Gestire gli obiettivi di sicurezza del cluster

Active IQ Unified Manager

NetApp
October 15, 2025

This PDF was generated from https://docs.netapp.com/it-it/active-iq-unified-manager-916/health-checker/reference_cluster_compliance_categories.html on October 15, 2025. Always check docs.netapp.com for the latest.

Sommario

Gestire gli obiettivi di sicurezza del cluster

Unified Manager fornisce una dashboard che identifica il livello di sicurezza dei 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 della dashboard di sicurezza è quello di mostrare tutte le aree in cui i cluster ONTAP non sono conformi alle linee guida consigliate da NetApp , in modo da poter risolvere questi potenziali problemi. Nella maggior parte dei casi è possibile risolvere i problemi utilizzando ONTAP System Manager o ONTAP CLI. La tua organizzazione potrebbe non seguire tutte le raccomandazioni, quindi in alcuni casi non sarà necessario apportare alcuna modifica.

Vedi il "Guida al rafforzamento della sicurezza NetApp per ONTAP 9" (TR-4569) per raccomandazioni e risoluzioni dettagliate.

Oltre a segnalare lo stato di sicurezza, Unified Manager genera anche eventi di sicurezza per qualsiasi cluster o SVM che presenti violazioni della sicurezza. È possibile tenere traccia di questi problemi nella pagina dell'inventario Gestione eventi e configurare avvisi per questi eventi in modo che l'amministratore dell'archiviazione venga avvisato quando si verificano nuovi eventi di sicurezza.

Per maggiori informazioni, vedere "Quali criteri di sicurezza vengono valutati".

Quali criteri di sicurezza vengono valutati

In generale, i criteri di sicurezza per i cluster ONTAP , le macchine virtuali di storage (SVM) e i volumi vengono valutati in base alle raccomandazioni definite nella *Guida al rafforzamento della sicurezza NetApp per ONTAP 9*.

Alcuni dei controlli di sicurezza includono:

- se un cluster utilizza un metodo di autenticazione sicuro, come SAML
- se i cluster peer hanno la loro comunicazione crittografata
- se una VM di archiviazione ha il suo registro di controllo abilitato
- se i tuoi volumi hanno la crittografia software o hardware abilitata

Vedere gli argomenti sulle categorie di conformità e "Guida al rafforzamento della sicurezza NetApp per ONTAP 9" per informazioni dettagliate.

> Anche gli eventi di aggiornamento segnalati dalla piattaforma Active IQ sono considerati eventi di sicurezza. Questi eventi identificano problemi per la cui risoluzione è necessario aggiornare il software ONTAP , il firmware del nodo o il software del sistema operativo (per gli avvisi di sicurezza). Questi eventi non vengono visualizzati nel pannello Sicurezza, ma sono disponibili nella pagina dell'inventario Gestione eventi.

Per maggiori informazioni, vedere "Gestione degli obiettivi di sicurezza del cluster".

Categorie di conformità del cluster

Questa tabella descrive i parametri di conformità alla sicurezza del cluster valutati da Unified Manager, la raccomandazione NetApp e se il parametro influisce sulla

determinazione complessiva della conformità o meno del cluster.

La presenza di SVM non conformi su un cluster influirà sul valore di conformità del cluster. Pertanto, in alcuni casi potrebbe essere necessario risolvere un problema di sicurezza con una SVM prima che la sicurezza del cluster venga considerata conforme.

Si noti che non tutti i parametri elencati di seguito sono presenti in tutte le installazioni. Ad esempio, se non hai cluster peering o se hai disabilitato AutoSupport su un cluster, non vedrai gli elementi Cluster Peering o AutoSupport HTTPS Transport nella pagina dell'interfaccia utente.

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.	Disabili	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
Cluster Peering	Indica se la comunicazione tra cluster peer è crittografata o non crittografata. Affinché questo parametro sia considerato conforme, è necessario che la crittografia sia configurata sia sul cluster di origine che su quello di destinazione.	Criptato	SÌ

