Configurer Unified Manager pour envoyer des notifications d'alerte

Active IQ Unified Manager

NetApp
October 15, 2025

Sommaire

Configurer Unified Manager pour envoyer des notifications d’alerte

Vous pouvez configurer Unified Manager pour envoyer des notifications qui vous alertent des événements dans votre environnement. Avant de pouvoir envoyer des notifications, vous devez configurer plusieurs autres options d’Unified Manager.

Avant de commencer

Vous devez disposer du rôle d’administrateur d’application.

Après avoir déployé Unified Manager 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 d’événements.

Étapes

1. "Configurer les paramètres de notification d’événement".

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

2. "Activer 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 différents d’utilisateurs locaux ou distants et attribuer des rôles spécifiques. Lorsque vous créez une alerte, vous attribuez un utilisateur pour recevoir les notifications d’alerte.

5. "Ajouter des alertes".

   Après avoir ajouté l’adresse e-mail pour l’envoi de 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.

Configurer les paramètres de notification d’événement

Vous pouvez configurer Unified Manager pour envoyer des notifications d’alerte lorsqu’un événement est généré ou lorsqu’un événement est attribué à un utilisateur. Vous pouvez configurer le serveur SMTP utilisé pour envoyer l’alerte et définir différents mécanismes de notification. Par exemple, les notifications d’alerte peuvent être envoyées sous forme

d’e-mails ou d’interruptions SNMP.

Avant de commencer

Vous devez avoir les informations suivantes :

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

  L’adresse e-mail apparaît dans le champ « De » dans les notifications d’alerte envoyées. Si l’e-mail ne peut pas être délivré pour une raison quelconque, cette adresse e-mail est également utilisée comme destinataire du courrier non distribuable.

- 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 l’interruption 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 de trappe sortante, doivent être les mêmes pour tous les hôtes de la liste.

Vous devez disposer du rôle d’administrateur d’application ou d’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.

   Remarques :

   - Si l’adresse de l’expéditeur est pré-remplie avec l’adresse « ActiveIQUnifiedManager@localhost.com », vous devez la remplacer par une adresse e-mail réelle et fonctionnelle pour vous assurer que toutes les notifications par e-mail sont envoyées avec succès.
   - 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.
3. Cliquez sur **Enregistrer**.
4. Si vous avez sélectionné l’option **Utiliser STARTTLS** ou **Utiliser SSL**, une page de certificat s’affiche après avoir cliqué sur le bouton **Enregistrer**. Vérifiez les détails du certificat et acceptez le certificat pour enregistrer les paramètres de notification.

   Vous pouvez cliquer sur le bouton **Afficher les détails du certificat** pour afficher les détails du certificat. Si le certificat existant a expiré, décochez la case **Utiliser STARTTLS** ou **Utiliser SSL**, enregistrez les paramètres de notification, puis cochez à nouveau la case **Utiliser STARTTLS** ou **Utiliser SSL** pour afficher un nouveau certificat.

Activer 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 d’Unified Manager pour gérer les objets de stockage et les données.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application.

> 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 d'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 la communication non sécurisée et 636 comme port par défaut pour la communication sécurisée.

> 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 de l'administrateur du serveur d'authentification dans l'un des formats suivants : ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name`(en utilisant la notation LDAP appropriée) • Mot de passe administrateur • Nom distinctif de base (en utilisant la notation LDAP appropriée)
Ouvrir le LDAP	• Lier le nom distinctif (dans la notation LDAP appropriée) • Lier le mot de passe • Nom distinctif de base

Si l'authentification d'un utilisateur Active Directory prend beaucoup de temps ou expire, le serveur d'authentification met probablement beaucoup de temps à 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 une connexion sécurisée pour le serveur d'authentification, Unified Manager communique avec le serveur d'authentification à l'aide du protocole Secure Sockets Layer (SSL).

4. **Facultatif :** ajoutez des serveurs d'authentification et testez l'authentification.
5. Cliquez sur **Enregistrer**.

Désactiver les groupes imbriqués de l'authentification à distance

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

Avant de commencer

- Vous devez disposer du rôle d'administrateur d'application.
- La désactivation des groupes imbriqués s'applique uniquement 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 de 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**.

Configurer les services d'authentification

Les services d'authentification permettent l'authentification des utilisateurs distants ou des groupes distants dans un serveur d'authentification avant de leur fournir l'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.

Avant de commencer

- Vous devez avoir activé l'authentification à distance.
- Vous devez disposer du rôle d'administrateur d'application.

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 fais ceci…
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, alors le nom distinctif de base est **cn=ou,dc=domain,dc=com**.
OpenLDAP	a. Saisissez le nom distinctif 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, alors le nom distinctif de base est **cn=ou,dc=domain,dc=com**.
Autres	a. Saisissez le nom distinctif 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, alors le nom distinctif de base est **cn=ou,dc=domain,dc=com**. c. Spécifiez la version du protocole LDAP prise en charge par le serveur d'authentification. d. Saisissez le nom d'utilisateur, l'appartenance au groupe, le groupe d'utilisateurs et les attributs du membre.

