Gérer les objectifs de sécurité du cluster

Active IQ Unified Manager

NetApp
October 15, 2025

Sommaire

Gérer les objectifs de sécurité du cluster

Unified Manager fournit un tableau de bord qui identifie le niveau de sécurité de vos clusters ONTAP , de vos machines virtuelles de stockage (SVM) et de vos volumes en fonction des recommandations définies dans le *Guide de renforcement de la sécurité NetApp pour ONTAP 9*.

L'objectif du tableau de bord de sécurité est d'afficher les zones dans lesquelles vos clusters ONTAP ne sont pas conformes aux directives recommandées par NetApp afin que vous puissiez résoudre ces problèmes potentiels. Dans la plupart des cas, vous résoudrez les problèmes à l'aide ONTAP System Manager ou de l' ONTAP CLI. Il est possible que votre organisation ne suive pas toutes les recommandations. Dans certains cas, vous n'aurez donc pas besoin d'apporter de modifications.

Voir le "Guide de renforcement de la sécurité NetApp pour ONTAP 9" (TR-4569) pour des recommandations et des résolutions détaillées.

En plus de signaler l'état de sécurité, Unified Manager génère également des événements de sécurité pour tout cluster ou SVM présentant des violations de sécurité. Vous pouvez suivre ces problèmes dans la page d'inventaire de gestion des événements et vous pouvez configurer des alertes pour ces événements afin que votre administrateur de stockage soit averti lorsque de nouveaux événements de sécurité se produisent.

Pour plus d'informations, voir "Quels critères de sécurité sont évalués".

Quels critères de sécurité sont évalués

En général, les critères de sécurité de vos clusters ONTAP , machines virtuelles de stockage (SVM) et volumes sont évalués par rapport aux recommandations définies dans le *Guide de renforcement de la sécurité NetApp pour ONTAP 9*.

Certains des contrôles de sécurité comprennent :

- si un cluster utilise une méthode d'authentification sécurisée, telle que SAML
- si les clusters appairés ont leur communication cryptée
- si le journal d'audit d'une machine virtuelle de stockage est activé
- si vos volumes ont un cryptage logiciel ou matériel activé

Consultez les rubriques sur les catégories de conformité et les "Guide de renforcement de la sécurité NetApp pour ONTAP 9" pour des informations détaillées.

> Les événements de mise à niveau signalés par la plateforme Active IQ sont également considérés comme des événements de sécurité. Ces événements identifient les problèmes pour lesquels la résolution nécessite la mise à niveau du logiciel ONTAP , du micrologiciel du nœud ou du logiciel du système d'exploitation (pour les avis de sécurité). Ces événements ne sont pas affichés dans le panneau Sécurité, mais ils sont disponibles à partir de la page d'inventaire Gestion des événements.

Pour plus d'informations, voir "Gestion des objectifs de sécurité des clusters".

Catégories de conformité des clusters

Ce tableau décrit les paramètres de conformité de sécurité du cluster évalués par Unified Manager, la recommandation NetApp et si le paramètre affecte la détermination globale de la conformité ou non du cluster.

La présence de SVM non conformes sur un cluster affectera la valeur de conformité du cluster. Ainsi, dans certains cas, vous devrez peut-être résoudre des problèmes de sécurité avec une SVM avant que la sécurité de votre cluster ne soit considérée comme conforme.

Notez que tous les paramètres répertoriés ci-dessous n'apparaissent pas pour toutes les installations. Par exemple, si vous n'avez pas de clusters appairés ou si vous avez désactivé AutoSupport sur un cluster, vous ne verrez pas les éléments Cluster Peering ou AutoSupport HTTPS Transport dans la page de l'interface utilisateur.