Parametro	Descrizione	Raccomandazione	Influisce sulla conformità del cluster
Protocollo di tempo di rete	Indica se il cluster ha uno o più server NTP configurati. Per garantire ridondanza e un servizio ottimale, NetApp 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 all'SVM e garantisce l'integrità e la validità dei certificati utilizzati in queste connessioni.	Abilitato	NO
Registrazione di audit remoto	Indica se l'inoltro del registro (Syslog) è crittografato o meno.	Criptato	SÌ
AutoSupport del 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.	Disabili	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 l'accesso singolo.	NO	NO
Utenti di Active Directory	Indica se Active Directory è configurato. Active Directory e LDAP sono i meccanismi di autenticazione preferiti dagli utenti che accedono ai cluster.	NO	NO
Utenti LDAP	Indica se LDAP è configurato. Active Directory e LDAP sono i meccanismi di autenticazione preferiti dagli utenti che gestiscono cluster rispetto agli utenti locali.	NO	NO
Utenti certificati	Indica se un utente 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 disattivato. Per l'accesso remoto sicuro è preferibile utilizzare Secure Shell (SSH).	Disabili	SÌ

Parametro	Descrizione	Raccomandazione	Influisce sulla conformità del cluster
MD5 in uso	Indica se gli account utente ONTAP utilizzano la funzione hash MD5 meno sicura. È preferibile la migrazione degli account utente con hash MD5 alla 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

Categorie di conformità delle VM di archiviazione

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

Parametro	Descrizione	Raccomandazione	Influisce sulla conformità SVM
Registro di controllo	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

Parametro	Descrizione	Raccomandazione	Influisce sulla conformità SVM
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'uso dell'autenticazione NIS.	Disabili	NO
Stato FPolicy Attivo	Indica se FPolicy è stato creato o meno.	SÌ	NO
Crittografia SMB abilitata	Indica se la firma e la sigillatura SMB non sono abilitate.	SÌ	NO
Firma SMB abilitata	Indica se la firma SMB non è abilitata.	SÌ	NO

Categorie di conformità del volume

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

Si noti che i parametri di crittografia del volume non influiscono sulla conformità del cluster o della VM di archiviazione.

Parametro	Descrizione
Software crittografato	Visualizza il numero di volumi protetti mediante 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).

Parametro	Descrizione
Software e hardware crittografati	Visualizza il numero di volumi protetti tramite crittografia software e hardware.
Non crittografato	Visualizza il numero di volumi non crittografati.

Cosa significa non conforme

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

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

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

Si noti che lo stato di crittografia del volume non influisce sulla conformità del cluster o dell'SVM.

Visualizza lo stato di sicurezza per cluster e VM di archiviazione

Active IQ Unified Manager consente di visualizzare lo stato di sicurezza degli oggetti di archiviazione nel proprio ambiente da diversi punti dell'interfaccia. È possibile raccogliere e analizzare informazioni e report in base a parametri definiti e rilevare comportamenti sospetti o modifiche non autorizzate del sistema sui cluster monitorati e sulle VM di archiviazione.

Per le raccomandazioni di sicurezza, vedere il "Guida al rafforzamento della sicurezza NetApp per ONTAP 9"

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

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Dashboard**.
2. A seconda che si desideri visualizzare lo stato di sicurezza per tutti i cluster monitorati o per un singolo cluster, selezionare **Tutti i cluster** oppure selezionare un singolo cluster dal menu a discesa.
3. Fare clic sulla freccia destra nel pannello **Sicurezza**. Viene visualizzata la pagina Sicurezza.

Facendo clic sui grafici a barre, conteggi e `View Reports` I collegamenti ti portano alla pagina Volumi, Cluster o VM di archiviazione per visualizzare i dettagli corrispondenti o generare report, a seconda delle 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 archiviazione**: lo stato di sicurezza (numero di VM di archiviazione conformi o non conformi) per tutte le VM di archiviazione nel tuo data center
- **Crittografia del volume**: lo stato di crittografia del volume (numero di volumi crittografati o non crittografati) di tutti i volumi nel tuo ambiente
- **Stato anti-ransomware del volume**: lo stato di sicurezza (numero di volumi con anti-ransomware abilitato o disabilitato) di tutti i volumi nel tuo ambiente
- **Autenticazione cluster e certificati**: il numero di cluster che utilizzano ciascun tipo di metodo di autenticazione, ad esempio SAML, Active Directory o tramite certificati e autenticazione locale. Il pannello mostra anche il numero di cluster i cui certificati sono scaduti o scadranno entro 60 giorni.

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

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

Passi

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

Vengono visualizzati i parametri di sicurezza predefiniti, quali Global FIPS, Telnet, impostazioni SSH non sicure, banner di accesso, protocollo di tempo di rete, AutoSupport HTTPS Transport e lo stato di scadenza del certificato del cluster.

