Exécution des tâches post-mise à niveau

OnCommand Insight

NetApp
April 01, 2024

Sommaire

Exécution des tâches post-mise à niveau . . . 1
Installation des correctifs de source de données . . . 1
Remplacement d’un certificat après la mise à niveau de OnCommand Insight . . . 1
Augmentation de la mémoire Cognos . . . 3
Restauration de la base de données Data Warehouse . . . 4
Restauration des rapports Data Warehouse personnalisés . . . 5
Vérification que Data Warehouse contient des données historiques . . . 5
Restauration de l’archive de performance . . . 6
Test des connecteurs . . . 6
Vérification de la planification d’extraction, de transformation et de chargement . . . 7
Mise à jour des modèles de disque . . . 7
Vérification de l’exécution des outils de veille stratégique . . . 8

Exécution des tâches post-mise à niveau

Vous devez effectuer des tâches supplémentaires après la mise à niveau vers la dernière version d'Insight.

Installation des correctifs de source de données

Le cas échéant, vous devez installer les derniers correctifs disponibles pour vos sources de données pour profiter des dernières fonctionnalités et améliorations. Après avoir téléchargé un correctif de source de données, vous pouvez l'installer sur toutes les sources de données du même type.

Avant de commencer

Vous devez avoir contacté le support technique et obtenu le `.zip` fichier contenant les derniers correctifs de source de données en leur fournissant la version à partir de laquelle vous effectuez la mise à niveau et la version vers laquelle vous souhaitez effectuer la mise à niveau.

Étapes

1. Placez le fichier correctif sur le serveur Insight.
2. Dans la barre d'outils Insight, cliquez sur **Admin**.
3. Cliquez sur **Patches**.
4. Dans le bouton actions, sélectionnez **appliquer patch**.
5. Dans la boîte de dialogue **Apply data source patch**, cliquez sur **Browse** pour localiser le fichier correctif téléchargé.
6. Examinez les types de sources de données **Patch name**, **Description** et **impactées**.
7. Si le correctif sélectionné est correct, cliquez sur **appliquer le correctif**.

   Toutes les sources de données du même type sont mises à jour avec ce correctif. Insight force automatiquement l'acquisition à redémarrer lorsque vous ajoutez une source de données. La découverte inclut la détection des modifications de la topologie réseau, notamment l'ajout ou la suppression de nœuds ou d'interfaces.

8. Pour forcer manuellement le processus de découverte, cliquez sur **sources de données** et cliquez sur **interroger à nouveau** en regard de la source de données pour forcer la collecte immédiate des données.

   Si la source de données est déjà dans un processus d'acquisition, Insight ignore la requête d'interrogation à nouveau.

Remplacement d'un certificat après la mise à niveau de OnCommand Insight

L'ouverture de l'interface utilisateur Web de OnCommand Insight après une mise à niveau entraîne un avertissement de certification. Le message d'avertissement s'affiche car un certificat auto-signé valide n'est pas disponible après la mise à niveau. Pour éviter

que le message d'avertissement ne s'affiche à l'avenir, vous pouvez installer un certificat auto-signé valide pour remplacer le certificat d'origine.

Avant de commencer

Votre système doit respecter le niveau de cryptage minimum (1024 bits).

Description de la tâche

L'avertissement de certification n'a aucun impact sur la facilité d'utilisation du système. À l'invite du message, vous pouvez indiquer que vous comprenez le risque, puis vous pouvez utiliser Insight.

Étapes

1. Répertoriez le contenu du magasin de clés : `C:\Program Files\SANscreen\java64\bin>keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   Lorsque vous êtes invité à saisir un mot de passe, entrez `changeit`.

   Il doit y avoir au moins un certificat dans le magasin de clés, `ssl certificate`.

