Réaliser les tâches de configuration et d'administration

Active IQ Unified Manager 9.10

NetApp
December 18, 2023

Sommaire

Réaliser les tâches de configuration et d'administration

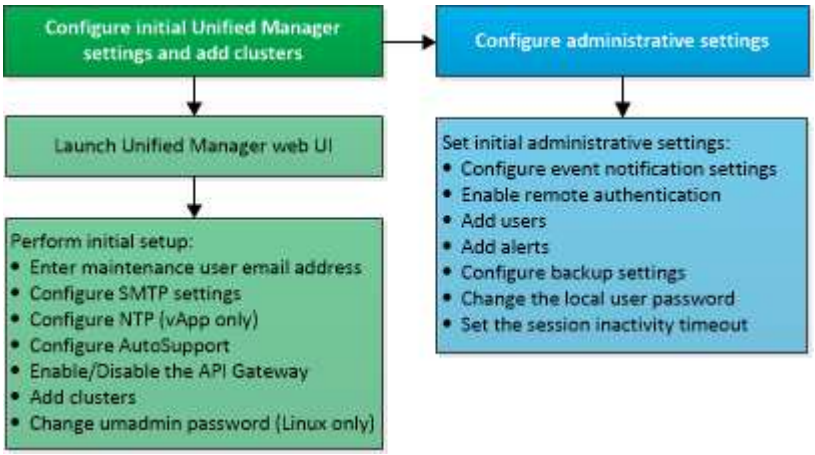
Configuration d'Active IQ Unified Manager en cours

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.

Ce dont vous aurez besoin

- 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.

> Si vous effectuez trois tentatives consécutives infructueuses pour vous connecter à l'interface utilisateur Web dans une heure, vous serez bloqué hors du système et vous devrez contacter votre administrateur système. Ceci s'applique uniquement aux utilisateurs locaux.

Configuration initiale de l'interface utilisateur Web de Unified Manager

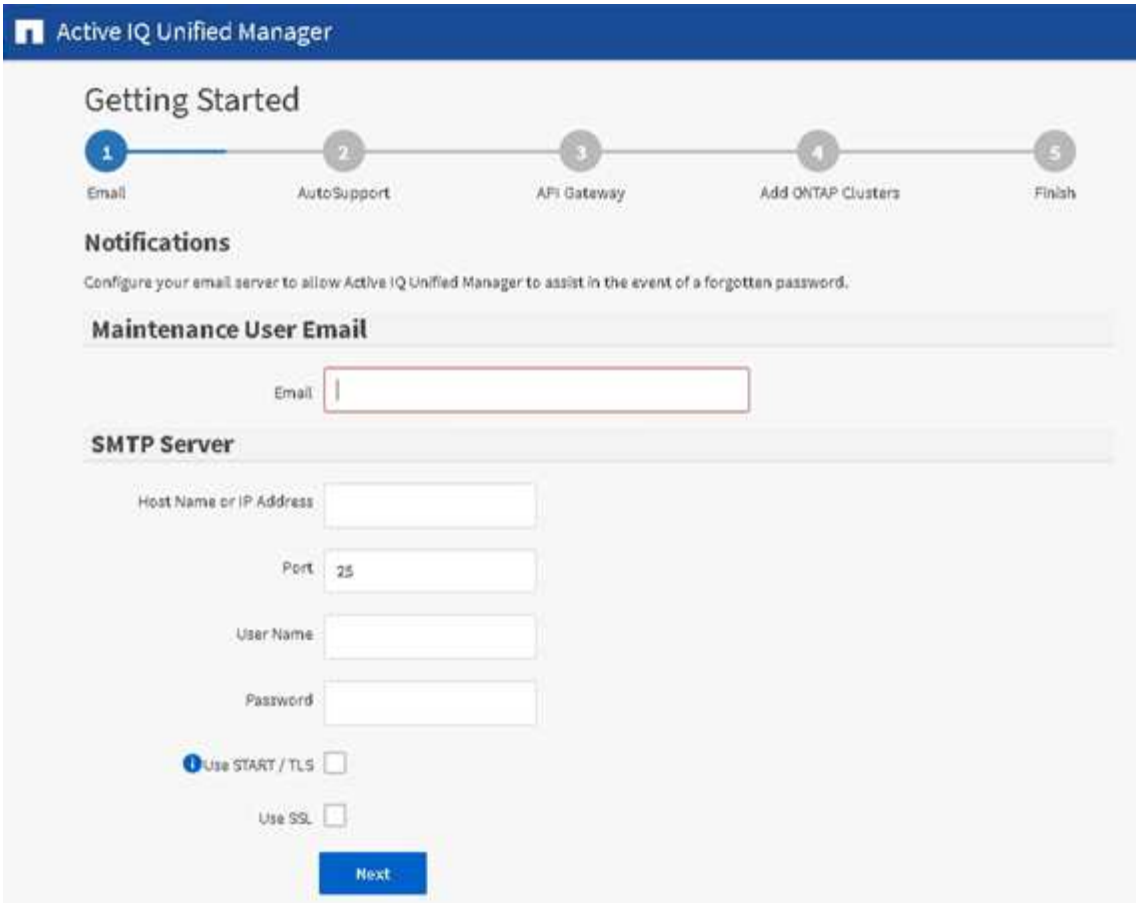
Pour utiliser Unified Manager, vous devez d'abord configurer les options de configuration initiale, notamment le serveur NTP, l'adresse e-mail de l'utilisateur de maintenance et l'hôte du serveur SMTP, ainsi que l'ajout de clusters ONTAP.

Ce dont vous aurez besoin

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

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.



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 **J'accepte et continue** pour activer l'envoi de 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 d'API, indiquez 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 d'API REST de 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 des API REST 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**.

La page mise en route se ferme et la page Tableau de bord de Unified Manager 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.

Ce dont vous aurez besoin

- 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.

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 Configuration du 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 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 Autoriser l'hôte, cliquez sur **Afficher le certificat** pour afficher les informations de certificat sur le 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.

Une fois que tous les objets d'un nouveau cluster sont découverts, Unified Manager commence à collecter les données d'historique de performances des 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.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

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.

Ce dont vous aurez besoin

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 pour vous assurer que toutes les notifications par e-mail ont été envoyées correctement.
   - 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.

Ce dont vous aurez besoin

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).

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	• 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. **Facultatif :** Ajoutez des serveurs d'authentification et testez l'authentification.
5. 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.

Ce dont vous aurez besoin

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

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**.

Configuration des services d'authentification

Les services d'authentification permettent l'authentification d'utilisateurs distants ou de groupes distants sur un serveur d'authentification avant de leur donner accès à Unified Manager. Vous pouvez authentifier les utilisateurs en utilisant des services d'authentification prédéfinis (tels qu'Active Directory ou OpenLDAP) ou en configurant votre propre mécanisme d'authentification.

Ce dont vous aurez besoin

- Vous devez avoir activé l'authentification à distance.
- Vous devez avoir le rôle Administrateur d'applications.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **authentification à distance**.
2. Sélectionnez l'un des services d'authentification suivants :

Si vous sélectionnez…	Alors, procédez comme ça…
Active Directory	a. Entrez le nom et le mot de passe de l'administrateur. b. Spécifiez le nom distinctif de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**.

Si vous sélectionnez…	Alors, procédez comme ça…
OpenLDAP	a. Entrez le nom distinctif de liaison et le mot de passe de liaison. b. Spécifiez le nom distinctif de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**.
Autres	a. Entrez le nom distinctif de liaison et le mot de passe de liaison. b. Spécifiez le nom distinctif de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**. c. Spécifiez la version du protocole LDAP prise en charge par le serveur d'authentification. d. Entrez le nom d'utilisateur, l'appartenance au groupe, le groupe d'utilisateurs et les attributs de membre.

Si vous souhaitez modifier le service d'authentification, vous devez supprimer tout serveur d'authentification existant, puis ajouter de nouveaux serveurs d'authentification.

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.

Ce dont vous aurez besoin

- 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.

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	a. Sélectionnez l'option **utiliser 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. Désactivez l'option **utiliser 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.

3. 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.

Ce dont vous aurez besoin

- 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.

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 le volet de navigation de gauche, cliquez sur **général** > **authentification à distance**.
2. Cliquez sur **Tester l'authentification**.
3. Dans la boîte de dialogue utilisateur de test, 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'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.

Ce dont vous aurez besoin

- 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.

