Configuration de OnCommand Workflow Automation

OnCommand Workflow Automation 5.1

NetApp
April 19, 2024

Sommaire

Configuration de OnCommand Workflow Automation

Une fois l'installation de OnCommand Workflow Automation (WFA) terminée, vous devez définir plusieurs paramètres de configuration. Vous devez accéder à WFA, configurer des utilisateurs, configurer des sources de données, configurer les identifiants et configurer WFA.

Accédez à OnCommand Workflow Automation

Vous pouvez accéder à OnCommand Workflow Automation (WFA) via un navigateur Web depuis n'importe quel système ayant accès au serveur WFA.

Vous devez avoir installé Adobe Flash Player pour votre navigateur Web.

Étapes

1. Ouvrez un navigateur Web et entrez l'un des éléments suivants dans la barre d'adresse :
   - `https://wfa_server_ip`

     wfa_Server_ip est l'adresse IP (IPv4 ou adresse IPv6) ou le nom de domaine complet (FQDN) du serveur WFA.
   - Si vous accédez à WFA sur le serveur WFA: `https://localhost/wfa`Si vous avez spécifié un port non par défaut pour WFA, vous devez inclure le numéro de port comme suit :
   - `https://wfa_server_ip:port`
   - `https://localhost:port`Le port est le numéro de port TCP que vous avez utilisé pour le serveur WFA lors de l'installation.
2. Dans la section connexion, entrez les informations d'identification de l'utilisateur admin que vous avez saisies lors de l'installation.
3. Dans le menu **Paramètres** > **Configuration**, configurez les informations d'identification et une source de données.
4. Ajoutez l'interface graphique Web WFA à vos favoris pour faciliter l'accès.

Sources de données OnCommand Workflow Automation

OnCommand Workflow Automation (WFA) fonctionne sur des données acquises à partir de sources de données. Plusieurs versions de Active IQ Unified Manager et de VMware vCenter Server sont fournies sous la forme de types de sources de données WFA prédéfinis. Vous devez connaître les types de sources de données prédéfinis avant de configurer les sources de données pour l'acquisition des données.

Une source de données est une structure de données en lecture seule qui sert de connexion à l'objet source de données d'un type de source de données spécifique. Par exemple, une source de données peut être une connexion à une base de données Active IQ Unified Manager d'un type de source de données Active IQ Unified Manager 6.3. Vous pouvez ajouter une source de données personnalisée à WFA après avoir défini le type de source de données requis.

Pour plus d'informations sur les types de sources de données prédéfinis, reportez-vous à la matrice d'interopérabilité.

Informations connexes

"Matrice d'interopérabilité NetApp"

Configuration d'un utilisateur de base de données sur DataFabric Manager

Vous devez créer un utilisateur de base de données sur DataFabric Manager 5.x pour configurer l'accès en lecture seule de la base de données DataFabric Manager 5.x vers OnCommand Workflow Automation.

Configurez un utilisateur de base de données en exécutant ocsetup sous Windows

Vous pouvez exécuter le fichier ocsetup sur le serveur DataFabric Manager 5.x pour configurer l'accès en lecture seule de la base de données DataFabric Manager 5.x à OnCommand Workflow Automation.

Étapes

1. Téléchargez le fichier wfa_ocsetup.exe dans un répertoire du serveur DataFabric Manager 5.x à l'emplacement suivant : *https*://WFA_Server_IP/download/wfa_ocsetup.exe.

   WFA_Server_IP est l'adresse IP (adresse IPv4 ou IPv6) de votre serveur WFA.

   Si vous avez spécifié un port non-par défaut pour WFA, vous devez inclure le numéro de port comme suit : *https*://wfa_Server_ip:port/download/wfa_ocsetup.exe.

   Port est le numéro de port TCP que vous avez utilisé pour le serveur WFA au cours de l'installation.

   Si vous spécifiez une adresse IPv6, vous devez l'inclure entre crochets.

2. Double-cliquez sur le fichier wfa_ocsetup.exe.
3. Lisez les informations de l'assistant d'installation et cliquez sur **Suivant**.
4. Parcourez ou tapez l'emplacement OpenJDK et cliquez sur **Suivant**.
5. Saisissez un nom d'utilisateur et un mot de passe pour remplacer les informations d'identification par défaut.

   Un nouveau compte utilisateur de base de données est créé avec accès à la base de données DataFabric Manager 5.x.

   > Si vous ne créez pas de compte d'utilisateur, les informations d'identification par défaut sont utilisées. Vous devez créer un compte utilisateur pour des raisons de sécurité.

6. Cliquez sur **Suivant** et examinez les résultats.
7. Cliquez sur **Suivant**, puis sur **Terminer** pour terminer l'assistant.

Configurez un utilisateur de base de données en exécutant ocsetup sous Linux

Vous pouvez exécuter le fichier ocsetup sur le serveur DataFabric Manager 5.x pour

configurer l'accès en lecture seule de la base de données DataFabric Manager 5.x à OnCommand Workflow Automation.

