



Réaliser les tâches de configuration et d'administration

Active IQ Unified Manager 9.9

NetApp
April 05, 2024

This PDF was generated from <https://docs.netapp.com/fr-fr/active-iq-unified-manager-99/config/concept-overview-of-the-configuration-sequence.html> on April 05, 2024. Always check docs.netapp.com for the latest.

Sommaire

- Réaliser les tâches de configuration et d'administration 1
 - Configuration d'Active IQ Unified Manager en cours 1
 - Configuration de la sauvegarde Unified Manager 29
 - Utilisation de la console de maintenance 29

Réaliser les tâches de configuration et d'administration

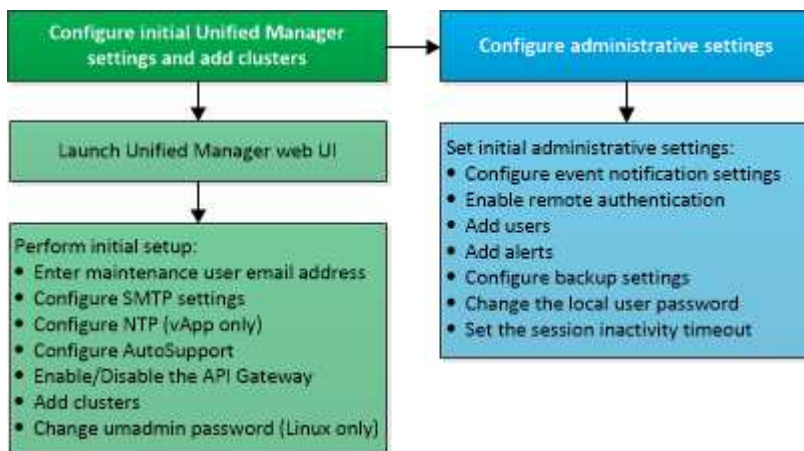
Configuration d'Active IQ Unified Manager en cours

Une fois Active IQ Unified Manager installé (anciennement OnCommand Unified Manager), vous devez effectuer la configuration initiale (également appelée premier assistant d'expérience) pour accéder à l'interface utilisateur Web. Vous pouvez ensuite effectuer des tâches de configuration supplémentaires, comme l'ajout de clusters, la configuration de l'authentification à distance, l'ajout d'utilisateurs et l'ajout d'alertes.

La configuration initiale de votre instance Unified Manager nécessite certaines des procédures décrites dans ce manuel. D'autres procédures sont des paramètres de configuration recommandés qui sont utiles pour configurer votre nouvelle instance ou dont vous devez connaître avant de lancer le contrôle régulier de vos systèmes ONTAP.

Présentation de la séquence de configuration

Le workflow de configuration décrit les tâches que vous devez effectuer avant d'utiliser Unified Manager.



Accès à l'interface utilisateur Web de Unified Manager

Une fois Unified Manager installé, vous pouvez accéder à l'interface utilisateur Web pour configurer Unified Manager de sorte que vous puissiez commencer à surveiller vos systèmes ONTAP.

Avant de commencer

- Si c'est la première fois que vous accédez à l'interface utilisateur Web, vous devez vous connecter en tant qu'utilisateur de maintenance (ou utilisateur umadmin pour les installations Linux).
- Si vous prévoyez d'autoriser les utilisateurs à accéder à Unified Manager à l'aide du nom court au lieu d'utiliser le nom de domaine complet (FQDN) ou l'adresse IP, votre configuration réseau doit résoudre ce nom court sur un FQDN valide.

- Si le serveur utilise un certificat numérique auto-signé, il se peut que le navigateur affiche un avertissement indiquant que le certificat n'est pas approuvé. Vous pouvez accepter le risque de continuer l'accès ou installer un certificat numérique signé par l'autorité de certification pour l'authentification du serveur.

Étapes

1. Pour démarrer l'interface utilisateur Web Unified Manager à partir de votre navigateur, utilisez l'URL affichée à la fin de l'installation. L'URL correspond à l'adresse IP ou au nom de domaine complet (FQDN) du serveur Unified Manager.

Le lien est au format suivant : `https://URL`.

1. Connectez-vous à l'interface utilisateur Web de Unified Manager à l'aide de vos identifiants de maintenance.

Configuration initiale de l'interface utilisateur Web de Unified Manager

Pour utiliser Unified Manager, vous devez d'abord configurer les options de configuration initiale, notamment le serveur NTP, l'adresse e-mail de l'utilisateur de maintenance et l'hôte du serveur SMTP, ainsi que l'ajout de clusters ONTAP.

Avant de commencer

Vous devez avoir effectué les opérations suivantes :

- L'interface utilisateur Web de Unified Manager a été lancée à l'aide de l'URL fournie après l'installation
- Connecté à l'aide du nom d'utilisateur et du mot de passe de maintenance (utilisateur umadmin pour les installations Linux) créés pendant l'installation

Description de la tâche

La page mise en route du Gestionnaire unifié Active IQ s'affiche uniquement lorsque vous accédez pour la première fois à l'interface utilisateur Web. La page ci-dessous provient d'une installation sur VMware.

Active IQ Unified Manager

Getting Started

1 Email 2 AutoSupport 3 API Gateway 4 Add ONTAP Clusters 5 Finish

Notifications

Configure your email server to allow Active IQ Unified Manager to assist in the event of a forgotten password.

Maintenance User Email

Email

SMTP Server

Host Name or IP Address

Port

User Name

Password

☒ Use START / TLS ☐

☐ Use SSL ☐

Next

Si vous souhaitez modifier l'une de ces options ultérieurement, vous pouvez sélectionner votre choix dans les options générales du volet de navigation gauche de Unified Manager. Notez que le paramètre NTP n'est utilisé que pour les installations VMware et peut être modifié par la suite à l'aide de la console de maintenance Unified Manager.

Étapes

1. Dans la page Configuration initiale de Active IQ Unified Manager, entrez l'adresse e-mail de l'utilisateur de maintenance, le nom d'hôte du serveur SMTP et toutes les options SMTP supplémentaires, ainsi que le serveur NTP (installations VMware uniquement). Cliquez ensuite sur **Continuer**.
2. Sur la page **AutoSupport**, cliquez sur **acceptez et continuez** pour activer l'envoi des messages AutoSupport depuis Unified Manager vers NetAppActive IQ.

Si vous devez désigner un proxy pour fournir un accès Internet afin d'envoyer du contenu AutoSupport ou si vous souhaitez désactiver AutoSupport, utilisez l'option **général** > **AutoSupport** de l'interface utilisateur Web.

3. Sur les systèmes Red Hat et CentOS, vous pouvez remplacer le mot de passe utilisateur umadmin par la chaîne ""admin" par une chaîne personnalisée.
4. Dans la page **configurer la passerelle API**, sélectionnez si vous souhaitez utiliser la fonctionnalité de passerelle d'API qui permet à Unified Manager de gérer les clusters ONTAP que vous prévoyez de contrôler à l'aide des API REST ONTAP. Cliquez ensuite sur **Continuer**.

Vous pouvez activer ou désactiver ce paramètre ultérieurement dans l'interface utilisateur Web à partir de **général** > **Paramètres de fonction** > **passerelle API**. Pour plus d'informations sur les API, voir ["Mise en route de Active IQ Unified Manager"](#).

5. Ajoutez les clusters que vous souhaitez gérer Unified Manager, puis cliquez sur **Suivant**. Pour chaque cluster que vous prévoyez de gérer, vous devez avoir le nom d'hôte ou l'adresse IP de gestion de cluster (IPv4 ou IPv6) avec le nom d'utilisateur et les identifiants de mot de passe. L'utilisateur doit avoir le rôle « admin ».

Cette étape est facultative. Vous pouvez ajouter des clusters ultérieurement dans l'interface utilisateur Web à partir de **Storage Management > Cluster Setup**.

6. Dans la page **Résumé**, vérifiez que tous les paramètres sont corrects et cliquez sur **Terminer**.

Résultats

La page mise en route se ferme et la page Tableau de bord Unified ManagerLe tableau de bord s'affiche.

Ajout de clusters

Vous pouvez ajouter un cluster à Active IQ Unified Manager afin de pouvoir contrôler le cluster. Il est donc possible d'obtenir des informations sur le cluster, notamment son état, sa capacité, ses performances et sa configuration, afin de trouver et de résoudre tous les problèmes potentiels.

Avant de commencer

- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.
- Vous devez disposer des informations suivantes :

- Nom d'hôte ou adresse IP de gestion du cluster

Le nom d'hôte est le FQDN ou le nom court que Unified Manager utilise pour se connecter au cluster. Le nom d'hôte doit être résolu sur l'adresse IP de gestion du cluster.

L'adresse IP de gestion du cluster doit être la LIF de gestion du cluster du serveur virtuel de stockage administratif (SVM). Si vous utilisez une LIF node-management, l'opération échoue.

- Le cluster doit exécuter la version 9.1 du logiciel ONTAP ou une version ultérieure.
- Nom d'utilisateur et mot de passe de l'administrateur ONTAP

Ce compte doit avoir le rôle *admin* avec accès application défini sur *ontapi*, *ssh* et *http*.

- Le numéro de port à connecter au cluster via le protocole HTTPS (en général le port 443)
- Vous disposez des certificats requis. Deux types de certificats sont requis :

Certificats de serveur : utilisés pour l'enregistrement. Un certificat valide est requis pour l'ajout d'un cluster. Si le certificat du serveur expire, vous devez le régénérer et redémarrer Unified Manager pour que les services soient à nouveau enregistrés automatiquement. Pour plus d'informations sur la génération du certificat, consultez l'article de la base de connaissances (KB) : ["Comment renouveler un certificat SSL dans ONTAP 9"](#)

Certificats client : utilisé pour l'authentification. Un certificat valide est requis pour l'ajout d'un cluster. Vous ne pouvez pas ajouter un cluster à Unified Manager avec un certificat expiré et si le certificat client a déjà expiré, vous devez le régénérer avant d'ajouter le cluster. Toutefois, si ce certificat expire pour un cluster déjà ajouté et qu'il est utilisé par Unified Manager, la messagerie EMS continue à

fonctionner avec le certificat expiré. Il n'est pas nécessaire de régénérer le certificat client.



Vous pouvez ajouter des clusters derrière un pare-feu/NAT à l'aide de l'adresse IP NAT Unified Manager. Tous les systèmes SnapProtect ou Workflow Automation connectés doivent également être situés derrière le pare-feu et les appels de l'API SnapProtect doivent utiliser l'adresse IP NAT pour identifier le cluster.

- L'espace requis doit être adéquat sur le serveur Unified Manager. Vous ne pouvez pas ajouter un cluster au serveur lorsque plus de 90 % d'espace dans le répertoire de base de données est déjà utilisé.

Description de la tâche

Dans le cas d'une configuration MetroCluster, vous devez ajouter les clusters locaux et distants, et les clusters doivent être configurés correctement.

Vous pouvez contrôler un cluster unique par deux instances de Unified Manager à condition que vous ayez configuré une deuxième LIF de gestion du cluster sur le cluster de manière à ce que chaque instance de Unified Manager se connecte via une autre LIF.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management > Cluster Setup**.
2. Sur la page **Cluster Setup**, cliquez sur **Add**.
3. Dans la boîte de dialogue **Ajouter un cluster**, spécifiez les valeurs requises, telles que le nom d'hôte ou l'adresse IP du cluster, le nom d'utilisateur, le mot de passe et le numéro de port.