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 **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 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 « + sample@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 :

Étapes

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**, saisissez **xyz** dans le champ **Nom contient**, puis cliquez sur **Ajouter**.
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** et saisissez **sample@domain.com** dans le champ Alert Aces 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**.

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.

Ce dont vous aurez besoin

Vous devez être connecté en tant qu'utilisateur local.

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**.

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).

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

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**.
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.

Ce dont vous aurez besoin

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.

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.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

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	Cliquez sur l'option **mettre à jour les attributs de certificat actuels**. 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. ⓘ • Les valeurs autorisées pour la taille de clé sont `2048`, `3072` et `4096`. • Les périodes de validité sont de 1 jour minimum à 36500 jours maximum. 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. • 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.

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.

Ce dont vous aurez besoin

L'appliance virtuelle est sous tension.

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

Vous pouvez également redémarrer la machine virtuelle depuis vSphere en utilisant 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.

Ce dont vous aurez besoin

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

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.

Vous devez avoir le rôle Administrateur d'applications.

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 "La gestion des opérations de sauvegarde et de restauration".

Gestion des paramètres des fonctions

La page Paramètres des fonctions vous permet d'activer et de désactiver certaines fonctions dans Active IQ Unified Manager. Cela inclut la création et la gestion d'objets de stockage basés sur des stratégies, l'activation de la passerelle d'API et de la bannière de connexion, le téléchargement de scripts pour la gestion des alertes, le timing d'une

session d'interface utilisateur Web basée sur le temps d'inactivité et la désactivation de la réception des événements de la plateforme Active IQ.

> La page Paramètres de la fonction n'est disponible que pour les utilisateurs ayant le rôle d'administrateur d'application.

Pour plus d'informations sur le téléchargement de scripts, reportez-vous à la section "Activation et désactivation du téléchargement des scripts".

Permettre la gestion du stockage basée sur des règles

L'option **gestion du stockage basée sur des règles** permet la gestion du stockage en fonction des objectifs de niveau de service (SLO). Cette option est activée par défaut.

Lorsque vous activez cette fonctionnalité, vous pouvez provisionner des charges de travail de stockage sur les clusters ONTAP ajoutés à votre instance Active IQ Unified Manager et gérer ces charges de travail en fonction des niveaux de service de performance et des règles d'efficacité du stockage qui lui sont attribuées.

Vous pouvez choisir d'activer ou de désactiver cette fonction à partir de **général** > **Paramètres de fonction** > **gestion du stockage basée sur des règles**. Lors de l'activation de cette fonction, les pages suivantes sont disponibles pour le fonctionnement et la surveillance :

- Provisionnement (provisionnement de la charge de travail de stockage)
- **Stratégies** > **niveaux de service de performance**
- **Stratégies** > **efficacité du stockage**
- Charges de travail gérées par Performance Service Level sur la page de configuration des clusters
- Performances de la charge de travail sur le **Tableau de bord**

Vous pouvez utiliser les écrans pour créer des niveaux de service Performance et des règles d'efficacité du stockage et provisionner des charges de travail de stockage. Vous pouvez également surveiller les charges de travail de stockage conformes aux niveaux de service de performances attribués, ainsi qu'aux charges non conformes. Le panneau performances des charges de travail et IOPS des charges de travail vous permet également d'évaluer les performances et la capacité totales, disponibles et utilisées (IOPS) des clusters de votre data Center, basées sur les charges de travail de stockage qui y sont provisionnées.

Après avoir activé cette fonctionnalité, vous pouvez exécuter les API REST Unified Manager pour effectuer certaines de ces fonctions à partir de la catégorie **barre de menus** > **bouton aide** > **Documentation API** > **fournisseur de stockage**. Vous pouvez également entrer le nom d'hôte ou l'adresse IP et l'URL pour accéder à la page de L'API REST au format https://<hostname>/docs/api/

Pour plus d'informations sur les API, voir "Mise en route des API REST de Active IQ Unified Manager"

Activation de la passerelle API

La fonctionnalité de passerelle d'API permet à Active IQ Unified Manager de devenir un plan de contrôle unique depuis lequel vous pouvez gérer plusieurs clusters ONTAP sans se connecter individuellement.

Vous pouvez activer cette fonctionnalité à partir des pages de configuration qui s'affichent lorsque vous vous connectez pour la première fois à Unified Manager. Vous pouvez également activer ou désactiver cette fonction à partir de **général** > **Paramètres de fonction** > **passerelle API**.

Les API REST de Unified Manager sont différentes des API REST de ONTAP. Toutes les fonctionnalités des API REST de ONTAP ne peuvent pas être disponibles via les API REST de Unified Manager. Toutefois, si vous devez accéder aux API ONTAP pour gérer des fonctionnalités spécifiques qui ne sont pas exposées à Unified Manager, vous pouvez activer la fonctionnalité de passerelle d'API et exécuter les API ONTAP. La passerelle agit comme un proxy pour le tunnel des requêtes API en maintenant les demandes d'en-tête et de corps dans le même format que dans les API ONTAP. Vous pouvez utiliser vos identifiants Unified Manager et exécuter des API spécifiques pour accéder aux clusters ONTAP et les gérer sans passer par les identifiants individuels du cluster. Unified Manager constitue un point de gestion unique pour l'exécution des API dans les clusters ONTAP gérés par votre instance Unified Manager. La réponse renvoyée par les API est la même que la réponse renvoyée par les API REST respectives ONTAP exécutées directement depuis ONTAP.

Une fois cette fonctionnalité activée, vous pouvez exécuter les API REST Unified Manager à partir de la catégorie **barre de menus** > **bouton aide** > **Documentation API** > **passerelle**. Vous pouvez également entrer le nom d'hôte ou l'adresse IP et l'URL pour accéder à la page de L'API REST au format `https://<hostname>/docs/api/`

Pour plus d'informations sur les API, voir "Mise en route des API REST de Active IQ Unified Manager".

Spécification du délai d'inactivité

Vous pouvez indiquer la valeur du délai d'inactivité pour Active IQ Unified Manager. Après une inactivité du temps spécifié, l'application est automatiquement déconnectée. Cette option est activée par défaut.

Vous pouvez désactiver cette fonction ou modifier l'heure dans **général** > **Paramètres de fonction** > **délai d'inactivité**. Une fois cette fonction activée, vous devez spécifier le délai d'inactivité (en minutes) dans le champ **LOGOUT AFTER**, après lequel le système se déconnecte automatiquement. La valeur par défaut est 4320 minutes (72 heures).

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

Activation des événements du portail Active IQ

Vous pouvez indiquer si vous souhaitez activer ou désactiver les événements du portail Active IQ. Ce paramètre permet au portail Active IQ de détecter et d'afficher d'autres événements relatifs à la configuration du système, au câblage, etc. Cette option est activée par défaut.

Lors de l'activation de cette fonctionnalité, Active IQ Unified Manager affiche les événements détectés par le portail Active IQ. Ces événements sont créés en exécutant un ensemble de règles par rapport aux messages AutoSupport générés à partir de tous les systèmes de stockage surveillés. Ces événements sont différents des autres événements Unified Manager et ils identifient les incidents et les risques liés à la configuration du système, au câblage, aux meilleures pratiques et aux problèmes de disponibilité.

Vous pouvez choisir d'activer ou de désactiver cette fonction à partir de **général** > **Paramètres de fonction** > **événements de portail Active IQ**. Dans les sites sans accès réseau externe, vous devez télécharger manuellement les règles à partir de **Storage Management** > **Event Setup** > **Upload Rules**.

Cette fonctionnalité est activée par défaut. La désactivation de cette fonctionnalité empêche la découverte ou l'affichage des événements Active IQ sur Unified Manager. Lorsque cette option est désactivée, l'activation de cette fonctionnalité permet à Unified Manager de recevoir les événements Active IQ sur un cluster à une heure

prédéfinie de 00:15 pour le fuseau horaire du cluster.

Activation et désactivation des paramètres de sécurité à des fins de conformité

En utilisant le bouton **Personnaliser** du panneau **Tableau de bord de sécurité** de la page Paramètres des fonctionnalités, vous pouvez activer ou désactiver les paramètres de sécurité pour la surveillance de la conformité sur Unified Manager.

