autenticazione con lo stesso server LDAP di Active Directory.

- Senza credenziali (per sistemi storage che operano in 7-Mode)

WFA tenta di stabilire una connessione utilizzando l'autenticazione del dominio. Questa modalità utilizza il protocollo Remote procedure Call, protetto mediante il protocollo NTLM.

- WFA verifica il certificato SSL (Secure Sockets Layer) per i sistemi ONTAP. Se il certificato SSL non è attendibile, agli utenti potrebbe essere richiesto di rivedere e accettare/negare la connessione ai sistemi ONTAP.
- È necessario immettere nuovamente le credenziali per ONTAP, NetApp Active IQ e LDAP (Lightweight Directory Access Protocol) dopo il ripristino di un backup o il completamento di un aggiornamento in-place.

Fasi

1. Accedere a WFA tramite un browser Web come amministratore.
2. Fare clic su **Impostazioni** e in **Configurazione** fare clic su **credenziali**.
3. Fare clic su  sulla barra degli strumenti.
4. Nella finestra di dialogo nuove credenziali, selezionare una delle seguenti opzioni dall'elenco **corrispondenza**:

- **Esatto**

Credenziali per un indirizzo IP o un nome host specifico

- **Modello**

Credenziali per l'intera subnet o intervallo IP



L'utilizzo della sintassi delle espressioni regolari non è supportato per questa opzione.

5. Selezionare il tipo di sistema remoto dall'elenco **Type** (tipo).
6. Immettere il nome host o l'indirizzo IPv4 o IPv6 della risorsa, il nome utente e la password.



WFA 5.1 verifica i certificati SSL di tutte le risorse aggiunte a Wfa. Poiché la verifica del certificato potrebbe richiedere di accettare i certificati, l'utilizzo dei caratteri jolly nelle credenziali non è supportato. Se si utilizzano più cluster con le stesse credenziali, non è possibile aggiungerli tutti contemporaneamente.

7. Verificare la connettività eseguendo la seguente procedura:

Se è stato selezionato il seguente tipo di corrispondenza...	Quindi...
Esatto	Fare clic su Test .
Modello	Salvare le credenziali e scegliere una delle seguenti opzioni: <ul style="list-style-type: none">• Selezionare la credenziale e fare clic su sulla barra degli strumenti.• Fare clic con il pulsante destro del mouse e selezionare Test Connectivity (verifica connettività).

8. Fare clic su **Save** (Salva).

Configurazione di OnCommand Workflow Automation

OnCommand Workflow Automation (WFA) consente di configurare diverse impostazioni, ad esempio AutoSupport e notifiche.

Durante la configurazione di WFA, è possibile configurare una o più delle seguenti opzioni, in base alle esigenze:

- AutoSupport per l'invio di messaggi AutoSupport al supporto tecnico
- Server Microsoft Active Directory Lightweight Directory Access Protocol (LDAP) per l'autenticazione LDAP e l'autorizzazione per gli utenti WFA
- Mail per notifiche e-mail sulle operazioni del workflow e l'invio di messaggi AutoSupport
- SNMP (Simple Network Management Protocol) per le notifiche sulle operazioni del flusso di lavoro
- Syslog per la registrazione remota dei dati

Configurare AutoSupport

È possibile configurare diverse impostazioni AutoSupport, ad esempio la pianificazione, il contenuto dei messaggi AutoSupport e il server proxy. AutoSupport invia registri settimanali dei contenuti selezionati al supporto tecnico per l'archiviazione e l'analisi dei problemi.

Fasi

1. Accedere a WFA tramite un browser Web come amministratore.

2. Fare clic su **Impostazioni** e sotto **Configurazione** fare clic su **AutoSupport**.
3. Assicurarsi che la casella **Enable AutoSupport** (attiva protocollo) sia selezionata.
4. Inserire le informazioni richieste.
5. Selezionare una delle seguenti opzioni dall'elenco **contenuto**:

Se si desidera includere...	Quindi scegliere questa opzione...
Solo i dettagli di configurazione, ad esempio utenti, flussi di lavoro e comandi dell'installazione WFA	send only configuration data
Dettagli di configurazione WFA e dati nelle tabelle della cache WFA, come lo schema	send configuration and cache data (impostazione predefinita)
Dettagli sulla configurazione DI WFA, dati nelle tabelle della cache WFA e dati nella directory di installazione	send configuration and cache extended data



La password di qualsiasi utente WFA è *non* inclusa nei dati AutoSupport.

