Réaliser les tâches de configuration et d'administration

OnCommand Unified Manager 9.5

NetApp
August 02, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/oncommand-unified-manager-95/config/concept-overview-of-the-configuration-sequence.html on August 02, 2024. Always check docs.netapp.com for the latest.

Sommaire

Réaliser les tâches de configuration et d’administration 1
Configuration d’Unified Manager 1

Réaliser les tâches de configuration et d'administration

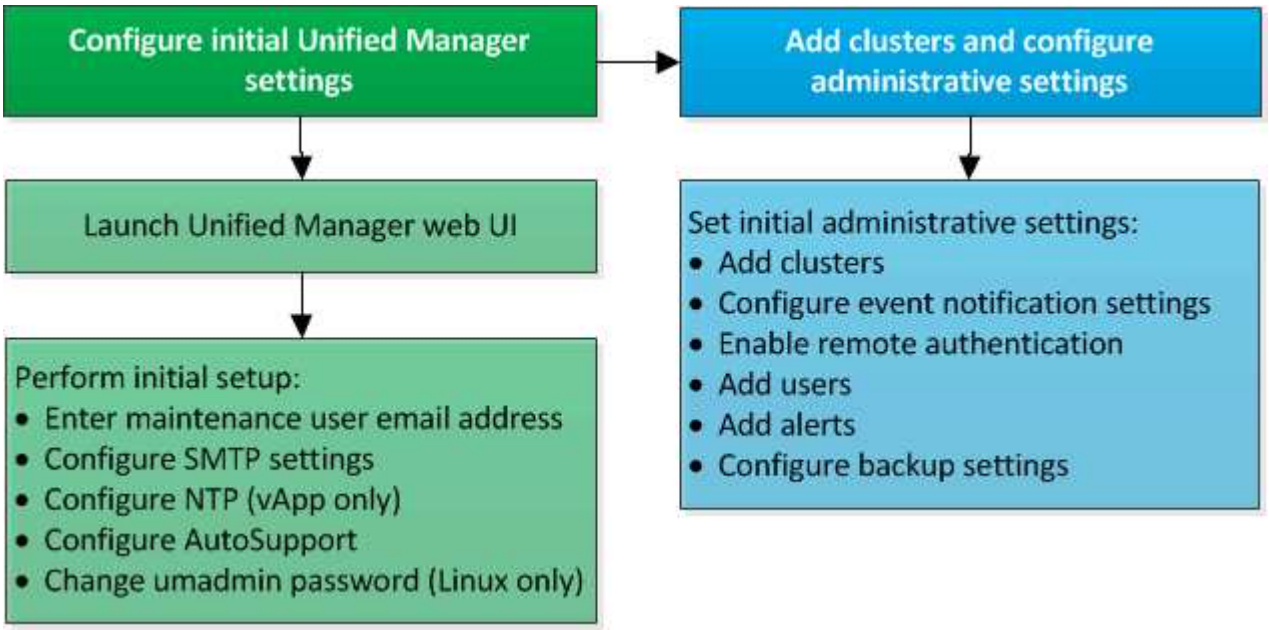
Configuration d'Unified Manager

Une fois Unified Manager installé, 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`.

2. 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 le nom d'hôte et les options du serveur SMTP.