Vous pouvez modifier l'adresse IP de gestion du cluster d'IPv6 au format IPv4 ou d'IPv4 à IPv6. La nouvelle adresse IP est indiquée dans la grille du cluster et la page de configuration du cluster une fois le cycle de surveillance suivant terminé.

4. Cliquez sur **soumettre**.
5. Dans la boîte de dialogue **Authorise Host**, cliquez sur **View Certificate** pour afficher les informations de certificat relatives au cluster.
6. Cliquez sur **Oui**.

Unified Manager vérifie le certificat uniquement lorsque le cluster est ajouté au départ. Unified Manager ne vérifie pas le certificat pour chaque appel d'API au ONTAP.

Résultats

Une fois que tous les objets d'un nouveau cluster sont découverts (15 minutes environ), Unified Manager commence à collecter les données de performance historiques pour les 15 jours précédents. Ces statistiques sont collectées à l'aide de la fonctionnalité de collecte de continuité des données. Cette fonctionnalité fournit des informations de performance sur plus de deux semaines pour un cluster immédiatement après son ajout. Une fois le cycle de collecte de continuité des données terminé, les données en temps réel des performances du cluster sont collectées, par défaut, toutes les cinq minutes.



Étant donné que la collecte de données de performances sur 15 jours consomme beaucoup de ressources CPU, il est conseillé d'échelonner l'ajout de nouveaux clusters pour que les sondages de collecte de la continuité des données ne s'exécutent pas simultanément sur un trop grand nombre de clusters. En outre, si vous redémarrez Unified Manager pendant la période de collecte de la continuité des données, la collecte sera interrompue et vous verrez des écarts dans les graphiques de performances pour les périodes manquantes.



Si vous recevez un message d'erreur que vous ne pouvez pas ajouter le cluster, vérifiez si les horloges sur les deux systèmes ne sont pas synchronisées et que la date de début du certificat HTTPS Unified Manager est postérieure à celle du cluster. Vous devez vous assurer que les horloges sont synchronisées à l'aide du protocole NTP ou d'un service similaire.

Configuration de Unified Manager pour envoyer des notifications d'alerte

Vous pouvez configurer Unified Manager pour qu'il envoie des notifications vous informant des événements de votre environnement. Avant d'envoyer des notifications, vous devez configurer plusieurs autres options Unified Manager.

Avant de commencer

Vous devez avoir le rôle Administrateur d'applications.

Description de la tâche

Une fois Unified Manager déployé et terminé la configuration initiale, vous devez envisager de configurer votre environnement pour déclencher des alertes et générer des e-mails de notification ou des interruptions SNMP en fonction de la réception des événements.

Étapes

1. [Configurer les paramètres de notification d'événements](#)

Si vous souhaitez recevoir des notifications d'alerte lorsque certains événements se produisent dans votre environnement, vous devez configurer un serveur SMTP et fournir une adresse électronique à partir de laquelle la notification d'alerte sera envoyée. Si vous souhaitez utiliser les interruptions SNMP, vous pouvez sélectionner cette option et fournir les informations nécessaires.

2. [Activez l'authentification à distance](#)

Si vous souhaitez que les utilisateurs LDAP ou Active Directory distants accèdent à l'instance Unified Manager et reçoivent des notifications d'alerte, vous devez activer l'authentification à distance.

3. [Ajouter des serveurs d'authentification](#)

Vous pouvez ajouter des serveurs d'authentification afin que les utilisateurs distants du serveur d'authentification puissent accéder à Unified Manager.

4. [Ajouter des utilisateurs](#)

Vous pouvez ajouter plusieurs types d'utilisateurs locaux ou distants et attribuer des rôles spécifiques. Lorsque vous créez une alerte, vous affectez un utilisateur pour recevoir les notifications d'alerte.

5. Ajouter des alertes

Une fois que vous avez ajouté l'adresse e-mail pour envoyer des notifications, ajouté des utilisateurs pour recevoir les notifications, configuré vos paramètres réseau et configuré les options SMTP et SNMP nécessaires à votre environnement, vous pouvez attribuer des alertes.

Configuration des paramètres de notification d'événement

Vous pouvez configurer Unified Manager pour qu'il envoie des notifications d'alerte lorsqu'un événement est généré ou lorsqu'un événement est affecté à un utilisateur. Vous pouvez configurer le serveur SMTP utilisé pour envoyer l'alerte et définir différents mécanismes de notification, par exemple, des notifications d'alerte peuvent être envoyées en tant qu'e-mails ou interruptions SNMP.

Avant de commencer

Vous devez disposer des informations suivantes :

- Adresse e-mail à partir de laquelle la notification d'alerte est envoyée

L'adresse e-mail apparaît dans le champ « de » des notifications d'alerte envoyées. Si l'e-mail ne peut pas être livré pour une raison quelconque, cette adresse e-mail est également utilisée comme destinataire pour le courrier non livrable.

- Le nom d'hôte du serveur SMTP ainsi que le nom d'utilisateur et le mot de passe pour accéder au serveur
- Nom d'hôte ou adresse IP de l'hôte de destination de déroutement qui recevra l'interruption SNMP, ainsi que la version SNMP, le port d'interruption sortant, la communauté et d'autres valeurs de configuration SNMP requises

Pour spécifier plusieurs destinations d'interruption, séparez chaque hôte par une virgule. Dans ce cas, tous les autres paramètres SNMP, tels que la version et le port d'interruption sortante, doivent être identiques pour tous les hôtes de la liste.

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général > Notifications**.
2. Dans la page **Notifications**, configurez les paramètres appropriés et cliquez sur **Enregistrer**.

Notes:

- Si l'adresse de expéditeur est pré-remplie avec l'adresse « ActiveIQUnifiedManager@localhost.com », vous devez la remplacer par une adresse e-mail réelle et opérationnelle afin de vous assurer que toutes les notifications par e-mail sont correctement envoyées.
- Si le nom d'hôte du serveur SMTP ne peut pas être résolu, vous pouvez spécifier l'adresse IP (IPv4 ou IPv6) du serveur SMTP au lieu du nom d'hôte.

Activation de l'authentification à distance

Vous pouvez activer l'authentification à distance afin que le serveur Unified Manager

puisse communiquer avec vos serveurs d'authentification. Les utilisateurs du serveur d'authentification peuvent accéder à l'interface graphique Unified Manager pour gérer les objets de stockage et les données.

Avant de commencer

Vous devez avoir le rôle Administrateur d'applications.



Le serveur Unified Manager doit être connecté directement au serveur d'authentification. Vous devez désactiver tous les clients LDAP locaux tels que SSSD (System Security Services Daemon) ou NSLCD (Name Service LDAP Caching Daemon).

Description de la tâche

Vous pouvez activer l'authentification à distance à l'aide de Open LDAP ou d'Active Directory. Si l'authentification à distance est désactivée, les utilisateurs distants ne peuvent pas accéder à Unified Manager.

L'authentification à distance est prise en charge via LDAP et LDAPS (Secure LDAP). Unified Manager utilise 389 comme port par défaut pour les communications non sécurisées et 636 comme port par défaut pour les communications sécurisées.



Le certificat utilisé pour authentifier les utilisateurs doit être conforme au format X.509.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général > authentification à distance**.
2. Cochez la case **Activer l'authentification à distance....**
3. Dans le champ **Service d'authentification**, sélectionnez le type de service et configurez le service d'authentification.

Pour le type d'authentification...	Entrez les informations suivantes...
Active Directory	<ul style="list-style-type: none">• Nom d'administrateur du serveur d'authentification dans l'un des formats suivants :<ul style="list-style-type: none">◦ domainname \ username◦ username@domainname◦ Bind Distinguished Name (Avec la notation LDAP appropriée)• Mot de passe administrateur• Nom distinctif de base (à l'aide de la notation LDAP appropriée)
Ouvrez LDAP	<ul style="list-style-type: none">• Nom distinctif de la liaison (dans la notation LDAP appropriée)• Lier le mot de passe• Nom distinctif de base

Si l'authentification d'un utilisateur Active Directory prend un certain temps ou plusieurs fois, le serveur d'authentification prend probablement beaucoup de temps pour répondre. La désactivation de la prise en charge des groupes imbriqués dans Unified Manager peut réduire le temps d'authentification.

Si vous sélectionnez l'option utiliser la connexion sécurisée pour le serveur d'authentification, Unified Manager communique avec le serveur d'authentification à l'aide du protocole SSL (Secure Sockets Layer).

1. Ajoutez des serveurs d'authentification et testez l'authentification.
2. Cliquez sur **Enregistrer**.

Désactivation des groupes imbriqués à partir de l'authentification à distance

Si l'authentification à distance est activée, vous pouvez désactiver l'authentification des groupes imbriqués de sorte que seuls les utilisateurs individuels, et non les membres du groupe, puissent s'authentifier à distance à Unified Manager. Vous pouvez désactiver les groupes imbriqués si vous souhaitez améliorer le temps de réponse de l'authentification Active Directory.

Avant de commencer

- Vous devez avoir le rôle Administrateur d'applications.
- La désactivation des groupes imbriqués n'est applicable que lors de l'utilisation d'Active Directory.

Description de la tâche

La désactivation de la prise en charge des groupes imbriqués dans Unified Manager peut réduire le temps d'authentification. Si la prise en charge des groupes imbriqués est désactivée et si un groupe distant est ajouté à Unified Manager, les utilisateurs individuels doivent être membres du groupe distant pour s'authentifier auprès d'Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général > authentification à distance**.
2. Cochez la case **Désactiver la recherche de groupe imbriqué**.
3. Cliquez sur **Enregistrer**.

Ajout de serveurs d'authentification

Vous pouvez ajouter des serveurs d'authentification et activer l'authentification à distance sur le serveur de gestion afin que les utilisateurs distants au sein du serveur d'authentification puissent accéder à Unified Manager.

Avant de commencer

- Les informations suivantes doivent être disponibles :
 - Nom d'hôte ou adresse IP du serveur d'authentification
 - Numéro de port du serveur d'authentification
- Vous devez avoir activé l'authentification à distance et configuré votre service d'authentification pour que le serveur de gestion puisse authentifier les utilisateurs ou groupes distants sur le serveur d'authentification.


- Vous devez avoir le rôle Administrateur d'applications.