6. Verificare che sia possibile scaricare un messaggio AutoSupport:
 - a. Fare clic su **Download**.
 - b. Nella finestra di dialogo visualizzata, selezionare la posizione in cui salvare il file .7z.
7. Verificare l'invio di un messaggio AutoSupport alla destinazione specificata facendo clic su **Invia ora**.
8. Fare clic su **Save** (Salva).

Configurare le impostazioni di autenticazione

È possibile configurare OnCommand Workflow Automation (Wfa) in modo che utilizzi un server LDAP (Lightweight Directory Access Protocol) per l'autenticazione e l'autorizzazione.

È necessario aver configurato un server Microsoft ad LDAP nel proprio ambiente.

Per Wfa è supportata solo l'autenticazione Microsoft ad LDAP. Non è possibile utilizzare altri metodi di autenticazione LDAP, inclusi Microsoft ad Lightweight Directory Services (ad LDS) o Microsoft Global Catalog.



Durante la comunicazione, LDAP invia il nome utente e la password in testo normale. Tuttavia, la comunicazione LDAPS (LDAP Secure) è crittografata e sicura.

Fasi

1. Accedere a WFA tramite un browser Web come amministratore.
2. Fare clic su **Impostazioni** e in **Setup** fare clic su **autenticazione**.
3. Selezionare la casella di controllo **Enable Active Directory** (attiva Active Directory).
4. Inserire le informazioni richieste nei campi:
 - a. Se si desidera utilizzare il formato utente@dominio per gli utenti di dominio, sostituire

sAMAccountName con userPrincipalName nel campo **User name Attribute**.

- b. Se per l'ambiente sono richiesti valori univoci, modificare i campi obbligatori.
- c. Immettere l'URI del server ad nel modo seguente:

ldap://active_directory_server_address\[:port\]

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

Se LDAP su SSL è stato attivato, è possibile utilizzare il seguente formato URI:

ldaps://active_directory_server_address\[:port\]

- a. Aggiungere un elenco di nomi di gruppi ad ai ruoli richiesti.



È possibile aggiungere un elenco di nomi di gruppi ad ai ruoli richiesti nella finestra gruppi Active Directory.

5. Fare clic su **Save** (Salva).
6. Se è richiesta la connettività LDAP a un array, configurare il servizio WFA per l'accesso come utente di dominio richiesto:
 - a. Aprire la console dei servizi Windows utilizzando Services.msc.
 - b. Fare doppio clic sul servizio **NetApp WFA Server**.
 - c. Nella finestra di dialogo NetApp WFA Server Properties (Proprietà server NetApp WFA), fare clic sulla scheda **Log on** (accesso), quindi selezionare **questo account**.
 - d. Immettere il nome utente e la password del dominio, quindi fare clic su **OK**.

Aggiungere gruppi Active Directory

È possibile aggiungere gruppi Active Directory in OnCommand Workflow Automation (WFA).

Fasi

1. Accedere a WFA tramite un browser Web come amministratore.
2. Fare clic su **Impostazioni** e in **Gestione**, fare clic su **gruppi Active Directory**.
3. Nella finestra gruppi Active Directory, fare clic sull'icona **nuovo**.
4. Nella finestra di dialogo New Active Directory Group (nuovo gruppo Active Directory), immettere le informazioni richieste.

Se si seleziona **Approvatore** dall'elenco a discesa **ruolo**, si consiglia di fornire l'ID email del responsabile dell'approvazione. Se sono presenti più responsabili dell'approvazione, è possibile fornire un ID e-mail di gruppo nel campo **e-mail**. Selezionare i diversi eventi del flusso di lavoro per cui la notifica deve essere inviata al gruppo Active Directory specifico.

5. Fare clic su **Save** (Salva).

Configurare le notifiche e-mail

È possibile configurare OnCommand Workflow Automation (Wfa) per inviare notifiche e-mail sulle operazioni del flusso di lavoro, ad esempio, il flusso di lavoro è stato avviato o il flusso di lavoro non è riuscito.

È necessario aver configurato un mail host nel proprio ambiente.

Fasi

1. Accedere a WFA tramite un browser Web come amministratore.
2. Fare clic su **Impostazioni** e sotto **Configurazione** fare clic su **Mail**.
3. Inserire le informazioni richieste nei campi.
4. Verificare le impostazioni e-mail procedendo come segue:
 - a. Fare clic su **Send test mail** (Invia email di prova).
 - b. Nella finestra di dialogo verifica connessione, immettere l'indirizzo e-mail a cui si desidera inviare il messaggio.
 - c. Fare clic su **Test**.
5. Fare clic su **Save** (Salva).

