Gestisci gli obiettivi di sicurezza del cluster

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/it-it/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.

Sommario

Gestisci gli obiettivi di sicurezza del cluster . . . 1
- Gestisci gli obiettivi di sicurezza del cluster in Active IQ Unified Manager . . . 1
- Quali criteri di sicurezza vengono valutati . . . 1
  - Scopri come Active IQ Unified Manager valuta i criteri di sicurezza . . . 1
  - Scopri le categorie di conformità dei cluster in Active IQ Unified Manager . . . 2
  - Comprendi le categorie di conformità delle Storage VM in Active IQ Unified Manager . . . 5
  - Comprendi le categorie di conformità del volume in Active IQ Unified Manager . . . 6
- Scopri lo stato di conformità del cluster e dell'SVM in Active IQ Unified Manager . . . 6
- Visualizza lo stato di sicurezza dei cluster e delle Storage VM in Active IQ Unified Manager . . . 6
  - Visualizza lo stato di sicurezza a livello di oggetto nella pagina Security . . . 7
  - Visualizza i dettagli di sicurezza di tutti i cluster nella pagina Clusters . . . 7
  - Visualizza i dettagli di sicurezza di tutti i cluster dalla pagina delle VM di storage . . . 8
- Visualizza gli eventi di sicurezza che potrebbero richiedere aggiornamenti software o firmware in Active IQ Unified Manager . . . 8
- Visualizza come i cluster gestiscono l'autenticazione degli utenti su tutti i cluster in Active IQ Unified Manager . . . 9
- Visualizza lo stato di crittografia di tutti i volumi in Active IQ Unified Manager . . . 9
- Visualizza lo stato anti-ransomware di tutti i volumi e le storage VM in Active IQ Unified Manager . . . 10
  - Visualizza i dettagli di sicurezza di tutti i volumi con rilevamento anti-ransomware . . . 10
  - Visualizza i dettagli di sicurezza di tutte le VM di storage con rilevamento anti-ransomware . . . 10
- Visualizza tutti gli eventi di sicurezza attivi in Active IQ Unified Manager . . . 10
- Aggiungi avvisi per eventi di sicurezza in Active IQ Unified Manager . . . 11
- Disabilita specifici eventi di sicurezza in Active IQ Unified Manager . . . 11
- Visualizza gli eventi di sicurezza in Active IQ Unified Manager . . . 12

Gestisci gli obiettivi di sicurezza del cluster

Gestisci gli obiettivi di sicurezza del cluster in Active IQ Unified Manager

Unified Manager fornisce una dashboard che identifica il livello di sicurezza dei tuoi cluster ONTAP, delle macchine virtuali di storage (SVM) e dei volumi in base alle raccomandazioni definite nella *NetApp Security Hardening Guide for ONTAP 9*.

L'obiettivo del dashboard di sicurezza è mostrare tutte le aree in cui i tuoi cluster ONTAP non sono allineati alle linee guida consigliate da NetApp, in modo che tu possa risolvere questi potenziali problemi. Nella maggior parte dei casi risolverai i problemi usando ONTAP System Manager o ONTAP CLI. La tua organizzazione potrebbe non seguire tutte le raccomandazioni, quindi in alcuni casi non dovrai apportare alcuna modifica.

Consulta "NetApp Security Hardening Guide per ONTAP 9" (TR-4569) per raccomandazioni e soluzioni dettagliate.

Oltre a segnalare lo stato della sicurezza, Unified Manager genera anche eventi di sicurezza per qualsiasi cluster o SVM che presenta violazioni della sicurezza. Puoi monitorare questi problemi nella pagina dell'inventario di Event Management e configurare avvisi per questi eventi, così il tuo amministratore dello storage viene avvisato quando si verificano nuovi eventi di sicurezza.

Per ulteriori informazioni, consulta "Quali criteri di sicurezza vengono valutati".

Quali criteri di sicurezza vengono valutati

Scopri come Active IQ Unified Manager valuta i criteri di sicurezza

In generale, i criteri di sicurezza per i tuoi cluster ONTAP, le macchine virtuali di storage (SVM) e i volumi vengono valutati in base alle raccomandazioni definite nella *NetApp Security Hardening Guide for ONTAP 9*.

