Gestion des objectifs de sécurité des clusters

Active IQ Unified Manager 9.14

NetApp
March 07, 2024

Sommaire

Gestion des objectifs de sécurité des clusters

Unified Manager fournit un tableau de bord identifiant la sécurité de vos clusters ONTAP, de vos serveurs de stockage virtuels (SVM) et de vos volumes à partir des recommandations définies dans le *guide NetApp de renforcement de la sécurité des environnements ONTAP 9*.

L'objectif du tableau de bord de sécurité est de fournir des informations sur les zones dans lesquelles les clusters ONTAP ne sont pas en adéquation avec les instructions recommandées par NetApp afin de résoudre ces problèmes potentiels. Dans la plupart des cas, vous pouvez résoudre les problèmes à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes de ONTAP. Il se peut que votre organisation ne suive pas toutes les recommandations. Dans certains cas, vous n'aurez donc pas besoin d'apporter de modifications.

Voir la "Guide NetApp sur le renforcement de la sécurité des environnements 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 la gestion des événements et configurer les alertes pour ces événements de sorte que votre administrateur de stockage soit averti en cas de nouveaux événements de sécurité.

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

Quels sont les critères de sécurité évalués

De manière générale, les critères de sécurité des clusters ONTAP, des serveurs de stockage virtuels (SVM) et des volumes sont évalués avec les recommandations définies dans le *guide NetApp de renforcement de la sécurité de la solution ONTAP 9*.

Voici quelques-unes des vérifications de sécurité :

- Indique si un cluster utilise une méthode d'authentification sécurisée, par exemple SAML
- les communications des clusters utilisant des canaux de connexion sont chiffrées
- Indique si le journal des audits d'un serveur virtuel de stockage est activé
- que le chiffrement logiciel ou matériel soit activé pour vos volumes

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

> Les événements de mise à niveau signalés sur la plate-forme Active IQ sont également considérés comme des événements de sécurité. Ces événements identifient les problèmes liés à la résolution des problèmes lorsque vous devez mettre à niveau le logiciel ONTAP, le firmware des nœuds ou le logiciel du système d'exploitation (pour les conseils de sécurité). Ces événements ne sont pas affichés dans le panneau sécurité, mais ils sont disponibles dans 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 que Unified Manager évalue, la recommandation NetApp et si le paramètre affecte la détermination globale du cluster plainte ou non.

L'utilisation de SVM non conformes sur un cluster affecte la valeur de conformité du cluster. Dans certains cas, vous devrez peut-être corriger les problèmes de sécurité avec un SVM avant que la sécurité du cluster ne soit considérée comme conforme.

Notez que tous les paramètres répertoriés ci-dessous ne s'affichent pas pour toutes les installations. Par exemple, si vous n'avez pas de cluster avec peering, ou si vous avez désactivé AutoSupport sur un cluster, vous ne verrez pas les éléments de peering de cluster ni de transport AutoSupport HTTPS dans la page de l'interface utilisateur.

Paramètre	Description	Recommandation	Concerne la conformité du cluster
FIPS global	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 les modèles TLSv1.1 et TLSv1.2 sont autorisés.	Activé	Oui.
Telnet	Indique si l'accès Telnet au système est activé ou désactivé. NetApp recommande un accès sécurisé à distance (SSH).	Désactivé	Oui.
Paramètres SSH non sécurisés	Indique si SSH utilise des chiffrements non sécurisés, par exemple les chiffrements commençant par *cbc.	Non	Oui.
Bannière de connexion	Indique si la bannière connexion est activée ou désactivée pour les utilisateurs accédant au système.	Activé	Oui.

Paramètre	Description	Recommandation	Concerne la conformité du cluster
Peering de clusters	Indique si la communication entre les clusters avec points de connexion est cryptée ou non chiffrée. Le chiffrement doit être configuré sur les clusters source et de destination pour que ce paramètre soit considéré comme conforme.	Chiffrées	Oui.
Protocole de temps réseau	Indique si le cluster possède un ou plusieurs serveurs NTP configurés. Pour la redondance et le meilleur service, NetApp vous recommande d'associer au moins trois serveurs NTP au cluster.	Configuré	Oui.
OCSP	Indique si des applications dans ONTAP ne sont pas configurées avec le protocole OCSP (Online Certificate Status Protocol) et que les communications ne sont donc pas cryptées. Les applications non conformes sont répertoriées.	Activé	Non
Consignation d'audit à distance	Indique si le transfert de journal (Syslog) est crypté ou non.	Chiffrées	Oui.
Transport AutoSupport HTTPS	Indique si HTTPS est utilisé comme protocole de transport par défaut pour l'envoi des messages AutoSupport au support NetApp.	Activé	Oui.