Les paramètres activés ou désactivés sur cette page régissent l'état de conformité global des clusters et des machines virtuelles de stockage sur Unified Manager. En fonction des sélections, les colonnes correspondantes sont visibles dans la vue **sécurité : tous les clusters** de la page d'inventaire clusters et dans la vue **sécurité : toutes les VM de stockage** de la page d'inventaire des VM de stockage.

> Seuls les utilisateurs disposant d'un rôle d'administrateur peuvent modifier ces paramètres.

Les critères de sécurité de vos clusters ONTAP, de vos VM de stockage et de vos volumes sont évalués sur la base des recommandations fournies dans le "Guide de renforcement de la sécurité des environnements NetApp ONTAP 9". Le panneau sécurité du tableau de bord et de la page sécurité affiche l'état de conformité de sécurité par défaut de vos clusters, machines virtuelles de stockage et volumes. Des événements de sécurité sont également générés et des actions de gestion sont activées pour les clusters et les machines virtuelles de stockage qui ont des violations de sécurité.

Personnalisation des paramètres de sécurité

Pour personnaliser les paramètres de contrôle de conformité applicables à votre environnement ONTAP, procédez comme suit :

Étapes

1. Cliquez sur **général > Paramètres des fonctions > Tableau de bord de sécurité > Personnaliser**. La fenêtre contextuelle **Personnaliser les paramètres du tableau de bord de sécurité** s'affiche.

   > Les paramètres de conformité de sécurité que vous activez ou désactivez peuvent directement affecter les vues de sécurité par défaut, les rapports et les rapports planifiés sur les écrans clusters et ordinateurs virtuels de stockage. Si vous avez téléchargé un rapport Excel à partir de ces écrans avant de modifier les paramètres de sécurité, il se peut que les rapports Excel téléchargés soient défectueux.

2. Pour activer ou désactiver les paramètres personnalisés de vos clusters ONTAP, sélectionnez le paramètre général requis sous **Cluster**. Pour plus d'informations sur les options de personnalisation de la conformité des clusters, reportez-vous à la section "Catégories de conformité des clusters"
3. Pour activer ou désactiver les paramètres personnalisés de vos machines virtuelles de stockage, sélectionnez le paramètre général requis sous **Storage VM**. Pour plus d'informations sur les options de personnalisation de la conformité de la VM de stockage, reportez-vous à la section "Catégories de conformité des VM de stockage".

Personnalisation des paramètres AutoSupport et d'authentification

Dans la section **Paramètres AutoSupport**, vous pouvez spécifier si le transport HTTPS doit être utilisé pour l'envoi de messages AutoSupport depuis ONTAP.

Dans la section **Paramètres d'authentification**, vous pouvez activer la génération d'alertes Unified Manager pour l'utilisateur administrateur ONTAP par défaut.

Activation et désactivation du téléchargement des scripts

La possibilité de télécharger les scripts vers Unified Manager et de les exécuter est activée par défaut. Si votre entreprise ne souhaite pas autoriser cette activité pour des raisons de sécurité, vous pouvez désactiver cette fonctionnalité.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Étapes

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

Les fonctions que vous recherchez…	Alors, procédez comme ça…
Désactiver les scripts	Dans le panneau **script Upload**, déplacez le curseur vers la gauche.
Activez les scripts	Dans le panneau **script Upload**, déplacez le curseur vers la droite.

Ajout d'une bannière de connexion

L'ajout d'une bannière de connexion permet à votre organisation d'afficher toutes les informations, telles que les personnes autorisées à accéder au système et les conditions d'utilisation lors de la connexion et de la déconnexion.

Tout utilisateur, tel que les opérateurs de stockage ou les administrateurs, peut afficher cette bannière de connexion pendant la connexion, la déconnexion et le délai d'expiration de la session.

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.

Diagnostique 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.

Ce dont vous aurez besoin

Vous devez avoir installé et configuré Unified Manager.

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.

Étape

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

Sur ce système d'exploitation…	Suivez ces étapes…
VMware	a. À l'aide de Secure Shell, connectez-vous à l'adresse IP ou au nom de domaine complet de l'appliance virtuelle Unified Manager. b. Connectez-vous à la console de maintenance à l'aide de votre nom d'utilisateur et de votre mot de passe de maintenance.
Linux	a. À l'aide de Secure Shell, connectez-vous à l'adresse IP ou au nom de domaine complet du système Unified Manager. b. Connectez-vous au système avec le nom et le mot de passe de l'utilisateur de maintenance (umadmin). c. Saisissez la commande `maintenance_console` Puis appuyez sur entrée.
Répertoires de base	a. Connectez-vous au système Unified Manager avec les identifiants d'administrateur. b. Lancez PowerShell en tant qu'administrateur Windows. c. Saisissez la commande `maintenance_console` 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.

Ce dont vous aurez besoin

- 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).

- **Modifier le service NTP**

Bascule entre le `ntp` et `systemd-timesyncd` administratifs.

- **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.

Ce dont vous aurez besoin

- 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.

Ce dont vous aurez besoin

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.

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.

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.

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.

Ce dont vous aurez besoin

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

L'appliance virtuelle doit être sous tension.

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

Étapes

1. Dans le menu principal de la console vSphere, 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.

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

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

5. Tapez **y** pour activer l'interface réseau.
6. 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**.

7. 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.

Ce dont vous aurez besoin

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

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. Lancer la commande chcon 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` a 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 fonctionne peut-être pas comme prévu.

8. 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
   ```

9. 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:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Supprimez le fichier abc pour que ce fichier externe ne provoque pas d'erreur dans la base de données à l'avenir.

11. Copiez le contenu des données de sauvegarde vers le contenu étendu `/opt/netapp/data` répertoire :

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. Si se Linux est activé, exécutez la commande suivante :

```
chcon -R --type=mysqld_db_t /opt/netapp/data
```

13. Démarrez le service MySQL :

```
systemctl start mysqld
```

14. Une fois le service MySQL démarré, démarrer les services ocie et ocieau dans l'ordre indiqué:

