Journalisation d'audit

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-918/config/concept_audit_logging.html on November 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Journalisation d’audit 1
Découvrez les journaux d’audit dans Active IQ Unified Manager 1
Configurer les journaux d’audit d’Active IQ Unified Manager 2
Activer la journalisation à distance des journaux d’audit dans Active IQ Unified Manager 2

Journalisation d’audit

Découvrez les journaux d’audit dans Active IQ Unified Manager

Vous pouvez détecter si le journal des audits a été compromis en utilisant Audit Logs. Toutes les activités effectuées par un utilisateur sont surveillées et consignées dans Audit Logs. Les audits sont effectués pour toutes les fonctionnalités de l’interface utilisateur et des API exposées publiquement de Active IQ Unified Manager.

Vous pouvez utiliser la vue **Journal des audits : fichier** pour afficher et consulter tous les fichiers du journal des audits disponibles dans votre Active IQ Unified Manager. Les fichiers de la vue Journal des audits : fichier sont répertoriés en fonction de leur date de création. Cette vue affiche les informations de tous les journaux des audits capturés dans le système depuis l’installation ou la mise à niveau jusqu’à aujourd’hui. 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 “File Integrity Status”, qui est surveillé activement pour détecter toute altération ou suppression du fichier journal. Les journaux des audits peuvent avoir l’un des états suivants lorsqu’ils sont disponibles dans le système :

État	Description
ACTIVE	Fichier dans lequel les journaux sont actuellement enregistrés.
NORMAL	Fichier inactif, compressé et stocké dans le système.
ALTÉRÉ	Fichier compromis par un utilisateur qui l’a modifié manuellement.
MANUAL_DELETE	Fichier supprimé par un utilisateur autorisé.
ROLLOVER_DELETE	Fichier supprimé en raison d’une rotation conformément à la stratégie de configuration de rotation.
SUPPRESSION_INATTENDUE	Fichier supprimé pour des raisons inconnues.

La page Journal des audits comprend les boutons de commande suivants :

- Configurer
- Supprimer
- Télécharger

Le bouton **DELETE** vous permet de supprimer n’importe lequel des journaux des audits répertoriés dans la vue Audit Logs. Vous pouvez supprimer un journal des audits et, si vous le souhaitez, indiquer le motif de la suppression du fichier, ce qui aidera ultérieurement à déterminer si la suppression était valide. La colonne REASON répertorie le motif ainsi que le nom de l’utilisateur qui a effectué l’opération de suppression.

La suppression d’un fichier journal supprime le fichier du système, mais pas l’entrée correspondante dans la table de la base de données.

Vous pouvez télécharger les journaux des audits depuis Active IQ Unified Manager à l’aide du bouton **TÉLÉCHARGER** dans la section Journaux des audits et exporter les fichiers de journal des audits. Les fichiers

marqués « NORMAL » ou « TAMPERED » sont téléchargés au format .gzip compressé.

Les fichiers du journal des audits sont archivés périodiquement et enregistrés dans la base de données à titre de référence. Avant leur archivage, les journaux des audits sont signés numériquement afin de garantir leur sécurité et leur intégrité.

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

Configurer les journaux d'audit d'Active IQ Unified Manager

Vous pouvez utiliser le bouton **Configure** dans la section Journal des audits pour configurer la politique de rotation des fichiers du journal des audits et activer également la journalisation à distance pour le journal des audits.

Vous pouvez définir les valeurs de **MAX FILE SIZE** et de **AUDIT LOG RETENTION DAYS** en fonction de la quantité et de la fréquence des données que vous souhaitez stocker dans le système. La valeur du champ **TOTAL AUDIT LOG SIZE** correspond à la taille totale des données du journal des audits présentes dans le système. La politique de rotation est déterminée par les valeurs des champs **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** et **TOTAL AUDIT LOG SIZE**. Lorsque la taille de la sauvegarde du journal des audits atteint la valeur configurée dans **TOTAL AUDIT LOG SIZE**, le fichier archivé en premier est supprimé. Cela signifie que le fichier le plus ancien est supprimé. Cependant, l'entrée du fichier reste disponible dans la base de données et est marquée comme "Rollover Delete". La valeur de **AUDIT LOG RETENTION DAYS** correspond au nombre de jours pendant lesquels les fichiers du journal des audits sont conservés. Tout fichier plus ancien que la valeur définie dans ce champ fait l'objet d'une rotation.

Étapes

1. Cliquez sur **Journaux des audits** > > **Configurer**.
2. Saisissez les valeurs dans les champs **TAILLE MAXIMALE DU FICHIER**, **TAILLE TOTALE DU JOURNAL DES AUDITS** et **JOURS DE CONSERVATION DU JOURNAL DES AUDITS**.

   Pour activer la journalisation à distance, sélectionnez **Activer la journalisation à distance**.

Activer la journalisation à distance des journaux d'audit dans Active IQ Unified Manager

Vous pouvez cocher la case **Enable Remote Logging** dans la boîte de dialogue Configure Audit Logs pour activer la journalisation à distance. Vous pouvez utiliser cette fonctionnalité pour transférer les journaux des audits vers un serveur Syslog distant. Cela vous permettra de gérer vos journaux des audits en cas de contraintes d'espace.

La journalisation à distance des journaux des audits fournit une sauvegarde inviolable au cas où les fichiers du journal des audits sur le serveur Active IQ Unified Manager seraient altérés.

Étapes

1. Dans la boîte de dialogue **Configurer les journaux des audits**, cochez la case **Activer la journalisation à distance**.

   Des champs supplémentaires pour configurer la journalisation à distance s'affichent.

2. Saisissez le **nom de l'hôte** et le **PORT** du serveur distant auquel vous souhaitez vous connecter.
3. Dans le champ **CERTIFICAT D'AC DU SERVEUR**, cliquez sur **PARCOURIR** pour sélectionner un certificat public du serveur cible.

   Le certificat doit être téléchargé au format `.pem`. Ce certificat doit être obtenu à partir du serveur Syslog cible et ne doit pas avoir expiré. Le certificat doit contenir le "hostname" sélectionné dans l'attribut `SubjectAltName` (SAN).

4. Saisissez les valeurs pour les champs suivants : **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   Les valeurs de ces champs doivent être exprimées en millisecondes.

5. Sélectionnez le format Syslog requis et la version requise du protocole TLS dans les champs **FORMAT** et **PROTOCOL**.
6. Cochez la case **Activer l'authentification de clients** si le serveur Syslog cible requiert une authentification basée sur des certificats.

   Vous devrez télécharger le certificat d'authentification de clients et le charger 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 de clients.

   Exemple : syslog-ng exige qu'un <hash> du certificat soit créé à l'aide de la commande `openssl x509 -noout -hash -in cert.pem`, puis vous devez créer un lien symbolique vers le certificat d'authentification de clients dans un fichier nommé d'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 des journaux d'audit.

> ⓘ La valeur de **Connection Timeout** peut affecter la configuration. Si la configuration met plus de temps à répondre que la valeur définie, cela peut entraîner un échec de la configuration en raison d'une erreur de connexion. Pour établir une connexion réussie, augmentez la valeur de **Connection Timeout** et réessayez la configuration.

Informations sur le copyright

Copyright © 2026 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.