Paramètre	Description	Recommandation	Concerne la conformité du cluster
Utilisateur Admin par défaut	Indique si l'utilisateur Admin par défaut (intégré) est activé ou désactivé. NetApp recommande de verrouiller (désactiver) tous les comptes intégrés inutiles.	Désactivé	Oui.
Utilisateurs SAML	Indique si le langage SAML est configuré. SAML 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 privilégiés pour les utilisateurs qui accèdent 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 le biais d'utilisateurs locaux.	Non	Non
Utilisateurs de certificats	Indique si un utilisateur de certificat est configuré pour se connecter au cluster.	Non	Non
Utilisateurs locaux	Indique si les utilisateurs locaux sont configurés pour se connecter au cluster.	Non	Non

Paramètre	Description	Recommandation	Concerne la conformité du cluster
Coque distante	Indique si le RSH est activé. Pour des raisons de sécurité, la fonction RSH doit être désactivée. Le protocole SSH (Secure Shell) est préféré pour un accès distant sécurisé.	Désactivé	Oui.
MD5 utilisé	Indique si les comptes utilisateur ONTAP utilisent la fonction de hachage MD5 moins sécurisée. Le MD5 hache les comptes utilisateur la migration vers la fonction de hachage cryptographique plus sécurisée comme SHA-512 est préférable.	Non	Oui.
Type émetteur de certificat	Indique le type de certificat numérique utilisé.	Signé CA	Non

Catégories de conformité des VM de stockage

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

Paramètre	Description	Recommandation	Concerne la conformité des 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, en commençant par le chiffrement `cbc*`.	Non	Oui.
Bannière de connexion	Indique si la bannière de connexion est activée ou désactivée pour les utilisateurs qui accèdent aux SVM sur le système.	Activé	Oui.

Paramètre	Description	Recommandation	Concerne la conformité des SVM
Cryptage LDAP	Indique si le chiffrement 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.	Désactivé	Non
État FPolicy actif	Indique si FPolicy est créé ou non.	Oui.	Non
Chiffrement SMB activé	Indique si SMB - Signature & scellage n'est pas activé.	Oui.	Non
Signature SMB activée	Indique si SMB -Signing n'est pas activé.	Oui.	Non

Catégories de conformité des volumes

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

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

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

Que signifie pas conforme

Les clusters et les SVM (Storage Virtual machine) sont considérés comme non conformes lorsque l'un des critères de sécurité évalués avec les recommandations définies dans le *guide NetApp de renforcement de la sécurité de la solution ONTAP 9* n'est pas satisfait. Par ailleurs, un cluster est considéré comme non conforme lorsqu'un SVM n'est pas signalé comme étant non conforme.

Les icônes d'état des cartes de sécurité ont la signification suivante 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 du chiffrement des volumes ne contribue pas à la conformité du cluster ou de la SVM.

Affichage de l'état de sécurité pour les clusters et les VM de stockage

Active IQ Unified Manager permet d'afficher l'état de sécurité des objets de stockage de votre environnement à partir de différents points de l'interface. Il est ainsi possible de collecter et d'analyser des informations et des rapports en fonction de paramètres définis. Il détecte également les comportements suspects ou les modifications non autorisées du système sur les clusters surveillés et les VM de stockage.

Pour connaître les recommandations de sécurité, reportez-vous au "Guide NetApp sur le renforcement de la sécurité des environnements 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 accéder à l'efficacité de sécurité de vos clusters ONTAP et de vos machines virtuelles de stockage au niveau du centre de données et du site. Les objets pris en charge sont le cluster, les VM de stockage et les volumes. Voici la procédure à suivre :

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Dashboard**.
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.

Cliquez sur les graphiques à barres, les comptes et `View Reports` Les liens vous permettent d'accéder à la page volumes, clusters ou machines virtuelles de stockage pour afficher les détails correspondants ou générer des rapports, selon les besoins.