```
systemctl start ocie ocieau
```

15. 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.

Ce dont vous aurez besoin

- 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.

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 du système**.
5. Dans le menu 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.

Ce dont vous aurez besoin

Vous devez disposer des privilèges d'administrateur Windows.

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"

Gestion de l’accès des utilisateurs

Vous pouvez créer des rôles et attribuer des fonctions pour contrôler l’accès des utilisateurs aux objets de cluster sélectionnés. Vous pouvez identifier les utilisateurs disposant des fonctionnalités requises pour accéder aux objets sélectionnés dans un cluster. Seuls ces utilisateurs ont accès pour gérer les objets du cluster.

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.

Ce dont vous aurez besoin

- 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.

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**.

Création d’un utilisateur de base de données

Pour prendre en charge une connexion entre Workflow Automation et Unified Manager, ou pour accéder aux vues de base de données, vous devez d’abord créer un utilisateur

de base de données avec le rôle Schéma d'intégration ou Schéma de rapport dans l'interface utilisateur Web d'Unified Manager.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Les utilisateurs de base de données offrent une intégration à Workflow Automation et un accès à des vues de base de données spécifiques aux rapports. Les utilisateurs de base de données n'ont pas accès à l'interface utilisateur Web d'Unified Manager ou à la console de maintenance, et ne peuvent pas exécuter d'appels API.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **utilisateurs**.
2. Dans la page utilisateurs, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un utilisateur, sélectionnez **Database User** dans la liste déroulante **Type**.
4. Saisissez un nom et un mot de passe pour l'utilisateur de la base de données.
5. Dans la liste déroulante **role**, sélectionnez le rôle approprié.

Si vous êtes…	Choisissez ce rôle
Connexion de Unified Manager à Workflow Automation	Schéma d'intégration
Accès aux rapports et autres vues de base de données	Schéma du rapport

6. Cliquez sur **Ajouter**.

Modification des paramètres utilisateur

Vous pouvez modifier les paramètres utilisateur, tels que l'adresse e-mail et le rôle, qui sont spécifiés par chaque utilisateur. Par exemple, vous pouvez modifier le rôle d'un utilisateur qui est un opérateur de stockage et attribuer des privilèges d'administrateur de stockage à cet utilisateur.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Lorsque vous modifiez le rôle attribué à un utilisateur, les modifications sont appliquées lorsque l'une des actions suivantes se produit :

- L'utilisateur se déconnecte et se reconnecte à Unified Manager.
- Le délai d'expiration de session de 24 heures est atteint.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **utilisateurs**.
2. Dans la page utilisateurs, sélectionnez l'utilisateur pour lequel vous souhaitez modifier les paramètres, puis cliquez sur **Modifier**.

3. Dans la boîte de dialogue Modifier l'utilisateur, modifiez les paramètres spécifiés pour l'utilisateur.
4. Cliquez sur **Enregistrer**.

Affichage des utilisateurs

Vous pouvez utiliser la page utilisateurs pour afficher la liste des utilisateurs qui gèrent les objets et les données de stockage à l'aide de Unified Manager. Vous pouvez afficher des détails sur les utilisateurs, tels que le nom d'utilisateur, le type d'utilisateur, l'adresse e-mail et le rôle attribué aux utilisateurs.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Étape

1. Dans le volet de navigation de gauche, cliquez sur **général** > **utilisateurs**.

Suppression d'utilisateurs ou de groupes

Vous pouvez supprimer un ou plusieurs utilisateurs de la base de données du serveur de gestion pour empêcher certains utilisateurs d'accéder à Unified Manager. Vous pouvez également supprimer des groupes de sorte que tous les utilisateurs du groupe ne puissent plus accéder au serveur de gestion.

Ce dont vous aurez besoin

- Lorsque vous supprimez des groupes distants, vous devez avoir réaffecté les événements qui sont affectés aux utilisateurs des groupes distants.

  Si vous supprimez des utilisateurs locaux ou distants, les événements qui sont affectés à ces utilisateurs sont automatiquement affectés.

- Vous devez avoir le rôle Administrateur d'applications.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **utilisateurs**.
2. Dans la page utilisateurs, sélectionnez les utilisateurs ou les groupes que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la suppression.

En quoi consiste le RBAC

Le contrôle d'accès basé sur des rôles (RBAC) vous permet de contrôler l'accès aux différentes fonctionnalités et ressources du serveur Active IQ Unified Manager.

Rôle du contrôle d'accès basé sur des rôles

Le contrôle d'accès basé sur des rôles (RBAC) permet aux administrateurs de gérer des groupes d'utilisateurs en définissant des rôles. Si vous devez restreindre l'accès à des

fonctionnalités spécifiques aux administrateurs sélectionnés, vous devez configurer des comptes d'administrateur pour eux. Si vous souhaitez limiter les informations que les administrateurs peuvent afficher et les opérations qu'ils peuvent effectuer, vous devez appliquer des rôles aux comptes d'administrateur que vous créez.

Le serveur de gestion utilise le contrôle d'accès basé sur les rôles pour les autorisations de connexion utilisateur et de rôle. Si vous n'avez pas modifié les paramètres par défaut du serveur de gestion pour l'accès administrateur utilisateur, vous n'avez pas besoin de vous connecter pour les afficher.

Lorsque vous lancez une opération qui nécessite des privilèges spécifiques, le serveur de gestion vous invite à vous connecter. Par exemple, pour créer des comptes d'administrateur, vous devez vous connecter à l'aide de l'accès au compte d'administrateur d'application.

Définitions des types d'utilisateur

Un type d'utilisateur spécifie le type de compte que l'utilisateur détient et inclut les utilisateurs distants, les groupes distants, les utilisateurs locaux, les utilisateurs de base de données et les utilisateurs de maintenance. Chacun de ces types a son propre rôle, qui est attribué par un utilisateur avec le rôle Administrateur.

Les types d'utilisateurs Unified Manager sont les suivants :

- **Utilisateur de maintenance**

  Créée lors de la configuration initiale de Unified Manager. L'utilisateur de maintenance crée ensuite des utilisateurs supplémentaires et attribue des rôles. L'utilisateur de maintenance est également le seul utilisateur ayant accès à la console de maintenance. Lorsque Unified Manager est installé sur un système Red Hat Enterprise Linux ou CentOS, l'utilisateur chargé de la maintenance se voit attribuer le nom d'utilisateur « umadmin ».

- **Utilisateur local**

  Accède à l'interface utilisateur Unified Manager et effectue des fonctions en fonction du rôle attribué par l'utilisateur de maintenance ou par un utilisateur disposant du rôle d'administrateur d'applications.

- **Groupe distant**

  Groupe d'utilisateurs qui accèdent à l'interface utilisateur Unified Manager à l'aide des informations d'identification stockées sur le serveur d'authentification. Le nom de ce compte doit correspondre au nom d'un groupe stocké sur le serveur d'authentification. Tous les utilisateurs du groupe distant peuvent accéder à l'interface utilisateur d'Unified Manager à l'aide de leurs identifiants individuels. Les groupes distants peuvent effectuer des fonctions en fonction de leurs rôles attribués.

- **Utilisateur distant**

  Permet d'accéder à l'interface utilisateur Unified Manager à l'aide des informations d'identification stockées sur le serveur d'authentification. Un utilisateur distant effectue des fonctions en fonction du rôle attribué par l'utilisateur de maintenance ou par un utilisateur disposant du rôle d'administrateur d'applications.

- **Utilisateur de base de données**

  Possède un accès en lecture seule aux données de la base de données Unified Manager, n'a pas accès à l'interface web Unified Manager ni à la console de maintenance, et ne peut pas exécuter d'appels d'API.

Définitions des rôles utilisateur

L'utilisateur de maintenance ou l'administrateur d'applications attribue un rôle à chaque utilisateur. Chaque rôle contient certains privilèges. L'étendue des activités que vous pouvez effectuer dans Unified Manager dépend du rôle que vous avez attribué et des privilèges qu'il contient.

Unified Manager inclut les rôles d'utilisateur prédéfinis suivants :

- **Opérateur**

  Affiche les informations relatives au système de stockage et les autres données collectées par Unified Manager, y compris les historiques et les tendances de la capacité. Ce rôle permet à l'opérateur de stockage d'afficher, d'affecter, d'accuser réception, de résoudre et d'ajouter des notes aux événements.

- **Administrateur de stockage**

  Configuration des opérations de gestion du stockage dans Unified Manager Ce rôle permet à l'administrateur du stockage de configurer des seuils et de créer des alertes ainsi que d'autres options et règles spécifiques à la gestion du stockage.

- **Administrateur d'applications**

  Configure des paramètres sans rapport avec la gestion du stockage. Ce rôle permet de gérer les utilisateurs, les certificats de sécurité, l'accès à la base de données et les options administratives, y compris l'authentification, SMTP, mise en réseau et AutoSupport.

