



Gestione degli obiettivi di sicurezza del cluster

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

Sommario

- Gestione degli obiettivi di sicurezza del cluster 1
 - Quali criteri di sicurezza vengono valutati 1
 - Cosa significa non conformità 6
 - Visualizzazione dello stato di sicurezza per cluster e VM di storage 7
 - Visualizzazione di eventi di sicurezza che potrebbero richiedere aggiornamenti software o firmware 8
 - Visualizzazione del modo in cui viene gestita l'autenticazione dell'utente su tutti i cluster 9
 - Visualizzazione dello stato di crittografia di tutti i volumi 9
 - Visualizzazione dello stato anti-ransomware di tutti i volumi e le VM di storage 10
 - Visualizzazione di tutti gli eventi di sicurezza attivi 11
 - Aggiunta di avvisi per eventi di sicurezza 11
 - Disattivazione di eventi di sicurezza specifici 12
 - Eventi di sicurezza 12

Gestione degli obiettivi di sicurezza del cluster

Unified Manager offre una dashboard che identifica la sicurezza dei cluster ONTAP, delle macchine virtuali di storage e dei volumi in base ai consigli definiti nella *Guida per l'aumento della sicurezza NetApp per ONTAP 9*.

L'obiettivo della dashboard di sicurezza è mostrare le aree in cui i cluster ONTAP non sono allineati con le linee guida consigliate da NetApp, in modo da poter risolvere questi potenziali problemi. Nella maggior parte dei casi, è possibile risolvere i problemi utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP. La tua organizzazione potrebbe non seguire tutti i consigli, quindi in alcuni casi non sarà necessario apportare modifiche.

Vedere ["Guida al rafforzamento della sicurezza di NetApp per ONTAP 9"](#) (TR-4569) per suggerimenti e risoluzioni dettagliate.

Oltre a segnalare lo stato di sicurezza, Unified Manager genera anche eventi di sicurezza per qualsiasi cluster o SVM che presenta violazioni della sicurezza. È possibile tenere traccia di questi problemi nella pagina di inventario di Event Management ed è possibile configurare gli avvisi per questi eventi in modo che l'amministratore dello storage riceva una notifica quando si verificano nuovi eventi di sicurezza.

Per ulteriori 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 ai consigli definiti nella *Guida per l'aumento della protezione di NetApp per ONTAP 9*.

Alcuni dei controlli di sicurezza includono:

- Se un cluster utilizza un metodo di autenticazione sicuro, ad esempio SAML
- se i cluster peered hanno la loro comunicazione crittografata
- Se una VM storage ha attivato il registro di controllo
- sia che i volumi dispongano della crittografia software o hardware abilitata

Consultare gli argomenti relativi alle categorie di conformità e a ["Guida al rafforzamento della sicurezza di NetApp per ONTAP 9"](#) per informazioni dettagliate.



Anche gli eventi di upgrade riportati dalla piattaforma Active IQ sono considerati eventi di sicurezza. Questi eventi identificano i problemi in cui la 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 vengono visualizzati nel pannello sicurezza, ma sono disponibili nella pagina inventario gestione eventi.

Per ulteriori informazioni, vedere ["Gestione degli obiettivi di sicurezza del cluster"](#).

Categorie di compliance del cluster

Questa tabella descrive i parametri di conformità della sicurezza del cluster che Unified Manager valuta, i consigli di NetApp e se il parametro influisce sulla determinazione

generale del cluster che presenta un reclamo o meno.

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

Si noti che non tutti i parametri elencati di seguito vengono visualizzati per tutte le installazioni. Ad esempio, se non si dispone di cluster peered o se AutoSupport è stato disattivato su un cluster, gli elementi di peering cluster o trasporto HTTPS AutoSupport non verranno visualizzati nella pagina dell'interfaccia utente.

| Parametro | Descrizione | Consiglio | Influisce sulla conformità del cluster |
|-----------------------------|---|---------------|--|
| FIPS globale | Indica se la modalità di conformità Global FIPS (Federal Information Processing Standard) 140-2 è attivata o disattivata. Quando FIPS è attivato, TLSv1 e SSLv3 sono disattivati e sono consentiti solo TLSv1.1 e TLSv1.2. | Attivato | Sì |
| Telnet | Indica se l'accesso Telnet al sistema è attivato o disattivato. 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 attivato o disattivato per gli utenti che accedono al sistema. | Attivato | Sì |
| Peering dei cluster | Indica se la comunicazione tra i cluster in peering è crittografata o non crittografata. La crittografia deve essere configurata sia sul cluster di origine che su quello di destinazione affinché questo parametro sia considerato conforme. | Crittografato | Sì |