Alcuni dei controlli di sicurezza includono:

- se un cluster utilizza un metodo di autenticazione sicuro, come SAML
- se la comunicazione dei cluster peered è crittografata
- se il log di audit di una VM di storage è abilitato
- se sui volumi è abilitata la crittografia software o hardware

Consulta gli argomenti sulle categorie di conformità e il "NetApp Security Hardening Guide per ONTAP 9" per informazioni dettagliate.

> Gli eventi di aggiornamento segnalati dalla piattaforma Active IQ sono considerati anche eventi di sicurezza. Questi eventi identificano problemi la cui risoluzione richiede l'aggiornamento del software ONTAP, del firmware del nodo o del software del sistema operativo (per gli avvisi di sicurezza). Questi eventi non sono visualizzati nel pannello Security, ma sono disponibili nella pagina di inventario Event Management.

Per ulteriori informazioni, consulta "Gestione degli obiettivi di sicurezza del cluster".

Scopri le categorie di conformità dei cluster in Active IQ Unified Manager

Questa tabella descrive i parametri di conformità della sicurezza del cluster che Unified Manager valuta, la raccomandazione di NetApp e se il parametro influisce sulla determinazione complessiva del fatto che il cluster sia conforme o non conforme.

La presenza di SVM non conformi su un cluster influirà sul valore di conformità del cluster. Quindi, in alcuni casi, devi risolvere un problema di sicurezza relativo a una SVM prima che la sicurezza del cluster venga considerata conforme.

Tieni presente che non tutti i parametri elencati di seguito vengono visualizzati per tutte le installazioni. Ad esempio, se non hai cluster con peering o se hai disabilitato AutoSupport su un cluster, nella pagina dell'interfaccia utente non vedrai le voci Cluster Peering o AutoSupport HTTPS Transport.

Parametro	Descrizione	Raccomandazione	Influisce sulla conformità del cluster
FIPS globale	Indica se la modalità di conformità Global FIPS (Federal Information Processing Standard) 140-2 è abilitata o disabilitata. Quando FIPS è abilitato, TLSv1 e SSLv3 sono disabilitati e sono consentiti solo TLSv1.1 e TLSv1.2.	Abilitato	Sì
Telnet	Indica se l'accesso Telnet al sistema è abilitato o disabilitato. NetApp consiglia Secure Shell (SSH) per un accesso remoto sicuro.	Disattivato	Sì
Impostazioni SSH non sicure	Indica se SSH utilizza cifrari non sicuri, ad esempio cifrari che iniziano con *cbc.	No	Sì
Banner di accesso	Indica se il banner di accesso è abilitato o disabilitato per gli utenti che accedono al sistema.	Abilitato	Sì
Peering del cluster	Indica se la comunicazione tra cluster peered è crittografata o non crittografata. La crittografia deve essere configurata su entrambi i cluster, di origine e di destinazione, affinché questo parametro sia considerato conforme.	Crittografato	Sì

Parametro	Descrizione	Raccomandazione	Influisce sulla conformità del cluster
Network Time Protocol	Indica se il cluster dispone di uno o più server NTP configurati. Per garantire ridondanza e un servizio ottimale NetApp ti consiglia di associare almeno tre server NTP al cluster.	Configurato	Sì
OCSP	A partire dalla versione 9.14.1, Active IQ Unified Manager fornisce informazioni sullo stato del protocollo OCSP (Online Certificate Status Protocol) a livello di macchina virtuale di archiviazione (SVM, precedentemente nota come Vserver). Ciò significa che la convalida OCSP viene applicata a tutte le connessioni SSL/TLS effettuate verso la SVM e garantisce l'integrità e la validità dei certificati utilizzati in tali connessioni.	Abilitato	No
Registrazione remota dell'audit	Indica se l'inoltro dei log (Syslog) è crittografato o meno.	Crittografato	Sì
AutoSupport Trasporto HTTPS	Indica se HTTPS viene utilizzato come protocollo di trasporto predefinito per l'invio di messaggi AutoSupport al supporto NetApp.	Abilitato	Sì
Utente amministratore predefinito	Indica se l'utente amministratore predefinito (integrato) è abilitato o disabilitato. NetApp consiglia di bloccare (disabilitare) tutti gli account integrati non necessari.	Disattivato	Sì