Description de la tâche

Si le serveur d'authentification que vous ajoutez fait partie d'une paire haute disponibilité (HA) (utilisant la même base de données), vous pouvez également ajouter le serveur d'authentification partenaire. Cela permet au serveur de gestion de communiquer avec le partenaire lorsque l'un des serveurs d'authentification est inaccessible.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général > authentification à distance**.
2. Activez ou désactivez l'option **utiliser la connexion sécurisée** :

Les fonctions que vous recherchez...	Alors, procédez comme ça...
Activez-la	<ol style="list-style-type: none"> 1. Sélectionnez l'option utiliser connexion sécurisée. 2. Dans la zone serveurs d'authentification, cliquez sur Ajouter. 3. Dans la boîte de dialogue Ajouter un serveur d'authentification, entrez le nom d'authentification ou l'adresse IP (IPv4 ou IPv6) du serveur. 4. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur Afficher le certificat. 5. Dans la boîte de dialogue Afficher le certificat, vérifiez les informations sur le certificat, puis cliquez sur Fermer. 6. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur Oui. <div>  <p>Lorsque vous activez l'option utiliser l'authentification Secure Connection, Unified Manager communique avec le serveur d'authentification et affiche le certificat. Unified Manager utilise 636 comme port par défaut pour les communications sécurisées et le port numéro 389 pour les communications non sécurisées.</p> </div>

Les fonctions que vous recherchez...	Alors, procédez comme ça...
Désactivez-le	<ol style="list-style-type: none"> 1. Désactivez l'option utiliser connexion sécurisée. 2. Dans la zone serveurs d'authentification, cliquez sur Ajouter. 3. Dans la boîte de dialogue Add Authentication Server (Ajouter un serveur d'authentification), spécifiez le nom d'hôte ou l'adresse IP (IPv4 ou IPv6) du serveur, ainsi que les détails du port. 4. Cliquez sur Ajouter.

Le serveur d'authentification que vous avez ajouté s'affiche dans la zone serveurs.

1. Effectuez un test d'authentification pour confirmer que vous pouvez authentifier les utilisateurs sur le serveur d'authentification que vous avez ajouté.

Test de la configuration des serveurs d'authentification

Vous pouvez valider la configuration de vos serveurs d'authentification pour vous assurer que le serveur de gestion peut communiquer avec eux. Vous pouvez valider la configuration en recherchant un utilisateur ou un groupe distant à partir de vos serveurs d'authentification et en les authentifiant à l'aide des paramètres configurés.

Avant de commencer

- Vous devez avoir activé l'authentification à distance et configuré votre service d'authentification pour que le serveur Unified Manager puisse authentifier l'utilisateur distant ou le groupe distant.
- Vous devez avoir ajouté vos serveurs d'authentification pour que le serveur de gestion puisse rechercher l'utilisateur ou le groupe distant à partir de ces serveurs et les authentifier.
- Vous devez avoir le rôle Administrateur d'applications.

Description de la tâche

Si le service d'authentification est défini sur Active Directory et que vous validez l'authentification d'utilisateurs distants appartenant au groupe principal du serveur d'authentification, les informations relatives au groupe principal ne s'affichent pas dans les résultats de l'authentification.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général > authentification à distance**.
2. Cliquez sur **Tester l'authentification**.
3. Dans la boîte de dialogue **Test User**, indiquez le nom d'utilisateur et le mot de passe de l'utilisateur distant ou le nom d'utilisateur du groupe distant, puis cliquez sur **Test**.

Si vous authentifiez un groupe distant, vous ne devez pas entrer le mot de passe.

Ajout d'utilisateurs

Vous pouvez ajouter des utilisateurs locaux ou des utilisateurs de base de données à l'aide de la page utilisateurs. Vous pouvez également ajouter des utilisateurs ou des groupes distants appartenant à un serveur d'authentification. Vous pouvez attribuer des rôles à ces utilisateurs et, en fonction des privilèges des rôles, les utilisateurs peuvent gérer les objets et les données de stockage à l'aide de Unified Manager ou afficher les données dans une base de données.

Avant de commencer

- Vous devez avoir le rôle Administrateur d'applications.
- Pour ajouter un utilisateur ou un groupe distant, vous devez avoir activé l'authentification à distance et configuré votre serveur d'authentification.
- Si vous prévoyez de configurer l'authentification SAML de sorte qu'un fournisseur d'identités authentifie les utilisateurs qui accèdent à l'interface graphique, assurez-vous que ces utilisateurs sont définis comme des utilisateurs « réels ».

L'accès à l'interface utilisateur n'est pas autorisé pour les utilisateurs de type « local » ou « provenance » lorsque l'authentification SAML est activée.

Description de la tâche

Si vous ajoutez un groupe à partir de Windows Active Directory, tous les membres directs et sous-groupes imbriqués peuvent s'authentifier auprès d'Unified Manager, à moins que les sous-groupes imbriqués ne soient désactivés. Si vous ajoutez un groupe à partir d'OpenLDAP ou d'autres services d'authentification, seuls les membres directs de ce groupe peuvent s'authentifier auprès d'Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général > utilisateurs**.
2. Sur la page **utilisateurs**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter un utilisateur**, sélectionnez le type d'utilisateur que vous souhaitez ajouter et entrez les informations requises.

Lorsque vous entrez les informations requises pour l'utilisateur, vous devez spécifier une adresse électronique unique pour cet utilisateur. Vous devez éviter de spécifier des adresses e-mail partagées par plusieurs utilisateurs.

4. Cliquez sur **Ajouter**.

Ajout d'alertes

Vous pouvez configurer des alertes pour vous avertir lorsqu'un événement particulier est généré. Vous pouvez configurer les alertes pour une seule ressource, pour un groupe de ressources ou pour les événements d'un type de sévérité particulier. Vous pouvez spécifier la fréquence à laquelle vous souhaitez être averti et associer un script à l'alerte.

Avant de commencer

- Vous devez avoir configuré des paramètres de notification tels que l'adresse e-mail de l'utilisateur, le serveur SMTP et l'hôte d'interruption SNMP pour permettre au serveur Active IQ Unified Manager d'utiliser ces paramètres pour envoyer des notifications aux utilisateurs lorsqu'un événement est généré.
- Vous devez connaître les ressources et les événements pour lesquels vous souhaitez déclencher l'alerte, ainsi que les noms d'utilisateur ou adresses e-mail des utilisateurs que vous souhaitez notifier.
- Si vous souhaitez que le script soit exécuté en fonction de l'événement, vous devez l'avoir ajouté à Unified Manager à l'aide de la page scripts.
- Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

Description de la tâche

Vous pouvez créer une alerte directement à partir de la page Détails de l'événement après avoir reçu un événement en plus de créer une alerte à partir de la page Configuration de l'alerte, comme décrit ici.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management > Alert Setup**.
2. Dans la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom**, puis entrez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources**, puis sélectionnez les ressources à inclure ou à exclure de l'alerte.

Vous pouvez définir un filtre en spécifiant une chaîne de texte dans le champ **Nom contient** pour sélectionner un groupe de ressources. En fonction de la chaîne de texte que vous spécifiez, la liste des ressources disponibles n'affiche que les ressources qui correspondent à la règle de filtre. La chaîne de texte que vous spécifiez est sensible à la casse.

Si une ressource est conforme à la fois aux règles inclure et exclure que vous avez spécifiées, la règle d'exclusion est prioritaire sur la règle inclure et l'alerte n'est pas générée pour les événements liés à la ressource exclue.

5. Cliquez sur **Événements**, puis sélectionnez les événements en fonction du nom de l'événement ou du type de gravité de l'événement pour lequel vous souhaitez déclencher une alerte.



Pour sélectionner plusieurs événements, appuyez sur la touche Ctrl pendant que vous effectuez vos sélections.

6. Cliquez sur **actions** et sélectionnez les utilisateurs que vous souhaitez notifier, choisissez la fréquence de notification, choisissez si une interruption SNMP sera envoyée au récepteur d'interruption et affectez un script à exécuter lorsqu'une alerte est générée.



Si vous modifiez l'adresse e-mail spécifiée pour l'utilisateur et rouvrez l'alerte pour modification, le champ Nom apparaît vide car l'adresse e-mail modifiée n'est plus mappée à l'utilisateur qui a été précédemment sélectionné. En outre, si vous avez modifié l'adresse e-mail de l'utilisateur sélectionné à partir de la page utilisateurs, l'adresse e-mail modifiée n'est pas mise à jour pour l'utilisateur sélectionné.

Vous pouvez également choisir de notifier les utilisateurs via les interruptions SNMP.

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

Dans cet exemple, vous apprendrez à créer une alerte conforme aux exigences suivantes :

- Nom de l'alerte : HealthTest
- Ressources : inclut tous les volumes dont le nom contient « abc » et exclut tous les volumes dont le nom contient « xyz ».
- Événements : inclut tous les événements de santé critiques
- Actions : inclut «ample@domain.com», un script «Test», et l'utilisateur doit être averti toutes les 15 minutes

Effectuez les opérations suivantes dans la boîte de dialogue Ajouter une alerte :

1. Cliquez sur **Nom** et saisissez HealthTest Dans le champ **Nom d'alerte**.
2. Cliquez sur **Ressources** et, dans l'onglet inclure, sélectionnez **volumes** dans la liste déroulante.
 - a. Entrez abc Dans le champ **Name contient** pour afficher les volumes dont le nom contient « abc ».
 - b. Sélectionnez <<All Volumes whose name contains 'abc'>> dans la zone Ressources disponibles, et déplacez-la dans la zone Ressources sélectionnées.
 - c. Cliquez sur **exclure**, puis saisissez xyz Dans le champ **Name contient**, puis cliquez sur **Add**.
3. Cliquez sur **Événements**, puis sélectionnez **critique** dans le champ gravité de l'événement.
4. Sélectionnez **tous les événements critiques** dans la zone événements de correspondance et déplacez-le dans la zone événements sélectionnés.
5. Cliquez sur **actions**, puis saisissez sample@domain.com Dans le champ Alert ces utilisateurs.
6. Sélectionnez **rappeler toutes les 15 minutes** pour avertir l'utilisateur toutes les 15 minutes.

Vous pouvez configurer une alerte pour qu'elle envoie régulièrement des notifications aux destinataires pendant une heure donnée. Vous devez déterminer l'heure à laquelle la notification d'événement est active pour l'alerte.

7. Dans le menu Select script to Execute, sélectionnez **Test** script.
8. Cliquez sur **Enregistrer**.

Événements EMS ajoutés automatiquement à Unified Manager

Les événements ONTAP EMS suivants sont ajoutés automatiquement à Unified Manager. Ces événements sont générés lorsqu'ils sont déclenchés sur un cluster que Unified Manager surveille.