Si vous souhaitez modifier le service d'authentification, vous devez supprimer tous les serveurs d'authentification existants, puis ajouter de nouveaux serveurs d'authentification.

3. Cliquez sur **Enregistrer**.

Ajouter des 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 du serveur d'authentification puissent accéder à Unified Manager.

Avant de commencer

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

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. Activer ou désactiver l'option **Utiliser une connexion sécurisée** :

Si vous voulez…	Alors fais ceci…
Activez-le	a. Sélectionnez l'option **Utiliser une 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 du 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 par connexion sécurisée**, Unified Manager communique avec le serveur d'authentification et affiche le certificat. Unified Manager utilise le port 636 comme port par défaut pour la communication sécurisée et le numéro de port 389 pour la communication non sécurisée.

Si vous voulez…	Alors fais ceci…
Désactivez-le	a. Désactivez l'option **Utiliser une connexion sécurisée**. b. Dans la zone Serveurs d'authentification, cliquez sur **Ajouter**. c. Dans la boîte de dialogue 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.

Tester la configuration des serveurs d'authentification

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

Avant de commencer

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

Si le service d'authentification est défini sur Active Directory et si vous validez l'authentification des utilisateurs distants qui appartiennent au groupe principal du serveur d'authentification, les informations sur le groupe principal ne s'affichent pas dans les résultats d'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 Tester l'utilisateur, spécifiez le nom d'utilisateur et le mot de passe de l'utilisateur distant ou le nom d'utilisateur du groupe distant, puis cliquez sur **Tester**.

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

Ajouter des alertes

Vous pouvez configurer des alertes pour vous avertir lorsqu'un événement particulier est généré. Vous pouvez configurer des alertes pour une seule ressource, pour un groupe de

ressources ou pour des événements d'un type de gravité particulier. Vous pouvez spécifier la fréquence à laquelle vous souhaitez être notifié et associer un script à l'alerte.

Avant de commencer

- Vous devez avoir configuré les 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 les adresses e-mail des utilisateurs que vous souhaitez notifier.
- Si vous souhaitez qu'un script s'exécute en fonction de l'événement, vous devez avoir ajouté le script à Unified Manager à l'aide de la page Scripts.
- Vous devez disposer du rôle d'administrateur d'application ou d'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 des alertes, comme décrit ici.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des alertes**.
2. Dans la page Configuration des alertes, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter une alerte, cliquez sur **Nom** et saisissez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources** et 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 **Le nom contient** pour sélectionner un groupe de ressources. En fonction de la chaîne de texte que vous spécifiez, la liste des ressources disponibles affiche uniquement 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 aux règles d'inclusion et d'exclusion que vous avez spécifiées, la règle d'exclusion a priorité sur la règle d'inclusion et l'alerte n'est pas générée pour les événements liés à la ressource exclue.

5. Cliquez sur **Événements** et sélectionnez les événements en fonction du nom de l'événement ou du type de gravité de l'événement pour lesquels 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 attribuez 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 précédemment sélectionné. De plus, 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 des interruptions SNMP.

7. Cliquez sur **Enregistrer**.

Exemple d'ajout d'une alerte

Cet exemple montre comment créer une alerte qui répond 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 notifié toutes les 15 minutes

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

Étapes

1. Cliquez sur **Nom** et saisissez **HealthTest** dans le champ **Nom de l'alerte**.
2. Cliquez sur **Ressources** et dans l'onglet Inclure, sélectionnez **Volumes** dans la liste déroulante.
   a. Saisissez **abc** dans le champ **Le nom 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-le vers la zone Ressources sélectionnées.
   c. Cliquez sur **Exclure**, saisissez **xyz** dans le champ **Le nom contient**, puis cliquez sur **Ajouter**.
3. Cliquez sur **Événements** et sélectionnez **Critique** dans le champ Gravité de l'événement.
4. Sélectionnez **Tous les événements critiques** dans la zone Événements correspondants et déplacez-les vers la zone Événements sélectionnés.
5. Cliquez sur **Actions** et saisissez **sample@domain.com** dans le champ Alerter ces utilisateurs.
6. Sélectionnez **Rappeler toutes les 15 minutes** pour avertir l'utilisateur toutes les 15 minutes.

   Vous pouvez configurer une alerte pour envoyer des notifications répétées aux destinataires pendant une durée spécifiée. Vous devez déterminer l'heure à partir de laquelle la notification d'événement est active pour l'alerte.

7. Dans le menu Sélectionner le script à exécuter, sélectionnez le script **Tester**.
8. Cliquez sur **Enregistrer**.

Informations sur le copyright

Informations sur les marques commerciales