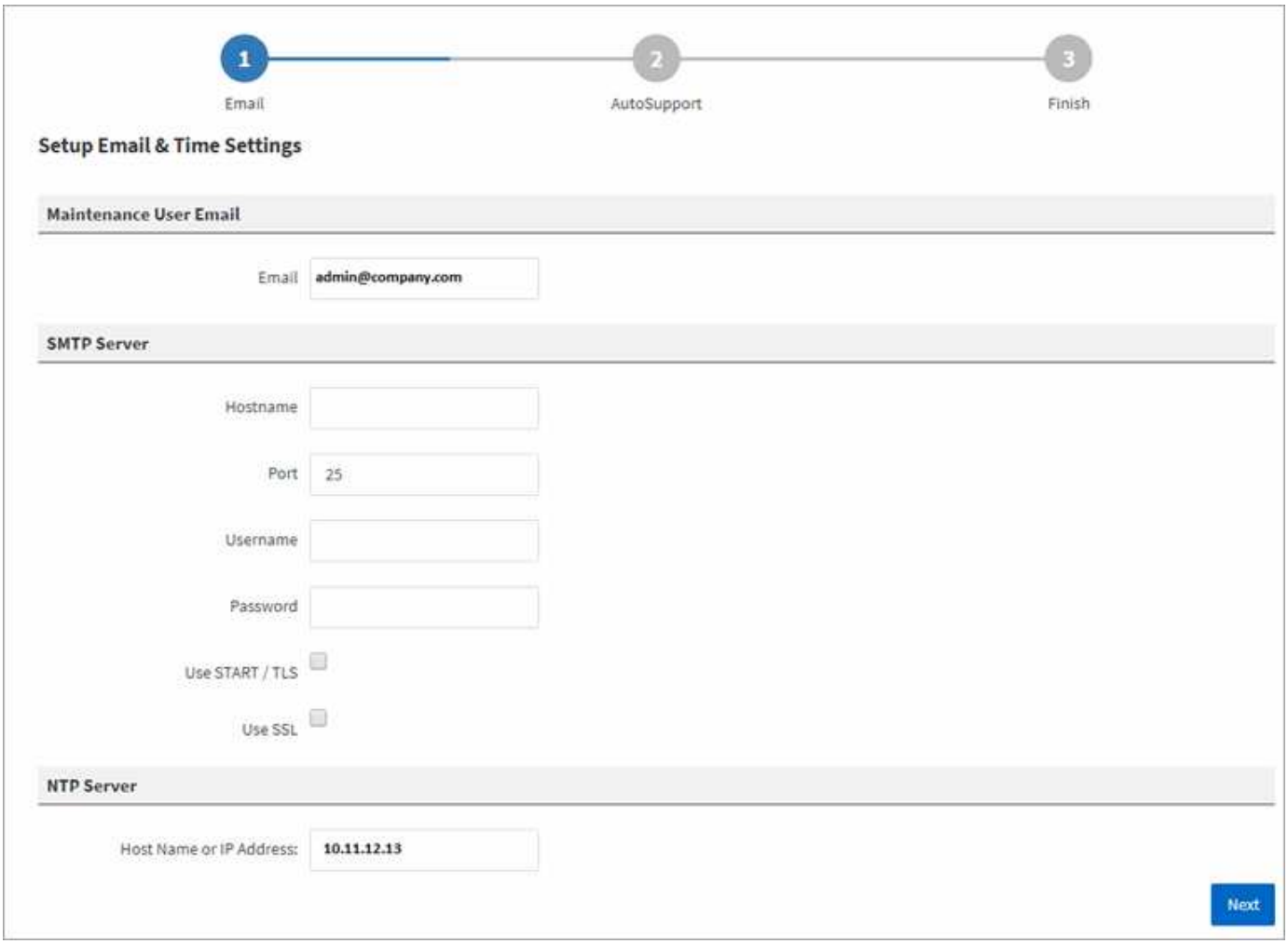
Avant de commencer

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 Configuration initiale de OnCommand Unified Manager n'apparaît que lorsque vous accédez pour la première fois à l'interface utilisateur Web. La page ci-dessous provient d'une installation sur VMware.



Si vous souhaitez modifier l'une de ces options ultérieurement, vous pouvez utiliser les options Administration, qui sont accessibles en cliquant sur Dans la barre d'outils Unified Manager.

Étapes

1. Dans la fenêtre **OnCommand Unified Manager initial Setup**, 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 **Suivant**.
2. Dans la page **AutoSupport**, cliquez sur **accepter et Continuer** pour activer AutoSupport.