  > Lorsque Unified Manager est installé sur des systèmes Linux, l'utilisateur initial ayant le rôle d'administrateur d'applications est automatiquement nommé « umadmin ».

- **Schéma d'intégration**

  Ce rôle permet un accès en lecture seule aux vues de bases de données Unified Manager pour l'intégration de Unified Manager avec OnCommand Workflow Automation (WFA).

- **Schéma de rapport**

  Ce rôle permet un accès en lecture seule au reporting et à d'autres vues de base de données directement depuis la base de données Unified Manager. Les bases de données qui peuvent être affichées sont les suivantes :

  - vue_modèle_netapp
  - performances_netapp
  - ocum
  - rapport_ocum
  - ocum_report_birt
  - opm
  - scatemonitor

Fonctionnalités et rôles utilisateur de Unified Manager

En fonction du rôle d'utilisateur que vous avez attribué, vous pouvez déterminer les opérations que vous pouvez effectuer dans Unified Manager.

Le tableau suivant affiche les fonctions que chaque rôle d'utilisateur peut effectuer :

Fonction	Opérateur	Administrateur du stockage	Administrateur d'applications	Schéma d'intégration	Schéma du rapport
Afficher des informations sur le système de stockage	•	•	•	•	•
Affichez d'autres données, telles que les historiques et les tendances en matière de capacité	•	•	•	•	•
Afficher, attribuer et résoudre les événements	•	•	•		
Affichez les objets des services de stockage, tels que les associations de SVM et les pools de ressources	•	•	•		
Afficher les stratégies de seuil	•	•	•		
Gérez les objets de service de stockage, tels que les associations de SVM et les pools de ressources		•	•		
Définir des alertes		•	•		

Fonction	Opérateur	Administrateur du stockage	Administrateur d'applications	Schéma d'intégration	Schéma du rapport
Gérer les options de gestion du stockage		•	•		
Gérez les règles de gestion du stockage		•	•		
Gérer les utilisateurs			•		
Gérer les options administratives			•		
Définir des règles de seuil			•		
Gérer l'accès à la base de données			•		
Gérez l'intégration avec WFA et fournissez l'accès aux vues de base de données				•	
Planifiez et enregistrez des rapports		•	•		
Exécuter les opérations « réparer » à partir des actions de gestion		•	•		
Fournir un accès en lecture seule aux vues de base de données					•

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.

Ce dont vous aurez besoin

- 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.

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.

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.

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 fournisseur d'identités utilisé pour l'authentification SAML

Vous pouvez modifier le fournisseur d'identités utilisé par Unified Manager pour authentifier les utilisateurs distants.

Ce dont vous aurez besoin

- Vous devez disposer de l'URL IDP et des métadonnées.
- Vous devez avoir accès au PDI.

Le nouveau IDP peut être configuré avant ou après avoir configuré Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **authentification SAML**.
2. Entrez le nouveau URI du IDP et les métadonnées IDP requises pour connecter le serveur Unified

Manager au IDP.

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

3. Copiez l'URI des métadonnées de Unified Manager ou enregistrez les métadonnées dans un fichier texte XML.
4. Cliquez sur **Enregistrer la configuration**.

   Un message s'affiche pour confirmer que vous souhaitez modifier la configuration.

5. Cliquez sur **OK**.

Accédez au nouveau IDP et entrez l'URI du serveur Unified Manager et les métadonnées pour terminer la configuration.

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

Mise à jour des paramètres d'authentification SAML après une modification du certificat de sécurité Unified Manager

Toute modification du certificat de sécurité HTTPS installé sur le serveur Unified Manager nécessite la mise à jour des paramètres de configuration de l'authentification SAML. Le certificat est mis à jour si vous renommez le système hôte, attribuez une nouvelle adresse IP au système hôte ou modifiez manuellement le certificat de sécurité du système.

Une fois le certificat de sécurité modifié et le serveur Unified Manager redémarré, l'authentification SAML ne fonctionnera pas et les utilisateurs ne pourront pas accéder à l'interface graphique Unified Manager. Vous devez mettre à jour les paramètres d'authentification SAML sur le serveur IDP et sur le serveur Unified Manager pour réactiver l'accès à l'interface utilisateur.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Menu principal**, entrez le numéro de l'option **Désactiver l'authentification SAML**.

   Un message s'affiche pour confirmer que vous souhaitez désactiver l'authentification SAML et redémarrer Unified Manager.

3. Lancez l'interface utilisateur Unified Manager à l'aide du FQDN ou de l'adresse IP mis à jour, acceptez le certificat de serveur mis à jour dans votre navigateur et connectez-vous à l'aide des informations d'identification de l'utilisateur de maintenance.
4. Dans la page **Configuration/authentification**, sélectionnez l'onglet **authentification SAML** et configurez la connexion IDP.
5. Copiez l'URI des métadonnées de l'hôte Unified Manager ou enregistrez les métadonnées de l'hôte dans un fichier texte XML.
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.
8. Accédez à votre serveur IDP, puis entrez l'URI du serveur Unified Manager et les métadonnées pour terminer la configuration.

Fournisseur d'identité	Étapes de configuration
ADFS	a. Supprimez l'entrée de confiance de la partie de confiance existante dans l'interface graphique de gestion ADFS. b. Ajoutez une nouvelle entrée de confiance de la partie de confiance à l'aide du `saml_sp_metadata.xml` À partir du serveur Unified Manager mis à jour. c. Définissez les trois règles de sinistre requises par Unified Manager pour analyser les réponses SAML ADFS pour cette entrée de confiance de tiers de confiance. d. Redémarrez le service Windows ADFS.
Hurlent	a. Mettez à jour le nouveau FQDN du serveur Unified Manager dans `attribute-filter.xml` et `relying-party.xml` fichiers. b. Redémarrez le serveur Web Apache Tomcat et attendez que le port 8005 soit en ligne.

9. Connectez-vous à Unified Manager et vérifiez que l'authentification SAML fonctionne comme prévu via votre IDP.

Désactivation de l'authentification SAML

Vous pouvez désactiver l'authentification SAML lorsque vous souhaitez arrêter l'authentification des utilisateurs distants via un fournisseur d'identités sécurisé avant de pouvoir vous connecter à l'interface utilisateur Web Unified Manager. Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés, tels qu'Active Directory ou LDAP, exécutent l'authentification d'identification.

Une fois l'authentification SAML désactivée, les utilisateurs locaux et les utilisateurs de maintenance pourront accéder à l'interface utilisateur graphique en plus des utilisateurs distants configurés.

Vous pouvez également désactiver l'authentification SAML à l'aide de la console de maintenance Unified Manager si vous n'avez pas accès à l'interface graphique.

> Unified Manager est redémarré automatiquement après la désactivation de l'authentification SAML.

Étapes

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

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

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

Lors de la prochaine tentative d'accès à l'interface graphique Unified Manager, les utilisateurs distants vont entrer leurs identifiants dans la page de connexion de Unified Manager au lieu de la page de connexion IDP.

Accédez à votre IDP et supprimez l'URI du serveur Unified Manager et les métadonnées.

Désactivation de l'authentification SAML à partir de la console de maintenance

Si vous n'avez pas accès à l'interface graphique Unified Manager, vous devrez peut-être désactiver l'authentification SAML à partir de la console de maintenance. Cela peut se produire en cas de mauvaise configuration ou si le IDP n'est pas accessible.

Ce dont vous aurez besoin

Comme utilisateur de maintenance, vous devez avoir accès à la console de maintenance.

Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés, tels qu'Active Directory ou LDAP, exécutent l'authentification d'identification. Les utilisateurs locaux et les utilisateurs de maintenance pourront accéder à l'interface utilisateur graphique en plus des utilisateurs distants configurés.

Vous pouvez également désactiver l'authentification SAML à partir de la page Configuration/authentification de l'interface utilisateur.

> Unified Manager est redémarré automatiquement après la désactivation de l'authentification SAML.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Menu principal**, entrez le numéro de l'option **Désactiver l'authentification SAML**.

   Un message s'affiche pour confirmer que vous souhaitez désactiver l'authentification SAML et redémarrer Unified Manager.

3. Tapez **y**, puis appuyez sur entrée et Unified Manager redémarre.

Lors de la prochaine tentative d'accès à l'interface graphique Unified Manager, les utilisateurs distants vont entrer leurs identifiants dans la page de connexion de Unified Manager au lieu de la page de connexion IDP.

Si nécessaire, accédez à votre IDP et supprimez l'URL du serveur Unified Manager et les métadonnées.

Page authentification SAML