Les événements EMS suivants sont disponibles lors de la surveillance des clusters exécutant ONTAP 9.5 ou une version supérieure du logiciel :

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité de Unified Manager
Accès au niveau cloud refusé pour le transfert d'agrégats	arl.netra.ca.check.failed	Agrégat	Erreur
Accès au niveau cloud refusé pour la relocalisation des agrégats pendant le basculement du stockage	gb.netra.ca.check.failed	Agrégat	Erreur
Resynchronisation de la réplication des miroirs FabricPool terminée	wafl.ca.resync.complete	Cluster	Erreur
Espace FabricPool presque plein	fabritpool.presque.plein	Cluster	Erreur
Le délai NVMe-of Grace a commencé	nvmf.graceperiod.start	Cluster	Avertissement
Délai de grâce NVMe-of actif	nvmf.graceperiod.active	Cluster	Avertissement
Délai de grâce NVMe-of expiré	nvmf.graceperiod.expired	Cluster	Avertissement
LUN supprimée	lun.destroy	LUN	Informations
MetaDataConnFail dans le cloud AWS	Cloud.aws.metadataConnFail	Nœud	Erreur
Cloud AWS IAMCredentistesExrequis	Cloud.aws.iamCredentistesExpired	Nœud	Erreur
Identifiants iAMCredentistspour Cloud AWS non valides	Cloud.aws.iamCredsinvalid	Nœud	Erreur
Des informations iAMCredentistsNotFound pour Cloud AWS	Cloud.aws.iamCredentistsNotFound	Nœud	Erreur
Cloud AWS IAMCredentistsNotInitialized	Cloud.aws.iamNotInitialized	Nœud	Informations

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité de Unified Manager
IAMRoleInvalid Cloud AWS	Cloud.aws.iamRoleInvalid	Nœud	Erreur
L'IAMRoleNotFound Cloud AWS	Cloud.aws.iamRoleNotFound	Nœud	Erreur
L'hôte Cloud Tier ne peut pas être résolu	objstore.host.non résolu	Nœud	Erreur
Panne LIF intercluster Cloud Tier	objstore.interclusterlifDown	Nœud	Erreur
Demander une signature de niveau de cloud différente	osc.signatureMismatch	Nœud	Erreur
Un des pools NFSv4 épuisés	NBlade.nfsV4PoolExhaust	Nœud	Primordial
QoS Monitor mémoire portée en mémoire	qos.monitor.memory.capacity maximale	Nœud	Erreur
Mémoire du moniteur QoS saturée	qos.monitor.memory.abated	Nœud	Informations
Détruire NVMeNS	NVMeNS.destroy	Espace de noms	Informations
NVMeNS en ligne	NVMeNS.offline	Espace de noms	Informations
NVMeNS hors ligne	NVMeNS.online	Espace de noms	Informations
NVMeNS hors de l'espace	NVMeNS.out.of.space	Espace de noms	Avertissement
Réplication synchrone hors synchronisation	sms.status.out.of.sync	Relation SnapMirror	Avertissement
Réplication synchrone restaurée	sms.status.in.sync	Relation SnapMirror	Informations
Échec de la resynchronisation automatique de la réplication synchrone	sms.resynchronisation.tentative.échec	Relation SnapMirror	Erreur

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité de Unified Manager
De nombreuses connexions CIFS	Nibd.cifsManyAuths	SVM	Erreur
Connexion CIFS maximale dépassée	NBlade.cifsMaxOpenSam etiFile	SVM	Erreur
Le nombre maximal de connexions CIFS par utilisateur a été dépassé	NBlade.cifsMaxSessPerU srConn	SVM	Erreur
Conflit de nom CIFS NetBIOS	NBlade.cifsNbNameConfli tt	SVM	Erreur
Tentatives de connexion sans partage CIFS	NBlade.cifsNoPrivShare	SVM	Primordial
Échec de l'opération CIFS Shadow Copy	cifs.shadowcopy.failure	SVM	Erreur
Virus détecté par le serveur AV	NBlade.vscanVirusDetect ed	SVM	Erreur
Aucune connexion au serveur AV pour virus Scan	NBlade.vscanNoScanner Conn	SVM	Primordial
Aucun serveur AV enregistré	NBlade.vscanNoRegdSca nner	SVM	Erreur
Pas de connexion au serveur AV réactive	NBlade.vscanConnInactif	SVM	Informations
Serveur AV trop occupé pour accepter une nouvelle demande de numérisation	NBlade.vscanConnBackP ressure	SVM	Erreur
Un utilisateur non autorisé tente d'utiliser le serveur AV	NBlade.vscanBadUserPri vAccess	SVM	Erreur
Les composants FlexGroup présentent des problèmes d'espace	flexgroup.constituants.hav e.space.issues	Volumétrie	Erreur

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité de Unified Manager
État de l'espace des composants FlexGroup OK	flexgroup.commettants.space.status.all.ok	Volumétrie	Informations
Les composants FlexGroup présentent des problèmes d'inodes	flexgroup.constituents.have.inodes.issues	Volumétrie	Erreur
État des inodes des composants FlexGroup OK	flexgroup.constituents.inodes.status.all.ok	Volumétrie	Informations
Espace logique du volume presque plein	monitor.vol.nearFull.inc.sav	Volumétrie	Avertissement
Espace logique du volume plein	monitor.vol.full.inc.sav	Volumétrie	Erreur
Volume Logical Space Normal	monitor.vol.one.ok.inc.sav	Volumétrie	Informations
Échec de la taille automatique du volume WAFL	wafl.vol.autoSize.fail	Volumétrie	Erreur
Taille automatique du volume WAFL terminée	wafl.vol.autoSize.done	Volumétrie	Informations
WAFL - délai d'attente de l'opération de FICHER DE REMADDIR	wafl.readdir.expiré	Volumétrie	Erreur

Abonnement aux événements ONTAP EMS

Vous pouvez vous abonner aux événements EMS (Event Management System) générés par les systèmes installés avec le logiciel ONTAP. Un sous-ensemble d'événements EMS est automatiquement signalé à Unified Manager, mais des événements EMS supplémentaires ne sont signalés que si vous êtes abonné à ces événements.

Avant de commencer

Ne vous abonnez pas aux événements EMS déjà ajoutés automatiquement à Unified Manager, car ils peuvent être source de confusion lors de la réception de deux événements pour le même problème.

Description de la tâche

Vous pouvez vous abonner à un certain nombre d'événements EMS. Tous les événements auxquels vous êtes abonné sont validés, et seuls les événements validés sont appliqués aux clusters que vous surveillez dans Unified Manager. Le catalogue d'événements EMS *ONTAP 9* fournit des informations détaillées sur tous les messages EMS pour la version spécifiée du logiciel ONTAP 9. Recherchez la version appropriée du catalogue d'événements *EMS* dans la page Documentation produit de ONTAP 9 pour obtenir la liste des événements applicables.

"Bibliothèque de produits ONTAP 9"

Vous pouvez configurer les alertes relatives aux événements EMS ONTAP auxquels vous êtes abonné et créer des scripts personnalisés à exécuter pour ces événements.



Si vous ne recevez pas les événements EMS ONTAP auxquels vous êtes abonné, il peut y avoir un problème de configuration DNS du cluster qui empêche le cluster d'atteindre le serveur Unified Manager. Pour résoudre ce problème, l'administrateur du cluster doit corriger la configuration DNS du cluster, puis redémarrer Unified Manager. Cette opération permet de vider les événements EMS en attente du serveur Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management > Event Setup**.
2. Dans la page **Event Setup**, cliquez sur le bouton **Subscribe to EMS Events**.
3. Dans la boîte de dialogue **s'abonner aux événements EMS**, entrez le nom de l'événement EMS ONTAP auquel vous souhaitez vous abonner.

Pour afficher les noms des événements EMS auxquels vous pouvez vous abonner, depuis le shell du cluster ONTAP, vous pouvez utiliser `event route show` (Avant ONTAP 9) ou le `event catalog show` (ONTAP 9 ou version ultérieure).

["Comment configurer et recevoir des alertes de l'abonnement aux événements EMS ONTAP dans Active IQ Unified Manager"](#)

4. Cliquez sur **Ajouter**.

L'événement EMS est ajouté à la liste des événements EMS auxquels vous êtes abonné, mais la colonne applicable au cluster affiche l'état « Inconnu » pour l'événement EMS que vous avez ajouté.

5. Cliquez sur **Enregistrer et fermer** pour enregistrer l'abonnement aux événements EMS avec le cluster.
6. Cliquez de nouveau sur **Abonnez-vous aux événements EMS**.

L'état « Oui » apparaît dans la colonne applicable au cluster pour l'événement EMS que vous avez ajouté.

Si le statut n'est pas « Oui », vérifiez l'orthographe du nom de l'événement EMS ONTAP. Si le nom n'est pas saisi correctement, vous devez supprimer l'événement incorrect, puis ajouter à nouveau l'événement.

Une fois que vous avez terminé

Lorsque l'événement EMS ONTAP se produit, l'événement s'affiche sur la page événements. Vous pouvez sélectionner l'événement pour afficher les détails de l'événement EMS sur la page Détails de l'événement. Vous pouvez également gérer la disposition de l'événement ou créer des alertes pour cet événement.

Gestion des paramètres d'authentification SAML

Une fois que vous avez configuré les paramètres d'authentification à distance, vous pouvez activer l'authentification SAML afin que les utilisateurs distants soient authentifiés par un fournisseur d'identités sécurisé avant d'accéder à l'interface utilisateur Web Unified Manager.

Notez que seuls les utilisateurs distants ont accès à l'interface utilisateur graphique Unified Manager une fois l'authentification SAML activée. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l'interface utilisateur. Cette configuration n'a aucun impact sur les utilisateurs qui accèdent à la console de maintenance.

Exigences du fournisseur d'identités

Lors de la configuration d'Unified Manager pour utiliser un fournisseur d'identités (IDP) pour effectuer l'authentification SAML de tous les utilisateurs distants, vous devez connaître certains paramètres de configuration requis afin que la connexion à Unified Manager soit établie.

Vous devez entrer l'URI Unified Manager et les métadonnées dans le serveur IDP. Vous pouvez copier ces informations à partir de la page Unified ManagerSAML Authentication. Unified Manager est considéré comme le fournisseur de services dans la norme SAML.

Normes de chiffrement prises en charge

- Advanced Encryption Standard (AES) : AES-128 et AES-256
- Algorithme de hachage sécurisé (SHA) : SHA-1 et SHA-256

Des fournisseurs d'identité validés

- Hurlent
- ADFS (Active Directory Federation Services)

Configuration requise pour ADFS

- Vous devez définir trois règles de sinistre dans l'ordre suivant qui sont nécessaires à Unified Manager pour analyser les réponses SAML ADFS pour cette entrée de confiance de tiers de confiance.

Règle de réclamation	Valeur
SAM-account-name	ID nom
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Groupes de jetons — Nom non qualifié	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Vous devez définir la méthode d'authentification sur « authentification des formulaires » pour que les utilisateurs puissent recevoir une erreur lors de la déconnexion d'Unified Manager . Voici la procédure à suivre :
 - a. Ouvrez la console de gestion ADFS.

- b. Cliquez sur le dossier Authentication Policies dans l'arborescence de gauche.
- c. Sous actions à droite, cliquez sur Modifier la stratégie d'authentification principale globale.
- d. Définissez la méthode d'authentification Intranet sur « authentification des formulaires » au lieu de « authentification Windows » par défaut.
- Dans certains cas, la connexion via le PDI est rejetée lorsque le certificat de sécurité Unified Manager est signé avec une autorité de certification. Il existe deux solutions pour résoudre ce problème :
 - Suivez les instructions indiquées dans le lien pour désactiver la vérification de révocation sur le serveur ADFS pour les certificats CA chaînés associés à la partie de confiance :

"Désactiver le contrôle de révocation par confiance de la partie utilisatrices"

- Demandez au serveur CA de se trouver dans le serveur ADFS pour signer la demande d'autorisation de serveur Unified Manager.

Autres exigences de configuration

- L'inclinaison de l'horloge de Unified Manager est définie sur 5 minutes, la différence de temps entre le serveur IDP et le serveur Unified Manager ne peut pas dépasser 5 minutes, sinon l'authentification échouera.

Activation de l'authentification SAML

Vous pouvez activer l'authentification SAML (Security assertion Markup Language) pour que les utilisateurs distants soient authentifiés par un fournisseur d'identités sécurisé avant d'accéder à l'interface utilisateur Web d'Unified Manager.

