



Gérer syslog

SANtricity 11.8

NetApp
December 16, 2024

Sommaire

- Gérer syslog 1
 - Afficher l'activité du journal d'audit 1
 - Définissez des règles de journal d'audit 3
 - Supprimer des événements du journal d'audit 4
 - Configuration du serveur syslog pour les journaux d'audit 5
 - Modifier les paramètres du serveur syslog pour les enregistrements du journal d'audit 6

Gérer syslog

Afficher l'activité du journal d'audit

En affichant les journaux d'audit, les utilisateurs disposant d'autorisations d'administrateur de sécurité peuvent surveiller les actions des utilisateurs, les échecs d'authentification, les tentatives de connexion non valides et la durée de vie des sessions utilisateur.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.



Étapes

1. Sélectionnez **Paramètres** > **gestion des accès**.
2. Sélectionnez l'onglet **Journal d'audit**.

L'activité du journal d'audit s'affiche sous forme de tableau, qui contient les colonnes d'informations suivantes :

- **Date/heure** — horodatage du moment où la matrice de stockage a détecté l'événement (en GMT).
 - **Nom d'utilisateur** — le nom d'utilisateur associé à l'événement. Pour toute action non authentifiée sur la matrice de stockage, « N/A » apparaît comme nom d'utilisateur. Les actions non authentifiées peuvent être déclenchées par le proxy interne ou un autre mécanisme.
 - **Code d'état** — Code d'état HTTP de l'opération (200, 400, etc.) et texte descriptif associé à l'événement.
 - **URL accédée** — URL complète (y compris l'hôte) et chaîne de requête.
 - **Adresse IP du client** — adresse IP du client associé à l'événement.
 - **Source** — Source de consignation associée à l'événement, qui peut être System Manager, CLI, Web Services ou support Shell.
 - **Description** — informations supplémentaires sur l'événement, le cas échéant.
3. Utilisez les sélections de la page Journal d'audit pour afficher et gérer les événements.

Détails de la sélection

| Sélection | Description |
|---|--|
| Afficher les événements du... | Événements de limite indiqués par plage de dates (24 dernières heures, 7 derniers jours, 30 derniers jours ou une plage de dates personnalisée). |
| Filtre | Limiter les événements indiqués par les caractères saisis dans le champ. Utilisez des guillemets ("") pour une correspondance exacte de mot, entrez OR pour retourner un ou plusieurs mots ou entrez un tiret (—) pour omettre des mots. |
| Actualisez | Sélectionnez Actualiser pour mettre à jour la page avec les événements les plus courants. |
| Afficher/modifier les paramètres | Sélectionnez Afficher/Modifier les paramètres pour ouvrir une boîte de dialogue qui vous permet de spécifier une stratégie de journalisation complète et le niveau d'actions à enregistrer. |
| Supprimer des événements | Sélectionnez Supprimer pour ouvrir une boîte de dialogue qui vous permet de supprimer d'anciens événements de la page. |
| Afficher/masquer les colonnes | <p>Cliquez sur l'icône de colonne Afficher/Masquer  pour sélectionner d'autres colonnes à afficher dans le tableau. Les colonnes supplémentaires incluent :</p> <ul style="list-style-type: none">• Méthode — la méthode HTTP (PAR exemple, POST, GET, DELETE, etc.).• Commande CLI exécutée — la commande CLI (grammaire) exécutée pour les requêtes Secure CLI.• CLI Return Status — Un code d'état CLI ou une demande de fichiers d'entrée du client.• Symbole procédure — la procédure de symbole exécutée.• Type d'événement SSH — Type d'événements Secure Shell (SSH), tels que login, logout et login_fail.• SSH session PID — Numéro d'ID de processus de la session SSH.• Durée(s) de session SSH — nombre de secondes pendant lesquelles l'utilisateur a été connecté.• Type d'authentification — les types peuvent inclure l'utilisateur local, LDAP, SAML et le jeton d'accès.• ID d'authentification — ID de la session authentifiée. |
| Activer/désactiver les filtres de colonne | Cliquez sur l'icône Toggle  pour ouvrir les champs de filtrage pour chaque colonne. Entrez des caractères dans un champ de colonne pour limiter les événements affichés par ces caractères. Cliquez à nouveau sur l'icône pour fermer les champs de filtrage. |

| Sélection | Description |
|---------------------------|---|
| Annuler les modifications | Cliquez sur l'icône Annuler  pour rétablir la configuration par défaut de la table. |
| Exporter | Cliquez sur Exporter pour enregistrer les données de la table dans un fichier CSV (valeurs séparées par des virgules). |