Parametro	Descrizione	Raccomandazione	Influisce sulla conformità del cluster
Utenti SAML	Indica se SAML è configurato. SAML consente di configurare l'autenticazione a più fattori (MFA) come metodo di accesso per single sign-on.	No	No
Utenti di Active Directory	Indica se Active Directory è configurato. Active Directory e LDAP sono i meccanismi di autenticazione preferiti per gli utenti che accedono ai cluster.	No	No
Utenti LDAP	Indica se LDAP è configurato. Active Directory e LDAP sono i meccanismi di autenticazione preferiti per gli utenti che gestiscono i cluster rispetto agli utenti locali.	No	No
Utenti dei certificati	Indica se un utente con certificato è configurato per accedere al cluster.	No	No
Utenti locali	Indica se gli utenti locali sono configurati per accedere al cluster.	No	No
Shell remota	Indica se RSH è abilitato. Per motivi di sicurezza, RSH dovrebbe essere disabilitato. Per un accesso remoto sicuro è preferibile utilizzare Secure Shell (SSH).	Disattivato	Sì
MD5 in uso	Indica se gli account utente ONTAP utilizzano la funzione hash MD5, meno sicura. Si consiglia la migrazione degli account utente con hash MD5 a una funzione hash crittografica più sicura come SHA-512.	No	Sì
Tipo di emittente del certificato	Indica il tipo di certificato digitale utilizzato.	Firmato CA	No

Comprendi le categorie di conformità delle Storage VM in Active IQ Unified Manager

Questa tabella descrive i criteri di conformità della sicurezza della storage virtual machine (SVM) valutati da Unified Manager, la raccomandazione di NetApp e se il parametro influisce sulla determinazione complessiva della conformità o meno della SVM.

Parametro	Descrizione	Raccomandazione	Influisce su SVM Compliance
Log di audit	Indica se la registrazione di controllo è abilitata o disabilitata.	Abilitato	Sì
Impostazioni SSH non sicure	Indica se SSH utilizza cifrari non sicuri, ad esempio cifrari che iniziano con `cbc*`.	No	Sì
Banner di accesso	Indica se il banner di accesso è abilitato o disabilitato per gli utenti che accedono alle SVM sul sistema.	Abilitato	Sì
Crittografia LDAP	Indica se la crittografia LDAP è abilitata o disabilitata.	Abilitato	No
Autenticazione NTLM	Indica se l'autenticazione NTLM è abilitata o disabilitata.	Abilitato	No
Firma del payload LDAP	Indica se la firma del payload LDAP è abilitata o disabilitata.	Abilitato	No
Impostazioni CHAP	Indica se CHAP è abilitato o disabilitato.	Abilitato	No
Kerberos V5	Indica se l'autenticazione Kerberos V5 è abilitata o disabilitata.	Abilitato	No
Autenticazione NIS	Indica se è configurato l'utilizzo dell'autenticazione NIS.	Disattivato	No
Stato FPolicy attivo	Indica se FPolicy è stata creata o meno.	Sì	No
Crittografia SMB abilitata	Indica se SMB -Signing & Sealing non è abilitato.	Sì	No
Firma SMB abilitata	Indica se SMB -Signing non è abilitato.	Sì	No

Comprendi le categorie di conformità del volume in Active IQ Unified Manager

Questa tabella descrive i parametri di crittografia del volume che Unified Manager valuta per determinare se i dati sui tuoi volumi sono adeguatamente protetti dall'accesso da parte di utenti non autorizzati.

Nota che i parametri di crittografia del volume non influiscono sul fatto che il cluster o la VM di storage siano considerati conformi.