Avant de commencer

- Vous devez avoir configuré l'authentification à distance et vérifié qu'elle a réussi.
- Vous devez avoir créé au moins un utilisateur distant ou un groupe distant avec le rôle Administrateur d'applications.
- Le fournisseur d'identités doit être pris en charge par Unified Manager et doit être configuré.
- Vous devez disposer de l'URL IDP et des métadonnées.
- Vous devez avoir accès au serveur IDP.

Description de la tâche

Une fois l'authentification SAML activée à partir d'Unified Manager, les utilisateurs ne peuvent pas accéder à l'interface utilisateur graphique tant que le IDP n'a pas été configuré avec les informations d'hôte du serveur Unified Manager. Vous devez donc être prêt à effectuer les deux parties de la connexion avant de lancer le processus de configuration. Le IDP peut être configuré avant ou après la configuration de Unified Manager.

Seuls les utilisateurs distants ont accès à l'interface utilisateur graphique Unified Manager une fois l'authentification SAML activée. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l'interface utilisateur. Cette configuration n'a aucun impact sur les utilisateurs qui accèdent à la console de maintenance, aux commandes Unified Manager ou aux ZAPI.



Unified Manager est redémarré automatiquement après la configuration SAML de cette page.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général > authentification SAML**.
2. Cochez la case **Activer l'authentification SAML**.

Les champs requis pour configurer la connexion IDP sont affichés.

3. Entrez l'URI du IDP et les métadonnées IDP requises pour connecter le serveur Unified Manager au serveur IDP.

Si le serveur IDP est accessible directement à partir du serveur Unified Manager, vous pouvez cliquer sur le bouton **Fetch IDP Metadata** après avoir saisi l'URI IDP pour remplir automatiquement le champ IDP Metadata.

4. Copiez l'URI des métadonnées de l'hôte Unified Manager ou enregistrez les métadonnées de l'hôte dans un fichier texte XML.

Vous pouvez configurer le serveur IDP avec ces informations pour le moment.

5. Cliquez sur **Enregistrer**.

Un message s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

6. Cliquez sur **confirmer et Déconnexion** et Unified Manager redémarre.

Résultats

Lors de la prochaine tentative d'accès à l'interface graphique Unified Manager, les utilisateurs distants autorisés saisissent leurs identifiants sur la page de connexion du fournisseur intégré au lieu de la page de connexion de Unified Manager.

Une fois que vous avez terminé

Si ce n'est pas déjà fait, accédez à votre IDP et entrez l'URI du serveur Unified Manager et les métadonnées pour terminer la configuration.



Lorsque vous utilisez ADFS en tant que fournisseur d'identité, l'interface graphique Unified Manager ne respecte pas le délai d'attente de l'ADFS et continue de fonctionner jusqu'à ce que le délai d'expiration de la session Unified Manager soit atteint. Vous pouvez modifier le délai d'expiration de la session de l'interface graphique en cliquant sur **général > Paramètres de fonction > délai d'inactivité**.

Modification du mot de passe de l'utilisateur local

Vous pouvez modifier votre mot de passe de connexion utilisateur local afin d'éviter tout risque de sécurité.

Avant de commencer

Vous devez être connecté en tant qu'utilisateur local.

Description de la tâche

Les mots de passe de l'utilisateur de maintenance et des utilisateurs distants ne peuvent pas être modifiés à l'aide de ces étapes. Pour modifier le mot de passe d'un utilisateur distant, contactez l'administrateur de votre mot de passe. Pour modifier le mot de passe utilisateur de maintenance, reportez-vous à la section "[Utilisation de la console de maintenance](#)".

Étapes

1. Connectez-vous à Unified Manager.
2. Dans la barre de menus supérieure, cliquez sur l'icône utilisateur, puis sur **changer mot de passe**.

L'option **Modifier le mot de passe** n'est pas affichée si vous êtes un utilisateur distant.

3. Dans la boîte de dialogue **Modifier le mot de passe**, entrez le mot de passe actuel et le nouveau mot de passe.
4. Cliquez sur **Enregistrer**.

Une fois que vous avez terminé

Si Unified Manager est configuré dans une configuration haute disponibilité, vous devez modifier le mot de passe sur le second nœud du setup. Les deux instances doivent avoir le même mot de passe.

Définition du délai d'inactivité de la session

Vous pouvez spécifier la valeur du délai d'inactivité pour Unified Manager afin que la session soit automatiquement arrêtée au bout d'un certain temps. Par défaut, le délai est défini sur 4,320 minutes (72 heures).

Avant de commencer

Vous devez avoir le rôle Administrateur d'applications.

Description de la tâche

Ce paramètre affecte toutes les sessions utilisateur connectées.



Cette option n'est pas disponible si vous avez activé l'authentification SAML (Security assertion Markup Language).

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général > Paramètres de fonction**.
2. Dans la page **Feature Settings**, spécifiez le délai d'inactivité en choisissant l'une des options suivantes :

Les fonctions que vous recherchez...	Alors, procédez comme ça...
Aucun délai défini pour que la session ne soit jamais fermée automatiquement	Dans le panneau délai d'inactivité , déplacez le curseur vers la gauche (désactivé) et cliquez sur appliquer .

Les fonctions que vous recherchez...	Alors, procédez comme ça...
Définissez un nombre spécifique de minutes comme valeur de délai d'inactivité	Dans le panneau délai d'inactivité , déplacez le curseur vers la droite (activé), spécifiez la valeur du délai d'inactivité en minutes, puis cliquez sur appliquer .

Modification du nom d'hôte Unified Manager

Il peut être nécessaire de modifier le nom d'hôte du système sur lequel vous avez installé Unified Manager. Par exemple, vous pouvez renommer l'hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de clusters surveillé.

Les étapes requises pour modifier le nom d'hôte sont différentes selon que Unified Manager s'exécute ou non sur un serveur VMware ESXi, sur un serveur Red Hat ou CentOS Linux, ou sur un serveur Microsoft Windows.

Modification du nom d'hôte de l'appliance virtuelle Unified Manager

Un nom est attribué à l'hôte réseau lors du premier déploiement de l'appliance virtuelle Unified Manager. Vous pouvez modifier le nom d'hôte après le déploiement. Si vous modifiez le nom d'hôte, vous devez également régénérer le certificat HTTPS.

Avant de commencer

Vous devez être connecté à Unified Manager en tant qu'utilisateur de maintenance, ou avoir le rôle d'administrateur d'applications qui vous est attribué pour effectuer ces tâches.

Description de la tâche

Vous pouvez utiliser le nom d'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur Web Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau pendant le déploiement, vous avez alors désigné un nom pour l'hôte réseau. Si vous avez configuré le réseau à l'aide de DHCP, le nom d'hôte doit être pris du DNS. Si DHCP ou DNS n'est pas correctement configuré, le nom d'hôte « Unified Manager » est automatiquement attribué et associé au certificat de sécurité.

Quel que soit le mode d'attribution du nom d'hôte, si vous modifiez le nom d'hôte et que vous prévoyez d'utiliser le nouveau nom d'hôte pour accéder à l'interface utilisateur Web Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface utilisateur Web à l'aide de l'adresse IP du serveur au lieu du nom d'hôte, vous n'avez pas à générer de nouveau certificat si vous modifiez le nom d'hôte. Toutefois, il est recommandé de mettre à jour le certificat de sorte que le nom d'hôte du certificat corresponde au nom d'hôte réel.

Si vous modifiez le nom d'hôte dans Unified Manager, vous devez mettre à jour manuellement le nom d'hôte dans OnCommand Workflow Automation (WFA). Le nom d'hôte n'est pas mis à jour automatiquement dans WFA.

Le nouveau certificat n'est effectif qu'après le redémarrage de la machine virtuelle Unified Manager.

Étapes

1. Générez un certificat de sécurité HTTPS

Si vous souhaitez utiliser le nouveau nom d'hôte pour accéder à l'interface utilisateur Web d'Unified Manager, vous devez régénérer le certificat HTTPS pour l'associer au nouveau nom d'hôte.

2. Redémarrez la machine virtuelle Unified Manager

Après la régénération du certificat HTTPS, vous devez redémarrer la machine virtuelle Unified Manager.

Génération d'un certificat de sécurité HTTPS

Lors de la première installation de Active IQ Unified Manager, un certificat HTTPS par défaut est installé. Vous pouvez générer un nouveau certificat de sécurité HTTPS qui remplace le certificat existant.

Avant de commencer

Vous devez avoir le rôle Administrateur d'applications.

Description de la tâche

Il peut y avoir plusieurs raisons de régénérer le certificat, par exemple si vous souhaitez avoir de meilleures valeurs pour le nom unique (DN) ou si vous voulez une taille de clé plus élevée, ou une période d'expiration plus longue ou si le certificat actuel a expiré.

Si vous n'avez pas accès à l'interface utilisateur Web d'Unified Manager, vous pouvez régénérer le certificat HTTPS avec les mêmes valeurs à l'aide de la console de maintenance. Pendant la régénération des certificats, vous pouvez définir la taille de la clé et la durée de validité de la clé. Si vous utilisez le `Reset Server Certificate` Disponible sur la console de maintenance, un nouveau certificat HTTPS est créé pendant 397 jours. Ce certificat sera doté d'une clé RSA de taille 2048 bits.


Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général > certificat HTTPS**.
2. Cliquez sur **régénérer le certificat HTTPS**.

La boîte de dialogue régénérer le certificat HTTPS s'affiche.

3. Sélectionnez l'une des options suivantes en fonction de la façon dont vous souhaitez générer le certificat :

Les fonctions que vous recherchez...	Procédez comme ça...
Régénérer le certificat avec les valeurs actuelles	Cliquez sur l'option régénérer en utilisant les attributs de certificat actuels .

Les fonctions que vous recherchez...	Procédez comme ça...
Générez le certificat à l'aide de valeurs différentes	<p data-bbox="443 191 1299 222">Cliquez sur l'option mettre à jour les attributs de certificat actuels.</p> <p data-bbox="443 254 1484 495">Les champs Nom commun et noms alternatifs utiliseront les valeurs du certificat existant si vous ne saisissez pas de nouvelles valeurs. Le « Nom commun » doit être défini sur le FQDN de l'hôte. Les autres champs ne nécessitent pas de valeurs, mais vous pouvez entrer des valeurs, par exemple pour l'E-MAIL, LA SOCIÉTÉ, LE SERVICE, Ville, État et pays si vous souhaitez que ces valeurs soient renseignées dans le certificat. Vous pouvez également sélectionner la TAILLE DE CLÉ disponible (l'algorithme clé est « RSA ») et LA PÉRIODE DE VALIDITÉ.</p> <div data-bbox="475 527 1484 1220">  <ul style="list-style-type: none"> <li data-bbox="618 537 1414 600">• Les valeurs autorisées pour la taille de clé sont 2048, 3072 et 4096. <li data-bbox="618 621 1414 684">• Les périodes de validité sont de 1 jour minimum à 36500 jours maximum. <p data-bbox="643 726 1455 936">Même si une période de validité de 36500 jours est autorisée, il est recommandé d'utiliser une période de validité d'au plus 397 jours ou 13 mois. Puisque si vous sélectionnez une période de validité de plus de 397 jours et que vous prévoyez d'exporter une RSC pour ce certificat et de l'obtenir signé par une CA connue, la validité du certificat signé vous sera réduite à 397 jours.</p> <ul style="list-style-type: none"> <li data-bbox="618 957 1446 1209">• Vous pouvez cocher la case « exclure les informations d'identification locales \ (par ex. localhost) » si vous souhaitez supprimer les informations d'identification locales du champ autres noms du certificat. Lorsque cette case est cochée, seul ce que vous saisissez dans le champ est utilisé dans le champ autres noms. Si le champ du certificat obtenu n'est pas renseigné, il n'y aura pas de champ autre nom. </div>

4. Cliquez sur **Oui** pour régénérer le certificat.

5. Redémarrez le serveur Unified Manager afin que le nouveau certificat prenne effet.

Une fois que vous avez terminé

Vérifiez les nouvelles informations de certificat en consultant le certificat HTTPS.