Étapes

1. Téléchargez le fichier wfa_ocsetup.sh dans votre répertoire personnel sur le serveur DataFabric Manager 5.x à l'aide de la commande suivante dans le terminal :

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

   WFA_Server_IP est l'adresse IP (adresse IPv4 ou IPv6) de votre serveur WFA.

   Si vous avez spécifié un port non par défaut pour WFA, vous devez inclure le numéro de port comme suit :

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

   Le port est le numéro de port TCP que vous avez utilisé pour le serveur WFA lors de l'installation.

   Si vous spécifiez une adresse IPv6, vous devez l'inclure entre crochets.

2. Utilisez la commande suivante dans le terminal pour remplacer le fichier wfa_ocsetup.sh par un exécutable : `chmod +x wfa_ocsetup.sh`
3. Exécutez le script en saisissant les éléments suivants dans le terminal :

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

   OpenJDK_PATH est le chemin d'accès à OpenJDK.

   /Opt/NTAPdfm/Java

   La sortie suivante s'affiche sur le terminal, indiquant que la configuration a réussi :

   ```
   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. Saisissez un nom d'utilisateur et un mot de passe pour remplacer les informations d'identification par défaut.

   Un nouveau compte utilisateur de base de données est créé avec accès à la base de données DataFabric Manager 5.x.

   > Si vous ne créez pas de compte d'utilisateur, les informations d'identification par défaut sont utilisées. Vous devez créer un compte utilisateur pour des raisons de sécurité.

   La sortie suivante s'affiche sur le terminal, indiquant que la configuration a réussi :