Puoi cliccare su pulsante Altre opzioni e scegliere di visualizzare i dettagli di sicurezza nella pagina **Sicurezza** di Unified Manager o in System Manager. Per visualizzare i dettagli su System Manager è necessario disporre di credenziali valide.

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

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

La pagina dei dettagli **VM di archiviazione / Sicurezza** consente di visualizzare lo stato di conformità della sicurezza a livello di VM di archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > VM di archiviazione**.
2. Selezionare **Visualizza > Sicurezza > Tutte le VM di archiviazione**. Viene visualizzato un elenco di cluster con i parametri di sicurezza.

È possibile avere una visualizzazione predefinita della conformità di sicurezza delle VM di archiviazione controllando i parametri di sicurezza, come VM di archiviazione, cluster, banner di accesso, registro di controllo e impostazioni SSH non sicure.

Puoi cliccare su pulsante Altre opzioni e scegliere di visualizzare i dettagli di sicurezza nella pagina **Sicurezza** di Unified Manager o in System Manager. Per visualizzare i dettagli su System Manager è necessario disporre di credenziali valide.

Per i dettagli sulla sicurezza anti-ransomware per volumi e VM di archiviazione, vedere"Visualizzazione dello stato anti-ransomware di tutti i volumi e delle VM di archiviazione" .

Visualizza gli eventi di sicurezza che potrebbero richiedere aggiornamenti software o firmware

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

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per alcuni di questi problemi potrebbe essere necessario intervenire immediatamente, mentre per altri potrebbe essere necessario attendere la successiva manutenzione programmata. È possibile visualizzare tutti questi eventi e assegnarli agli utenti in grado di risolvere i problemi. Inoltre, se ci sono determinati eventi di aggiornamento della sicurezza di cui non vuoi essere informato, questo elenco può aiutarti a identificare tali eventi in modo da poterli disabilitare.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi**.

   Per impostazione predefinita, tutti gli eventi attivi (nuovi e riconosciuti) vengono visualizzati nella pagina dell'inventario Gestione eventi.

2. Dal menu Visualizza, seleziona **Aggiorna eventi**.

   La pagina visualizza tutti gli eventi di sicurezza di aggiornamento attivi.

Visualizza come viene gestita l'autenticazione utente su tutti i cluster

Nella pagina Sicurezza vengono visualizzati i tipi di autenticazione utilizzati per autenticare gli utenti su ciascun cluster e il numero di utenti che accedono al cluster utilizzando ciascun tipo. Ciò consente di verificare che l'autenticazione dell'utente venga eseguita in modo sicuro, come definito dalla propria organizzazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Dashboard**.

2. Nella parte superiore della dashboard, seleziona **Tutti i cluster** dal menu a discesa.
3. Fare clic sulla freccia destra nel pannello **Sicurezza** per visualizzare la pagina **Sicurezza**.
4. Visualizza la scheda **Autenticazione cluster** per vedere il numero di utenti che accedono al sistema utilizzando ciascun tipo di autenticazione.
5. Visualizzare la scheda **Sicurezza cluster** 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, è possibile disabilitare il metodo.

Visualizza lo stato di crittografia di tutti i volumi

È possibile visualizzare un elenco di tutti i volumi e del loro stato di crittografia attuale, in modo da poter determinare se i dati sui volumi sono adeguatamente protetti dall'accesso da parte di utenti non autorizzati.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

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

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione** > **Volumi**.
2. Nel menu Visualizza, seleziona **Salute** > **Crittografia volumi**
3. Nella vista **Integrità: Crittografia volumi**, ordinare in base al campo **Tipo di crittografia** oppure utilizzare il filtro per visualizzare i volumi che hanno un tipo di crittografia specifico o che non sono crittografati (Tipo di crittografia "Nessuno").

Visualizzazione dello stato anti-ransomware di tutti i volumi e delle VM di archiviazione

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

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Per ulteriori informazioni sui diversi stati anti-ransomware, vedere"ONTAP: Abilita anti-ransomware" .

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione** > **Volumi**.
2. Nel menu Visualizza, seleziona **Salute** > **Sicurezza** > **Anti-ransomware**
3. Nella vista **Sicurezza: Anti-ransomware**, è possibile ordinare in base ai vari campi oppure utilizzare il Filtro.

L'anti-ransomware non è supportato per volumi offline, volumi con restrizioni, volumi SnapLock , volumi FlexGroup , volumi FlexCache , volumi solo SAN, volumi di VM di storage arrestate, volumi root di VM di storage o volumi di protezione dati.