Redémarrage de la machine virtuelle Unified Manager

Vous pouvez redémarrer le serveur virtuel à partir de la console de maintenance d'Unified Manager. Vous devez redémarrer après avoir généré un nouveau certificat de sécurité ou en cas de problème avec la machine virtuelle.

Avant de commencer

L'appliance virtuelle est sous tension.

En tant qu'utilisateur de maintenance, vous êtes connecté à la console de maintenance.

Description de la tâche

Vous pouvez également redémarrer la machine virtuelle depuis vSphere à l'aide de l'option **redémarrer invité**. Pour plus d'informations, consultez la documentation VMware.

Étapes

1. Accéder à la console de maintenance.
2. Sélectionnez **Configuration du système > redémarrer la machine virtuelle**.

Modification du nom d'hôte Unified Manager sur les systèmes Linux

À un moment donné, il peut être nécessaire de modifier le nom d'hôte de l'ordinateur Red Hat Enterprise Linux ou CentOS sur lequel vous avez installé Unified Manager. Par exemple, vous pouvez renommer l'hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de clusters surveillé lorsque vous répertoriez vos machines Linux.

Avant de commencer

Vous devez avoir un accès utilisateur root au système Linux sur lequel Unified Manager est installé.

Description de la tâche

Vous pouvez utiliser le nom d'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur Web Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau pendant le déploiement, vous avez alors désigné un nom pour l'hôte réseau. Si vous avez configuré le réseau à l'aide de DHCP, le nom d'hôte doit être pris du serveur DNS.

Quel que soit le mode d'attribution du nom d'hôte, si vous modifiez le nom d'hôte et que vous envisagez d'utiliser le nouveau nom d'hôte pour accéder à l'interface utilisateur Web d'Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface utilisateur Web à l'aide de l'adresse IP du serveur au lieu du nom d'hôte, vous n'avez pas à générer de nouveau certificat si vous modifiez le nom d'hôte. Toutefois, il est recommandé de mettre à jour le certificat, de sorte que le nom d'hôte du certificat corresponde au nom d'hôte réel. Le nouveau certificat ne prend pas effet tant que la machine Linux n'est pas redémarrée.

Si vous modifiez le nom d'hôte dans Unified Manager, vous devez mettre à jour manuellement le nom d'hôte dans OnCommand Workflow Automation (WFA). Le nom d'hôte n'est pas mis à jour automatiquement dans WFA.

Étapes

1. Connectez-vous en tant qu'utilisateur root au système Unified Manager que vous souhaitez modifier.
2. Pour arrêter le logiciel Unified Manager et le logiciel MySQL associé, saisissez la commande suivante :
`systemctl stop ocieau ocie mysqld`
3. Modifiez le nom d'hôte à l'aide de Linux `hostnamectl` commande : `hostnamectl set-hostname new_FQDN`

```
hostnamectl set-hostname nuhost.corp.widget.com
```

4. Régénérer le certificat HTTPS pour le serveur : `/opt/netapp/essentials/bin/cert.sh create`
5. Redémarrez le service réseau : `service network restart`
6. Une fois le service redémarré, vérifiez si le nouveau nom d'hôte peut s'envoyer par commande ping : `ping new_hostname`

`ping nuhost`

Cette commande doit renvoyer la même adresse IP que celle définie précédemment pour le nom d'hôte d'origine.
7. Une fois que vous avez terminé et vérifié la modification de votre nom d'hôte, redémarrez Unified Manager en entrant la commande suivante : `systemctl start mysqld ocie ocieau`

Activation et désactivation de la gestion du stockage basée sur des règles

Depuis la version 9.7 de Unified Manager, vous pouvez provisionner les charges de travail de stockage (volumes et LUN) sur vos clusters ONTAP, et gérer ces charges de travail en fonction de niveaux de service de performances attribués. Cette fonctionnalité est similaire à la création des charges de travail dans ONTAP System Manager et à l'ajout de règles de QoS. Toutefois, lorsqu'elle est appliquée à l'aide de Unified Manager, vous pouvez provisionner et gérer les charges de travail sur l'ensemble des clusters qui surveillent votre instance Unified Manager.

Avant de commencer

Vous devez avoir le rôle Administrateur d'applications.

Description de la tâche

Activation par défaut de cette option, mais désactivation si vous ne souhaitez pas provisionner et gérer les charges de travail à l'aide d'Unified Manager.

Lorsqu'elle est activée, cette option fournit de nombreux nouveaux éléments dans l'interface utilisateur :

Nouveau contenu	Emplacement
Une page pour provisionner de nouveaux workloads	Disponible à partir de tâches courantes > mise en service
Une page pour créer des règles de niveau de service de performances	Disponible à partir de Paramètres > stratégies > niveaux de service de performance
Une page pour créer des règles d'efficacité du stockage de performance	Disponible à partir de Paramètres > stratégies > efficacité du stockage
Des panneaux décrivent les performances de vos charges de travail et les IOPS de vos charges de travail actuelles	Disponible dans le tableau de bord

Pour plus d'informations sur ces pages et sur cette fonctionnalité, reportez-vous à l'aide en ligne du produit.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général > Paramètres de fonction**.
2. Dans la page **Feature Settings**, désactivez ou activez la gestion du stockage basée sur des règles en choisissant l'une des options suivantes :

Les fonctions que vous recherchez...	Alors, procédez comme ça...
Désactiver la gestion du stockage basée sur des règles	Dans le panneau gestion du stockage basée sur des règles*, déplacez le curseur vers la gauche.
Mettez en œuvre la gestion du stockage basée sur des règles	Dans le panneau gestion du stockage basée sur des règles*, déplacez le curseur vers la droite.

Configuration de la sauvegarde Unified Manager

Vous pouvez configurer la fonctionnalité de sauvegarde sur Unified Manager par le biais d'un ensemble d'étapes de configuration à effectuer sur les systèmes hôtes et sur via la console de maintenance.

Pour plus d'informations sur les étapes de configuration, reportez-vous à la section «gestion des opérations de sauvegarde et de restauration» dans le *Active IQ® Unified Manager Workflow Guide de gestion de l'intégrité du cluster*.

Utilisation de la console de maintenance

La console de maintenance vous permet de configurer les paramètres réseau, de configurer et de gérer le système sur lequel Unified Manager est installé, et d'effectuer d'autres tâches de maintenance qui vous aideront à prévenir et à résoudre d'éventuels problèmes.

Fonctionnalités offertes par la console de maintenance

La console de maintenance Unified Manager vous permet de conserver les paramètres de votre système Unified Manager et d'effectuer les modifications nécessaires afin d'éviter tout problème.

Selon le système d'exploitation sur lequel Unified Manager est installé, la console de maintenance offre les fonctions suivantes :

- Résolvez les problèmes liés à votre appliance virtuelle, notamment si l'interface Web Unified Manager n'est pas disponible
- Mise à niveau vers les dernières versions de Unified Manager
- Générez des modules de support pour envoyer au support technique
- Configurez les paramètres réseau

- Modifier le mot de passe utilisateur de maintenance
- Connectez-vous à un fournisseur de données externe pour envoyer des statistiques de performances
- Modifiez la collecte des données de performances interne
- Restaurez les paramètres de base de données et de configuration de Unified Manager à partir d'une version de sauvegarde précédente.

Rôle de l'utilisateur de maintenance

L'utilisateur de maintenance est créé lors de l'installation de Unified Manager sur un système Red Hat Enterprise Linux ou CentOS. Le nom d'utilisateur de maintenance est l'utilisateur « umadmin ». L'utilisateur de maintenance a le rôle d'administrateur d'applications dans l'interface utilisateur Web, et cet utilisateur peut créer des utilisateurs ultérieurs et leur attribuer des rôles.

L'utilisateur qui se sert de la maintenance, ou utilisateur umin, peut également accéder à la console de maintenance de Unified Manager.

Diagnostic des capacités utilisateur

L'accès au diagnostic a pour but de permettre au support technique de vous aider à résoudre les problèmes et de l'utiliser uniquement sur demande du support technique.

L'utilisateur de diagnostic peut exécuter des commandes au niveau du système d'exploitation sur demande du support technique, à des fins de dépannage.

Accès à la console de maintenance

Si l'interface utilisateur Unified Manager n'est pas en cours de fonctionnement ou si vous devez effectuer des fonctions qui ne sont pas disponibles dans l'interface utilisateur, vous pouvez accéder à la console de maintenance pour gérer votre système Unified Manager.

Avant de commencer

Vous devez avoir installé et configuré Unified Manager.

Description de la tâche

Après 15 minutes d'inactivité, la console de maintenance vous déconnecte.



Lorsqu'il est installé sur VMware, si vous vous êtes déjà connecté en tant qu'utilisateur de maintenance via la console VMware, vous ne pouvez pas vous connecter simultanément à l'aide de Secure Shell.

Étapes

1. La procédure suivante permet d'accéder à la console de maintenance :

Sur ce système d'exploitation...	Suivez ces étapes...
VMware	<ol style="list-style-type: none"> 1. À l'aide de Secure Shell, connectez-vous à l'adresse IP ou au nom de domaine complet de l'appliance virtuelle Unified Manager. 2. Connectez-vous à la console de maintenance à l'aide de votre nom d'utilisateur et de votre mot de passe de maintenance.
Linux	<ol style="list-style-type: none"> 1. À l'aide de Secure Shell, connectez-vous à l'adresse IP ou au nom de domaine complet du système Unified Manager. 2. Connectez-vous au système avec le nom et le mot de passe de l'utilisateur de maintenance (umadmin). 3. Saisissez la commande <code>maintenance_console</code>. Puis appuyez sur entrée.
Répertoires de base	<ol style="list-style-type: none"> 1. Connectez-vous au système Unified Manager avec les identifiants d'administrateur. 2. Lancez PowerShell en tant qu'administrateur Windows. 3. Saisissez la commande <code>maintenance_console</code>. Puis appuyez sur entrée.

Le menu de la console de maintenance Unified Manager s'affiche.

Accès à la console de maintenance à l'aide de la console de machine virtuelle vSphere

Si l'interface utilisateur Unified Manager n'est pas en cours de fonctionnement ou si vous devez effectuer des fonctions qui ne sont pas disponibles dans l'interface utilisateur, vous pouvez accéder à la console de maintenance pour reconfigurer l'appliance virtuelle.

Avant de commencer

- Vous devez être l'utilisateur de maintenance.
- L'appliance virtuelle doit être mise sous tension pour accéder à la console de maintenance.

Étapes

1. Dans vSphere client, recherchez l'appliance virtuelle Unified Manager.
2. Cliquez sur l'onglet **Console**.
3. Cliquez dans la fenêtre de la console pour vous connecter.
4. Connectez-vous à la console de maintenance à l'aide de votre nom d'utilisateur et de votre mot de passe.