```
***** 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 *****
```

Configurer un utilisateur de base de données sur Active IQ Unified Manager

Vous devez créer un utilisateur de base de données sur Active IQ Unified Manager pour configurer l'accès en lecture seule de la base de données Active IQ Unified Manager à OnCommand Workflow Automation.

Étapes

1. Connectez-vous à Active IQ Unified Manager à l'aide des identifiants d'administrateur.
2. Cliquez sur **Paramètres** > **utilisateurs**.
3. Cliquez sur **Ajouter un nouvel utilisateur**.
4. Sélectionnez **Database User** comme type d'utilisateur.

   Le même utilisateur doit être utilisé dans OnCommand Workflow Automation lors de l'ajout de Active IQ Unified Manager en tant que source de données dans OnCommand Workflow Automation.

Configurer une source de données

Vous devez établir une connexion avec une source de données dans OnCommand Workflow Automation (WFA) pour pouvoir acquérir des données à partir de cette source.

- Pour Active IQ Unified Manager 6.0 et versions ultérieures, vous devez avoir créé un compte utilisateur de base de données sur le serveur Unified Manager.

  Consultez l'aide en ligne de *OnCommand Unified Manager* pour plus de détails.

- Le port TCP des connexions entrantes sur le serveur Unified Manager doit être ouvert.

  Consultez la documentation de votre pare-feu pour plus de détails.

  Les numéros de port TCP par défaut sont les suivants :

Numéro de port TCP	Version du serveur Unified Manager	Description
3306	6.x	Serveur de base de données MySQL

- Pour Performance Advisor, vous devez avoir créé un compte utilisateur Active IQ Unified Manager ayant le rôle minimal de GlobalRead.

  Consultez l'aide en ligne de *OnCommand Unified Manager* pour plus de détails.

- Pour VMware vCenter Server, vous devez avoir créé un compte utilisateur sur le serveur vCenter.

  Pour plus de détails, consultez la documentation de VMware vCenter Server.

  > Vous devez avoir installé VMware PowerCLI. Si vous souhaitez exécuter des flux de travail uniquement sur les sources de données vCenter Server, il n'est pas nécessaire de configurer le serveur Unified Manager en tant que source de données.

- Le port TCP pour les connexions entrantes sur le serveur VMware vCenter doit être ouvert.

  Le numéro de port TCP par défaut est 443. Consultez la documentation de votre pare-feu pour plus de détails.

Cette procédure permet d'ajouter plusieurs sources de données de serveur Unified Manager à WFA. Cependant, vous ne devez pas utiliser cette procédure pour coupler Unified Manager Server 6.3 et les versions ultérieures avec WFA et utiliser la fonctionnalité de protection du serveur Unified Manager.

Pour plus d'informations sur le couplage de WFA au serveur Unified Manager 6.x, consultez l'aide en ligne de *OnCommand Unified Manager*.

> Lors de la configuration d'une source de données avec WFA, vous devez savoir que les types de sources de données Active IQ Unified Manager 6.0, 6.1 et 6.2 sont obsolètes dans la version WFA 4.0, et que ces types de sources de données ne seront pas pris en charge dans les prochaines versions.

Étapes

1. Accédez à WFA à l'aide d'un navigateur Web.
2. Cliquez sur **Paramètres** et sous **Configuration**, cliquez sur **sources de données**.
3. Choisissez l'action appropriée :

Pour…	Procédez comme ça…
Créer une nouvelle source de données	Cliquez sur dans la barre d'outils.
Modifiez une source de données restaurée si vous avez mis à niveau WFA	Sélectionnez l'entrée de la source de données existante, puis cliquez sur dans la barre d'outils.

   Si vous avez ajouté une source de données de serveur Unified Manager à WFA, puis mis à niveau la version du serveur Unified Manager, WFA ne reconnaîtra pas la version mise à niveau du serveur Unified Manager. Vous devez supprimer la version précédente du serveur Unified Manager, puis ajouter la version mise à niveau du serveur Unified Manager à WFA.

4. Dans la boîte de dialogue Nouvelle source de données, sélectionnez le type de source de données requis et entrez un nom pour la source de données et le nom d'hôte.

   En fonction du type de source de données sélectionné, les champs port, nom d'utilisateur, mot de passe et

délai d'attente peuvent être automatiquement renseignés avec les données par défaut, si disponibles. Vous pouvez modifier ces entrées si nécessaire.

5. Choisissez une action appropriée :

Pour…	Procédez comme ça…
Active IQ Unified Manager 6.3 et versions ultérieures	Entrez les informations d'identification du compte utilisateur de la base de données que vous avez créé sur le serveur Unified Manager. Voir l'aide en ligne de *OnCommand Unified Manager* pour plus de détails sur la création d'un compte utilisateur de base de données. Vous ne devez pas fournir les informations d'identification d'un compte utilisateur de base de données Active IQ Unified Manager créé à l'aide de l'interface de ligne de commande ou de l'outil ocsetup.
Serveur VMware vCenter (uniquement pour Windows)	(Uniquement pour Windows) Entrez le nom d'utilisateur et le mot de passe de l'utilisateur que vous avez créé sur le serveur VMware vCenter.

6. Cliquez sur **Enregistrer**.
7. Dans le tableau sources de données, sélectionnez la source de données, puis cliquez sur dans la barre d'outils.