   Si vous devez désigner un proxy pour fournir un accès Internet afin d'envoyer du contenu AutoSupport à l'assistance, ou si vous souhaitez désactiver AutoSupport, utilisez les options d'administration.

3. Sur les systèmes Red Hat et CentOS, vous pouvez choisir de modifier le mot de passe utilisateur umadmin de la chaîne par défaut « admin » à une chaîne personnalisée.

Résultats

La fenêtre Configuration initiale se ferme et l'interface utilisateur Web de Unified Manager s'affiche. La page sources de données de configuration/cluster s'affiche pour vous permettre d'ajouter des clusters à votre système.

Ajout de clusters

Vous pouvez ajouter un cluster à OnCommand 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 d'administrateur OnCommand ou d'administrateur du 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.
  - Nom d'utilisateur et mot de passe de l'administrateur Data ONTAP

    Ce compte doit avoir le rôle *admin* avec accès application défini sur *ontapi*, *ssh* et *http*.
  - Type de protocole (HTTP ou HTTPS) pouvant être configuré sur le cluster et numéro de port utilisé pour la connexion au cluster

    > 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.
- Le FQDN de Unified Manager doit pouvoir exécuter une commande ping au système ONTAP.

  Pour le vérifier, utilisez la commande ONTAP suivante : `ping -node node_name -destination Unified_Manager_FQDN`.
- 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 **Configuration** > **sources de données de cluster**.
2. Sur la page **sources de données de configuration/cluster**, cliquez sur **Ajouter**.

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, le protocole de communication et le numéro de port.

   Par défaut, le protocole HTTPS et le port 443 sont sélectionnés.

   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. Si HTTPS est sélectionné, effectuez les opérations suivantes :

   a. Dans la boîte de dialogue **Authorise Host** , cliquez sur **View Certificate** pour afficher les informations de certificat relatives au cluster.
   b. 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.

   Si le certificat a expiré, vous ne pouvez pas ajouter un nouveau cluster. Vous devez d'abord renouveler le certificat SSL, puis ajouter le cluster.

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 ne permettant pas d'ajouter le cluster, vérifiez si les problèmes suivants existent :

- Si les horloges sur les deux systèmes ne sont pas synchronisées et que la date de début du certificat HTTPS de Unified Manager est postérieure à la date sur le cluster. Vous devez vous assurer que les horloges sont synchronisées à l'aide du protocole NTP ou d'un service similaire.
- Si le cluster a atteint le nombre maximal de destinations de notification EMS, l'adresse Unified Manager ne peut pas être ajoutée. Par défaut, seules 20 destinations de notification EMS peuvent être définies sur le cluster.

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 d'administrateur OnCommand.

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
- Version SNMP, adresse IP de l'hôte de destination d'interruption, port d'interruption sortant et communauté pour configurer l'interruption SNMP

Vous devez avoir le rôle d'administrateur OnCommand ou d'administrateur du stockage.

Étapes

1. Dans la barre d'outils, cliquez sur ⚙, puis cliquez sur **Notifications** dans le menu Configuration de gauche.
2. Dans la page **Configuration/Notifications**, configurez les paramètres appropriés et cliquez sur **Enregistrer**.

   Notes:

   - Si l'adresse de expéditeur est pré-remplie avec l'adresse « OnCommand@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 d'administrateur OnCommand.

> 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 la barre d'outils, cliquez sur , puis cliquez sur **authentification** dans le menu Configuration de gauche.
2. Dans la page **Configuration/authentification**, sélectionnez **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	• Nom d'administrateur du serveur d'authentification dans l'un des formats suivants : ◦ `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	• 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).

4. Ajoutez des serveurs d'authentification et testez l'authentification.
5. Cliquez sur **Enregistrer et fermer**.

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 d'administrateur OnCommand.
- 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 la barre d'outils, cliquez sur , puis cliquez sur **authentification** dans le menu Configuration de gauche.
2. Dans la page **Configuration/authentification**, 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 d'administrateur OnCommand.

