Gérer les objectifs de sécurité du cluster

Active IQ Unified Manager

NetApp
November 13, 2026

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

Sommaire

Gérer les objectifs de sécurité du cluster . . . 1
Gérer les objectifs de sécurité du cluster dans Active IQ Unified Manager . . . 1
Quels critères de sécurité sont évalués . . . 1
Comprendre comment Active IQ Unified Manager évalue les critères de sécurité . . . 1
Comprendre les catégories de conformité des clusters dans Active IQ Unified Manager . . . 2
Comprendre les catégories de conformité des machines virtuelles de stockage dans Active IQ Unified Manager . . . 5
Comprendre les catégories de conformité des volumes dans Active IQ Unified Manager . . . 6
Découvrez l’état de conformité des clusters et des SVM dans Active IQ Unified Manager . . . 7
Consultez l’état de sécurité des clusters et des Storage VMs dans Active IQ Unified Manager . . . 7
Consultez l’état de sécurité au niveau de l’objet sur la page Sécurité . . . 7
Consultez les détails de sécurité de tous les clusters sur la page Clusters . . . 8
Consultez les détails de sécurité de tous les clusters depuis la page des machines virtuelles de stockage . . . 8
Consultez les événements de sécurité susceptibles de nécessiter des mises à jour logicielles ou micrologicielles dans Active IQ Unified Manager . . . 9
Découvrez comment les clusters gèrent l’authentification des utilisateurs sur tous les clusters dans Active IQ Unified Manager . . . 9
Affichez l’état de chiffrement de tous les volumes dans Active IQ Unified Manager . . . 10
Consultez l’état de protection anti-ransomware de tous les volumes et machines virtuelles de stockage dans Active IQ Unified Manager . . . 10
Consultez les détails de sécurité de tous les volumes dotés d’une détection anti-ransomware . . . 11
Consultez les détails de sécurité de toutes les machines virtuelles de stockage dotées d’une détection anti-ransomware . . . 11
Consultez tous les événements de sécurité actifs dans Active IQ Unified Manager . . . 11
Ajoutez des alertes pour les événements de sécurité dans Active IQ Unified Manager . . . 12
Désactiver certains événements de sécurité dans Active IQ Unified Manager . . . 12
Consultez les événements de sécurité dans Active IQ Unified Manager . . . 13

Gérer les objectifs de sécurité du cluster

Gérer les objectifs de sécurité du cluster dans Active IQ Unified Manager

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 *NetApp Security Hardening Guide for ONTAP 9*.

Le tableau de bord de sécurité a pour objectif de montrer les domaines dans lesquels vos clusters ONTAP ne sont pas conformes aux recommandations de NetApp, afin que vous puissiez corriger ces problèmes potentiels. Dans la plupart des cas, vous corrigerez les problèmes à l'aide de ONTAP System Manager ou de ONTAP CLI. Votre organisation ne suit peut-être pas toutes les recommandations, donc, dans certains cas, vous n'aurez pas besoin d'apporter de modifications.

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

Outre le signalement de 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 Event Management, et configurer des alertes afin que votre administrateur du stockage soit notifié lorsque de nouveaux événements de sécurité se produisent.

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

Quels critères de sécurité sont évalués

Comprendre comment Active IQ Unified Manager évalue les critères de sécurité

En général, les critères de sécurité de vos clusters ONTAP, de vos machines virtuelles de stockage (SVM) et de vos volumes sont évalués en fonction des recommandations définies dans le *NetApp Security Hardening Guide for ONTAP 9*.

Voici quelques exemples de contrôles de sécurité :

- si un cluster utilise une méthode d'authentification sécurisée, telle que SAML
- si les communications entre les clusters appariés sont chiffrées
- vérifier si une VM de stockage a son journal des audits activé
- si le chiffrement logiciel ou matériel est activé sur vos volumes

Consultez les rubriques relatives aux catégories de conformité et le "NetApp Guide de renforcement de la sécurité pour ONTAP 9" pour obtenir 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 des problèmes dont la résolution vous oblige à mettre à niveau le logiciel ONTAP, le firmware des nœuds ou le logiciel du système d'exploitation (pour les avis de sécurité). Ces événements ne s'affichent pas dans le panneau Security, mais ils sont disponibles depuis la page d'inventaire Event

Management.

Pour plus d'informations, consultez "Gestion des objectifs de sécurité du cluster".