Définissez des règles de journal d'audit

Vous pouvez modifier la stratégie d'écrasement et les types d'événements enregistrés dans le journal d'audit.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Description de la tâche

Cette tâche décrit comment modifier les paramètres du journal d'audit, qui incluent la stratégie de remplacement des anciens événements et la stratégie d'enregistrement des types d'événements.



Étapes

1. Sélectionnez **Paramètres** > **gestion des accès**.
2. Sélectionnez l'onglet **Journal d'audit**.
3. Sélectionnez **Afficher/Modifier les paramètres**.

La boîte de dialogue Paramètres du journal d'audit s'ouvre.

4. Modifiez la politique de remplacement ou les types d'événements enregistrés.

Détails du champ

| Réglage | Description |
|--------------------------------|--|
| Politique d'écrasement | <p>Détermine la stratégie d'écrasement des anciens événements lorsque la capacité maximale est atteinte :</p> <ul style="list-style-type: none">• Permettre l'écrasement des événements les plus anciens du journal d'audit lorsque le journal d'audit est plein — écrase les anciens événements lorsque le journal d'audit atteint 50,000 enregistrements.• Exiger la suppression manuelle des événements du journal d'audit — indique que les événements ne seront pas automatiquement supprimés ; un avertissement de seuil apparaît au pourcentage défini. Les événements doivent être supprimés manuellement. <p> Si la stratégie de remplacement est désactivée et que les entrées du journal d'audit atteignent la limite maximale, l'accès à System Manager est refusé aux utilisateurs sans les autorisations d'administrateur de sécurité. Pour restaurer l'accès au système aux utilisateurs sans autorisations d'administrateur de sécurité, un utilisateur affecté au rôle d'administrateur de sécurité doit supprimer les anciens enregistrements d'événements.</p> <p> Les règles d'écrasement ne s'appliquent pas si un serveur syslog est configuré pour l'archivage des journaux d'audit.</p> |
| Niveau des actions à consigner | <p>Détermine les types d'événements à enregistrer :</p> <ul style="list-style-type: none">• Événements de modification d'enregistrement uniquement — affiche uniquement les événements où une action utilisateur implique d'effectuer un changement dans le système.• Enregistrer tous les événements de modification et de lecture seule — affiche tous les événements, y compris une action utilisateur qui implique la lecture ou le téléchargement d'informations. |

5. Cliquez sur **Enregistrer**.

Supprimer des événements du journal d'audit

Vous pouvez effacer le journal d'audit des anciens événements, ce qui facilite la recherche à travers les événements. Vous avez la possibilité d'enregistrer les anciens événements dans un fichier CSV (valeurs séparées par des virgules) lors de la suppression.

Avant de commencer

Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.

Étapes

1. Sélectionnez **Paramètres > gestion des accès**.
2. Sélectionnez l'onglet **Journal d'audit**.
3. Sélectionnez **Supprimer**.

La boîte de dialogue Supprimer le journal d'audit s'ouvre.

4. Sélectionnez ou entrez le nombre d'événements les plus anciens que vous souhaitez supprimer.
5. Si vous souhaitez exporter les événements supprimés dans un fichier CSV (recommandé), cochez la case. Vous êtes invité à saisir un nom de fichier et un emplacement lorsque vous cliquez sur **Supprimer** à l'étape suivante. Sinon, si vous ne souhaitez pas enregistrer les événements dans un fichier CSV, cochez la case pour le désélectionner.
6. Cliquez sur **Supprimer**.

Une boîte de dialogue de confirmation s'ouvre.

7. Saisissez `delete` le champ, puis cliquez sur **Supprimer**.

Les événements les plus anciens sont supprimés de la page Journal d'audit.