Parametro	Descrizione
Software crittografato	Visualizza il numero di volumi protetti tramite le soluzioni di crittografia software NetApp Volume Encryption (NVE) o NetApp Aggregate Encryption (NAE).
Crittografia hardware	Visualizza il numero di volumi protetti mediante la crittografia hardware NetApp Storage Encryption (NSE).
Software e hardware crittografati	Visualizza il numero di volumi protetti sia dalla crittografia software che da quella hardware.
Non crittografato	Visualizza il numero di volumi non crittografati.

Scopri lo stato di conformità del cluster e dell'SVM in Active IQ Unified Manager

I cluster e le macchine virtuali di storage (SVM) sono considerati non conformi quando non viene soddisfatto uno qualsiasi dei criteri di sicurezza valutati rispetto alle raccomandazioni definite nella *NetApp Security Hardening Guide for ONTAP 9*. Inoltre, un cluster è considerato non conforme quando una qualsiasi SVM è contrassegnata come non conforme.

Le icone di stato presenti sulle schede di sicurezza hanno i seguenti significati in relazione alla loro conformità:

- - Il parametro è configurato come raccomandato.
- - Il parametro non è configurato come raccomandato.
- - La funzionalità non è abilitata sul cluster oppure il parametro non è configurato come raccomandato, ma questo parametro non contribuisce alla conformità dell'oggetto.

Tieni presente che lo stato della crittografia del volume non influisce sul fatto che il cluster o la SVM siano considerati conformi.

Visualizza lo stato di sicurezza dei cluster e delle Storage VM in Active IQ Unified Manager

Active IQ Unified Manager ti consente di visualizzare lo stato di sicurezza degli oggetti di storage nel tuo ambiente da diversi punti dell'interfaccia. Puoi raccogliere e analizzare informazioni e report basati su parametri definiti, nonché rilevare comportamenti sospetti

o modifiche di sistema non autorizzate sui cluster e sulle VM di storage monitorati.

Per le raccomandazioni sulla sicurezza, consulta il "NetApp Security Hardening Guide per ONTAP 9"

Visualizza lo stato di sicurezza a livello di oggetto nella pagina Security

In qualità di system administrator, puoi utilizzare la pagina **Sicurezza** per avere visibilità sul livello di sicurezza dei cluster ONTAP e delle VM di storage a livello di data center e di sito. Gli oggetti supportati sono cluster, VM di storage e volumi. Segui questi passaggi:

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Dashboard**.
2. A seconda che tu voglia visualizzare lo stato di sicurezza per tutti i cluster monitorati o per un singolo cluster, seleziona **Tutti i cluster** oppure seleziona un singolo cluster dal menu a discesa.
3. Fai clic sulla freccia a destra nel pannello **Sicurezza**. Si apre la pagina Sicurezza.

Facendo clic sui grafici a barre, sui conteggi e `View Reports` sui link, vai alla pagina Volumes, Clusters o Storage VMs per visualizzare i dettagli corrispondenti o generare report, secondo necessità.

La pagina Sicurezza visualizza i seguenti pannelli:

- **Conformità del cluster**: lo stato di sicurezza (numero di cluster conformi o non conformi) di tutti i cluster in un data center
- **Conformità delle VM di storage**: lo stato di sicurezza (numero di VM di storage conformi o non conformi) per tutte le VM di storage nel tuo data center
- **Crittografia dei volumi**: lo stato di crittografia dei volumi (numero di volumi crittografati o non crittografati) di tutti i volumi nel tuo ambiente
- **Stato anti-ransomware dei volumi**: lo stato di sicurezza (numero di volumi con anti-ransomware abilitato o disabilitato) di tutti i volumi nel tuo ambiente
- **Autenticazione e certificati dei cluster**: il numero di cluster che utilizzano ciascun tipo di metodo di autenticazione, come SAML, Active Directory o tramite certificati e autenticazione locale. Il pannello visualizza anche il numero di cluster i cui certificati sono scaduti o stanno per scadere entro 60 giorni.

Visualizza i dettagli di sicurezza di tutti i cluster nella pagina Clusters

La pagina dei dettagli **Cluster / Sicurezza** ti consente di visualizzare lo stato di conformità della sicurezza a livello di cluster.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Archiviazione > Cluster**.
2. Seleziona **Visualizza > Sicurezza > Tutti i cluster**.