La page sécurité affiche les panneaux suivants :

- **Cluster Compliance** : état de sécurité (nombre de clusters conformes ou non) de tous les clusters d'un centre de données
- **Conformité des machines virtuelles de stockage** : état de sécurité (nombre de machines virtuelles de stockage conformes ou non) pour toutes les machines virtuelles de stockage de votre centre de données
- **Volume Encryption** : état du chiffrement du volume (nombre de volumes cryptés ou non) de tous les volumes de votre environnement
- **Volume anti-ransomware Status** : état de sécurité (nombre de volumes avec anti-ransomware activé ou désactivé) de tous les volumes de votre environnement
- **Authentification et certificats de cluster** : nombre de clusters utilisant chaque type de méthode d'authentification, tel que SAML, Active Directory, ou via des certificats et l'authentification locale. Le panneau affiche également le nombre de grappes 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 sécurité au niveau du cluster.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage > clusters**.
2. Sélectionnez **Affichage > sécurité > tous les clusters**.

Paramètres de sécurité par défaut, tels que Global FIPS, Telnet, paramètres SSH non sécurisés, bannière de connexion, protocole d'heure réseau, Le transport AutoSupport HTTPS et l'état de l'expiration du certificat du cluster sont affichés.

Vous pouvez cliquer sur ⋮ Bouton plus d'options et choisissez d'afficher les détails de sécurité sur la page **sécurité** de Unified Manager ou System Manager. Vous devez disposer d'identifiants valides pour afficher les détails dans System Manager.

> Si un cluster a un certificat expiré, vous pouvez cliquer sur `expired` Sous **validité du certificat de cluster**, et renouvelez-le à partir de System Manager (9.10.1 et versions ultérieures). Vous ne pouvez pas cliquer sur `expired` Si l'instance de System Manager est antérieure à la version 9.10.1.

Afficher les détails de sécurité de tous les clusters à partir de la page VM de stockage

La page de détails **Storage VM / Security** vous permet d'afficher l'état de conformité de sécurité au niveau d'une 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**. La liste des clusters avec les paramètres de sécurité s'affiche.

Vous pouvez afficher la conformité de sécurité des machines virtuelles de stockage par défaut 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 ⋮ Bouton plus d'options et choisissez d'afficher les détails de sécurité sur la page **sécurité** de Unified Manager ou System Manager. Vous devez disposer d'identifiants valides pour afficher les détails dans System Manager.

Pour plus d'informations sur la sécurité des volumes et des machines virtuelles de stockage par ransomware, consultez "Affichage de l'état anti-ransomware de tous les volumes et machines virtuelles de stockage".

Affichage des événements de sécurité qui peuvent nécessiter des mises à jour logicielles ou micrologicielles

Certains événements de sécurité ont une zone d'impact de « mise à niveau ». Ces événements sont signalés sur la plateforme Active IQ et ils identifient les problèmes liés à la résolution lorsque vous devez mettre à niveau le logiciel ONTAP, le firmware des nœuds ou le logiciel du système d'exploitation (pour les conseils de sécurité).

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Vous pouvez effectuer une action corrective immédiatement pour certains de ces problèmes, alors que d'autres peuvent attendre la prochaine maintenance planifiée. Vous pouvez afficher tous ces événements et les attribuer à des utilisateurs capables de résoudre ces problèmes. En outre, si certains événements de mise à niveau de sécurité que vous ne souhaitez pas être avertis, cette liste peut vous aider à identifier ces événements afin de pouvoir les désactiver.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Event Management**.

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

2. Dans le menu Affichage, sélectionnez **mettre à niveau les événements**.

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

Affichage de la façon dont l'authentification utilisateur 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, conformément à la définition de votre organisation.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Dashboard**.
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. Affichez la carte **Cluster Authentication** pour voir le nombre d'utilisateurs qui accèdent au système à l'aide de chaque type d'authentification.
5. Affichez la carte **Cluster Security** 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 si cette méthode n'est pas recommandée par NetApp, vous pouvez la désactiver.

Affichage de l'état de chiffrement de tous les volumes

Vous pouvez afficher la liste de tous les volumes, ainsi que leur état de cryptage actuel, afin de déterminer si les données de vos volumes sont correctement protégées contre tout accès par des utilisateurs non autorisés.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Les types de chiffrement pouvant être appliqués à un volume sont les suivants :

- Logiciels : volumes protégés à l'aide de solutions NetApp Volume Encryption (NVE) ou de chiffrement logiciel de chiffrement d'agrégats NetApp (NAE).
- Matériel : volumes protégés à l'aide du chiffrement matériel NetApp Storage Encryption (NSE).
- Logiciel et matériel : volumes protégés par le chiffrement logiciel et matériel.
- Aucun : volumes qui ne sont pas chiffrés.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans le menu Affichage, sélectionnez **Santé** > **chiffrement des volumes**

3. Dans la vue **Santé : volumes Encryption**, triez le champ **Type de cryptage** ou utilisez le filtre pour afficher les volumes ayant un type de cryptage spécifique ou qui ne sont pas cryptés (Type de cryptage « aucun »).

