



Gestion de l'authentification

Active IQ Unified Manager 9.9

NetApp
October 22, 2024

Sommaire

Gestion de l'authentification	1
Activation de l'authentification à distance	1
Désactivation des groupes imbriqués à partir de l'authentification à distance	2
Configuration des services d'authentification	3
Ajout de serveurs d'authentification	4
Test de la configuration des serveurs d'authentification	6
Modification des serveurs d'authentification	6
Suppression des serveurs d'authentification	7
Authentification avec Active Directory ou OpenLDAP	7
Activation de l'authentification SAML	8
Exigences du fournisseur d'identités	9
Modification du fournisseur d'identités utilisé pour l'authentification SAML	10
Désactivation de l'authentification SAML	11
Consignation d'audits	12
Description des fenêtres d'authentification et des boîtes de dialogue	15

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.

Vous pouvez également activer l'authentification SAML pour que les utilisateurs distants soient authentifiés par un fournisseur d'identités sécurisé avant de se connecter à l'interface utilisateur Web Unified Manager.

Activation de l'authentification à distance

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

Avant de commencer

Vous devez avoir le rôle Administrateur d'applications.



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

Description de la tâche

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

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



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

Étapes

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

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

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

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

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

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

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

Avant de commencer

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

Description de la tâche

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

auprès d'Unified Manager.

Étapes

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

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.

Avant de commencer

- 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	<ol style="list-style-type: none">1. Entrez le nom et le mot de passe de l'administrateur.2. Spécifiez le nom distinctif de base du serveur d'authentification. <p>Par exemple, si le nom de domaine du serveur d'authentification est <code>ou@domain.com</code>, le nom distinctif de base est <code>cn=ou,dc=domain,dc=com</code>.</p>
OpenLDAP	<ol style="list-style-type: none">1. Entrez le nom distinctif de liaison et le mot de passe de liaison.2. Spécifiez le nom distinctif de base du serveur d'authentification. <p>Par exemple, si le nom de domaine du serveur d'authentification est <code>ou@domain.com</code>, le nom distinctif de base est <code>cn=ou,dc=domain,dc=com</code>.</p>

Si vous sélectionnez...	Alors, procédez comme ça...
Autres	<ol style="list-style-type: none"> 1. Entrez le nom distinctif de liaison et le mot de passe de liaison. 2. Spécifiez le nom distinctif de base du serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est <code>ou@domain.com</code>, le nom distinctif de base est <code>cn=ou,dc=domain,dc=com</code>. 3. Spécifiez la version du protocole LDAP prise en charge par le serveur d'authentification. 4. 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.

1. Cliquez sur **Enregistrer**.

Ajout de serveurs d'authentification

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

Avant de commencer

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


Description de la tâche

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

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général > authentification à distance**.

2. Activez ou désactivez l'option **utiliser la connexion sécurisée** :

Les fonctions que vous recherchez...	Alors, procédez comme ça...
Activez-la	<ol style="list-style-type: none">1. Sélectionnez l'option utiliser connexion sécurisée.2. Dans la zone serveurs d'authentification, cliquez sur Ajouter.3. Dans la boîte de dialogue Ajouter un serveur d'authentification, entrez le nom d'authentification ou l'adresse IP (IPv4 ou IPv6) du serveur.4. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur Afficher le certificat.5. Dans la boîte de dialogue Afficher le certificat, vérifiez les informations sur le certificat, puis cliquez sur Fermer.6. Dans la boîte de dialogue Autoriser l'hôte, cliquez sur Oui. <div data-bbox="987 814 1490 1176" style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;"><p>Lorsque vous activez l'option utiliser l'authentification Secure Connection, Unified Manager communique avec le serveur d'authentification et affiche le certificat. Unified Manager utilise 636 comme port par défaut pour les communications sécurisées et le port numéro 389 pour les communications non sécurisées.</p></div>
Désactivez-le	<ol style="list-style-type: none">1. Désactivez l'option utiliser connexion sécurisée.2. Dans la zone serveurs d'authentification, cliquez sur Ajouter.3. Dans la boîte de dialogue Add Authentication Server (Ajouter un serveur d'authentification), spécifiez le nom d'hôte ou l'adresse IP (IPv4 ou IPv6) du serveur, ainsi que les détails du port.4. Cliquez sur Ajouter.

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

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

Test de la configuration des serveurs d'authentification

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

Avant de commencer

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

Description de la tâche

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

Étapes

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

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

Modification des serveurs d'authentification

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

Avant de commencer

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.

Avant de commencer

Vous devez avoir le rôle Administrateur d'applications.

Description de la tâche

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.

Activation de l'authentification SAML

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

Avant de commencer

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

Description de la tâche

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

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



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

Étapes

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

Les champs requis pour configurer la connexion IDP sont affichés.

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

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

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

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

5. Cliquez sur **Enregistrer**.

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

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

Résultats

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

Une fois que vous avez terminé

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



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

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 Manager SAML 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 :
 - Ouvrez la console de gestion ADFS.
 - Cliquez sur le dossier Authentication Policies dans l'arborescence de gauche.
 - Sous actions à droite, cliquez sur Modifier la stratégie d'authentification principale globale.
 - 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.

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.

Avant de commencer

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

Description de la tâche

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**.

Une fois que vous avez terminé

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.

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.

Description de la tâche

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.

Résultats

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.

Une fois que vous avez terminé

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

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.
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 .zip 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.

Description de la tâche

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.

Description de la tâche

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 falsifiés.

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.

Description des fenêtres d'authentification et des boîtes de dialogue

Vous pouvez activer l'authentification LDAP à partir de la page Configuration/authentification.

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=domain,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=domain,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=domain,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.

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.

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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