Vengono visualizzati i parametri di sicurezza predefiniti, come FIPS globale, Telnet, impostazioni SSH non sicure, banner di accesso, protocollo orario di rete, trasporto HTTPS di AutoSupport e lo stato di scadenza del certificato del cluster.

Puoi fare clic sul pulsante ⋮ Altre opzioni e scegliere di visualizzare i dettagli di sicurezza nella pagina **Sicurezza** di Unified Manager o in System Manager. Devi disporre di credenziali valide per visualizzare i dettagli in System Manager.

Se un cluster ha un certificato scaduto, puoi fare clic `expired` in **Validità certificato cluster** e rinnovarlo da System Manager (9.10.1 e versioni successive). Non puoi fare clic `expired` se l'istanza di System Manager ha una release precedente alla 9.10.1.

Visualizza i dettagli di sicurezza di tutti i cluster dalla pagina delle VM di storage

La pagina dei dettagli **Storage VMs / Security** ti consente di visualizzare lo stato di conformità della sicurezza a livello di storage VM.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Archiviazione > Macchine virtuali di archiviazione**.
2. Seleziona **Visualizza > Sicurezza > Tutte le VM di archiviazione**. Compare un elenco di cluster con i parametri di sicurezza.

Puoi avere una vista predefinita della conformità della sicurezza delle VM di storage controllando i parametri di sicurezza, come VM di storage, cluster, banner di accesso, log di audit e impostazioni SSH non sicure.

Puoi fare clic sul pulsante ⋮ Altre opzioni e scegliere di visualizzare i dettagli di sicurezza nella pagina **Sicurezza** di Unified Manager o in System Manager. Devi disporre di credenziali valide per visualizzare i dettagli in System Manager.

Per i dettagli sulla sicurezza anti-ransomware per i volumi e le VM di storage, vedi "Visualizzazione dello stato anti-ransomware di tutti i volumi e delle Storage VMs".

Visualizza gli eventi di sicurezza che potrebbero richiedere aggiornamenti software o firmware in Active IQ Unified Manager

Esistono determinati eventi di sicurezza che hanno un'area di impatto "Upgrade". Questi eventi vengono segnalati dalla piattaforma Active IQ e identificano problemi la cui risoluzione richiede di aggiornare il software ONTAP, il firmware del nodo o il software del sistema operativo (per gli avvisi di sicurezza).

Prima di iniziare

Devi disporre del ruolo di Operatore, Amministratore di applicazioni o Amministratore di archiviazione.

Potresti voler intervenire immediatamente per risolvere alcuni di questi problemi, mentre altri possono attendere fino alla prossima manutenzione programmata. Puoi visualizzare tutti questi eventi e assegnarli agli utenti che possono risolvere i problemi. Inoltre, se ci sono determinati eventi di upgrade della sicurezza per cui non vuoi ricevere notifiche, questo elenco può aiutarti a identificarli, così puoi disabilitarli.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Event Management**.

   Per impostazione predefinita, la pagina di inventario Event Management mostra tutti gli eventi attivi (nuovi e confermati).

2. Dal menu Visualizza, seleziona **Eventi di aggiornamento**.

   La pagina visualizza tutti gli eventi di sicurezza dell'upgrade attivi.

Visualizza come i cluster gestiscono l’autenticazione degli utenti su tutti i cluster in Active IQ Unified Manager

La pagina Security mostra i tipi di autenticazione utilizzati per autenticare gli utenti su ciascun cluster e il numero di utenti che accedono al cluster utilizzando ciascun tipo. Questo ti consente di verificare che l’autenticazione degli utenti venga eseguita in modo sicuro, come definito dalla tua organizzazione.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Dashboard**.
2. Nella parte superiore della dashboard, seleziona **Tutti i cluster** dal menu a tendina.
3. Fai clic sulla freccia a destra nel pannello **Sicurezza** e viene visualizzata la pagina **Sicurezza**.
4. Visualizza la scheda **Cluster Authentication** per vedere il numero di utenti che accedono al sistema utilizzando ciascun tipo di autenticazione.
5. Consulta la scheda **Cluster Security** per visualizzare i meccanismi di autenticazione utilizzati per autenticare gli utenti su ciascun cluster.