Après 15 minutes d'inactivité, la console de maintenance vous déconnecte.

Menus de la console de maintenance

La console de maintenance se compose de différents menus qui vous permettent de maintenir et de gérer des fonctionnalités spéciales et des paramètres de configuration du serveur Unified Manager.

Selon le système d'exploitation sur lequel Unified Manager est installé, la console de maintenance se compose des menus suivants :

- Mise à niveau de Unified Manager (VMware uniquement)
- Configuration réseau (VMware uniquement)
- Configuration du système (VMware uniquement)
- Support/Diagnostics
- Réinitialiser le certificat du serveur
- Fournisseur de données externes
- Configuration de l'intervalle d'interrogation des performances

Menu Configuration réseau

Le menu Configuration réseau vous permet de gérer les paramètres réseau. Vous devez utiliser ce menu lorsque l'interface utilisateur de Unified Manager n'est pas disponible.



Ce menu n'est pas disponible si Unified Manager est installé sur Red Hat Enterprise Linux, CentOS ou sur Microsoft Windows.

Les options de menu suivantes sont disponibles.

- **Paramètres d'adresse IP d'affichage**

Affiche les paramètres réseau actuels de l'appliance virtuelle, y compris l'adresse IP, le réseau, l'adresse de diffusion, le masque de réseau, la passerelle, Et des serveurs DNS.

- **Modifier les paramètres d'adresse IP**

Permet de modifier n'importe quel paramètre réseau de l'appliance virtuelle, y compris l'adresse IP, le masque de réseau, la passerelle ou les serveurs DNS. Si vous passez des paramètres réseau de DHCP à la mise en réseau statique à l'aide de la console de maintenance, vous ne pouvez pas modifier le nom d'hôte. Vous devez sélectionner **valider les modifications** pour que les modifications soient effectuées.

- **Afficher les paramètres de recherche du nom de domaine**

Affiche la liste de recherche de noms de domaine utilisée pour résoudre les noms d'hôte.

- **Modifier les paramètres de recherche de noms de domaine**

Vous permet de modifier les noms de domaine pour lesquels vous voulez rechercher lors de la résolution des noms d'hôte. Vous devez sélectionner **valider les modifications** pour que les modifications soient effectuées.

- **Afficher les routes statiques**

Affiche les routes réseau statiques actuelles.

- **Modifier les routes statiques**

Permet d'ajouter ou de supprimer des routes réseau statiques. Vous devez sélectionner **valider les modifications** pour que les modifications soient effectuées.

- **Ajouter un itinéraire**

Vous permet d'ajouter une route statique.

- **Supprimer l'itinéraire**

Vous permet de supprimer une route statique.

- **Retour**

Vous ramène au **Menu principal**.

- **Quitter**

Quitte la console de maintenance.

- **Désactiver l'interface réseau**

Désactive toutes les interfaces réseau disponibles. Si une seule interface réseau est disponible, vous ne pouvez pas la désactiver. Vous devez sélectionner **valider les modifications** pour que les modifications soient effectuées.

- **Activer l'interface réseau**

Active les interfaces réseau disponibles. Vous devez sélectionner **valider les modifications** pour que les modifications soient effectuées.

- **Valider les modifications**

Applique les modifications apportées aux paramètres réseau de l'appliance virtuelle. Vous devez sélectionner cette option pour mettre en œuvre les modifications effectuées, sinon les modifications ne se produisent pas.

- **Ping a Host**

Commande ping un hôte cible pour confirmer les modifications d'adresse IP ou les configurations DNS.

- **Rétablir les paramètres par défaut**

Réinitialise tous les paramètres par défaut. Vous devez sélectionner **valider les modifications** pour que les modifications soient effectuées.

- **Retour**

Vous ramène au **Menu principal**.

- **Quitter**

Quitte la console de maintenance.

Menu Configuration du système

Le menu Configuration du système vous permet de gérer votre appliance virtuelle en fournissant diverses options, telles que l’affichage de l’état du serveur, le redémarrage et l’arrêt de la machine virtuelle.



Lorsque Unified Manager est installé sur un système Linux ou Microsoft Windows, seule l’option « Restaurer à partir d’une sauvegarde Unified Manager » est disponible à partir de ce menu.

Les options de menu suivantes sont disponibles :

- **Affichage de l’état du serveur**

Affiche l’état actuel du serveur. Les options d’état incluent en cours d’exécution ou non en cours d’exécution.

Si le serveur n’est pas en cours d’exécution, vous devrez peut-être contacter le support technique.

- **Redémarrer la machine virtuelle**

Redémarre la machine virtuelle et arrête tous les services. Après le redémarrage, la machine virtuelle et les services redémarrent.

- **Arrêter la machine virtuelle**

Arrête la machine virtuelle et arrête tous les services.

Vous ne pouvez sélectionner cette option qu’à partir de la console de la machine virtuelle.

- **Modifier <utilisateur connecté> Mot de passe utilisateur**

Modifie le mot de passe de l’utilisateur actuellement connecté, qui ne peut être que l’utilisateur de maintenance.

- **Augmenter la taille du disque de données**

Augmente la taille du disque de données (disque 3) de la machine virtuelle.

- **Augmenter la taille du disque d’échange**

Augmente la taille du disque d’échange (disque 2) de la machine virtuelle.

- **Changer fuseau horaire**

Change le fuseau horaire en fonction de votre emplacement.

- **Changer serveur NTP**

Modifie les paramètres du serveur NTP, tels que l’adresse IP ou le nom de domaine complet (FQDN).

- **Restaurer à partir d’une sauvegarde Unified Manager**

Restaure les paramètres de base de données et de configuration Unified Manager à partir d’une version précédemment sauvegardée.

- **Réinitialiser le certificat du serveur**

Réinitialise le certificat de sécurité du serveur.

- **Changer le nom d'hôte**

Modifie le nom de l'hôte sur lequel l'appliance virtuelle est installée.

- **Retour**

Quitte le menu Configuration du système et revient au menu principal.

- **Quitter**

Quitte le menu de la console de maintenance.

Menu support and Diagnostics

Le menu support and Diagnostics vous permet de générer un bundle de support que vous pouvez envoyer au support technique pour obtenir de l'aide au dépannage.

Les options de menu suivantes sont disponibles :

- **Générer ensemble support léger**

Permet de produire un pack de support léger contenant seulement 30 jours d'enregistrements de base de données de configuration et de journaux — cela exclut les données de performances, les fichiers d'enregistrement d'acquisition et le vidage de mémoire du serveur.

- **Générer un pack de support**

Permet de créer un ensemble de support complet (fichier 7-Zip) contenant des informations de diagnostic dans le répertoire de base de l'utilisateur de diagnostic. Si votre système est connecté à Internet, vous pouvez également télécharger le pack de support à NetApp.

Le fichier contient des informations générées par un message AutoSupport, le contenu de la base de données Unified Manager, des données détaillées sur les composants internes du serveur Unified Manager et des journaux de niveau détaillé qui ne sont pas normalement inclus dans les messages AutoSupport ou dans le bundle de support léger.

Options de menu supplémentaires

Les options de menu suivantes vous permettent d'effectuer diverses tâches administratives sur le serveur Unified Manager.

Les options de menu suivantes sont disponibles :

- **Réinitialiser le certificat du serveur**

Régénère le certificat du serveur HTTPS.

Vous pouvez régénérer le certificat de serveur dans l'interface utilisateur graphique Unified Manager en cliquant sur **général > certificats HTTPS > régénérer le certificat HTTPS**.

- **Désactiver l'authentification SAML**

Désactive l'authentification SAML de sorte que le fournisseur d'identités ne fournit plus d'authentification

d'identification pour les utilisateurs qui accèdent à l'interface graphique Unified Manager. Cette option console est généralement utilisée lorsqu'un problème de serveur IDP ou de configuration SAML empêche les utilisateurs d'accéder à l'interface graphique Unified Manager.

- **Fournisseur de données externes**

Fournit des options pour connecter Unified Manager à un fournisseur de données externe. Une fois la connexion établie, les données relatives aux performances sont envoyées à un serveur externe afin que les experts en performance du stockage puissent créer un diagramme des indicateurs de performances à l'aide d'un logiciel tiers. Les options suivantes sont affichées :

- **Configuration du serveur d'affichage**--affiche les paramètres de connexion et de configuration actuels pour un fournisseur de données externe.
- **Ajouter/Modifier la connexion au serveur**--permet de saisir de nouveaux paramètres de connexion pour un fournisseur de données externe ou de modifier les paramètres existants.
- **Modifier la configuration du serveur**--permet de saisir de nouveaux paramètres de configuration pour un fournisseur de données externe ou de modifier les paramètres existants.
- **Supprimer la connexion au serveur**--supprime la connexion à un fournisseur de données externe.

Une fois la connexion supprimée, Unified Manager perd sa connexion au serveur externe.

- **Configuration de l'intervalle d'interrogation des performances**

Fournit une option permettant de configurer la fréquence à laquelle Unified Manager collecte des données statistiques de performances à partir de clusters. L'intervalle de collecte par défaut est de 5 minutes.

Vous pouvez modifier cet intervalle à 10 ou 15 minutes si vous constatez que les collections des grands groupes ne sont pas réalisées à temps.

- **Afficher/Modifier les ports d'application**

La fonctionnalité offre une option permettant de modifier les ports par défaut qu'Unified Manager utilise pour les protocoles HTTP et HTTPS, si nécessaire pour la sécurité. Les ports par défaut sont 80 pour HTTP et 443 pour HTTPS.

- **Quitter**

Quitte le menu de la console de maintenance.

Modification du mot de passe utilisateur de maintenance sous Windows

Vous pouvez modifier le mot de passe utilisateur responsable de la maintenance d'Unified Manager si nécessaire.

Étapes

1. Dans la page de connexion à l'interface utilisateur Web de Unified Manager, cliquez sur **Mot de passe oublié**.

Une page s'affiche et vous demande le nom de l'utilisateur dont vous souhaitez réinitialiser le mot de passe.

2. Entrez le nom d'utilisateur et cliquez sur **Envoyer**.

Un e-mail contenant un lien pour réinitialiser le mot de passe est envoyé à l'adresse e-mail définie pour ce nom d'utilisateur.

3. Cliquez sur le lien **reset mot de passe** dans l'e-mail et définissez le nouveau mot de passe.
4. Revenez à l'interface utilisateur Web et connectez-vous à Unified Manager à l'aide du nouveau mot de passe.

Modification du mot de passe umadmin sur les systèmes Linux

Pour des raisons de sécurité, vous devez modifier le mot de passe par défaut de l'utilisateur Unified Manager umadmin immédiatement après avoir terminé l'installation. Si nécessaire, vous pouvez modifier le mot de passe à nouveau ultérieurement.

Avant de commencer

- Unified Manager doit être installé sur un système Red Hat Enterprise Linux ou CentOS Linux.
- Vous devez disposer des informations d'identification utilisateur root pour le système Linux sur lequel Unified Manager est installé.

Étapes

1. Connectez-vous en tant qu'utilisateur root au système Linux sur lequel Unified Manager s'exécute.
2. Modifier le mot de passe umadmin : `passwd umadmin`

Le système vous invite à entrer un nouveau mot de passe pour l'utilisateur umadmin.