Vous pouvez utiliser la page authentification SAML pour configurer Unified Manager afin d'authentifier les utilisateurs distants à l'aide de SAML via un fournisseur d'identités sécurisé avant de pouvoir vous connecter à l'interface utilisateur Web Unified Manager.

- Vous devez avoir le rôle Administrateur d'applications pour créer ou modifier la configuration SAML.
- Vous devez avoir configuré l'authentification à distance.
- Vous devez avoir configuré au moins un utilisateur distant ou un groupe distant.

Une fois l'authentification à distance et les utilisateurs distants configurés, vous pouvez cocher la case Activer l'authentification SAML pour activer l'authentification à l'aide d'un fournisseur d'identité sécurisé.

- **URI IDP**

  URI permettant d'accéder au IDP à partir du serveur Unified Manager. Les exemples d'URI sont répertoriés ci-dessous.

  Exemple d'URI ADFS :

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Exemple d'URI :

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Métadonnées IDP**

  Les métadonnées IDP au format XML.

  Si l'URL IDP est accessible à partir du serveur Unified Manager, vous pouvez cliquer sur le bouton **extraire les métadonnées IDP** pour remplir ce champ.

- **Système hôte (FQDN)**

  Le FQDN du système hôte Unified Manager tel que défini lors de l'installation. Vous pouvez modifier cette valeur si nécessaire.

- **URI hôte**

  URI permettant d'accéder au système hôte Unified Manager à partir du IDP.

- **Métadonnées hôte**

  Métadonnées du système hôte au format XML.

Gestion de l'authentification

Vous pouvez activer l'authentification à l'aide de LDAP ou d'Active Directory sur le serveur Unified Manager et le configurer pour qu'il fonctionne avec vos serveurs afin d'authentifier les utilisateurs distants.

Pour activer l'authentification à distance, configurer les services d'authentification et ajouter des serveurs d'authentification, reportez-vous à la section précédente sur **configurer Unified Manager pour envoyer des notifications d'alerte**.

Modification des serveurs d'authentification

Vous pouvez modifier le port utilisé par le serveur Unified Manager pour communiquer avec votre serveur d'authentification.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

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. Dans la zone **serveurs d'authentification**, sélectionnez le serveur d'authentification que vous souhaitez modifier, puis cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Edit Authentication Server**, modifiez les détails du port.
5. Cliquez sur **Enregistrer**.

Suppression des serveurs d'authentification

Vous pouvez supprimer un serveur d'authentification si vous souhaitez empêcher le serveur Unified Manager de communiquer avec le serveur d'authentification. Par exemple, si vous souhaitez modifier un serveur d'authentification avec lequel le serveur de gestion communique, vous pouvez supprimer le serveur d'authentification et ajouter un nouveau serveur d'authentification.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications.

Lorsque vous supprimez un serveur d'authentification, les utilisateurs ou groupes distants du serveur d'authentification ne pourront plus accéder à Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **authentification à distance**.
2. Sélectionnez un ou plusieurs serveurs d'authentification que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Cliquez sur **Oui** pour confirmer la demande de suppression.

   Si l'option **Use Secure Connection** est activée, les certificats associés au serveur d'authentification sont supprimés avec le serveur d'authentification.

Authentification avec Active Directory ou OpenLDAP

Vous pouvez activer l'authentification à distance sur le serveur de gestion et configurer le

serveur de gestion pour qu'il communique avec vos serveurs d'authentification afin que les utilisateurs des serveurs d'authentification puissent accéder à Unified Manager.

Vous pouvez utiliser l'un des services d'authentification prédéfinis suivants ou spécifier votre propre service d'authentification :

- Microsoft Active Directory

  Vous ne pouvez pas utiliser Microsoft Lightweight Directory Services.

- OpenLDAP

Vous pouvez sélectionner le service d'authentification requis et ajouter les serveurs d'authentification appropriés pour permettre aux utilisateurs distants du serveur d'authentification d'accéder à Unified Manager. Les informations d'identification des utilisateurs ou groupes distants sont gérées par le serveur d'authentification. Le serveur de gestion utilise le protocole LDAP (Lightweight Directory Access Protocol) pour authentifier les utilisateurs distants au sein du serveur d'authentification configuré.

Pour les utilisateurs locaux créés dans Unified Manager, le serveur de gestion conserve sa propre base de données de noms d'utilisateur et de mots de passe. Le serveur de gestion effectue l'authentification et n'utilise pas Active Directory ou OpenLDAP pour l'authentification.

Consignation d'audits

Vous pouvez détecter si les journaux d'audit ont été compromis avec l'utilisation des journaux d'audit. Toutes les activités effectuées par un utilisateur sont surveillées et consignées dans les journaux d'audit. Les audits sont effectués pour toutes les interfaces utilisateur et les fonctionnalités des API exposées publiquement de Active IQ Unified Manager.

Vous pouvez utiliser la vue fichier du journal d'audit pour afficher et accéder à tous les fichiers journaux d'audit disponibles dans Active IQ Unified Manager. Les fichiers de la vue Journal d'audit : fichier sont répertoriés en fonction de leur date de création. Cette vue affiche les informations de tous les journaux d'audit qui sont enregistrés à partir de l'installation ou de la mise à niveau vers le présent dans le système. Chaque fois que vous effectuez une action dans Unified Manager, les informations sont mises à jour et disponibles dans les journaux. L'état de chaque fichier journal est capturé à l'aide de l'attribut « Etat d'intégrité des fichiers » qui est activement surveillé pour détecter la modification ou la suppression du fichier journal. Les journaux d'audit peuvent avoir l'un des États suivants lorsque les journaux d'audit sont disponibles dans le système :

État	Description
ACTIF	Fichier dans lequel les journaux sont en cours de journalisation.
NORMALE	Fichier inactif, compressé et stocké dans le système.
FALSIFIÉ	Fichier compromis par un utilisateur qui a modifié manuellement le fichier.
SUPPRESSION_MANUELLE	Fichier supprimé par un utilisateur autorisé.

État	Description
SUPPRESSION_DU_SURVOL	Fichier supprimé en raison de la désactivation en fonction de la stratégie de configuration de roulement.
UNEXPECTED_DELETE	Fichier supprimé pour des raisons inconnues.

La page Journal d'audit comprend les boutons de commande suivants :

- Configurer
- Supprimer
- Télécharger

Le bouton **DELETE** permet de supprimer tous les journaux d'audit répertoriés dans la vue journaux d'audit. Vous pouvez supprimer un journal d'audit et éventuellement fournir une raison de supprimer le fichier, ce qui permet à l'avenir de déterminer une suppression valide. La colonne MOTIF répertorie la raison ainsi que le nom de l'utilisateur qui a effectué l'opération de suppression.

> La suppression d'un fichier journal entraînera la suppression du fichier du système, mais l'entrée de la table DB ne sera pas supprimée.

Vous pouvez télécharger les journaux d'audit à partir de Active IQ Unified Manager à l'aide du bouton **DOWNLOAD** de la section journaux d'audit et exporter les fichiers journaux d'audit. Les fichiers marqués « NORMAL » ou « FALSIFIÉ » sont téléchargés dans un fichier compressé `.gzip` format.

Lorsqu'un bundle AutoSupport complet est généré, le bundle de support inclut à la fois des fichiers journaux d'audit archivés et actifs. Mais lorsqu'un bundle de support léger est généré, il inclut uniquement les journaux d'audit actifs. Les journaux d'audit archivés ne sont pas inclus.

Configuration des journaux d'audit

Vous pouvez utiliser le bouton **configurer** de la section journaux d'audit pour configurer la stratégie de déploiement des fichiers journaux d'audit et activer la journalisation à distance des journaux d'audit.

Vous pouvez définir les valeurs dans les JOURS de RÉTENTION du JOURNAL * **MAX ET *AUDIT LOG** en fonction de la quantité et de la fréquence de données que vous souhaitez stocker dans le système. La valeur du champ **TAILLE TOTALE DU JOURNAL D'AUDIT** est la taille totale des données du journal d'audit présentes dans le système. La stratégie de reprise est déterminée par les valeurs du champ **JOURS DE RÉTENTION DU JOURNAL D'AUDIT**, **taille DU FICHIER MAX** et **TAILLE TOTALE DU JOURNAL D'AUDIT**. Lorsque la taille de la sauvegarde du journal d'audit atteint la valeur configurée dans **TAILLE TOTALE DU JOURNAL D'AUDIT**, le fichier qui a été archivé en premier est supprimé. Cela signifie que le fichier le plus ancien est supprimé. Mais l'entrée de fichier continue d'être disponible dans la base de données et est marquée comme ""Suppression de substitution"". La valeur **JOURS de CONSERVATION DU JOURNAL D'AUDIT** correspond au nombre de jours pendant lesquels les fichiers journaux d'audit sont conservés. Tout fichier antérieur à la valeur définie dans ce champ est redéployé.

Étapes

1. Cliquez sur **journaux d'audit** > **configurer**.
2. Entrez des valeurs dans les champs **MAX FILE SIZE**, **TOTAL AUDIT LOG SIZE** et **AUDIT LOG**

RETENTION DAYS.

Si vous souhaitez activer la journalisation à distance, sélectionnez **Activer la journalisation à distance**.