8. Vérifier l'état du processus d'acquisition de données.

Ajoutez un serveur Unified Manager mis à niveau en tant que source de données

Si le serveur Unified Manager (5.x ou 6.x) est ajouté en tant que source de données à WFA, le serveur Unified Manager est mis à niveau, Vous devez ajouter le serveur Unified Manager mis à niveau en tant que source de données, car les données associées à la version mise à niveau ne sont pas renseignées dans WFA sauf si elles sont ajoutées manuellement en tant que source de données.

Étapes

1. Connectez-vous à l'interface graphique WFA en tant qu'administrateur.
2. Cliquez sur **Paramètres** et sous **Configuration**, cliquez sur **sources de données**.
3. Cliquez sur dans la barre d'outils.
4. Dans la boîte de dialogue Nouvelle source de données, sélectionnez le type de source de données requis, puis entrez un nom pour la source de données et le nom d'hôte.

   En fonction du type de source de données sélectionné, les champs port, nom d'utilisateur, mot de passe et délai d'attente peuvent être automatiquement renseignés avec les données par défaut, si disponibles. Vous pouvez modifier ces entrées si nécessaire.

5. Cliquez sur **Enregistrer**.
6. Sélectionnez la version précédente du serveur Unified Manager, puis cliquez sur dans la barre d'outils.
7. Dans la boîte de dialogue de confirmation Supprimer le type de source de données, cliquez sur **Oui**.
8. Dans le tableau sources de données, sélectionnez la source de données, puis cliquez sur dans la barre d'outils.
9. Vérifiez l'état de l'acquisition de données dans la table Historique.

Créez des utilisateurs locaux

OnCommand Workflow Automation (WFA) vous permet de créer et de gérer des utilisateurs WFA locaux avec des autorisations spécifiques pour différents rôles, tels qu'invité, opérateur, approbateur, architecte, l'administrateur et la sauvegarde.

Vous devez avoir installé WFA et vous connecter en tant qu'administrateur.

WFA vous permet de créer des utilisateurs pour les rôles suivants :

- **Invité**

  Cet utilisateur peut afficher le portail et l'état de l'exécution d'un flux de travail, et peut être averti d'un changement de statut d'exécution d'un flux de travail.

- **Opérateur**

  Cet utilisateur est autorisé à prévisualiser et à exécuter des flux de travail pour lesquels l'utilisateur a accès.

- **Approbateur**

  Cet utilisateur est autorisé à prévisualiser, exécuter, approuver et rejeter les flux de travail pour lesquels l'utilisateur a accès.

  > Il est recommandé de fournir l'ID d'e-mail de l'approbateur. S'il existe plusieurs approbateurs, vous pouvez fournir un ID d'e-mail de groupe dans le champ **E-mail**.

- **Architecte**

  Cet utilisateur dispose d'un accès complet pour créer des flux de travail, mais ne peut pas modifier les paramètres globaux du serveur WFA.

- **Admin**

  Cet utilisateur dispose d'un accès complet au serveur WFA.

- **Sauvegarde**

  Il s'agit du seul utilisateur pouvant générer des sauvegardes à distance du serveur WFA. Toutefois, l'utilisateur est limité à tout autre accès.

Étapes

1. Cliquez sur **Paramètres** et sous **gestion**, cliquez sur **utilisateurs**.

2. Créez un nouvel utilisateur en cliquant sur dans la barre d'outils.
3. Entrez les informations requises dans la boîte de dialogue nouvel utilisateur.
4. Cliquez sur **Enregistrer**.

Configurer les informations d'identification d'un système cible

Vous pouvez configurer les identifiants d'un système cible dans OnCommand Workflow Automation (WFA) et utiliser ces identifiants pour vous connecter à ce système spécifique et exécuter des commandes.

Après l'acquisition initiale des données, vous devez configurer les informations d'identification des matrices sur lesquelles les commandes sont exécutées. La connexion du contrôleur WFA PowerShell fonctionne en deux modes :

- Avec identifiants

  WFA tente d'établir une connexion à l'aide de HTTPS d'abord, puis d'utiliser HTTP. Vous pouvez également utiliser l'authentification LDAP Microsoft Active Directory pour connecter des baies sans définir d'informations d'identification dans WFA. Pour utiliser Active Directory LDAP, vous devez configurer la baie de manière à effectuer une authentification avec le même serveur LDAP Active Directory.

- Sans identifiants (pour les systèmes de stockage en 7-mode)

  WFA tente d'établir une connexion à l'aide de l'authentification de domaine. Ce mode utilise le protocole d'appel de procédure distante, sécurisé à l'aide du protocole NTLM.

- WFA vérifie le certificat SSL (Secure Sockets Layer) pour les systèmes ONTAP. Les utilisateurs peuvent être invités à vérifier et accepter/refuser la connexion aux systèmes ONTAP si le certificat SSL n'est pas approuvé.
- Vous devez saisir à nouveau les identifiants pour ONTAP, NetApp Active IQ et Lightweight Directory Access Protocol (LDAP) après la restauration d'une sauvegarde ou la mise à niveau sans déplacement des données.

Étapes

1. Connectez-vous à WFA via un navigateur Web en tant qu'administrateur.
2. Cliquez sur **Paramètres** et sous **Configuration**, cliquez sur **informations d'identification**.
3. Cliquez sur dans la barre d'outils.
4. Dans la boîte de dialogue nouvelles informations d'identification, sélectionnez l'une des options suivantes dans la liste **correspondance** :

