Gestion de l'authentification

Active IQ Unified Manager

NetApp
June 23, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager/config/task_edit_authentication_servers.html on June 23, 2025. Always check docs.netapp.com for the latest.

Sommaire

Gestion de l’authentification . . . 1
- Modification des serveurs d’authentification . . . 1
- Suppression des serveurs d’authentification . . . 1
- Authentification avec Active Directory ou OpenLDAP . . . 2
- Consignation d’audits . . . 2
  - Configuration des journaux d’audit . . . 3
  - Activation de la journalisation à distance des journaux d’audit . . . 4
- Page authentification à distance . . . 5
  - Zone serveurs d’authentification . . . 7

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.

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.

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 **Audit Log: File View** pour afficher et accéder à tous les fichiers journaux d'audit disponibles dans votre 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.

État	Description
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 `.gzip` format.

Les fichiers journaux d'audit sont archivés régulièrement et enregistrés dans la base de données pour référence. Avant l'archivage, les journaux d'audit sont signés numériquement afin de préserver la sécurité et l'intégrité.

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.

   La valeur **Connection Timeout** peut affecter la configuration. Si la réponse de la configuration est plus longue que la valeur définie, elle peut entraîner une défaillance de la configuration en raison d'une erreur de connexion. Pour établir une connexion réussie, augmentez la valeur **Connection Timeout** et réessayez la configuration.

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 LDAP.

◦ **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.

  Les valeurs que vous entrez pour les attributs *Member*, *User Object Class* et *Group Object Class* doivent être identiques à celles ajoutées dans vos configurations Active Directory, OpenLDAP et LDAP. Dans le cas contraire, l'authentification pourrait échouer.

- 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.

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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