Paramètre	Description	Recommandation	Affecte la conformité du cluster
FIPS mondial	Indique si le mode de conformité Global FIPS (Federal Information Processing Standard) 140-2 est activé ou désactivé. Lorsque FIPS est activé, TLSv1 et SSLv3 sont désactivés et seuls TLSv1.1 et TLSv1.2 sont autorisés.	Activé	Oui
Telnet	Indique si l'accès Telnet au système est activé ou désactivé. NetApp recommande Secure Shell (SSH) pour un accès à distance sécurisé.	Désactivées	Oui
Paramètres SSH non sécurisés	Indique si SSH utilise des chiffrements non sécurisés, par exemple des chiffrements commençant par *cbc.	Non	Oui
Bannière de connexion	Indique si la bannière de connexion est activée ou désactivée pour les utilisateurs accédant au système.	Activé	Oui

Paramètre	Description	Recommandation	Affecte la conformité du cluster
Appairage de cluster	Indique si la communication entre les clusters homologues est chiffrée ou non chiffrée. Le chiffrement doit être configuré sur les clusters source et de destination pour que ce paramètre soit considéré comme conforme.	Crypté	Oui
Protocole de temps réseau	Indique si le cluster dispose d'un ou plusieurs serveurs NTP configurés. Pour la redondance et un meilleur service, NetApp recommande d'associer au moins trois serveurs NTP au cluster.	Configuré	Oui
Protocole OCSP	À partir de la version 9.14.1, Active IQ Unified Manager fournit des informations sur l'état du protocole OCSP (Online Certificate Status Protocol) au niveau de la machine virtuelle de stockage (SVM, anciennement appelée Vserver). Cela signifie que la validation OCSP est appliquée à toutes les connexions SSL/TLS établies avec le SVM et garantit l'intégrité et la validité des certificats utilisés dans ces connexions.	Activé	Non
Journalisation d'audit à distance	Indique si la transmission du journal (Syslog) est chiffrée ou non.	Crypté	Oui

Paramètre	Description	Recommandation	Affecte la conformité du cluster
Transport HTTPS AutoSupport	Indique si HTTPS est utilisé comme protocole de transport par défaut pour l'envoi de messages AutoSupport au support NetApp .	Activé	Oui
Utilisateur administrateur par défaut	Indique si l'utilisateur administrateur par défaut (intégré) est activé ou désactivé. NetApp recommande de verrouiller (désactiver) tous les comptes intégrés inutiles.	Désactivées	Oui
Utilisateurs SAML	Indique si SAML est configuré. SAML vous permet de configurer l'authentification multifacteur (MFA) comme méthode de connexion pour l'authentification unique.	Non	Non
Utilisateurs Active Directory	Indique si Active Directory est configuré. Active Directory et LDAP sont les mécanismes d'authentification préférés pour les utilisateurs accédant aux clusters.	Non	Non
Utilisateurs LDAP	Indique si LDAP est configuré. Active Directory et LDAP sont les mécanismes d'authentification préférés des utilisateurs gérant des clusters par rapport aux utilisateurs locaux.	Non	Non
Utilisateurs de certificats	Indique si un utilisateur de certificat est configuré pour se connecter au cluster.	Non	Non

Paramètre	Description	Recommandation	Affecte la conformité du cluster
Utilisateurs locaux	Indique si les utilisateurs locaux sont configurés pour se connecter au cluster.	Non	Non
Shell distant	Indique si RSH est activé. Pour des raisons de sécurité, RSH doit être désactivé. Le Secure Shell (SSH) pour un accès distant sécurisé est privilégié.	Désactivées	Oui
MD5 en cours d'utilisation	Indique si les comptes d'utilisateur ONTAP utilisent une fonction de hachage MD5 moins sécurisée. La migration des comptes utilisateurs hachés MD5 vers la fonction de hachage cryptographique plus sécurisée comme SHA-512 est préférée.	Non	Oui
Type d'émetteur de certificat	Indique le type de certificat numérique utilisé.	Signé par une autorité de certification	Non

Catégories de conformité des machines virtuelles de stockage

Ce tableau décrit les critères de conformité de sécurité de la machine virtuelle de stockage (SVM) évalués par Unified Manager, la recommandation NetApp et si le paramètre affecte la détermination globale de la conformité ou non de la SVM.