   - **Exact**

     Informations d'identification pour une adresse IP ou un nom d'hôte spécifique

   - **Modèle**

     Informations d'identification pour l'ensemble du sous-réseau ou de la plage IP

     L'utilisation de la syntaxe d'expression régulière n'est pas prise en charge pour cette option.

5. Sélectionnez le type de système distant dans la liste **Type**.
6. Entrez le nom d'hôte ou l'adresse IPv4 ou IPv6 de la ressource, le nom d'utilisateur et le mot de passe.

> WFA 5.1 vérifie les certificats SSL de toutes les ressources ajoutées à WFA. Comme la vérification du certificat peut vous inviter à accepter les certificats, l'utilisation de caractères génériques dans les informations d'identification n'est pas prise en charge. Si plusieurs clusters utilisent les mêmes identifiants, vous ne pouvez pas tous les ajouter simultanément.

7. Testez la connectivité en effectuant l'action suivante :

Si vous avez sélectionné le type de correspondance suivant…	Alors…
Exact	Cliquez sur **Test**.
Modèle	Enregistrez les informations d'identification et choisissez l'une des options suivantes : • Sélectionnez les informations d'identification et cliquez sur dans la barre d'outils. • Cliquez avec le bouton droit de la souris et sélectionnez **Tester la connectivité**.

8. Cliquez sur **Enregistrer**.

Configuration d'OnCommand Workflow Automation en cours

OnCommand Workflow Automation (WFA) vous permet de configurer différents paramètres, par exemple AutoSupport et les notifications.

Lors de la configuration de WFA, vous pouvez configurer un ou plusieurs des éléments suivants, si nécessaire :

- AutoSupport pour l'envoi de messages AutoSupport au support technique
- Serveur Microsoft Active Directory Lightweight Directory Access Protocol (LDAP) pour l'authentification LDAP et l'autorisation pour les utilisateurs de WFA
- Recevez des notifications par e-mail concernant le fonctionnement du workflow et l'envoi de messages AutoSupport
- Simple Network Management Protocol (SNMP) pour les notifications sur les opérations de workflow
- Syslog pour la consignation de données à distance

Configurez AutoSupport

Vous pouvez configurer plusieurs paramètres AutoSupport tels que la planification, le contenu des messages AutoSupport et le serveur proxy. AutoSupport envoie chaque semaine des journaux du contenu que vous avez sélectionné à des fins de support

technique pour l'archivage et l'analyse des problèmes.

Étapes

1. Connectez-vous à WFA via un navigateur Web en tant qu'administrateur.
2. Cliquez sur **Paramètres** et sous **Configuration**, cliquez sur **AutoSupport**.
3. Assurez-vous que la case **Activer AutoSupport** est sélectionnée.
4. Entrez les informations requises.
5. Sélectionnez l'une des options suivantes dans la liste **contenu** :

Si vous souhaitez inclure…	Choisissez ensuite cette option…
Uniquement les détails de configuration, tels que les utilisateurs, les flux de production et les commandes de votre installation WFA	`send only configuration data`
Détails de la configuration WFA et données dans des tables cache WFA telles que le schéma	`send configuration and cache data` (valeur par défaut)
Détails de la configuration WFA, données dans les tables cache WFA et données dans le répertoire d'installation	`send configuration and cache extended data`

Le mot de passe d'un utilisateur WFA est *not* inclus dans les données AutoSupport.

6. Vérifiez que vous pouvez télécharger un message AutoSupport :
   a. Cliquez sur **Télécharger**.
   b. Dans la boîte de dialogue qui s'ouvre, sélectionnez l'emplacement d'enregistrement du fichier .7z.
7. Testez l'envoi d'un message AutoSupport à la destination spécifiée en cliquant sur **Envoyer maintenant**.
8. Cliquez sur **Enregistrer**.

Configurer les paramètres d'authentification

Vous pouvez configurer OnCommand Workflow Automation (WFA) pour qu'il utilise un serveur Microsoft Active Directory (AD) LDAP (Lightweight Directory Access Protocol) à des fins d'authentification et d'autorisation.

Vous devez avoir configuré un serveur LDAP Microsoft AD dans votre environnement.

Seule l'authentification LDAP Microsoft AD est prise en charge pour WFA. Vous ne pouvez pas utiliser d'autres méthodes d'authentification LDAP, notamment Microsoft AD Lightweight Directory Services (AD LDS) ou Microsoft Global Catalog.

Lors de la communication, LDAP envoie le nom d'utilisateur et le mot de passe en texte brut. Cependant, les communications LDAPS (LDAP Secure) sont cryptées et sécurisées.

Étapes

1. Connectez-vous à WFA via un navigateur Web en tant qu'administrateur.
2. Cliquez sur **Paramètres** et sous **Configuration**, cliquez sur **authentification**.
3. Cochez la case **Activer Active Directory**.
4. Entrez les informations requises dans les champs :

   a. Si vous souhaitez utiliser le format user@domain pour les utilisateurs de domaine, remplacez sAMAccountName par userPrincipalName dans le champ **User name attribute**.

   b. Si des valeurs uniques sont requises pour votre environnement, modifiez les champs obligatoires.

   c. Saisissez l'URI du serveur AD comme suit :
   `ldap://active_directory_server_address\[:port\]`

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

   Si vous avez activé LDAP sur SSL, vous pouvez utiliser le format URI suivant :