2. Supprimez le `ssl certificate`: `keytool -delete -alias ssl certificate -keystore c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Générer une nouvelle clé : `keytool -genkey -alias OCI.hostname.com -keyalg RSA -keysize 2048 -keystore "c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. Lorsque vous êtes invité à entrer le prénom et le nom de famille, entrez le nom de domaine complet (FQDN) que vous souhaitez utiliser.
   b. Fournissez les informations suivantes sur votre organisation et votre structure organisationnelle :
      - Pays : abréviation ISO à deux lettres pour votre pays (par exemple, États-Unis)
      - État ou province : nom de l'État ou de la province où se trouve le siège social de votre organisation (par exemple, Massachusetts)
      - Localité : nom de la ville où se trouve le siège social de votre organisation (Waltham, par exemple)
      - Nom de l'organisation : nom de l'organisation qui possède le nom de domaine (par exemple, NetApp)
      - Nom de l'unité organisationnelle : nom du service ou du groupe qui utilisera le certificat (par exemple, support)
      - Nom de domaine/Nom commun : nom de domaine complet utilisé pour les recherches DNS de votre serveur (par exemple, www.example.com). Le système répond avec des informations similaires à ce qui suit : `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
   c. Entrez `Yes` Lorsque le nom commun (CN) est égal au nom de domaine complet.
   d. Lorsque vous êtes invité à saisir le mot de passe de la clé, entrez le mot de passe ou appuyez sur la touche entrée pour utiliser le mot de passe existant de la base de stockage de clés.
4. Générer un fichier de demande de certificat : `keytool -certreq -alias localhost -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

`-file c:\localhost.csr`

Le `c:\localhost.csr` fichier est le fichier de demande de certificat qui vient d'être généré.

5. Soumettre le `c:\localhost.csr` Soumettez-le à votre autorité de certification (CA) pour approbation.

   Une fois le fichier de demande de certificat approuvé, vous souhaitez que le certificat vous soit renvoyé dans `.der` format. Il se peut que le fichier soit renvoyé en tant que `.der` fichier. Le format de fichier par défaut est `.cer` Pour les services CA de Microsoft.

6. Importer le certificat approuvé : `keytool -importcert -alias localhost -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. Lorsque vous êtes invité à saisir un mot de passe, entrez le mot de passe de la base de stockage de clés.

      Le système affiche le message suivant : `Certificate reply was installed in keystore`

7. Redémarrez le service du serveur SANscreen.

Résultats

Le navigateur Web ne signale plus les avertissements de certificat.

Augmentation de la mémoire Cognos

Avant de restaurer la base de données Data Warehouse, vous devez augmenter l'allocation Java pour Cognos de 768 Mo à 2048 Mo pour réduire le temps de génération des rapports.

Étapes

1. Ouvrez une fenêtre d'invite de commande en tant qu'administrateur sur le serveur Data Warehouse.
2. Accédez au `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` répertoire.
3. Tapez la commande suivante : `cogconfigw`

   La fenêtre Configuration IBM Cognos s'affiche.

   > L'application de raccourci IBM Cognos Configuration pointe vers `disk drive:\Program Files\SANscreen\cognos\c10_64\bin64\cognosconfigw.bat`. Si Insight est installé dans le répertoire Program Files (espace entre), qui est le répertoire par défaut, au lieu de ProgramFiles (pas d'espace), le `.bat` le fichier ne fonctionnera pas. Si cela se produit, cliquez avec le bouton droit de la souris sur le raccourci de l'application et modifiez-le `cognosconfigw.bat` à `cognosconfig.exe` pour corriger le raccourci.

4. Dans le volet de navigation de gauche, développez **Environnement**, développez **IBM Cognos services**, puis cliquez sur **IBM Cognos**.
5. Sélectionnez **mémoire maximale pour Tomcat en Mo** et remplacez 768 Mo par 2048 Mo.
6. Dans la barre d'outils Configuration IBM Cognos, cliquez sur (Enregistrer).

Un message d'information s'affiche pour vous informer des tâches que Cognos effectue.

7. Cliquez sur **Fermer**.
8. Dans la barre d'outils Configuration IBM Cognos, cliquez sur (Arrêt).
9. Dans la barre d'outils Configuration IBM Cognos, cliquez sur (Démarrage).

Restauration de la base de données Data Warehouse

Lorsque vous sauvegardez la base de données Data Warehouse, Data Warehouse crée un `.zip` fichier que vous pouvez utiliser ultérieurement pour restaurer cette même base de données.

Description de la tâche

Lorsque vous restaurez la base de données Data Warehouse, vous pouvez également restaurer les informations de compte utilisateur à partir de la sauvegarde. Les tables de gestion des utilisateurs sont utilisées par le moteur de rapport Data Warehouse dans une installation Data Warehouse uniquement.