Activation de la journalisation à distance des journaux d'audit

Vous pouvez sélectionner la case à cocher **Activer la journalisation à distance** dans la boîte de dialogue configurer les journaux d'audit pour activer la journalisation d'audit à distance. Vous pouvez utiliser cette fonction pour transférer les journaux d'audit vers un serveur Syslog distant. Cela vous permettra de gérer vos journaux d'audit lorsqu'il existe des contraintes d'espace.

La journalisation à distance des journaux d'audit assure une sauvegarde inviolable si les fichiers journaux d'audit sur le serveur Active IQ Unified Manager sont falsités.

Étapes

1. Dans la boîte de dialogue **configurer les journaux d'audit**, cochez la case **Activer la journalisation à distance**.

   Des champs supplémentaires pour configurer la journalisation à distance sont affichés.

2. Saisissez le **NOM D'HÔTE** et le **PORT** du serveur distant auquel vous souhaitez vous connecter.
3. Dans le champ **SERVER CA CERTIFICATE**, cliquez sur **BROWSE** pour sélectionner un certificat public du serveur cible.

   Le certificat doit être téléchargé dans `.pem` format. Ce certificat doit être obtenu à partir du serveur Syslog cible et ne doit pas avoir expiré. Le certificat doit contenir le « nom d'hôte » sélectionné dans le cadre du `SubjectAltName` (SAN) attribut.

4. Saisissez les valeurs des champs suivants : **CHARSET**, **DÉLAI DE CONNEXION**, **DÉLAI DE RECONNEXION**.

   Les valeurs doivent être exprimées en millisecondes pour ces champs.

5. Sélectionnez le format Syslog et la version du protocole TLS requis dans les champs **FORMAT** et **PROTOCOLE**.
6. Cochez la case **Activer l'authentification client** si le serveur Syslog cible nécessite une authentification par certificat.

   Vous devrez télécharger le certificat d'authentification client et le télécharger sur le serveur Syslog avant d'enregistrer la configuration du journal d'audit, sinon la connexion échouera. Selon le type de serveur Syslog, vous devrez peut-être créer un hachage du certificat d'authentification client.

   Exemple : syslog-ng requiert que <hash> du certificat soit créé à l'aide de la commande `openssl x509 -noout -hash -in cert.pem`, puis, vous devez lier symboliquement le certificat d'authentification client à un fichier nommé après le <hash> .0.

7. Cliquez sur **Enregistrer** pour configurer la connexion avec votre serveur et activer la journalisation à distance.

   Vous serez redirigé vers la page journaux d'audit.

Page authentification à distance

Vous pouvez utiliser la page authentification à distance pour configurer Unified Manager pour communiquer avec votre serveur d'authentification afin d'authentifier les utilisateurs distants qui tentent de se connecter à l'interface utilisateur Web Unified Manager.

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

Après avoir sélectionné la case à cocher Activer l'authentification à distance, vous pouvez activer l'authentification à distance à l'aide d'un serveur d'authentification.

- **Service d'authentification**

  Vous permet de configurer le serveur de gestion pour authentifier les utilisateurs des fournisseurs de services d'annuaire, tels qu'Active Directory, OpenLDAP ou spécifier votre propre mécanisme d'authentification. Vous pouvez spécifier un service d'authentification uniquement si vous avez activé l'authentification à distance.

  - **Active Directory**
    - Nom de l'administrateur

      Indique le nom d'administrateur du serveur d'authentification.

    - Mot de passe

      Spécifie le mot de passe pour accéder au serveur d'authentification.

    - Nom unique de base

      Indique l'emplacement des utilisateurs distants dans le serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**.

    - Désactiver la recherche de groupes imbriqués

      Indique s'il faut activer ou désactiver l'option de recherche de groupe imbriqué. Par défaut, cette option est désactivée. Si vous utilisez Active Directory, vous pouvez accélérer l'authentification en désactivant la prise en charge des groupes imbriqués.

    - Utiliser connexion sécurisée

      Spécifie le service d'authentification utilisé pour communiquer avec les serveurs d'authentification.

  - **OpenLDAP**
    - Lier le nom unique

      Spécifie le nom distinctif de liaison utilisé avec le nom distinctif de base pour trouver des utilisateurs distants dans le serveur d'authentification.

    - Lier le mot de passe

      Spécifie le mot de passe pour accéder au serveur d'authentification.

    - Nom unique de base

Indique l'emplacement des utilisateurs distants dans le serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**.

- Utiliser connexion sécurisée

  Indique que Secure LDAP est utilisé pour communiquer avec les serveurs d'authentification LDAPS.

- **Autres**
  - Lier le nom unique

    Spécifie le nom distinctif de liaison utilisé avec le nom distinctif de base pour trouver des utilisateurs distants dans le serveur d'authentification que vous avez configuré.

  - Lier le mot de passe

    Spécifie le mot de passe pour accéder au serveur d'authentification.

  - Nom unique de base

    Indique l'emplacement des utilisateurs distants dans le serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, le nom distinctif de base est **cn=ou,dc=domaine,dc=com**.

  - Version du protocole

    Spécifie la version LDAP (Lightweight Directory Access Protocol) prise en charge par votre serveur d'authentification. Vous pouvez spécifier si la version du protocole doit être automatiquement détectée ou définir la version sur 2 ou 3.

  - Attribut de nom d'utilisateur

    Spécifie le nom de l'attribut dans le serveur d'authentification qui contient les noms de connexion utilisateur à authentifier par le serveur de gestion.

  - Attribut d'appartenance au groupe

    Spécifie une valeur qui attribue l'appartenance au groupe de serveurs de gestion aux utilisateurs distants en fonction d'un attribut et d'une valeur spécifiés dans le serveur d'authentification de l'utilisateur.

  - UGID

    Si les utilisateurs distants sont inclus en tant que membres d'un objet groupeOfUniqueNames dans le serveur d'authentification, cette option vous permet d'affecter l'appartenance au groupe de serveurs de gestion aux utilisateurs distants en fonction d'un attribut spécifié dans cet objet groupeOfUniqueNames.

  - Désactiver la recherche de groupes imbriqués

    Indique s'il faut activer ou désactiver l'option de recherche de groupe imbriqué. Par défaut, cette option est désactivée. Si vous utilisez Active Directory, vous pouvez accélérer l'authentification en désactivant la prise en charge des groupes imbriqués.

- Membre

  Indique le nom d'attribut utilisé par votre serveur d'authentification pour stocker des informations sur les membres individuels d'un groupe.

- Classe d'objets utilisateur

  Spécifie la classe d'objet d'un utilisateur dans le serveur d'authentification distant.

- Classe d'objet de groupe

  Spécifie la classe d'objet de tous les groupes du serveur d'authentification distant.

- Utiliser connexion sécurisée

  Spécifie le service d'authentification utilisé pour communiquer avec les serveurs d'authentification.

> Si vous souhaitez modifier le service d'authentification, assurez-vous de supprimer tout serveur d'authentification existant et d'ajouter de nouveaux serveurs d'authentification.

Zone serveurs d'authentification

La zone serveurs d'authentification affiche les serveurs d'authentification avec lesquels le serveur de gestion communique pour trouver et authentifier les utilisateurs distants. Les informations d'identification des utilisateurs ou groupes distants sont gérées par le serveur d'authentification.

- **Boutons de commande**

  Permet d'ajouter, de modifier ou de supprimer des serveurs d'authentification.

  - Autres

    Permet d'ajouter un serveur d'authentification.

  Si le serveur d'authentification que vous ajoutez fait partie d'une paire haute disponibilité (à l'aide de 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.

  - Modifier

    Permet de modifier les paramètres d'un serveur d'authentification sélectionné.

  - Supprimer

    Supprime les serveurs d'authentification sélectionnés.

- **Nom ou adresse IP**

  Affiche le nom d'hôte ou l'adresse IP du serveur d'authentification utilisé pour authentifier l'utilisateur sur le serveur de gestion.

- **Port**

  Affiche le numéro de port du serveur d'authentification.

- **Test d’authentification**

  Ce bouton valide la configuration de votre serveur d’authentification en authentifiant un utilisateur ou un groupe distant.

  Lors du test, si vous spécifiez uniquement le nom d’utilisateur, le serveur de gestion recherche l’utilisateur distant dans le serveur d’authentification, mais n’authentifie pas l’utilisateur. Si vous spécifiez à la fois le nom d’utilisateur et le mot de passe, le serveur de gestion recherche et authentifie l’utilisateur distant.

  Vous ne pouvez pas tester l’authentification si l’authentification à distance est désactivée.

Gestion des certificats de sécurité

Vous pouvez configurer HTTPS sur le serveur Unified Manager pour surveiller et gérer les clusters via une connexion sécurisée.

Affichage du certificat de sécurité HTTPS

Vous pouvez comparer les détails du certificat HTTPS au certificat récupéré dans votre navigateur pour vous assurer que la connexion chiffrée de votre navigateur à Unified Manager n’est pas interceptée.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d’applications ou administrateur de stockage.