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Archiviazione > VM di archiviazione**.
2. Selezionare **Visualizza > Sicurezza > Anti-ransomware**. Viene visualizzato un elenco di SVM con stato anti-ransomware.

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

Visualizza tutti gli eventi di sicurezza attivi

È possibile visualizzare tutti gli eventi di sicurezza attivi e quindi assegnare ciascuno di essi a un utente in grado di risolvere il problema. Inoltre, se ci sono determinati eventi di sicurezza che non desideri ricevere, questo elenco può aiutarti a identificare gli eventi che vuoi disabilitare.

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione eventi**.

   Per impostazione predefinita, gli eventi Nuovi e Riconosciuti vengono visualizzati nella pagina dell'inventario Gestione eventi.

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

È possibile 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 le email alla stessa persona, puoi creare un singolo avviso per essere avvisato quando vengono attivati eventi di sicurezza.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

L'esempio seguente mostra come creare un avviso per l'evento di sicurezza "Protocollo Telnet abilitato". Verrà inviato un avviso se l'accesso Telnet è configurato per l'accesso amministrativo remoto al cluster. È possibile utilizzare la stessa metodologia per creare avvisi per tutti gli eventi di sicurezza.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione** > **Configurazione avvisi**.
2. Nella pagina **Impostazione avviso**, fare clic su **Aggiungi**.
3. Nella finestra di dialogo **Aggiungi avviso**, fare clic su **Nome** e immettere un nome e una descrizione per l'avviso.
4. Fare clic su **Risorse** e selezionare il cluster o i cluster su cui si desidera abilitare questo avviso.
5. Fare clic su **Eventi** ed eseguire le seguenti azioni:
   a. Nell'elenco Gravità evento, selezionare **Avviso**.
   b. Nell'elenco Eventi corrispondenti, selezionare **Protocollo Telnet abilitato**.
6. Fare clic su **Azioni** e quindi selezionare il nome dell'utente che riceverà l'e-mail di avviso nel campo **Avvisa questi utenti**.
7. Configurare qualsiasi altra opzione in questa pagina per la frequenza delle notifiche, l'emissione di tap SNMP e l'esecuzione di uno script.
8. Fare clic su **Salva**.

Disabilitare eventi di sicurezza specifici

Tutti gli eventi sono abilitati per impostazione predefinita. È possibile disabilitare eventi specifici per impedire la generazione di notifiche per quegli eventi che non sono importanti nel proprio ambiente. È possibile abilitare gli eventi disabilitati se si desidera riprendere a ricevere le relative notifiche.

Prima di iniziare

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Quando si disabilitano gli eventi, gli eventi generati in precedenza nel sistema vengono contrassegnati come obsoleti e gli avvisi configurati per tali eventi non vengono attivati. Quando si abilitano eventi disabilitati, le notifiche per questi eventi vengono generate a partire dal ciclo di monitoraggio successivo.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione** > **Configurazione evento**.
2. Nella pagina Impostazione **Evento**, disabilita o abilita gli eventi scegliendo una delle seguenti opzioni:

Se lo desidera…	Allora fai così…
Disabilitare gli eventi	a. Fare clic su **Disabilita**. b. Nella finestra di dialogo Disabilita eventi, selezionare la gravità **Avviso**. Questa è la categoria per tutti gli eventi di sicurezza. c. Nella colonna Eventi corrispondenti, seleziona gli eventi di sicurezza che desideri disabilitare, quindi fai clic sulla freccia destra per spostare tali eventi nella colonna Disabilita eventi. d. Fare clic su **Salva e chiudi**. e. Verificare che gli eventi disabilitati siano visualizzati nella vista elenco della pagina Impostazione evento.
Abilita eventi	a. Dall'elenco degli eventi disabilitati, seleziona la casella di controllo relativa all'evento o agli eventi che desideri riabilitare. b. Fare clic su **Abilita**.

Eventi di sicurezza

Gli eventi di sicurezza forniscono informazioni sullo stato di sicurezza dei cluster ONTAP , delle macchine virtuali di archiviazione (SVM) e dei volumi in base ai parametri definiti nella *NetApp Security Hardening Guide for ONTAP 9*. Questi eventi ti avvisano di potenziali problemi, in modo che tu possa valutarne la gravità e, se necessario, risolverli.

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

Informazioni sul copyright

Copyright © 2025 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.