Étapes

1. Connectez-vous au portail Data Warehouse à l'adresse `https://fqdn/dwh`.
2. Dans le volet de navigation de gauche, cliquez sur **Sauvegarder/Restaurer**.
3. Dans la section **Restaurer la base de données et les rapports**, cliquez sur **Parcourir** et localisez le `.zip` Fichier contenant la sauvegarde de l'entrepôt de données.
4. Il est recommandé de laisser les deux options suivantes sélectionnées :
   - **Restaurer la base de données**

     Inclut les paramètres Data Warehouse, les magasins de données, les connexions et les informations de compte utilisateur.

   - **Restaurer les rapports**

     Inclut les rapports personnalisés, les rapports prédéfinis, les modifications apportées aux rapports prédéfinis que vous avez effectués et les paramètres de rapport que vous avez définis dans Reporting Connection.

5. Cliquez sur **Restaurer**.

   Ne quittez pas l'état de restauration. Si vous le faites, l'état de la restauration ne s'affiche plus et vous ne recevez aucune indication lorsque l'opération de restauration est terminée.

6. Pour vérifier le processus de mise à niveau, consultez le `dwh_upgrade.log` fichier, qui se trouve à l'emplacement suivant : `<install directory>\SANscreen\wildfly\standalone\log`.

   Une fois le processus de restauration terminé, un message apparaît juste en dessous du bouton **Restaurer**. Si le processus de restauration a réussi, le message indique que le processus a réussi. Si le processus de restauration échoue, le message indique l'exception spécifique qui s'est produite à l'origine de l'échec. Dans ce cas, contactez le support technique et fournissez-lui `dwh_upgrade.log` fichier. Si une exception se produit et que l'opération de restauration échoue, la base de données d'origine est automatiquement réinitialisée.

> Si l'opération de restauration échoue avec le message ""échec de la mise à niveau du magasin de contenu cognos"", restaurez la base de données Data Warehouse sans ses rapports (base de données uniquement) et utilisez vos sauvegardes de rapport XML pour importer vos rapports.

Restauration des rapports Data Warehouse personnalisés

Le cas échéant, vous pouvez restaurer manuellement tous les rapports personnalisés que vous avez sauvegardés avant la mise à niveau ; cependant, vous n'avez besoin de le faire que si vous perdez des rapports sur s'ils sont corrompus.

Étapes

1. Ouvrez votre rapport à l'aide d'un éditeur de texte, puis sélectionnez et copiez son contenu.
2. Connectez-vous au portail de rapports à l'adresse `https://fqdn/reporting`.
3. Dans la barre d'outils Data Warehouse, cliquez sur Pour ouvrir le portail Insight Reporting.
4. Dans le menu Démarrer, sélectionnez **Report Studio**.
5. Sélectionnez n'importe quel package.

   Report Studio s'affiche.

6. Cliquez sur **Créer nouveau**.
7. Sélectionnez **liste**.
8. Dans le menu Outils, sélectionnez **Ouvrir le rapport à partir du presse-papiers**.

   La boîte de dialogue **Ouvrir le rapport à partir du presse-papiers** s'affiche.

9. Dans le menu fichier, sélectionnez **Enregistrer sous** et enregistrez le rapport dans le dossier Rapports personnalisés.
10. Ouvrez le rapport pour vérifier qu'il a été importé.

    Répétez cette tâche pour chaque rapport.

> Vous pouvez voir une « erreur d'analyse syntaxique de l'expression » lorsque vous chargez un rapport. Cela signifie que la requête contient une référence à au moins un objet qui n'existe pas, ce qui signifie qu'aucun package n'est sélectionné dans la fenêtre Source pour valider le rapport. Dans ce cas, cliquez avec le bouton droit de la souris sur une dimension de magasin de données dans la fenêtre Source, sélectionnez ensemble de rapports, Puis sélectionnez le package associé au rapport (par exemple, le package d'inventaire s'il s'agit d'un rapport d'inventaire ou l'un des packages de performances s'il s'agit d'un rapport de performances) afin que Report Studio puisse le valider et que vous puissiez l'enregistrer.

Vérification que Data Warehouse contient des données historiques

Après avoir restauré vos rapports personnalisés, vous devez vérifier que Data

Warehouse collecte des données historiques en affichant vos rapports personnalisés.