Configurare SNMP

È possibile configurare OnCommand Workflow Automation (Wfa) per inviare trap SNMP (Simple Network Management Protocol) sullo stato delle operazioni del flusso di lavoro.

WFA ora supporta i protocolli SNMP v1 e SNMP v3. SNMP v3 offre funzionalità di sicurezza aggiuntive.

Il file .mib WFA fornisce informazioni sui trap inviati dal server WFA. Il file .mib si trova nella directory <WFA_install_location> del server WFA.



Il server WFA invia tutte le notifiche trap con un identificatore di oggetto generico (1.3.6.1.4.1.789.1.1.12.0).

Non è possibile utilizzare stringhe di comunità SNMP come community_string@SNMP_host per la configurazione SNMP.

Configurare SNMP versione 1

Fasi

1. Accedere a WFA tramite un browser Web come utente amministratore, quindi accedere al server WFA.
2. Fare clic su **Settings** (Impostazioni) e in **Setup** (Configurazione) fare clic su **SNMP**.
3. Selezionare la casella di controllo **Enable SNMP** (attiva SNMP).
4. Nell'elenco a discesa **versione**, selezionare **versione 1**.
5. Inserire un indirizzo IPv4 o IPv6 o il nome host e il numero di porta dell'host di gestione.

WFA invia i trap SNMP al numero di porta specificato. Il numero di porta predefinito è 162.

6. Nella sezione notifica su, selezionare una o più delle seguenti caselle di controllo:
 - Esecuzione del flusso di lavoro avviata
 - Esecuzione del flusso di lavoro completata correttamente
 - Esecuzione del flusso di lavoro non riuscita/parzialmente riuscita
 - Esecuzione del workflow in attesa di approvazione

- Errore di acquisizione
7. Fare clic su **Send Test Notification** (Invia notifica test) per verificare le impostazioni.
 8. Fare clic su **Save** (Salva).

Configurare SNMP versione 3

È inoltre possibile configurare OnCommand Workflow Automation (Wfa) per inviare trap SNMP (Simple Network Management Protocol) versione 3 sullo stato delle operazioni del flusso di lavoro.

La versione 3 offre due opzioni di sicurezza aggiuntive:

- Versione 3 con autenticazione

I trap vengono inviati non crittografati sulla rete. Le applicazioni di gestione SNMP, configurate con gli stessi parametri di autenticazione dei messaggi trap SNMP, possono ricevere trap.

- Versione 3 con autenticazione e crittografia

I trap vengono inviati in modo crittografato sulla rete. Per ricevere e decrittare questi trap, è necessario configurare le applicazioni di gestione SNMP con gli stessi parametri di autenticazione e chiave di crittografia dei trap SNMP.

Fasi

1. Accedere a WFA tramite un browser Web come utente amministratore, quindi accedere al server WFA.
2. Fare clic su **Settings** (Impostazioni) e in **Setup** (Configurazione) fare clic su **SNMP**.
3. Selezionare la casella di controllo **Enable SNMP** (attiva SNMP).
4. Nell'elenco a discesa **Version**, selezionare una delle seguenti opzioni:
 - Versione 3
 - Versione 3 con autenticazione
 - Versione 3 con autenticazione e crittografia
5. Selezionare le opzioni di configurazione SNMP corrispondenti all'opzione SNMP versione 3 selezionata al passaggio 4.
6. Inserire un indirizzo IPv4 o IPv6 o il nome host e il numero di porta dell'host di gestione. WFA invia i trap SNMP al numero di porta specificato. Il numero di porta predefinito è 162.
7. Nella sezione notifica su, selezionare una o più delle seguenti caselle di controllo:
 - Pianificazione del workflow avviata/non riuscita/completata
 - Esecuzione del flusso di lavoro avviata
 - Esecuzione del flusso di lavoro completata correttamente
 - Esecuzione del flusso di lavoro non riuscita/parzialmente riuscita
 - Esecuzione del workflow in attesa di approvazione
 - Errore di acquisizione
8. Fare clic su **Send Test Notification** (Invia notifica test) per verificare le impostazioni.
9. Fare clic su **Save** (Salva).