Se alcuni utenti accedono al sistema utilizzando un metodo non sicuro o un metodo non consigliato da NetApp, puoi disabilitarlo.

Visualizza lo stato di crittografia di tutti i volumi in Active IQ Unified Manager

Puoi visualizzare un elenco di tutti i volumi e il loro stato di crittografia attuale, in modo da determinare se i dati sui tuoi volumi sono adeguatamente protetti dall’accesso da parte di utenti non autorizzati.

Prima di iniziare

Devi disporre del ruolo di Operatore, Amministratore di applicazioni o Amministratore di archiviazione.

I tipi di crittografia che possono essere applicati a un volume sono:

- Software - Volumi protetti tramite le soluzioni di crittografia software NetApp Volume Encryption (NVE) o NetApp Aggregate Encryption (NAE).
- Hardware - Volumi protetti tramite la crittografia hardware NetApp Storage Encryption (NSE).
- Software e hardware - volumi protetti sia dalla crittografia software che hardware.
- Nessuno - Volumi non crittografati.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Archiviazione** > **Volumi**.
2. Nel menu Visualizza, seleziona **Integrità** > **Crittografia dei volumi**
3. Nella vista **Integrità: Crittografia dei volumi**, ordina in base al campo **Tipo di crittografia** oppure utilizza il filtro per visualizzare i volumi che hanno un tipo di crittografia specifico o che non sono crittografati (Tipo di crittografia “None”).

Visualizza lo stato anti-ransomware di tutti i volumi e le storage VM in Active IQ Unified Manager

Puoi visualizzare un elenco di tutti i volumi e delle VM di storage (SVM) e il loro stato anti-ransomware attuale, in modo da determinare se i dati sui volumi e sulle SVM sono adeguatamente protetti dagli attacchi ransomware.

Prima di iniziare

Devi disporre del ruolo di Operatore, Amministratore di applicazioni o Amministratore di archiviazione.

Per ulteriori informazioni sui diversi stati anti-ransomware, consulta "ONTAP: Abilita la protezione anti-ransomware".

Visualizza i dettagli di sicurezza di tutti i volumi con rilevamento anti-ransomware

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Archiviazione** > **Volumi**.
2. Nel menu Visualizza, seleziona **Health** > **Security** > **Anti-ransomware**
3. Nella vista **Sicurezza: Anti-ransomware**, puoi ordinare in base ai vari campi o usare il filtro.

La protezione anti-ransomware non è supportata per i volumi offline, i volumi con restrizioni, i volumi SnapLock, i volumi FlexGroup, i volumi FlexCache, i volumi solo SAN, i volumi di storage VM arrestate, i volumi root delle storage VM o i volumi di protezione dei dati.

Visualizza i dettagli di sicurezza di tutte le VM di storage con rilevamento anti-ransomware

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Archiviazione > Macchine virtuali di archiviazione**.
2. Seleziona **Visualizza > Sicurezza > Anti-ransomware**. Vedi un elenco di SVM con lo stato anti-ransomware.

Il monitoraggio anti-ransomware non è supportato sulle VM di storage che non hanno il protocollo NAS abilitato.

Visualizza tutti gli eventi di sicurezza attivi in Active IQ Unified Manager

Puoi visualizzare tutti gli eventi di sicurezza attivi e assegnarli a un utente in grado di risolvere il problema. Inoltre, se non vuoi ricevere determinati eventi di sicurezza, questo elenco può aiutarti a identificare quelli che vuoi disabilitare.

Prima di iniziare

Devi disporre del ruolo di Operatore, Amministratore di applicazioni o Amministratore di archiviazione.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Event Management**.

Per impostazione predefinita, nella pagina dell'inventario di Event Management vengono mostrati gli eventi nuovi e confermati.

2. Dal menu Visualizza, seleziona **Eventi di sicurezza attivi**.

   La pagina visualizza tutti gli eventi di sicurezza nuovi e riconosciuti generati negli ultimi 7 giorni.