Étapes

1. Connectez-vous au portail Data Warehouse à l'adresse `https://fqdn/dwh`.
2. Dans la barre d'outils Data Warehouse, cliquez sur Pour ouvrir le portail Insight Reporting et vous connecter.
3. Ouvrez le dossier contenant vos rapports personnalisés (par exemple, Rapports personnalisés).
4. Cliquez sur pour ouvrir les options de format de sortie de ce rapport.
5. Sélectionnez les options de votre choix et cliquez sur **Exécuter** pour vous assurer qu'elles sont remplies de données d'historique de stockage, de calcul et de commutation.

Restauration de l'archive de performance

Pour les systèmes exécutant un archivage performant, le processus de mise à niveau ne restaure que sept jours de données archivées. Vous pouvez restaurer les données d'archive restantes après la mise à niveau.

Description de la tâche

Pour restaurer l'archive de performances, procédez comme suit.

Étapes

1. Dans la barre d'outils, cliquez sur **Admin** > **Dépannage**
2. Dans la section Restaurer, sous **Charger l'archive de performances**, cliquez sur **Charger**.

   Le chargement de l'archive est géré en arrière-plan. Le chargement de l'archive complète peut prendre beaucoup de temps car les données de performances archivées de chaque jour sont renseignées dans Insight. L'état du chargement de l'archive s'affiche dans la section archive de cette page.

Test des connecteurs

Après la mise à niveau, vous souhaitez tester les connecteurs pour vous assurer que vous disposez d'une connexion entre l'entrepôt de données OnCommand Insight et le serveur OnCommand Insight.

Étapes

1. Connectez-vous au portail Data Warehouse à l'adresse `https://fqdn/dwh`.
2. Dans le volet de navigation de gauche, cliquez sur **connecteurs**.
3. Sélectionnez le premier connecteur.

   La page Modifier le connecteur s'affiche.

4. Cliquez sur **Test**.

5. Si le test réussit, cliquez sur **Fermer** ; si le test échoue, entrez le nom du serveur Insight dans le champ **Nom** et son adresse IP dans le champ **hôte** et cliquez sur **Test**.
6. Lorsque la connexion entre l'entrepôt de données et le serveur Insight est établie, cliquez sur **Enregistrer**.

   Si le problème ne se produit pas, vérifiez la configuration de la connexion et assurez-vous que le serveur Insight ne présente aucun problème.

7. Cliquez sur **Test**.

   Data Warehouse teste la connexion.

Vérification de la planification d'extraction, de transformation et de chargement

Après la mise à niveau, vous devez vous assurer que le processus ETL (extraction, transformation et chargement) récupère les données des bases de données OnCommand Insight, les transforme et les enregistre dans les magasins de données.

Étapes

1. Connectez-vous au portail Data Warehouse à l'adresse `https://fqdn/dwh`.
2. Dans le volet de navigation de gauche, cliquez sur **Agenda**.
3. Cliquez sur **Modifier le programme**.
4. Sélectionnez **quotidien** ou **hebdomadaire** dans la liste **Type**.

   Il est recommandé de planifier l'exécution du CÉC une fois par jour.

5. Vérifiez que l'heure sélectionnée correspond à l'heure à laquelle vous souhaitez que le travail s'exécute.

   Cela permet de s'assurer que le travail de création s'exécute automatiquement.

6. Cliquez sur **Enregistrer**.

Mise à jour des modèles de disque

Après la mise à niveau, vous devez disposer de modèles de disques mis à jour. Toutefois, si pour une raison quelconque, Insight n'a pas pu détecter de nouveaux modèles de disques, vous pouvez les mettre à jour manuellement.

Avant de commencer

Vous devez avoir obtenu du support technique du `.zip` fichier contenant les derniers correctifs de source de données.

Étapes

1. Arrêtez le service SANscreen Acq.
2. Accédez au répertoire suivant : `<install`

`directory>\SANscreen\wildfly\standalone\deployments\datasources.war`.

3. Déplacer le courant `diskmodels.jar` fichier à un autre emplacement.
4. Copiez le nouveau `diskmodels.jar` classez-les dans le `datasources.war` répertoire.
5. Démarrez le service SANscreen Acq.

Vérification de l'exécution des outils de veille stratégique

Le cas échéant, vous devez vérifier que vos outils de veille stratégique sont en cours d'exécution et récupérer les données après la mise à niveau.

Vérifier que les outils de veille stratégique tels que BMC Atrium et ServiceNow sont en cours d'exécution et en mesure de récupérer les données. Cela inclut le connecteur BMC et les solutions qui exploitent REST.