Configurare Syslog

È possibile configurare OnCommand Workflow Automation (Wfa) in modo che invii i dati di log a un server Syslog specifico per scopi come la registrazione degli eventi e l'analisi delle informazioni di log.

È necessario aver configurato il server Syslog per accettare i dati dal server WFA.

Fasi

1. Accedere a WFA tramite un browser Web come amministratore.
2. Fare clic su **Impostazioni** e sotto **manutenzione** fare clic su **Syslog**.
3. Selezionare la casella di controllo **Enable Syslog** (attiva Syslog).
4. Inserire il nome host Syslog e selezionare il livello del registro Syslog.
5. Fare clic su **Save** (Salva).

Configurare i protocolli per la connessione ai sistemi remoti

È possibile configurare il protocollo utilizzato da OnCommand Workflow Automation (Wfa) per la connessione ai sistemi remoti. È possibile configurare il protocollo in base ai requisiti di sicurezza dell'organizzazione e al protocollo supportato dal sistema remoto.

Fasi

1. Accedere a WFA tramite un browser Web come amministratore.
2. Fare clic su **progettazione origine dati > tipi di sistema remoto**.
3. Eseguire una delle seguenti operazioni:

Se si desidera...	Eseguire questa operazione...
Configurare un protocollo per un nuovo sistema remoto	<ol style="list-style-type: none">a. Fare clic su .b. Nella finestra di dialogo nuovo tipo di sistema remoto, specificare i dettagli, ad esempio nome, descrizione e versione.
Modificare la configurazione del protocollo di un sistema remoto esistente	<ol style="list-style-type: none">a. Selezionare e fare doppio clic sul sistema remoto che si desidera modificare.b. Fare clic su .

4. Dall'elenco Connection Protocol (protocollo di connessione), selezionare una delle seguenti opzioni:
 - HTTPS con fallback su HTTP (impostazione predefinita)
 - Solo HTTPS
 - Solo HTTP
 - Personalizzato
5. Specificare i dettagli relativi al protocollo, alla porta predefinita e al timeout predefinito.
6. Fare clic su **Save** (Salva).

Disattiva il criterio password predefinito

OnCommand Workflow Automation (WFA) è configurato per applicare una policy sulle password per gli utenti locali. Se non si desidera utilizzare il criterio password, è possibile disattivarlo.

È necessario aver effettuato l'accesso al sistema host WFA come amministratore.

In questa procedura viene utilizzato il percorso di installazione predefinito di WFA. Se è stata modificata la posizione predefinita durante l'installazione, è necessario utilizzare il percorso di installazione WFA modificato.

Fasi

1. Aprire Esplora risorse e accedere alla seguente directory: `WFA_install_location\WFA\bin\`.
2. Fare doppio clic sul file `ps.cmd`.

Viene visualizzato un prompt dell'interfaccia a riga di comando (CLI) PowerShell con i moduli ONTAP e WFA caricati.

3. Quando richiesto, immettere quanto segue:

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

4. Quando richiesto, riavviare i servizi WFA.

Modificare il criterio password predefinito per Windows

OnCommand Workflow Automation (Wfa) applica una policy sulle password per gli utenti locali. È possibile modificare il criterio password predefinito per impostare una password in base alle proprie esigenze.

È necessario accedere al sistema host WFA come utente root.

- In questa procedura viene utilizzato il percorso di installazione predefinito di WFA.

Se è stata modificata la posizione predefinita durante l'installazione, è necessario utilizzare il percorso di installazione WFA personalizzato.

- Il comando per modificare il criterio password predefinito è `..wfa --password-policy=default`.

L'impostazione predefinita è

`"minLength=true,8;specialeChar=true,1;digitalChar=true,1;lowercaseChar=true,1;uppercaseChar=true,1;whitespaceChar=false"`. In base a questa impostazione per il criterio password predefinito, la password deve avere una lunghezza minima di otto caratteri, deve contenere almeno un carattere speciale, una cifra, un carattere minuscolo e un carattere maiuscolo e non deve contenere spazi.

Fasi

1. Al prompt dei comandi, accedere alla seguente directory sul server WFA:

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

2. Modificare il criterio password predefinito:

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

Abilitare l'accesso remoto al database OnCommand Workflow Automation su Windows

Per impostazione predefinita, è possibile accedere al database OnCommand Workflow Automation (Wfa) solo dai client in esecuzione sul sistema host WFA. È possibile modificare le impostazioni predefinite se si desidera accedere al database WFA da un sistema remoto.