Aggiungi avvisi per eventi di sicurezza in Active IQ Unified Manager

Puoi configurare avvisi per singoli eventi di sicurezza, proprio come per qualsiasi altro evento ricevuto da Unified Manager. Inoltre, se vuoi trattare tutti gli eventi di sicurezza allo stesso modo e inviare un'e-mail alla stessa persona, puoi creare un singolo avviso che ti notifichi quando viene attivato un qualsiasi evento di sicurezza.

Prima di iniziare

Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.

L'esempio seguente mostra come creare un avviso per l'evento di sicurezza "Telnet Protocol Enabled". Questo invierà un avviso se l'accesso Telnet è configurato per l'accesso amministrativo remoto al cluster. Puoi usare questa stessa metodologia per creare avvisi per tutti gli eventi di sicurezza.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Storage Management** > **Alert Setup**.
2. Nella pagina **Configurazione avvisi**, fai clic su **Aggiungi**.
3. Nella finestra di dialogo **Aggiungi avviso**, fai clic su **Nome** e immetti un nome e una descrizione per l'avviso.
4. Fai clic su **Risorse** e seleziona il cluster o i cluster su cui vuoi abilitare questo avviso.
5. Fai clic su **Eventi** ed esegui le seguenti azioni:
   a. Nell'elenco Gravità dell'evento, seleziona **Warning**.
   b. Nell'elenco Eventi corrispondenti, seleziona **Telnet Protocol Enabled**.
6. Fai clic su **Azioni** e poi seleziona il nome dell'utente che riceverà l'e-mail di avviso nel campo **Avvisa questi utenti**.
7. Configura altre opzioni in questa pagina per la frequenza delle notifiche, l'invio di trap SNMP e l'esecuzione di script.
8. Fare clic su **Save**.

Disabilita specifici eventi di sicurezza in Active IQ Unified Manager

Tutti gli eventi sono abilitati per impostazione predefinita. Puoi disabilitare eventi specifici per impedire la generazione di notifiche per gli eventi che non sono importanti nel tuo ambiente. Puoi abilitare gli eventi disabilitati se vuoi riprendere a ricevere le relative notifiche.

Prima di iniziare

Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.

Quando disattivi gli eventi, quelli generati in precedenza nel sistema vengono contrassegnati come obsoleti e gli avvisi configurati per tali eventi non vengono attivati. Quando riattivi gli eventi disattivati, le notifiche relative a questi eventi vengono generate a partire dal ciclo di monitoraggio successivo.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Storage Management** > **Event Setup**.
2. Nella pagina di configurazione di **Event**, puoi disabilitare o abilitare gli eventi scegliendo una delle seguenti opzioni:

Se vuoi…	Poi fai così…
Disabilita gli eventi	a. Fai clic su **Disable**. b. Nella finestra di dialogo Disabilita eventi, seleziona il livello di gravità **Avviso**. Questa è la categoria per tutti gli eventi di sicurezza. c. Nella colonna Eventi corrispondenti, seleziona gli eventi di sicurezza che vuoi disabilitare, quindi fai clic sulla freccia a destra per spostare questi eventi nella colonna Disabilita eventi. d. Fai clic su **Save and Close**. e. Verifica che gli eventi che hai disabilitato vengano visualizzati nella vista elenco della pagina Configurazione eventi.
Abilita eventi	a. Dall'elenco degli eventi disabilitati, seleziona la check box corrispondente all'evento o agli eventi che desideri riattivare. b. Fai clic su **Enable**.

Visualizza gli eventi di sicurezza in Active IQ Unified Manager

Gli eventi di sicurezza ti forniscono informazioni sullo stato di sicurezza dei cluster ONTAP, delle macchine virtuali di storage (SVM) e dei volumi, in base ai parametri definiti in *NetApp Security Hardening Guide for ONTAP 9*. Questi eventi ti segnalano potenziali problemi, così puoi valutarne la gravità e, se necessario, risolverli.

Gli eventi di sicurezza sono raggruppati per tipo di origine e includono il nome dell'evento e della trap, il livello di impatto e la gravità. Questi eventi vengono visualizzati nelle categorie di eventi del cluster e della VM di storage.

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.