Paramètre	Description	Recommandation	Affecte la conformité SVM
Journal d'audit	Indique si la journalisation d'audit est activée ou désactivée.	Activé	Oui
Paramètres SSH non sécurisés	Indique si SSH utilise des chiffrements non sécurisés, par exemple des chiffrements commençant par `cbc*` .	Non	Oui

Paramètre	Description	Recommandation	Affecte la conformité SVM
Bannière de connexion	Indique si la bannière de connexion est activée ou désactivée pour les utilisateurs accédant aux SVM sur le système.	Activé	Oui
Cryptage LDAP	Indique si le cryptage LDAP est activé ou désactivé.	Activé	Non
Authentification NTLM	Indique si l'authentification NTLM est activée ou désactivée.	Activé	Non
Signature de charge utile LDAP	Indique si la signature de charge utile LDAP est activée ou désactivée.	Activé	Non
Paramètres CHAP	Indique si CHAP est activé ou désactivé.	Activé	Non
Kerberos V5	Indique si l'authentification Kerberos V5 est activée ou désactivée.	Activé	Non
Authentification NIS	Indique si l'utilisation de l'authentification NIS est configurée.	Désactivées	Non
Statut de la politique FPolicy actif	Indique si FPolicy est créé ou non.	Oui	Non
Cryptage SMB activé	Indique si la signature et le scellement SMB ne sont pas activés.	Oui	Non
Signature SMB activée	Indique si la signature SMB n'est pas activée.	Oui	Non

Catégories de conformité en termes de volume

Ce tableau décrit les paramètres de chiffrement de volume qu'Unified Manager évalue pour déterminer si les données de vos volumes sont correctement protégées contre l'accès par des utilisateurs non autorisés.

Notez que les paramètres de chiffrement du volume n'affectent pas la conformité du cluster ou de la machine virtuelle de stockage.

Paramètre	Description
Logiciel crypté	Affiche le nombre de volumes protégés à l'aide des solutions de chiffrement logiciel NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE).
Matériel crypté	Affiche le nombre de volumes protégés à l'aide du chiffrement matériel NetApp Storage Encryption (NSE).
Logiciel et matériel cryptés	Affiche le nombre de volumes protégés par un chiffrement logiciel et matériel.
Non crypté	Affiche le nombre de volumes qui ne sont pas chiffrés.

Que signifie « non conforme »

Les clusters et les machines virtuelles de stockage (SVM) sont considérés comme non conformes lorsque l'un des critères de sécurité évalués par rapport aux recommandations définies dans le *Guide de renforcement de la sécurité NetApp pour ONTAP 9* n'est pas respecté. De plus, un cluster est considéré comme non conforme lorsqu'un SVM est signalé comme n'étant pas conforme.

Les icônes d'état dans les cartes de sécurité ont les significations suivantes par rapport à leur conformité :

- - Le paramètre est configuré comme recommandé.
- - Le paramètre n'est pas configuré comme recommandé.
- - Soit la fonctionnalité n'est pas activée sur le cluster, soit le paramètre n'est pas configuré comme recommandé, mais ce paramètre ne contribue pas à la conformité de l'objet.

Notez que l'état de chiffrement du volume ne contribue pas à déterminer si le cluster ou le SVM sont considérés comme conformes.

Afficher l'état de sécurité des clusters et des machines virtuelles de stockage

Active IQ Unified Manager vous permet d'afficher l'état de sécurité des objets de stockage dans votre environnement à partir de différents points de l'interface. Vous pouvez collecter et analyser des informations et des rapports en fonction de paramètres définis et détecter des comportements suspects ou des modifications système non autorisées sur les clusters surveillés et les machines virtuelles de stockage.

Pour les recommandations de sécurité, voir le "Guide de renforcement de la sécurité NetApp pour ONTAP 9"

Afficher l'état de sécurité au niveau de l'objet sur la page Sécurité

En tant qu'administrateur système, vous pouvez utiliser la page **Sécurité** pour obtenir une visibilité sur le niveau de sécurité de vos clusters ONTAP et de vos machines virtuelles de stockage aux niveaux du centre de données et du site. Les objets pris en charge sont les clusters, les machines virtuelles de stockage et les volumes. Suivez ces étapes :

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Tableau de bord**.
2. Selon que vous souhaitez afficher l'état de sécurité de tous les clusters surveillés ou d'un seul cluster, sélectionnez **Tous les clusters** ou sélectionnez un seul cluster dans le menu déroulant.
3. Cliquez sur la flèche droite dans le panneau **Sécurité**. La page Sécurité s'affiche.

En cliquant sur les graphiques à barres, les nombres et `View Reports` les liens vous amènent à la page Volumes, Clusters ou Machines virtuelles de stockage pour vous permettre d'afficher les détails correspondants ou de générer des rapports, selon vos besoins.