Comprendre les catégories de conformité des clusters dans Active IQ Unified Manager

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

La présence de SVM non conformes au sein d'un cluster affectera le niveau de conformité de ce dernier. Il peut donc être nécessaire, dans certains cas, de corriger une faille de sécurité liée à une SVM avant que la sécurité du 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 aucun cluster apparié, ou si vous avez désactivé AutoSupport sur un cluster, vous ne verrez pas les éléments « Appairage de clusters » ou « Transport HTTPS de AutoSupport » dans la page de l'interface utilisateur.

Paramètre	Description	Recommandation	Affecte 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 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 distant 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
Interconnexion de clusters	Indique si la communication entre les clusters appariés 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.	Chiffré	Oui
Protocole de temps réseau	Indique si le cluster possède un ou plusieurs serveurs NTP configurés. Pour une redondance et un service optimaux, NetApp recommande d'associer au moins trois serveurs NTP au cluster.	configuré	Oui
OCSP	À partir de la version 9.14.1, Active IQ Unified Manager fournit des informations d'état 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 la SVM et garantit l'intégrité et la validité des certificats utilisés dans ces connexions.	Activé	Non
Journalisation des audits à distance	Indique si le transfert des journaux (Syslog) est chiffré ou non chiffré.	Chiffré	Oui
Transport HTTPS AutoSupport	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	Affecte la conformité du cluster
Utilisateur administrateur par défaut	Indique si l'utilisateur administrateur par défaut (intégré) est activé ou désactivé. NetApp recommande de verrouiller (désactiver) tout compte intégré inutile.	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 privilégiés pour les utilisateurs accédant aux clusters.	Non	Non
Utilisateurs LDAP	Indique si LDAP est configuré. Active Directory et LDAP sont les mécanismes d'authentification privilégiés pour les utilisateurs gérant des clusters par rapport aux utilisateurs locaux.	Non	Non
Utilisateurs de certificats	Indique si un utilisateur disposant d'un 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	Affecte la conformité du cluster
Shell à distance	Indique si le protocole RSH est activé. Pour des raisons de sécurité, il est recommandé de désactiver RSH. L'utilisation de Secure Shell (SSH) est préférable pour un accès distant sécurisé.	Désactivées	Oui
MD5 en cours d'utilisation	Indique si les comptes utilisateurs ONTAP utilisent la fonction de hachage MD5 moins sécurisée. Il est recommandé de migrer les comptes utilisateurs utilisant le hachage MD5 vers une fonction de hachage cryptographique plus sécurisée, telle que SHA-512.	Non	Oui
Type d'émetteur de certificat	Indique le type de certificat numérique utilisé.	Signé par CA	Non

Comprendre les catégories de conformité des machines virtuelles de stockage dans Active IQ Unified Manager

Ce tableau décrit les critères de conformité de sécurité des machines virtuelles de stockage (SVM) qu'Unified Manager évalue, la recommandation de NetApp, et indique si le paramètre affecte la détermination globale de la conformité ou non de la SVM.

Paramètre	Description	Recommandation	Affecte la conformité de la 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
Bannière de connexion	Indique si la bannière de connexion est activée ou désactivée pour les utilisateurs accédant aux SVMs sur le système.	Activé	Oui

Paramètre	Description	Recommandation	Affecte la conformité de la SVM
Chiffrement 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 la charge utile LDAP	Indique si LDAP Payload Signing est activé ou désactivé.	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 FPolicy actif	Indique si FPolicy est créé ou non.	Oui	Non
Chiffrement SMB activé	Indique si SMB -Signing & Sealing n'est pas activé.	Oui	Non
Signature SMB activée	Indique si SMB -Signing n'est pas activé.	Oui	Non

Comprendre les catégories de conformité des volumes dans Active IQ Unified Manager

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

Notez que les paramètres de chiffrement du volume n'ont aucune incidence sur la conformité du cluster ou de la machine virtuelle de stockage.

Paramètre	Description
Chiffré par logiciel	Affiche le nombre de volumes protégés à l'aide des solutions de chiffrement logiciel 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).
Logiciels et matériels chiffrés	Affiche le nombre de volumes protégés à la fois par le chiffrement logiciel et matériel.

Paramètre	Description
Non chiffré	Affiche le nombre de volumes non chiffrés.

Découvrez l'état de conformité des clusters et des SVM dans Active IQ Unified Manager

Les clusters et les machines virtuelles de stockage (SVM) sont considérés comme non conformes lorsqu'un des critères de sécurité évalués par rapport aux recommandations définies dans le *NetApp Security Hardening Guide for ONTAP 9* n'est pas respecté. De plus, un cluster est considéré comme non conforme lorsqu'une SVM est signalée comme non conforme.