   `ldaps://active_directory_server_address\[:port\]`

   a. Ajouter une liste de noms de groupe AD aux rôles requis.

   > Vous pouvez ajouter une liste de noms de groupes AD aux rôles requis dans la fenêtre groupes Active Directory.

5. Cliquez sur **Enregistrer**.
6. Si une connectivité LDAP à une baie est requise, configurez le service WFA pour qu'il se connecte comme utilisateur de domaine requis :

   a. Ouvrez la console des services Windows en utilisant services.msc.

   b. Double-cliquez sur le service **NetApp WFA Server**.

   c. Dans la boîte de dialogue Propriétés du serveur NetApp WFA, cliquez sur l'onglet **connexion**, puis sélectionnez **ce compte**.

   d. Entrez le nom d'utilisateur et le mot de passe du domaine, puis cliquez sur **OK**.

Ajouter des groupes Active Directory

Vous pouvez ajouter des groupes Active Directory dans OnCommand Workflow Automation (WFA).

Étapes

1. Connectez-vous à WFA via un navigateur Web en tant qu'administrateur.
2. Cliquez sur **Paramètres** et sous **gestion**, cliquez sur **groupes Active Directory**.
3. Dans la fenêtre groupes Active Directory, cliquez sur l'icône **Nouveau**.
4. Dans la boîte de dialogue Nouveau groupe Active Directory, entrez les informations requises.

   Si vous sélectionnez **approbateur** dans la liste déroulante **rôle**, il est recommandé de fournir l'ID e-mail de l'approbateur. S'il existe plusieurs approbateurs, vous pouvez fournir un ID d'e-mail de groupe dans le champ **E-mail**. Sélectionnez les différents événements du flux de travail pour lesquels la notification doit être envoyée au groupe Active Directory en particulier.

5. Cliquez sur **Enregistrer**.

Configurez les notifications par e-mail

Vous pouvez configurer OnCommand Workflow Automation (WFA) pour vous envoyer des notifications par e-mail concernant les opérations de flux de travail, par exemple le flux de travail démarré ou l'échec du flux de travail.

Vous devez avoir configuré un hôte de messagerie dans votre environnement.

Étapes

1. Connectez-vous à WFA via un navigateur Web en tant qu'administrateur.
2. Cliquez sur **Paramètres** et sous **Configuration**, cliquez sur **Mail**.
3. Entrez les informations requises dans les champs.
4. Testez les paramètres de courrier en procédant comme suit :
   a. Cliquez sur **Envoyer courriel test**.
   b. Dans la boîte de dialogue Tester la connexion, entrez l'adresse électronique à laquelle vous souhaitez envoyer l'e-mail.
   c. Cliquez sur **Test**.
5. Cliquez sur **Enregistrer**.

Configurez SNMP

Vous pouvez configurer OnCommand Workflow Automation (WFA) pour envoyer des interruptions SNMP (simple Network Management Protocol) concernant l'état des opérations des flux de travail.

WFA supporte désormais les protocoles SNMP v1 et SNMP v3. SNMP v3 offre des fonctions de sécurité supplémentaires.

Le fichier WFA .mib fournit des informations sur les traps envoyés par le serveur WFA. Le fichier .mib est situé dans le répertoire <WFA_install_location>\wfa\bin\wfa.mib sur le serveur WFA.

> Le serveur WFA envoie toutes les notifications d'interruption avec un identificateur d'objet générique (1.3.6.1.4.1.789.1.1.12.0).

Vous ne pouvez pas utiliser de chaînes de communauté SNMP telles que community_string@SNMP_host pour la configuration SNMP.

Configurer SNMP version 1

Étapes

1. Connectez-vous à WFA via un navigateur Web en tant qu'utilisateur administrateur, puis accédez au serveur WFA.
2. Cliquez sur **Paramètres** et sous **Configuration**, cliquez sur **SNMP**.
3. Cochez la case **Activer SNMP**.
4. Dans la liste déroulante **version**, sélectionnez **version 1**.
5. Entrez une adresse IPv4 ou IPv6 ou le nom d'hôte, ainsi que le numéro de port de l'hôte de gestion.

WFA envoie des traps SNMP au numéro de port spécifié. Le numéro de port par défaut est 162.

6. Dans la section notifier sur, cochez une ou plusieurs des cases suivantes :
   - L'exécution du workflow a démarré
   - L'exécution du workflow a réussi
   - Échec/échec partiel de l'exécution du workflow
   - Exécution du workflow en attente d'approbation
   - Échec de l'acquisition
7. Cliquez sur **Envoyer notification de test** pour vérifier les paramètres.
8. Cliquez sur **Enregistrer**.

Configurez SNMP version 3

Vous pouvez également configurer OnCommand Workflow Automation (WFA) pour envoyer des interruptions SNMP (simple Network Management Protocol) version 3 concernant l'état des opérations des flux de travail.

La version 3 offre deux options de sécurité supplémentaires :

- Version 3 avec authentification

  Les interruptions sont envoyées de manière non chiffrée sur le réseau. Les applications de gestion SNMP, qui sont configurées par les mêmes paramètres d'authentification que les messages d'interruption SNMP, peuvent recevoir des traps.

- Version 3 avec authentification et cryptage

  Les interruptions sont envoyées chiffrées sur le réseau. Pour recevoir et décrypter ces traps, vous devez configurer des applications de management SNMP avec les mêmes paramètres d'authentification et clé de cryptage que les traps SNMP.

Étapes

1. Connectez-vous à WFA via un navigateur Web en tant qu'utilisateur administrateur, puis accédez au serveur WFA.
2. Cliquez sur **Paramètres** et sous **Configuration**, cliquez sur **SNMP**.