La page Sécurité affiche les panneaux suivants :

- **Conformité du cluster** : l'état de sécurité (nombre de clusters conformes ou non conformes) de tous les clusters d'un centre de données
- **Conformité des machines virtuelles de stockage** : l'état de sécurité (nombre de machines virtuelles de stockage conformes ou non conformes) pour toutes les machines virtuelles de stockage de votre centre de données
- **Chiffrement du volume** : l'état de chiffrement du volume (nombre de volumes chiffrés ou non chiffrés) de tous les volumes de votre environnement
- **Statut anti-ransomware du volume** : l'état de sécurité (nombre de volumes avec anti-ransomware activé ou désactivé) de tous les volumes de votre environnement
- **Authentification et certificats de cluster** : le nombre de clusters utilisant chaque type de méthode d'authentification, comme SAML, Active Directory ou via des certificats et une authentification locale. Le panneau affiche également le nombre de clusters dont les certificats ont expiré ou sont sur le point d'expirer dans 60 jours.

Afficher les détails de sécurité de tous les clusters sur la page Clusters

La page de détails **Clusters / Sécurité** vous permet d'afficher l'état de conformité de la sécurité au niveau du cluster.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Clusters**.
2. Sélectionnez **Affichage > Sécurité > Tous les clusters**.

Les paramètres de sécurité par défaut, tels que Global FIPS, Telnet, les paramètres SSH non sécurisés, la bannière de connexion, le protocole de temps réseau, AutoSupport HTTPS Transport et l'état d'expiration du certificat de cluster sont affichés.

Vous pouvez cliquer sur le Cliquez sur le bouton Plus d'options et choisissez d'afficher les détails de sécurité sur la page **Sécurité** d'Unified Manager ou sur System Manager. Vous devez disposer d'informations d'identification valides pour afficher les détails sur le Gestionnaire système.

Si un cluster a un certificat expiré, vous pouvez cliquer sur `expired` sous **Validité du certificat de cluster** et renouvelez-le à partir du Gestionnaire système (9.10.1 et versions ultérieures). Vous ne pouvez pas cliquer `expired` si l'instance du Gestionnaire système est d'une version antérieure à 9.10.1.

Afficher les détails de sécurité de tous les clusters à partir de la page des machines virtuelles de stockage

La page de détails **VM de stockage / Sécurité** vous permet d'afficher l'état de conformité de la sécurité au niveau de la machine virtuelle de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Machines virtuelles de stockage**.
2. Sélectionnez **Affichage > Sécurité > Toutes les machines virtuelles de stockage**. Une liste de clusters avec les paramètres de sécurité s'affiche.

Vous pouvez avoir une vue par défaut de la conformité de sécurité des machines virtuelles de stockage en vérifiant les paramètres de sécurité, tels que les machines virtuelles de stockage, le cluster, la bannière de connexion, le journal d'audit et les paramètres SSH non sécurisés.

Vous pouvez cliquer sur le Cliquez sur le bouton Plus d'options et choisissez d'afficher les détails de sécurité sur la page **Sécurité** d'Unified Manager ou sur System Manager. Vous devez disposer d'informations d'identification valides pour afficher les détails sur le Gestionnaire système.

Pour plus de détails sur la sécurité anti-ransomware pour les volumes et les machines virtuelles de stockage, voir"Affichage de l'état anti-ransomware de tous les volumes et machines virtuelles de stockage" .

Afficher les événements de sécurité pouvant nécessiter des mises à jour de logiciels ou de micrologiciels

Certains événements de sécurité ont une zone d'impact de « Mise à niveau ». Ces événements sont signalés à partir de la plateforme Active IQ et identifient les problèmes pour lesquels la résolution nécessite la mise à niveau du logiciel ONTAP , du micrologiciel du nœud ou du logiciel du système d'exploitation (pour les avis de sécurité).

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Vous souhaiterez peut-être effectuer une action corrective immédiate pour certains de ces problèmes, tandis que d'autres problèmes pourront attendre votre prochaine maintenance programmée. Vous pouvez afficher tous ces événements et les attribuer à des utilisateurs capables de résoudre les problèmes. De plus, s'il existe certains événements de mise à niveau de sécurité dont vous ne souhaitez pas être informé, cette liste peut vous aider à identifier ces événements afin que vous puissiez les désactiver.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.