Les icônes d'état figurant sur les cartes de sécurité ont les significations suivantes en matière de conformité :

- - Le paramètre est configuré comme recommandé.
- - Ce 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 n'a aucune incidence sur le fait que le cluster ou la SVM soient considérés comme conformes.

Consultez l'état de sécurité des clusters et des Storage VMs dans Active IQ Unified Manager

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

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

Consultez 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. Procédez comme suit :

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Tableau de bord**.
2. Selon que vous souhaitiez 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 vers la droite dans le panneau **Sécurité**. La page Sécurité s'affiche.

Lorsque vous cliquez sur les graphiques à barres, les décomptes et les `View Reports` liens, vous êtes redirigé vers la page Volumes, Clusters ou Storage VMs afin de consulter les détails correspondants ou de générer des rapports, selon vos besoins.

La page Sécurité affiche les panneaux suivants :

- **Conformité des clusters** : 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** : état de sécurité (nombre de machines virtuelles de stockage conformes ou non conformes) de toutes les machines virtuelles de stockage de votre centre de données
- **Chiffrement des volumes** : état du chiffrement des volumes (nombre de volumes chiffrés ou non chiffrés) de tous les volumes de votre environnement
- **État de la protection anti-ransomware des volumes** : état de sécurité (nombre de volumes avec protection anti-ransomware activée ou désactivée) de tous les volumes de votre environnement
- **Authentification et certificats des clusters** : le nombre de clusters utilisant chaque type de méthode d'authentification, comme SAML, Active Directory, ou via des certificats et l'authentification locale. Le panneau affiche également le nombre de clusters dont les certificats ont expiré ou vont expirer dans 60 jours.

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

La page de détails **Clusters / Sécurité** vous permet de consulter l'état de conformité en matière 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**.

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

Vous pouvez cliquer sur le bouton ⋮ Plus d'options et choisir d'afficher les détails de sécurité sur la page **Security** de Unified Manager ou dans System Manager. Vous devez disposer d'identifiants valides pour consulter ces détails dans System Manager.

ⓘ Si le certificat d'un cluster a expiré, vous pouvez cliquer `expired` sous **Validité du certificat du cluster** et le renouveler depuis System Manager (9.10.1 et versions ultérieures). Vous ne pouvez pas cliquer `expired` si l'instance de System Manager exécute une version antérieure à 9.10.1.

Consultez les détails de sécurité de tous les clusters depuis la page des machines virtuelles de stockage

La page de détails **VM de stockage / Sécurité** vous permet de consulter l'état de conformité de sécurité au niveau d'une VM de stockage.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Stockage > VM de stockage**.

2. Sélectionnez **Affichage > Sécurité > Toutes les VM de stockage**. Une liste des clusters avec les paramètres de sécurité s'affiche.

Vous pouvez obtenir 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 des audits et les paramètres SSH non sécurisés.

Vous pouvez cliquer sur le bouton ⋮ Plus d'options et choisir d'afficher les détails de sécurité sur la page **Security** de Unified Manager ou dans System Manager. Vous devez disposer d'identifiants valides pour consulter ces détails dans System Manager.

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

Consultez les événements de sécurité susceptibles de nécessiter des mises à jour logicielles ou micrologicielles dans Active IQ Unified Manager

Certains événements de sécurité ont une zone d'impact de "Upgrade". Ces événements sont signalés par la plateforme Active IQ et identifient des problèmes dont la résolution nécessite que vous mettiez à niveau le logiciel ONTAP, le microprogramme du nœud ou le logiciel du système d'exploitation (pour les avis de sécurité).

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Vous pouvez prendre immédiatement des mesures correctives pour certains de ces problèmes, tandis que d'autres peuvent attendre votre prochaine maintenance planifiée. Vous pouvez consulter 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 pour lesquels vous ne souhaitez pas recevoir de notification, 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 acquittés) s'affichent sur la page d'inventaire de gestion des événements.

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

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

Découvrez comment les clusters gèrent l'authentification des utilisateurs sur tous les clusters dans Active IQ Unified Manager

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 en utilisant chaque type. Cela vous permet de vérifier que l'authentification des

utilisateurs est effectuée de manière sécurisée, conformément aux exigences de 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 vers la droite dans le panneau **Sécurité** pour afficher la page **Sécurité**.
4. Consultez la carte **Authentification du cluster** pour voir le nombre d'utilisateurs qui accèdent au système avec chaque type d'authentification.
5. Consultez la carte **Cluster Security** pour voir 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 cette méthode.