Configuration du serveur syslog pour les journaux d'audit

Si vous souhaitez archiver les journaux d'audit sur un serveur syslog externe, vous pouvez configurer les communications entre ce serveur et la matrice de stockage. Une fois la connexion établie, les journaux d'audit sont automatiquement enregistrés sur le serveur syslog.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- L'adresse, le protocole et le numéro de port du serveur syslog doivent être disponibles. L'adresse du serveur peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Si votre serveur utilise un protocole sécurisé (par exemple TLS), un certificat d'autorité de certification (CA) doit être disponible sur votre système local. Les certificats CA identifient les propriétaires de sites Web pour des connexions sécurisées entre serveurs et clients.

Étapes

1. Sélectionnez **Paramètres > gestion des accès**.
2. Dans l'onglet Journal d'audit, sélectionnez **configurer les serveurs Syslog**.

La boîte de dialogue configurer les serveurs Syslog s'ouvre.

3. Cliquez sur **Ajouter**.

La boîte de dialogue Ajouter un serveur Syslog s'ouvre.

4. Entrez les informations relatives au serveur, puis cliquez sur **Ajouter**.

- **Adresse du serveur** — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- **Protocole** — sélectionnez un protocole dans la liste déroulante (par exemple, TLS, UDP ou TCP).
- **Télécharger le certificat (facultatif)** — si vous avez sélectionné le protocole TLS et que vous n'avez pas encore téléchargé de certificat d'autorité de certification signé, cliquez sur **Parcourir** pour télécharger un fichier de certificat. Les journaux d'audit ne sont pas archivés sur un serveur syslog sans certificat de confiance.



Si le certificat devient non valide ultérieurement, l'établissement de liaison TLS échouera. Par conséquent, un message d'erreur est affiché dans le journal d'audit et les messages ne sont plus envoyés au serveur syslog. Pour résoudre ce problème, vous devez corriger le certificat sur le serveur syslog, puis aller dans le menu Paramètres[Journal d'audit > configurer les serveurs Syslog > tout tester].

- **Port** — Entrez le numéro de port du récepteur syslog. Après avoir cliqué sur **Ajouter**, la boîte de dialogue configurer les serveurs Syslog s'ouvre et affiche votre serveur syslog configuré sur la page.

5. Pour tester la connexion du serveur avec la matrice de stockage, sélectionnez **Tester tout**.

Résultats

Après la configuration, tous les nouveaux journaux d'audit sont envoyés au serveur syslog. Les journaux précédents ne sont pas transférés. Pour configurer davantage les paramètres syslog des alertes, reportez-vous à la section "[Configurer le serveur syslog pour les alertes](#)".

NOTE: If multiple syslog servers are configured, all configured syslog servers will receive an audit log.

Modifier les paramètres du serveur syslog pour les enregistrements du journal d'audit

Vous pouvez modifier les paramètres du serveur syslog utilisé pour l'archivage des journaux d'audit et télécharger également un nouveau certificat d'autorité de certification (CA) pour le serveur.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- L'adresse, le protocole et le numéro de port du serveur syslog doivent être disponibles. L'adresse du serveur peut être un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
- Si vous téléchargez un nouveau certificat d'autorité de certification, celui-ci doit être disponible sur votre système local.

Étapes

1. Sélectionnez **Paramètres > gestion des accès**.
2. Dans l'onglet Journal d'audit, sélectionnez **configurer les serveurs Syslog**.

Les serveurs syslog configurés sont affichés sur la page.

3. Pour modifier les informations sur le serveur, sélectionnez l'icône **Modifier** (crayon) à droite du nom du serveur, puis apportez les modifications souhaitées dans les champs suivants :
 - **Adresse du serveur** — Entrez un nom de domaine complet, une adresse IPv4 ou une adresse IPv6.
 - **Protocole** — sélectionnez un protocole dans la liste déroulante (par exemple, TLS, UDP ou TCP).
 - **Port** — Entrez le numéro de port du récepteur syslog.
4. Si vous avez modifié le protocole en protocole TLS sécurisé (UDP ou TCP), cliquez sur **Importer un certificat approuvé** pour télécharger un certificat d'autorité de certification.
5. Pour tester la nouvelle connexion avec la matrice de stockage, sélectionnez **Tester tout**.

Résultats

Après la configuration, tous les nouveaux journaux d'audit sont envoyés au serveur syslog. Les journaux précédents ne sont pas transférés.

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 DÉLICTEUELLE (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.