   Par défaut, tous les événements actifs (nouveaux et reconnus) sont affichés sur la page d'inventaire de gestion des événements.

2. Dans le menu Affichage, sélectionnez **Événements de mise à niveau**.

   La page affiche tous les événements de sécurité de mise à niveau actifs.

Afficher comment l'authentification des utilisateurs est gérée sur tous les clusters

La page Sécurité affiche les types d'authentification utilisés pour authentifier les utilisateurs sur chaque cluster, ainsi que le nombre d'utilisateurs qui accèdent au cluster à l'aide de chaque type. Cela vous permet de vérifier que l'authentification des utilisateurs est effectuée de manière sécurisée, comme défini par votre organisation.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Tableau de bord**.
2. En haut du tableau de bord, sélectionnez **Tous les clusters** dans le menu déroulant.
3. Cliquez sur la flèche droite dans le panneau **Sécurité** et la page **Sécurité** s'affiche.
4. Consultez la carte **Authentification de cluster** pour voir le nombre d'utilisateurs qui accèdent au système à l'aide de chaque type d'authentification.
5. Consultez la carte **Sécurité du cluster** pour afficher les mécanismes d'authentification utilisés pour authentifier les utilisateurs sur chaque cluster.

Si certains utilisateurs accèdent au système à l'aide d'une méthode non sécurisée ou d'une méthode non recommandée par NetApp, vous pouvez désactiver la méthode.

Afficher l'état de chiffrement de tous les volumes

Vous pouvez afficher une liste de tous les volumes et leur état de chiffrement actuel afin de déterminer si les données de vos volumes sont correctement protégées contre tout accès par des utilisateurs non autorisés.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Les types de cryptage qui peuvent être appliqués à un volume sont :

- Logiciel - Volumes protégés à l'aide des solutions de chiffrement logiciel NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE).
- Matériel - Volumes protégés à l'aide du chiffrement matériel NetApp Storage Encryption (NSE).
- Logiciel et matériel - Volumes protégés par un cryptage logiciel et matériel.
- Aucun - Volumes qui ne sont pas chiffrés.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Santé** > **Chiffrement des volumes**
3. Dans la vue **Santé : Chiffrement des volumes**, triez sur le champ **Type de chiffrement** ou utilisez le filtre pour afficher les volumes qui ont un type de chiffrement spécifique ou qui ne sont pas chiffrés (type de

chiffrement « Aucun »).

Affichage de l'état anti-ransomware de tous les volumes et machines virtuelles de stockage

Vous pouvez afficher une liste de tous les volumes et machines virtuelles de stockage (SVM) et leur état anti-ransomware actuel afin de déterminer si les données sur vos volumes et SVM sont correctement protégées contre les attaques de ransomware.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Pour plus d'informations sur les différents statuts anti-ransomware, consultez"ONTAP: Activer l'anti-ransomware" .

Afficher les détails de sécurité de tous les volumes avec détection anti-ransomware

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage** > **Volumes**.
2. Dans le menu Affichage, sélectionnez **Santé** > **Sécurité** > **Anti-ransomware**
3. Dans la vue **Sécurité : Anti-ransomware**, vous pouvez trier selon les différents champs ou utiliser le filtre.

L'anti-ransomware n'est pas pris en charge pour les volumes hors ligne, les volumes restreints, les volumes SnapLock , les volumes FlexGroup , les volumes FlexCache , les volumes SAN uniquement, les volumes de machines virtuelles de stockage arrêtées, les volumes racine de machines virtuelles de stockage ou les volumes de protection des données.

Afficher les détails de sécurité de toutes les machines virtuelles de stockage avec détection anti-ransomware

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > Machines virtuelles de stockage**.
2. Sélectionnez **Affichage > Sécurité > Anti-ransomware**. Une liste des SVM avec le statut anti-ransomware s'affiche.

La surveillance anti-ransomware n'est pas prise en charge sur les machines virtuelles de stockage sur lesquelles le protocole NAS n'est pas activé.

Afficher tous les événements de sécurité actifs

Vous pouvez afficher tous les événements de sécurité actifs, puis attribuer chacun d'eux à un utilisateur capable de résoudre le problème. De plus, si vous ne souhaitez pas recevoir certains événements de sécurité, cette liste peut vous aider à identifier les événements que vous souhaitez désactiver.