Affichez l'état de chiffrement de tous les volumes dans Active IQ Unified Manager

Vous pouvez consulter la liste de tous les volumes et leur état de chiffrement actuel afin de déterminer si les données de vos volumes sont suffisamment protégées contre l'accès par des utilisateurs non autorisés.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Les types de chiffrement pouvant 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 chiffrement à la fois logiciel et matériel.
- Aucun - Volumes non 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 « `None` »).

Consultez l'état de protection anti-ransomware de tous les volumes et machines virtuelles de stockage dans Active IQ Unified Manager

Vous pouvez consulter la liste de tous les volumes et machines virtuelles de stockage

(SVM), ainsi que leur état actuel de protection anti-ransomware, afin de déterminer si les données de vos volumes et SVM sont correctement protégées contre les attaques de ransomware.

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Pour plus d'informations sur les différents statuts anti-ransomware, voir "ONTAP: Activer la protection anti-ransomware".

Consultez les détails de sécurité de tous les volumes dotés d'une 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 différents champs ou utiliser le filtre.

> La protection anti-ransomware n'est pas prise 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 des machines virtuelles de stockage arrêtées, les volumes racine des machines virtuelles de stockage ou les volumes de protection des données.

Consultez les détails de sécurité de toutes les machines virtuelles de stockage dotées d'une détection anti-ransomware

Étapes

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

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

Consultez tous les événements de sécurité actifs dans Active IQ Unified Manager

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

Avant de commencer

Vous devez avoir le rôle Operator, Application Administrator ou Storage Administrator.

Étapes

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

Par défaut, les événements New et Acknowledged sont affichés sur la page d'inventaire Event Management.

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

   Cette page affiche tous les événements de sécurité nouveaux et reconnus générés au cours des 7 derniers jours.

Ajoutez des alertes pour les événements de sécurité dans Active IQ Unified Manager

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 qui vous notifiera lorsque des événements de sécurité sont déclenchés.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

L'exemple ci-dessous montre comment créer une alerte pour l'événement de sécurité « `Telnet Protocol Enabled` ». Cela enverra une alerte si l'accès Telnet est configuré pour l'administration à distance du cluster. Vous pouvez utiliser cette même méthode 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. Sur la page **Configuration des alertes**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Ajouter une alerte**, cliquez sur **Nom**, puis saisissez un nom et une description pour l'alerte.
4. Cliquez sur **Ressources** et sélectionnez le ou les clusters sur lesquels 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 les autres options sur cette page concernant la fréquence des notifications, l'émission de traps SNMP et l'exécution d'un script.
8. Cliquez sur **Enregistrer**.

Désactiver certains événements de sécurité dans Active IQ Unified Manager

Tous les événements sont activés par défaut. Vous pouvez désactiver certains événements pour éviter la génération de notifications concernant ceux qui ne sont pas importants dans votre environnement. Vous pouvez réactiver les événements désactivés

si vous souhaitez à nouveau recevoir des notifications les concernant.

Avant de commencer

Vous devez disposer du rôle Application Administrator ou Storage Administrator.

Lorsque vous désactivez des événements, ceux 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 de l'événement**.
2. Dans la page de configuration **Event**, désactivez ou activez les événements en choisissant l'une des options suivantes :

Si vous voulez…	Ensuite, faites ceci…
Désactiver les événements	a. Cliquez sur **Disable**. b. Dans la boîte de dialogue Désactiver les événements, sélectionnez le niveau de gravité **Avertissement**. Il s'agit de la catégorie de 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 vers la 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 apparaissent dans la vue de liste de la page Configuration des événements.
Activer les événements	a. Dans la liste des événements désactivés, cochez la case à cocher correspondant à l'événement ou aux événements que vous souhaitez réactiver. b. Cliquez sur **Enable**.

Consultez les événements de sécurité dans Active IQ Unified Manager

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 signalent les problèmes potentiels afin que vous puissiez en évaluer la gravité et les corriger si nécessaire.

Les événements de sécurité sont regroupés par type de source et comprennent le nom de l'événement et du trap, le niveau d'impact et la gravité. Ces événements apparaissent dans les catégories d'événements du cluster et des VM de stockage.

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.