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 la barre d'outils, cliquez sur , puis cliquez sur **authentification** dans le menu Configuration de gauche.
2. Dans la page **Configuration/authentification**, cliquez sur **Management Server** > **authentification**.
3. Activez ou désactivez l'option **utiliser l'authentification de connexion sécurisée** :

Les fonctions que vous recherchez…	Alors, procédez comme ça…
Activez-la	a. Dans la case Activer l'authentification à distance, sélectionnez l'option **utiliser la connexion sécurisée**. b. Dans la zone serveurs d'authentification, cliquez sur **Ajouter**. c. Dans la boîte de dialogue Ajouter un serveur d'authentification, entrez le nom d'authentification ou l'adresse IP (IPv4 ou IPv6) du serveur. d. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur Afficher le certificat. e. Dans la boîte de dialogue Afficher le certificat, vérifiez les informations sur le certificat, puis cliquez sur **Fermer**. f. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur **Oui**. ⓘ 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.
Désactivez-le	a. Dans la case Activer l'authentification à distance, désactivez l'option **utiliser la connexion sécurisée**. b. Dans la zone serveurs d'authentification, cliquez sur **Ajouter**. c. 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. d. Cliquez sur **Ajouter**.

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

4. 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 d'administrateur OnCommand.

Description de la tâche

Si le service d'authentification est défini sur Active Directory et que vous valiez 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 la barre d'outils, cliquez sur , puis cliquez sur **authentification** dans le menu Configuration de gauche.
2. Dans la page **Configuration/authentification**, cliquez sur **Test 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 gestion/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 d'administrateur OnCommand.
- 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 la barre d'outils, cliquez sur , puis cliquez sur **utilisateurs** dans le menu de gestion de gauche.
2. Sur la page **Management/Users**, cliquez sur **Add**.
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 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 gestion/scripts.
- Vous devez avoir le rôle d'administrateur OnCommand ou d'administrateur du 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/alerte, comme décrit ici.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Configuration** > **Alerting**.
2. Dans la page **Configuration/Alerting**, 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 **Evénements**, 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 gestion/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, puis déplacez-le dans la zone Ressources sélectionnées.
   c. Cliquez sur **exclure**, puis saisissez `xyz` Dans le champ **Name contient**, puis cliquez sur **Add**.
3. Cliquez sur **Evénements**, 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 (Sélectionner un script à exécuter), sélectionnez **Test** script .
8. Cliquez sur **Enregistrer**.

Événements EMS ajoutés automatiquement à Unified Manager

Lors de l'utilisation du logiciel Unified Manager 9.4 ou version supérieure, 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 la ONTAP
Accès au magasin d'objets refusé pour le transfert d'agrégats	arl.netra.ca.check.failed	Agrégat	Erreur
Accès au magasin d'objets refusé pour le transfert d'agrégats durant le basculement du stockage	gb.netra.ca.check.failed	Agrégat	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

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité de la ONTAP
MetaDataConnFail dans le cloud AWS	Cloud.aws.metadataConnFail	Nœud	Erreur
Cloud AWS IAMCredentistesExrequis	Cloud.aws.iamCredentistesExpired	Nœud	Erreur
Identifiants iAMCredentiststpour Cloud AWS non valides	Cloud.aws.iamCredsinvalide	Nœud	Erreur
Des informations iAMCredentistsNotFound pour Cloud AWS	Cloud.aws.iamCredentisNotFound	Nœud	Erreur
Cloud AWS IAMCredentistsNotInitialized	Cloud.aws.iamNotInitialized	Nœud	Informations
IAMRleInvalid Cloud AWS	Cloud.aws.iamRoleinvalide	Nœud	Erreur
L'IAMRleNotFound Cloud AWS	Cloud.aws.iamRoleNotFound	Nœud	Erreur
Objstore Host ne peut pas être résolu	objstore.host.non résolu	Nœud	Erreur
Objstore InterClusterLifDown	objstore.interclusterlifDown	Nœud	Erreur
Demande de signature de magasin d'objets différente	osc.signatureMismatch	Nœud	Erreur
Un des pools NFSv4 épuisés	NBlade.nfsV4PoolExhaust	Nœud	Primordial
QoS Monitor mémoire portée en mémoire	qos.monitor.memory.capacité maximale	Nœud	Erreur
Mémoire du moniteur QoS saturée	qos.monitor.memory.abated	Nœud	Informations
Détruire NVMeNS	NVMeNS.destroy	Espace de noms	Informations