Avant de commencer

Vous devez disposer du rôle d'opérateur, d'administrateur d'application ou d'administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion des événements**.

   Par défaut, les événements nouveaux et reconnus sont affichés sur la page d'inventaire de gestion des événements.

2. Dans le menu Affichage, sélectionnez **Événements de sécurité actifs**.

   La page affiche tous les événements de sécurité nouveaux et reconnus qui ont été générés au cours des 7 derniers jours.

Ajouter des alertes pour les événements de sécurité

Vous pouvez configurer des alertes pour des événements de sécurité individuels, comme pour tout autre événement reçu par Unified Manager. De plus, si vous souhaitez traiter tous les événements de sécurité de la même manière et envoyer un e-mail à la même personne, vous pouvez créer une alerte unique pour vous avertir lorsque des événements de sécurité sont déclenchés.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

L'exemple ci-dessous montre comment créer une alerte pour l'événement de sécurité « Protocole Telnet activé ». Cela enverra une alerte si l'accès Telnet est configuré pour l'accès administratif à distance au cluster. Vous pouvez utiliser cette même méthodologie pour créer des alertes pour tous les événements de sécurité.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des alertes**.
2. Dans la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom** et saisissez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources** et sélectionnez le cluster ou le cluster sur lequel vous souhaitez activer cette alerte.
5. Cliquez sur **Événements** et effectuez les actions suivantes :
   a. Dans la liste Gravité de l'événement, sélectionnez **Avertissement**.
   b. Dans la liste des événements correspondants, sélectionnez **Protocole Telnet activé**.
6. Cliquez sur **Actions** puis sélectionnez le nom de l'utilisateur qui recevra l'e-mail d'alerte dans le champ **Alerter ces utilisateurs**.
7. Configurez toutes les autres options sur cette page pour la fréquence de notification, l'émission de taps SNMP et l'exécution d'un script.
8. Cliquez sur **Enregistrer**.

Désactiver des événements de sécurité spécifiques

Tous les événements sont activés par défaut. Vous pouvez désactiver des événements

spécifiques pour empêcher la génération de notifications pour les événements qui ne sont pas importants dans votre environnement. Vous pouvez activer les événements désactivés si vous souhaitez reprendre la réception des notifications les concernant.

Avant de commencer

Vous devez disposer du rôle d'administrateur d'application ou d'administrateur de stockage.

Lorsque vous désactivez les événements, les événements précédemment générés dans le système sont marqués comme obsolètes et les alertes configurées pour ces événements ne sont pas déclenchées. Lorsque vous activez des événements désactivés, les notifications pour ces événements sont générées à partir du prochain cycle de surveillance.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Gestion du stockage** > **Configuration des événements**.
2. Dans la page de configuration **Événement**, désactivez ou activez les événements en choisissant l'une des options suivantes :

Si vous voulez…	Alors fais ceci…
Désactiver les événements	a. Cliquez sur **Désactiver**. b. Dans la boîte de dialogue Désactiver les événements, sélectionnez la gravité **Avertissement**. Il s'agit de la catégorie pour tous les événements de sécurité. c. Dans la colonne Événements correspondants, sélectionnez les événements de sécurité que vous souhaitez désactiver, puis cliquez sur la flèche droite pour déplacer ces événements vers la colonne Désactiver les événements. d. Cliquez sur **Enregistrer et fermer**. e. Vérifiez que les événements que vous avez désactivés s'affichent dans la vue de liste de la page Configuration des événements.
Activer les événements	a. Dans la liste des événements désactivés, cochez la case correspondant à l'événement ou aux événements que vous souhaitez réactiver. b. Cliquez sur **Activer**.

Événements de sécurité

Les événements de sécurité vous fournissent des informations sur l'état de sécurité des clusters ONTAP , des machines virtuelles de stockage (SVM) et des volumes en fonction des paramètres définis dans le *Guide de renforcement de la sécurité NetApp pour ONTAP 9*. Ces événements vous informent des problèmes potentiels afin que vous puissiez évaluer leur gravité et résoudre le problème si nécessaire.

Les événements de sécurité sont regroupés par type de source et incluent le nom de l'événement et de l'interruption, le niveau d'impact et la gravité. Ces événements apparaissent dans les catégories d'événements de cluster et de machine virtuelle de stockage.