3. Cochez la case **Activer SNMP**.
4. Dans la liste déroulante **version**, sélectionnez l'une des options suivantes :
   - Version 3
   - Version 3 avec authentification
   - Version 3 avec authentification et cryptage
5. Sélectionnez les options de configuration SNMP correspondant à l'option SNMP version 3 spécifique que vous avez choisie à l'étape 4.
6. Entrez une adresse IPv4 ou IPv6 ou le nom d'hôte, ainsi que le numéro de port de l'hôte de gestion. WFA envoie des traps SNMP au numéro de port spécifié. Le numéro de port par défaut est 162.
7. Dans la section notifier sur, cochez une ou plusieurs des cases suivantes :

- Planification du workflow démarrée/échouée/terminée
- L'exécution du workflow a démarré
- L'exécution du workflow a réussi
- Échec/échec partiel de l'exécution du workflow
- Exécution du workflow en attente d'approbation
- Échec de l'acquisition

8. Cliquez sur **Envoyer notification de test** pour vérifier les paramètres.
9. Cliquez sur **Enregistrer**.

Configurer Syslog

Vous pouvez configurer OnCommand Workflow Automation (WFA) pour qu'il envoie des données de journal à un serveur Syslog spécifique à des fins telles que la journalisation des événements et l'analyse des informations de journal.

Vous devez avoir configuré le serveur Syslog pour accepter les données du serveur WFA.

Étapes

1. Connectez-vous à WFA via un navigateur Web en tant qu'administrateur.
2. Cliquez sur **Paramètres** et sous **Maintenance**, cliquez sur **Syslog**.
3. Cochez la case **Activer Syslog**.
4. Entrez le nom d'hôte Syslog et sélectionnez le niveau de journal Syslog.
5. Cliquez sur **Enregistrer**.

Configurez les protocoles pour la connexion à des systèmes distants

Vous pouvez configurer le protocole utilisé par OnCommand Workflow Automation (WFA) pour la connexion aux systèmes distants. Vous pouvez configurer le protocole en fonction des exigences de sécurité de votre entreprise et du protocole pris en charge par le système distant.

Étapes

1. Connectez-vous à WFA via un navigateur Web en tant qu'administrateur.
2. Cliquez sur **conception de la source de données** > **types de systèmes distants**.
3. Effectuez l'une des opérations suivantes :

Les fonctions que vous recherchez…	Procédez comme ça…
Configurer un protocole pour un nouveau système distant	a. Cliquez sur . b. Dans la boîte de dialogue Nouveau type de système distant, spécifiez les détails tels que le nom, la description et la version.

Les fonctions que vous recherchez…	Procédez comme ça…
Modifier la configuration du protocole d'un système distant existant	a. Sélectionnez et double-cliquez sur le système distant que vous souhaitez modifier. b. Cliquez sur .

4. Dans la liste Protocole de connexion, sélectionnez l'une des options suivantes :
   - HTTPS avec retour au HTTP (par défaut)
   - HTTPS uniquement
   - HTTP uniquement
   - Personnalisées
5. Spécifiez les détails du protocole, du port par défaut et du délai par défaut.
6. Cliquez sur **Enregistrer**.

Désactivez la stratégie de mot de passe par défaut

OnCommand Workflow Automation (WFA) est configuré pour appliquer une politique de mots de passe aux utilisateurs locaux. Si vous ne souhaitez pas utiliser la stratégie de mot de passe, vous pouvez la désactiver.

Vous devez avoir ouvert une session sur le système hôte WFA en tant qu'administrateur.

Le chemin d'installation par défaut de WFA est utilisé dans cette procédure. Si vous avez modifié l'emplacement par défaut lors de l'installation, vous devez utiliser le chemin d'installation WFA modifié.

Étapes

1. Ouvrez l'Explorateur Windows et accédez au répertoire suivant : `WFA_install_location\WFA\bin\`.
2. Double-cliquez sur le fichier ps.cmd.

   Une invite d'interface de ligne de commande PowerShell s'ouvre avec les modules ONTAP et WFA chargés.

3. À l'invite, saisissez les informations suivantes :

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

4. Lorsque vous y êtes invité, redémarrez les services WFA.

Modifier la stratégie de mot de passe par défaut pour Windows

OnCommand Workflow Automation (WFA) applique une politique de mots de passe aux utilisateurs locaux. Vous pouvez modifier la stratégie de mot de passe par défaut pour définir un mot de passe selon vos besoins.

Vous devez être connecté au système hôte WFA en tant qu'utilisateur root.

- Le chemin d'installation par défaut de WFA est utilisé dans cette procédure.

  Si vous avez modifié l'emplacement par défaut lors de l'installation, vous devez utiliser le chemin d'installation personnalisé de WFA.

- La commande permettant de modifier la stratégie de mots de passe par défaut est .\wfa --password -policy=default.

  Le paramètre par défaut est "minLength=true,8;specialChar=true,1;digitalChar=true,1;lowercasChar=true,1;uppercaseChar=true,1;blanceChar=false`. Conformément à ce paramètre pour la stratégie de mot de passe par défaut, le mot de passe doit comporter au moins huit caractères, au moins un caractère spécial, un chiffre, un caractère minuscule et un caractère majuscule et ne doit pas contenir d'espace.

Étapes

1. À l'invite de commande, accédez au répertoire suivant sur le serveur WFA:

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

2. Modifier la stratégie de mots de passe par défaut :