Changement des ports que Unified Manager utilise pour les protocoles HTTP et HTTPS

Le cas échéant, les ports par défaut utilisés par Unified Manager pour les protocoles HTTP et HTTPS peuvent être modifiés après l'installation. Les ports par défaut sont 80 pour HTTP et 443 pour HTTPS.

Avant de commencer

Vous devez disposer d'un ID utilisateur et d'un mot de passe autorisés pour vous connecter à la console de maintenance du serveur Unified Manager.



Certains ports sont considérés comme dangereux lors de l'utilisation des navigateurs Mozilla Firefox ou Google Chrome. Vérifiez auprès de votre navigateur avant d'attribuer un nouveau numéro de port pour le trafic HTTP et HTTPS. La sélection d'un port non sécurisé peut rendre le système inaccessible, ce qui vous oblige à contacter le support client pour obtenir une résolution.

Description de la tâche

L'instance de Unified Manager est redémarrée automatiquement après avoir modifié le port. Assurez-vous donc que le système est bien arrêté pendant un court laps de temps.

Étapes

1. Connectez-vous en utilisant SSH en tant qu'utilisateur de maintenance sur l'hôte Unified Manager.

Les invites de la console de maintenance Unified Manager s'affichent.

2. Tapez le numéro de l'option de menu **Afficher/Modifier les ports d'application**, puis appuyez sur entrée.
3. Si vous y êtes invité, saisissez à nouveau le mot de passe utilisateur pour la maintenance.
4. Saisissez les nouveaux numéros de port pour les ports HTTP et HTTPS, puis appuyez sur entrée.

Si vous laissez un numéro de port vide, le port par défaut du protocole est affecté.

Vous êtes invité à modifier les ports et à redémarrer Unified Manager maintenant.

5. Tapez **y** pour modifier les ports et redémarrer Unified Manager.
6. Sortir de la console de maintenance.

Résultats

Après cette modification, les utilisateurs doivent inclure le nouveau numéro de port dans l'URL pour accéder à l'interface utilisateur Web d'Unified Manager, par exemple `https://host.company.com:1234`, `https://12.13.14.15:1122` ou `https://[2001:db8:0:1]:2123`.

Ajout d'interfaces réseau

Vous pouvez ajouter de nouvelles interfaces réseau si vous devez séparer le trafic réseau.

Avant de commencer

Vous devez avoir ajouté l'interface réseau à l'appliance virtuelle à l'aide de vSphere.

L'appliance virtuelle doit être sous tension.

Description de la tâche



Vous ne pouvez pas effectuer cette opération si Unified Manager est installé sur Red Hat Enterprise Linux ou sur Microsoft Windows.

Étapes

1. Dans la console vSphere **Menu principal**, sélectionnez **Configuration du système > redémarrer le système d'exploitation**.

Après le redémarrage, la console de maintenance peut détecter l'interface réseau qui vient d'être ajoutée.

1. Accéder à la console de maintenance.
2. Sélectionnez **Configuration réseau > Activer l'interface réseau**.
3. Sélectionnez la nouvelle interface réseau et appuyez sur **entrée**.

Sélectionnez **eth1** et appuyez sur **entrée**.

1. Tapez **y** pour activer l'interface réseau.
2. Entrez les paramètres réseau.

Si vous utilisez une interface statique ou si DHCP n'est pas détecté, vous êtes invité à entrer les paramètres réseau.

Après avoir saisi les paramètres réseau, vous revenez automatiquement au menu **Configuration réseau**.

1. Sélectionnez **valider les modifications**.

Vous devez valider les modifications pour ajouter l'interface réseau.

Ajout d'espace disque au répertoire de base de données Unified Manager

Le répertoire de base de données Unified Manager contient toutes les données d'intégrité et de performances collectées à partir des systèmes ONTAP. Dans certaines circonstances, vous devrez peut-être augmenter la taille du répertoire de base de données.

Par exemple, le répertoire de la base de données peut devenir complet si Unified Manager collecte les données à partir d'un grand nombre de clusters où chaque cluster possède plusieurs nœuds. Vous recevrez un événement d'avertissement lorsque le répertoire de base de données est plein à 90 % et un événement critique lorsque le répertoire est plein à 95 %.



Aucune donnée supplémentaire n'est collectée depuis les clusters après le répertoire dans son intégralité, à 95 %.

Les étapes requises pour ajouter de la capacité au répertoire de données sont différentes selon que Unified Manager s'exécute ou non sur un serveur VMware ESXi, sur un serveur Red Hat ou CentOS Linux, ou sur un serveur Microsoft Windows.

Ajout d'espace au répertoire de données de l'hôte Linux

Si vous avez alloué un espace disque insuffisant à l' `/opt/netapp/data` Répertoire pour prendre en charge Unified Manager lorsque vous configurez l'hôte Linux à l'origine, puis que Unified Manager a été installé, vous pouvez ajouter de l'espace disque après l'installation en augmentant l'espace disque sur le `/opt/netapp/data` répertoire.

Avant de commencer

Vous devez avoir un accès utilisateur root à la machine Red Hat Enterprise Linux ou CentOS Linux sur laquelle Unified Manager est installé.

Description de la tâche

Nous vous recommandons de sauvegarder la base de données Unified Manager avant d'augmenter la taille du répertoire de données.

Étapes

1. Connectez-vous en tant qu'utilisateur root à la machine Linux sur laquelle vous souhaitez ajouter de l'espace disque.

2. Arrêtez le service Unified Manager et le logiciel MySQL associé dans l'ordre indiqué : `systemctl stop ocieau ocie mysqld`
3. Créer un dossier de sauvegarde temporaire (par exemple, `/backup-data`) avec suffisamment d'espace disque pour contenir les données dans le courant `/opt/netapp/data` répertoire.
4. Copie de la configuration de contenu et de privilège de l'existant `/opt/netapp/data` répertoire vers le répertoire de données de sauvegarde : `cp -arp /opt/netapp/data/* /backup-data`
5. Si se Linux est activé :

- a. Obtenir le type se Linux pour les dossiers existants `/opt/netapp/data` dossier :

```
se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
head -1
```

Le système renvoie une confirmation similaire à ce qui suit :

```
echo $se_type
mysqld_db_t
```

- a. Exécutez le `chcon` Commande pour définir le type se Linux du répertoire de sauvegarde : `chcon -R --type=mysqld_db_t /backup-data`

6. Retirez le contenu du `/opt/netapp/data` répertoire :

- a. `cd /opt/netapp/data`
- b. `rm -rf *`

7. Développez la taille du `/opt/netapp/data` Répertoire d'au moins 150 Go via les commandes LVM ou en ajoutant des disques supplémentaires.



Si vous avez créé `/opt/netapp/data` à partir d'un disque, n'essayez pas de monter `/opt/netapp/data` En tant que partage NFS ou CIFS. Car, dans ce cas, si vous essayez d'étendre l'espace disque, certaines commandes LVM, telles que `resize` et `extend` ne fonctionnent peut-être pas comme prévu.

1. Confirmez que le `/opt/netapp/data` le propriétaire du répertoire (mysql) et le groupe (root) sont inchangés: `ls -ltr /opt/netapp/ | grep data`

Le système renvoie une confirmation similaire à ce qui suit :

```
drwxr-xr-x. 17 mysql root 4096 Aug 28 13:08 data
```

1. Si se Linux est activé, confirmez que le contexte de l' `/opt/netapp/data` le répertoire est toujours défini sur `mysqld_db_t`:
 - a. `touch /opt/netapp/data/abc`
 - b. `ls -Z /opt/netapp/data/abc`

Le système renvoie une confirmation similaire à ce qui suit :

```
-rw-r--r--. root root unconfined_u:object_r:mysql_db_t:s0
/opt/netapp/data/abc
```

1. Supprimez le fichier `abc` ainsi, ce fichier externe ne provoque pas d'erreur de base de données à l'avenir.
2. Copiez le contenu à partir de `backup-data` retour à la développée `/opt/netapp/data` répertoire : `cp -arp /backup-data/* /opt/netapp/data/`
3. Si se Linux est activé, exécutez la commande suivante : `chcon -R --type=mysql_db_t /opt/netapp/data`
4. Démarrez le service MySQL : `systemctl start mysqld`
5. Une fois le service MySQL démarré, démarrer les services `ocie` et `ocieau` dans l'ordre indiqué: `systemctl start ocie ocieau`
6. Une fois tous les services démarrés, supprimez le dossier de sauvegarde `/backup-data`: `rm -rf /backup-data`

Ajout d'espace au disque de données de la machine virtuelle VMware

Si vous devez augmenter la quantité d'espace sur le disque de données de la base de données Unified Manager, vous pouvez ajouter de la capacité après l'installation en augmentant l'espace disque à l'aide de la console de maintenance Unified Manager.

Avant de commencer

- Vous devez avoir accès au client vSphere.
- Aucun snapshot ne doit être stocké localement sur la machine virtuelle.
- Vous devez disposer des informations d'identification de l'utilisateur de maintenance.

Description de la tâche

Nous vous recommandons de sauvegarder votre machine virtuelle avant d'augmenter la taille des disques virtuels.

Étapes

1. Dans le client vSphere, sélectionnez la machine virtuelle Unified Manager, puis ajoutez de la capacité de disque aux données `disk 3`. Pour plus de détails, consultez la documentation VMware.

Dans de rares cas, le déploiement de Unified Manager utilise « disque dur 2 » pour le disque de données au lieu de « disque dur 3 ». Si cela s'est produit au cours de votre déploiement, vous augmentez l'espace disque le plus important. Le disque de données aura toujours plus d'espace que l'autre disque.

2. Dans le client vSphere, sélectionnez la machine virtuelle Unified Manager, puis sélectionnez l'onglet **Console**.
3. Cliquez sur dans la fenêtre de la console, puis connectez-vous à la console de maintenance à l'aide de votre nom d'utilisateur et de votre mot de passe.
4. Dans le **Menu principal**, entrez le numéro de l'option **Configuration système**.
5. Dans le **Menu de configuration du système**, entrez le numéro de l'option **augmenter la taille du disque**

de données.

Ajout d'espace au lecteur logique du serveur Microsoft Windows

Si vous devez augmenter la quantité d'espace disque pour la base de données Unified Manager, vous pouvez ajouter de la capacité au lecteur logique sur lequel Unified Manager est installé.

Avant de commencer

Vous devez disposer des privilèges d'administrateur Windows.

Description de la tâche

Nous vous recommandons de sauvegarder la base de données Unified Manager avant d'ajouter de l'espace disque.

Étapes

1. Connectez-vous en tant qu'administrateur au serveur Windows sur lequel vous souhaitez ajouter de l'espace disque.
2. Suivez l'étape qui correspond à la méthode que vous souhaitez utiliser pour ajouter de l'espace :

Option	Description
Sur un serveur physique, ajoutez de la capacité au lecteur logique sur lequel le serveur Unified Manager est installé.	Suivez les étapes de la rubrique Microsoft : "Extension d'un volume de base"
Sur un serveur physique, ajoutez un disque dur.	Suivez les étapes de la rubrique Microsoft : "Ajout de disques durs"
Sur une machine virtuelle, augmentez la taille d'une partition de disque.	Suivez les étapes du sujet VMware : "Augmentation de la taille d'une partition de disque"

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.