- È necessario aver effettuato l'accesso al sistema host WFA come utente amministratore.
- Se sul sistema host WFA è installato un firewall, è necessario aver configurato le impostazioni del firewall per consentire l'accesso dal sistema remoto.

In questa procedura viene utilizzato il percorso di installazione predefinito di WFA. Se è stata modificata la posizione predefinita durante l'installazione, è necessario utilizzare il percorso di installazione WFA personalizzato.

Fasi

1. Aprire Esplora risorse e accedere alla seguente directory: WFA_install_location
2. Eseguire una delle seguenti operazioni:

Per...	Immettere il seguente comando...
Abilitare l'accesso remoto	.\wfa --db-access=public --restart
Disattiva l'accesso remoto	.\wfa --db-access=default --restart

Limitare i diritti di accesso di OnCommand Workflow Automation sull'host

Per impostazione predefinita, OnCommand Workflow Automation (Wfa) esegue i flussi di lavoro come amministratore del sistema host. È possibile limitare i diritti WFA sul sistema host modificando le impostazioni predefinite.

È necessario aver effettuato l'accesso al sistema host WFA come amministratore.

Fasi

1. Creare un nuovo account utente Windows con autorizzazioni per aprire socket e scrivere nella home directory Wfa.
2. Aprire la console dei servizi Windows utilizzando Services.msc e fare doppio clic su **NetApp WFA Database**.
3. Fare clic sulla scheda **Log on** (accesso).
4. Selezionare **questo account** e immettere le credenziali del nuovo utente creato, quindi fare clic su **OK**.

5. Fare doppio clic su **NetApp WFA Server**.
6. Fare clic sulla scheda **Log on** (accesso).
7. Selezionare **questo account** e immettere le credenziali del nuovo utente creato, quindi fare clic su **OK**.
8. Riavviare i servizi * NetApp WFA Database* e * NetApp WFA Server*.

Modificare l'impostazione di timeout della transazione di OnCommand Workflow Automation

Per impostazione predefinita, la transazione del database OnCommand Workflow Automation (WFA) viene fuori servizio in 300 secondi. È possibile aumentare la durata di timeout predefinita durante il ripristino di un database WFA di grandi dimensioni da un backup per evitare potenziali errori di ripristino del database.

È necessario aver effettuato l'accesso al sistema host WFA come amministratore.

In questa procedura viene utilizzato il percorso di installazione predefinito di WFA. Se è stata modificata la posizione predefinita durante l'installazione, è necessario utilizzare il percorso di installazione WFA modificato.

Fasi

1. Aprire Esplora risorse e accedere alla seguente directory:

`WFA_install_location\WFA\bin`

2. Fare doppio clic sul file `ps.cmd`.

Viene visualizzato un prompt dell'interfaccia a riga di comando (CLI) PowerShell con i moduli ONTAP e WFA caricati.

3. Quando richiesto, immettere quanto segue:

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

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

4. Quando richiesto, riavviare i servizi WFA.

Configurare il valore di timeout per Workflow Automation

È possibile configurare il valore di timeout per la GUI Web di automazione del flusso di lavoro (WFA), invece di utilizzare il valore di timeout predefinito.

Il valore di timeout predefinito per la GUI Web WFA è 180 minuti. È possibile configurare il valore di timeout per soddisfare i requisiti tramite CLI. Non è possibile impostare il valore di timeout dalla GUI Web WFA.



Il valore di timeout impostato è un timeout assoluto anziché un timeout correlato all'inattività. Ad esempio, se si imposta questo valore su 30 minuti, si viene disconnessi dopo 30 minuti, anche se si è attivi al termine di questo intervallo di tempo.

Fasi

1. Accedere come amministratore sul computer host WFA.

2. Impostare il valore di timeout:

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

Abilitazione delle cifrazioni e aggiunta di nuove cifrazioni

OnCommand Workflow Automation 5.1 supporta una serie di cifrari pronti all'uso. Inoltre, è possibile aggiungere ulteriori cifrari in base alle esigenze.

È possibile attivare le seguenti crittografia senza l'uso della confezione:

```
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"
```

È possibile aggiungere ulteriori cifrari a questa configurazione in `standalone-full.xml` file. Questo file si trova in: `<installdir>/jboss/standalone/configuration/standalone-full.xml`.

Il file può essere modificato in modo da supportare altre cifrazioni come segue:

```
<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"/>
```

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.