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

Vous pouvez afficher la liste de tous les volumes et de toutes les machines virtuelles de stockage (SVM) ainsi que leur statut actuel anti-ransomware afin de déterminer si les données de vos volumes et de vos SVM sont correctement protégées contre les attaques par ransomware.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Pour plus d'informations sur les différents États de lutte contre les ransomwares, consultez "ONTAP : activation d'une protection contre les ransomwares".

Afficher les informations de sécurité de tous les volumes avec la détection anti-ransomware

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage** > **volumes**.
2. Dans le menu Affichage, sélectionnez **Santé** > **sécurité** > **anti-ransomware**
3. Dans la vue **Security: Anti-ransomware**, vous pouvez trier les différents champs ou utiliser le filtre.

> Une protection contre les ransomwares n'est pas prise en charge pour les volumes hors ligne, les volumes restreints, les volumes SnapLock, les volumes FlexGroup, les volumes FlexCache, Volumes SAN uniquement, volumes des VM de stockage arrêtés, volumes root de VM de stockage, ou volumes de protection des données.

Affichez les informations de sécurité de toutes les machines virtuelles de stockage avec la détection anti-ransomwares

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **stockage > machines virtuelles de stockage**.
2. Sélectionnez **Affichage > sécurité > anti-ransomware**. La liste des SVM avec le statut anti-ransomware est affichée.

> 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.

Affichage de tous les événements de sécurité actifs

Vous pouvez afficher tous les événements de sécurité actifs, puis les attribuer à un utilisateur qui peut résoudre le problème. En outre, si vous ne souhaitez pas recevoir

certains événements de sécurité, cette liste peut vous aider à identifier les événements que vous souhaitez désactiver.

Ce dont vous aurez besoin

Vous devez avoir le rôle opérateur, administrateur d'applications ou administrateur de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Event Management**.

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

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

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

Ajout d'alertes pour les événements de sécurité

Vous pouvez configurer les alertes pour les événements de sécurité individuels comme pour tous les autres événements reçus par Unified Manager. En outre, si vous souhaitez traiter tous les événements de sécurité, et que vous avez envoyé un e-mail à la même personne, vous pouvez créer une alerte unique pour vous avertir lorsque des événements de sécurité sont déclenchés.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

L'exemple ci-dessous montre comment créer une alerte pour l'événement de sécurité « Protocole Telnet activé ». Une alerte sera envoyée 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 **Storage Management** > **Alert Setup**.
2. Dans la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom**, puis entrez 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 **Evénements** et effectuez les opérations suivantes :
   a. Dans la liste gravité de l'événement, sélectionnez **Avertissement**.
   b. Dans la liste Evénements 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 **Alert thavent Users**.
7. Configurez toutes les autres options de cette page pour la fréquence de notification, l'émission de taps SNMP et l'exécution d'un script.

8. Cliquez sur **Enregistrer**.

Désactivation d'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 de notifications pour eux.

Ce dont vous aurez besoin

Vous devez avoir le rôle Administrateur d'applications ou Administrateur de stockage.

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

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Storage Management** > **Event Setup**.
2. Dans la page Configuration **Event**, désactivez ou activez les événements en choisissant l'une des options suivantes :

Les fonctions que vous recherchez…	Alors, procédez comme ça…
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 de tous les événements de sécurité. c. Dans la colonne Matching Events, sélectionnez les événements de sécurité que vous souhaitez désactiver, puis cliquez sur la flèche de droite pour déplacer ces événements vers la colonne Disable Events. d. Cliquez sur **Enregistrer et fermer**. e. Vérifiez que les événements que vous avez désactivés s'affichent dans la vue 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 fournissent des informations sur l'état de sécurité des clusters ONTAP, des serveurs de stockage virtuels (SVM) et des volumes basés sur des paramètres définis dans le *guide NetApp de renforcement de la sécurité de la solution ONTAP 9*. Ces événements vous avertissent des problèmes potentiels afin que vous puissiez évaluer leur gravité et corriger 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 du cluster et de la machine virtuelle de stockage.