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité de la ONTAP
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
De nombreuses connexions CIFS	Nibd.cifsManyAuths	SVM	Erreur
Connexion CIFS maximale dépassée	NBlade.cifsMaxOpenSametiFile	SVM	Erreur
Le nombre maximal de connexions CIFS par utilisateur a été dépassé	NBlade.cifsMaxSessPerUsrConn	SVM	Erreur
Conflit de nom CIFS NetBIOS	NBlade.cifsNbNameConflitt	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.vscanVirusDetected	SVM	Erreur
Aucune connexion au serveur AV pour virus Scan	NBlade.vscanNoScannerConn	SVM	Primordial

Nom de l'événement Unified Manager	Nom de l'événement EMS	Ressource affectée	Gravité de la ONTAP
Aucun serveur AV enregistré	NBlade.vscanNoRegdScanner	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.vscanConnBackPressure	SVM	Erreur
Un utilisateur non autorisé tente d'utiliser le serveur AV	NBlade.vscanBadUserPrivAccess	SVM	Erreur
Les composants FlexGroup présentent des problèmes d'espace	flexgroup.constituants.have.space.issues	Volumétrie	Erreur
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	Moniteur.vol.approche complète	Volumétrie	Avertissement
Espace logique du volume plein	moniteur.vol.plein	Volumétrie	Erreur
Volume Logical Space Normal	monitor.vol.one.ok	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

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 **Configuration** > **gérer les événements**.
2. Dans la page **Configuration/gestion des événements**, cliquez sur le bouton **s'abonner aux événements EMS**.
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 les abonnements aux événements ONTAP EMS dans OnCommand Unified Manager / 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 lors de l'utilisation d'Internet Explorer. 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 :

    http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/

  - 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.
- Lorsque les utilisateurs tentent d'accéder à Unified Manager à l'aide d'Internet Explorer, ils peuvent voir le message **le site Web ne peut pas afficher la page**. Si cela se produit, assurez-vous que ces utilisateurs décochez l'option "Enregistrer les messages d'erreur HTTP conviviaux" dans **Outils** > **Options Internet** > **Avancé**.

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 OnCommand.
- 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 la barre d'outils, cliquez sur , puis cliquez sur **authentification** dans le menu Configuration de gauche.
2. Dans la page **Configuration/authentification**, sélectionnez l'onglet **authentification SAML**.
3. Cochez la case **Activer l'authentification SAML**.

   Les champs requis pour configurer la connexion IDP sont affichés.

4. 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.

5. 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.

6. Cliquez sur **Enregistrer**.

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

7. 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. Lorsque Unified Manager est déployé sur Windows, Red Hat ou CentOS, vous pouvez modifier le délai d'expiration de la session de l'interface utilisateur graphique à l'aide de la commande Unified Manager CLI suivante : `um option set absolute.session.timeout=00:15:00`Cette commande définit le délai d'expiration de la session de l'interface graphique Unified Manager à 15 minutes.