L’affichage du certificat vous permet de vérifier le contenu d’un certificat régénéré ou d’afficher les noms des objets (SAN) à partir desquels vous pouvez accéder à Unified Manager.

Étape

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

   Le certificat HTTPS s’affiche en haut de la page

Si vous avez besoin d’afficher des informations plus détaillées sur le certificat de sécurité par rapport à ce qui s’affiche sur la page certificat HTTPS, vous pouvez afficher le certificat de connexion dans votre navigateur.

Téléchargement d’une demande de signature de certificat HTTPS

Vous pouvez télécharger une demande de signature de certification pour le certificat de sécurité HTTPS actuel afin de pouvoir fournir le fichier à une autorité de certification à signer. Un certificat signé par une autorité de certification contribue à prévenir les attaques de l’homme du milieu et offre une meilleure protection contre la sécurité qu’un certificat auto-signé.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d’applications.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **certificat HTTPS**.
2. Cliquez sur **Télécharger demande de signature de certificat HTTPS**.
3. Enregistrez le `<hostname>.csr` fichier.

Vous pouvez fournir le fichier à une autorité de certification pour signer, puis installer le certificat signé.

L'installation d'une autorité de certification a signé et renvoyé un certificat HTTPS

Vous pouvez télécharger et installer un certificat de sécurité une fois qu'une autorité de certification l'a signé et l'a renvoyé. Le fichier que vous téléchargez et installez doit être une version signée du certificat auto-signé existant. Un certificat signé par une autorité de certification contribue à prévenir les attaques de l'homme au milieu et offre une meilleure protection contre la sécurité qu'un certificat auto-signé.

Ce dont vous aurez besoin

Vous devez avoir effectué les actions suivantes :

- A téléchargé le fichier de demande de signature de certificat et l'a signé par une autorité de certification
- Enregistré la chaîne de certificats au format PEM
- Inclus tous les certificats de la chaîne, du certificat du serveur Unified Manager au certificat de signature racine, y compris tous les certificats intermédiaires présents

Vous devez avoir le rôle Administrateur d'applications.

> Si la validité du certificat pour lequel une RSC a été créée est supérieure à 397 jours, la validité sera réduite à 397 jours par l'AC avant de signer et de retourner le certificat

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **certificat HTTPS**.
2. Cliquez sur **installer le certificat HTTPS**.
3. Dans la boîte de dialogue qui s'affiche, cliquez sur **choisir le fichier…** pour localiser le fichier à télécharger.
4. Sélectionnez le fichier, puis cliquez sur **installer** pour l'installer.

   "Installation d'un certificat HTTPS généré à l'aide d'outils externes"

Exemple de chaîne de certificat

L'exemple suivant montre comment le fichier de chaîne de certificats peut s'afficher :

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Installation d'un certificat HTTPS généré à l'aide d'outils externes

Vous pouvez installer des certificats qui sont auto-signés ou qui sont générés à l'aide d'un outil externe tel que OpenSSL, BoringSSL, LetsEncrypt.

Vous devez charger la clé privée avec la chaîne de certificats car ces certificats sont des paires de clés publiques-privées générées par l'extérieur. Les algorithmes de paire de clés autorisés sont « RSA » et « EC ». L'option **installer le certificat HTTPS** est disponible dans la page certificats HTTPS de la section général. Le fichier que vous téléchargez doit avoir le format d'entrée suivant.

1. Clé privée du serveur appartenant à l'hôte Active IQ MU
2. Certificat du serveur correspondant à la clé privée
3. Certificat des autorités de certification en sens inverse jusqu'à la racine, qui sont utilisés pour signer le certificat ci-dessus

Format de chargement d'un certificat avec une paire de clés EC

Les courbes autorisées sont « prime256v1 » et « sept-4r1 ». Exemple de certificat avec une paire EC générée en externe :

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Format de chargement d'un certificat avec une paire de clés RSA

Les tailles de clé autorisées pour la paire de clés RSA appartenant au certificat hôte sont 2048, 3072 et 4096. Certificat avec une paire de clés **RSA générée en externe** :

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Une fois le certificat téléchargé, vous devez redémarrer l'instance Active IQ Unified Manager pour que les modifications prennent effet.

Vérifie lors du téléchargement de certificats générés en externe

Le système effectue des vérifications pendant le chargement d'un certificat généré à l'aide d'outils externes. Si l'une des vérifications échoue, le certificat est rejeté. Il existe également une validation pour les certificats générés à partir de la RSC dans le produit et pour les certificats générés à l'aide d'outils externes.

- La clé privée de l'entrée est validée par rapport au certificat hôte dans l'entrée.
- Le nom commun (CN) du certificat hôte est vérifié par rapport au FQDN de l'hôte.

- Le nom commun (CN) du certificat hôte ne doit pas être vide ou vide et ne doit pas être défini sur localhost.
- La date de début de validité ne doit pas être ultérieure et la date d'expiration de validité du certificat ne doit pas être antérieure.
- Si une autorité de certification intermédiaire ou une autorité de certification existe, la date de début de validité du certificat ne doit pas être ultérieure et la date d'expiration de la validité ne doit pas être antérieure.

> La clé privée de l'entrée ne doit pas être chiffrée. Si des clés privées sont cryptées, elles sont rejetées par le système.

Exemple 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Exemple 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Exemple 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Descriptions des pages pour la gestion des certificats

Vous pouvez utiliser la page certificat HTTPS pour afficher les certificats de sécurité actuels et générer de nouveaux certificats HTTPS.

Page certificat HTTPS

La page certificat HTTPS vous permet d'afficher le certificat de sécurité actuel, de télécharger une demande de signature de certificat, de générer un nouveau certificat HTTPS ou d'installer un nouveau certificat HTTPS.

Si vous n'avez pas généré de nouveau certificat HTTPS, le certificat qui apparaît sur cette page est le certificat qui a été généré lors de l'installation.

Boutons de commande

Les boutons de commande permettent d'effectuer les opérations suivantes :

- **Télécharger demande de signature de certificat HTTPS**

  Télécharge une demande de certification pour le certificat HTTPS actuellement installé. Votre navigateur vous invite à enregistrer le fichier <HOSTNAME>.csr pour que vous puissiez fournir le fichier à une autorité de certification à signer.

- **Installer le certificat HTTPS**

  Vous permet de télécharger et d'installer un certificat de sécurité une fois qu'une autorité de certification a signé et renvoyé ce certificat. Le nouveau certificat est en vigueur après le redémarrage du serveur de gestion.

- **Régénérer le certificat HTTPS**

  Vous permet de générer un certificat HTTPS, qui remplace le certificat de sécurité actuel. Le nouveau certificat est en vigueur après le redémarrage d'Unified Manager.

Boîte de dialogue régénérer le certificat HTTPS

La boîte de dialogue régénérer le certificat HTTPS vous permet de personnaliser les informations de sécurité, puis de générer un nouveau certificat HTTPS avec ces informations.

Les informations actuelles sur le certificat apparaissent sur cette page.

Les sélections « régénérer à l'aide des attributs de certificat actuels » et « mettre à jour les attributs de certificat actuels » vous permettent de régénérer le certificat avec les informations actuelles ou de générer un certificat avec de nouvelles informations.

- **Nom commun**

  Obligatoire. Le nom de domaine complet (FQDN) que vous souhaitez sécuriser.

  Dans les configurations haute disponibilité Unified Manager, utilisez l'adresse IP virtuelle.

- **Courriel**

  Facultatif. Une adresse e-mail pour contacter votre organisation, généralement l'adresse e-mail de l'administrateur de certificat ou DU service INFORMATIQUE.

- **Société**

  Facultatif. Généralement le nom incorporé de votre société.

- **Ministère**

  Facultatif. Le nom du service de votre entreprise.

- **Ville**

  Facultatif. La ville de votre entreprise.

- **État**

  Facultatif. L’emplacement de l’État ou de la province, non abrégé, de votre entreprise.

- **Pays**

  Facultatif. Pays de votre entreprise. Il s’agit généralement d’un code ISO à deux lettres du pays.

- **Noms alternatifs**

  Obligatoire. Noms de domaine supplémentaires non primaires pouvant être utilisés pour accéder à ce serveur en plus de l’hôte local existant ou d’autres adresses réseau. Séparez les différents noms par une virgule.

  Cochez 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.

- **TAILLE DE CLÉ (ALGORITHME CLÉ : RSA)**

  L’algorithme clé est défini sur RSA. Vous pouvez choisir parmi l’une des tailles de touches : 2048, 3072 ou 4096 bits. La taille de clé par défaut est de 2048 bits.

- * PÉRIODE DE VALIDITÉ*

  La période de validité par défaut est de 397 jours. Si vous avez effectué une mise à niveau à partir d’une version précédente, la validité du certificat peut changer.