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

Activez l'accès à distance à la base de données OnCommand Workflow Automation sous Windows

Par défaut, la base de données OnCommand Workflow Automation (WFA) est accessible uniquement aux clients qui s'exécutent sur le système hôte WFA. Vous pouvez modifier les paramètres par défaut pour accéder à la base de données WFA à partir d'un système distant.

- Vous devez avoir ouvert une session sur le système hôte WFA en tant qu'utilisateur admin.
- Si un pare-feu est installé sur le système hôte WFA, vous devez avoir configuré les paramètres de votre pare-feu pour autoriser l'accès au système distant.

Le chemin d'installation par défaut de WFA est utilisé dans cette procédure. Si vous avez modifié l'emplacement par défaut lors de l'installation, vous devez utiliser le chemin d'installation personnalisé de WFA.

Étapes

1. Ouvrez l'Explorateur Windows et accédez au répertoire suivant : WFA_install_location\WFA\bin
2. Effectuez l'une des opérations suivantes :

Pour…	Saisissez la commande suivante…
Activer l'accès à distance	`.\wfa --db-access=public --restart`
Désactiver l'accès à distance	`.\wfa --db-access=default --restart`

Limiter les droits d'accès de OnCommand Workflow Automation sur l'hôte

Par défaut, OnCommand Workflow Automation (WFA) exécute les flux de travail en tant qu'administrateur du système hôte. Vous pouvez restreindre les droits WFA sur le système hôte en modifiant les paramètres par défaut.

Vous devez avoir ouvert une session sur le système hôte WFA en tant qu'administrateur.

Étapes

1. Créez un nouveau compte utilisateur Windows avec des autorisations d'ouvrir des sockets et d'écrire dans le répertoire de base WFA.
2. Ouvrez la console de services Windows en utilisant services.msc et double-cliquez sur **NetApp WFA Database**.
3. Cliquez sur l'onglet **connexion**.
4. Sélectionnez **ce compte** et entrez les informations d'identification du nouvel utilisateur que vous avez créé, puis cliquez sur **OK**.
5. Double-cliquez sur **NetApp WFA Server**.
6. Cliquez sur l'onglet **connexion**.
7. Sélectionnez **ce compte** et entrez les informations d'identification du nouvel utilisateur que vous avez créé, puis cliquez sur **OK**.
8. Redémarrez les services **NetApp WFA Database** et **NetApp WFA Server**.

Modifiez le paramètre d'expiration de transaction de OnCommand Workflow Automation

Par défaut, le délai de transaction de la base de données OnCommand Workflow Automation (WFA) est fixée à 300 secondes. Vous pouvez augmenter la durée du délai par défaut lors de la restauration d'une base de données WFA de grande taille à partir d'une sauvegarde pour éviter toute défaillance potentielle de la restauration de la base de données.

Vous devez avoir ouvert une session sur le système hôte WFA en tant qu'administrateur.

Le chemin d'installation par défaut de WFA est utilisé dans cette procédure. Si vous avez modifié l'emplacement par défaut lors de l'installation, vous devez utiliser le chemin d'installation WFA modifié.

Étapes

1. Ouvrez l'Explorateur Windows et accédez au répertoire suivant :

   ```
   WFA_install_location\WFA\bin
   ```

2. Double-cliquez sur le fichier ps.cmd.

   Une invite d'interface de ligne de commande PowerShell s'ouvre avec les modules ONTAP et WFA chargés.

3. À l'invite, saisissez les informations suivantes :

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

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

4. Lorsque vous y êtes invité, redémarrez les services WFA.

Configurez la valeur du délai d'expiration pour Workflow Automation

Vous pouvez configurer la valeur de temporisation pour l'interface graphique Web WFA (Workflow Automation), au lieu d'utiliser la valeur de délai par défaut.

La valeur par défaut du délai d'expiration pour l'interface graphique Web de WFA est de 180 minutes. Vous pouvez configurer la valeur du délai d'expiration pour répondre à vos exigences via l'interface de ligne de commande. Vous ne pouvez pas définir la valeur de temporisation à partir de l'interface Web de WFA.

> La valeur de temporisation que vous avez définie correspond à un délai d'inactivité absolu plutôt qu'à un délai d'inactivité. Par exemple, si vous définissez cette valeur sur 30 minutes, vous êtes déconnecté après 30 minutes, même si vous êtes actif à la fin de cette période.

Étapes

1. Connectez-vous en tant qu'administrateur sur la machine hôte WFA.
2. Définissez la valeur de temporisation :

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

Activation des chiffrements et ajout de nouveaux chiffrements

OnCommand Workflow Automation 5.1 prend en charge un certain nombre de chiffrements hors de l'emballage. En outre, vous pouvez ajouter des chiffrements supplémentaires si nécessaire.

Les chiffrements suivants peuvent être activés hors de la boîte :

```
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"
```

Des chiffrements supplémentaires peuvent être ajoutés à cette configuration dans le `standalone-full.xml` fichier. Ce fichier se trouve à l'adresse suivante : `<installdir>/jboss/standalone/configuration/standalone-full.xml`.

Le fichier peut être modifié pour prendre en charge des chiffrements supplémentaires comme suit :

```
<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"/>
```