Configuration des paramètres de sauvegarde de la base de données

Vous pouvez configurer les paramètres de sauvegarde de la base de données Unified Manager pour définir le chemin de sauvegarde de la base de données, le nombre de rétention et les planifications de sauvegarde. Vous pouvez activer des sauvegardes planifiées quotidiennement ou hebdomadaires. Par défaut, les sauvegardes planifiées sont désactivées.

Avant de commencer

- Vous devez avoir le rôle opérateur, administrateur OnCommand ou administrateur stockage.
- Vous devez disposer d'au moins 150 Go d'espace disponible dans l'emplacement que vous définissez comme chemin de sauvegarde.

  Il est recommandé d'utiliser un emplacement distant externe au système hôte Unified Manager.

- Lorsque Unified Manager est installé sur un système Linux, vérifiez que l'utilisateur « jboss » dispose des autorisations d'écriture sur le répertoire de sauvegarde.
- Vous ne devez pas planifier d'opérations de sauvegarde immédiatement après l'ajout d'un nouveau cluster alors que Unified Manager collecte 15 jours de données historiques de performance.

Description de la tâche

La première sauvegarde est effectuée moins de temps que les sauvegardes suivantes, car la première sauvegarde est une sauvegarde complète. Une sauvegarde complète peut dépasser 1 Go et peut prendre entre trois et quatre heures. Les sauvegardes suivantes sont incrémentielles et requièrent moins de temps.

Étapes

1. Dans la barre d'outils, cliquez sur , puis cliquez sur **Management** > **Database Backup**.
2. Dans la page **Management/Database Backup**, cliquez sur **actions** > **Database Backup Settings**.
3. Configurez les valeurs appropriées pour un chemin de sauvegarde et le nombre de rétention.

   La valeur par défaut pour le nombre de rétention est 10 ; vous pouvez utiliser 0 pour créer des sauvegardes illimitées.

4. Dans la section **fréquence de programmation**, cochez la case **Activer**, puis spécifiez un horaire quotidien ou hebdomadaire.

- **Tous les jours**

  Si vous sélectionnez cette option, vous devez entrer une heure au format 24 heures pour la création de la sauvegarde. Par exemple, si vous spécifiez 18:30, une sauvegarde est créée quotidiennement à 6:30 PM.

- **Hebdomadaire**

  Si vous sélectionnez cette option, vous devez spécifier l'heure et le jour de la création de la sauvegarde. Par exemple, si vous indiquez le jour comme lundi et l'heure comme 16:30, une sauvegarde hebdomadaire est créée chaque lundi à 4:30 PM.

5. Cliquez sur **Enregistrer et fermer**.

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.

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 vous devez affecter le rôle d'administrateur OnCommand 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 « OnCommand » 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

Vous pouvez générer un nouveau certificat de sécurité HTTPS pour plusieurs raisons, notamment si vous souhaitez vous connecter à une autre autorité de certification ou si le certificat de sécurité actuel a expiré. Le nouveau certificat remplace le certificat existant.

Avant de commencer

Vous devez avoir le rôle d'administrateur OnCommand.

Description de la tâche

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.

Étapes

1. Dans la barre d'outils, cliquez sur , puis cliquez sur **certificat HTTPS** dans le menu **Setup**.
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	`Click the *Update the Current Certificate Attributes* option. Les champs Nom commun et noms alternatifs utiliseront les valeurs du certificat existant si vous ne saisissez pas de nouvelles valeurs. Les autres champs ne nécessitent pas de valeurs, mais vous pouvez entrer des valeurs, par exemple, pour la ville, l'état et le pays si vous souhaitez que ces valeurs soient renseignées dans le certificat.` Vous pouvez cocher la case « exclure les informations d'identification locales (par exemple 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. +

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. Arrêtez le logiciel Unified Manager et le logiciel MySQL associé en entrant les commandes suivantes dans l'ordre indiqué :

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 votre changement de nom d'hôte, redémarrez Unified Manager en entrant les commandes suivantes dans l'ordre indiqué :

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 DÉLICTUELLE (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.