| Parametro | Descrizione | Consiglio | Influisce sulla conformità del cluster |
|-----------------------------|--|------------------|---|
| Network Time Protocol | Indica se il cluster dispone di uno o più server NTP configurati. Per la ridondanza e il miglior servizio, NetApp consiglia di associare almeno tre server NTP al cluster. | Configurato | Sì |
| OCSP | Indica se in ONTAP sono presenti applicazioni non configurate con OCSP (Online Certificate Status Protocol) e quindi le comunicazioni non sono crittografate. Vengono elencate le applicazioni non conformi. | Attivato | No |
| Log di controllo remoto | Indica se l'inoltro dei log (Syslog) è crittografato o meno. | Crittografato | Sì |
| Trasporto HTTPS AutoSupport | Indica se HTTPS è utilizzato come protocollo di trasporto predefinito per l'invio di messaggi AutoSupport al supporto NetApp. | Attivato | Sì |
| Admin User predefinito | Indica se l'utente amministratore predefinito (incorporato) è attivato o disattivato. NetApp consiglia di bloccare (disabilitare) gli account integrati non necessari. | Disattivato | Sì |
| Utenti SAML | Indica se SAML è configurato. SAML consente di configurare l'autenticazione a più fattori (MFA) come metodo di accesso per il single sign-on. | No | No |

| Parametro | Descrizione | Consiglio | Influisce sulla conformità del cluster |
|------------------------------------|--|------------------|---|
| 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 su 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 l'accesso al cluster. | No | No |
| Shell remota | Indica se RSH è attivato. Per motivi di sicurezza, RSH deve essere disattivato. È preferibile utilizzare Secure Shell (SSH) per un accesso remoto sicuro. | Disattivato | Sì |
| MD5 in uso | Indica se gli account utente ONTAP utilizzano una funzione hash MD5 meno sicura. Si preferisce la migrazione degli account utente con hash MD5 alla funzione hash crittografica più sicura come SHA-512. | No | Sì |
| Tipo di autorità di certificazione | Indica il tipo di certificato digitale utilizzato. | Firma CA | No |

Categorie di conformità delle VM di storage

Questa tabella descrive i criteri di conformità della sicurezza SVM (Storage Virtual Machine) che Unified Manager valuta, i consigli di NetApp e se il parametro influisce sulla determinazione generale della SVM che presenta un reclamo o meno.

| Parametro | Descrizione | Consiglio | Influisce sulla conformità SVM |
|-----------------------------|---|-------------|--------------------------------|
| Log di audit | Indica se la registrazione dell'audit è attivata o disattivata. | Attivato | Sì |
| Impostazioni SSH non sicure | Indica se SSH utilizza cifrari non sicuri, ad esempio cifrari che iniziano con <code>cbc*</code> . | No | Sì |
| Banner di accesso | Indica se il banner di accesso è attivato o disattivato per gli utenti che accedono alle SVM sul sistema. | Attivato | Sì |
| Crittografia LDAP | Indica se la crittografia LDAP è attivata o disattivata. | Attivato | No |
| Autenticazione NTLM | Indica se l'autenticazione NTLM è attivata o disattivata. | Attivato | No |
| Firma del payload LDAP | Indica se la firma del payload LDAP è attivata o disattivata. | Attivato | No |
| Impostazioni CHAP | Indica se CHAP è attivato o disattivato. | Attivato | No |
| Kerberos V5 | Indica se l'autenticazione Kerberos V5 è attivata o disattivata. | Attivato | No |
| Autenticazione NIS | Indica se è configurato l'utilizzo dell'autenticazione NIS. | Disattivato | No |
| Stato FPolicy attivo | Indica se FPolicy è stato creato o meno. | Sì | No |

| Parametro | Descrizione | Consiglio | Influisce sulla conformità SVM |
|---------------------------|---|-----------|--------------------------------|
| Crittografia SMB attivata | Indica se SMB -signing & sealing non è abilitato. | Sì | No |
| Firma SMB abilitata | Indica se la firma SMB non è abilitata. | Sì | No |

Categorie di compliance ai volumi

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 sul fatto che la VM del cluster o dello storage sia considerata conforme.

| 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). |
| Crittografia software e hardware | Visualizza il numero di volumi protetti dalla crittografia software e hardware. |
| Non crittografato | Visualizza il numero di volumi non crittografati. |

Cosa significa non conformità

I cluster e le macchine virtuali di storage (SVM) sono considerati non conformi quando uno qualsiasi dei criteri di sicurezza valutati in base alle raccomandazioni definite nella *Guida per l'hardware di sicurezza NetApp per ONTAP 9* non viene soddisfatto. Inoltre, un cluster viene considerato non conforme quando una 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 viene configurato come consigliato.
-  - Il parametro non è configurato come consigliato.
-  - La funzionalità non è attivata sul cluster o il parametro non è configurato come consigliato, ma questo

parametro non contribuisce alla compliance dell'oggetto.

Si noti che lo stato di crittografia del volume non contribuisce a stabilire se il cluster o la SVM sono considerati conformi.

Visualizzazione dello stato di sicurezza per cluster e VM di storage

Active IQ Unified Manager consente di visualizzare lo stato di sicurezza degli oggetti di storage nell'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 di sistema non autorizzate sui cluster monitorati e sulle VM di storage.

Per i consigli sulla sicurezza, consultare ["Guida al rafforzamento della sicurezza di NetApp per ONTAP 9"](#)

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

In qualità di amministratore di sistema, è possibile utilizzare la pagina **sicurezza** per ottenere visibilità sul livello di sicurezza dei cluster ONTAP e delle VM di storage a livello di data center e sito. Gli oggetti supportati sono cluster, VM di storage e volumi. Attenersi alla seguente procedura:

Fasi

1. Nel riquadro di spostamento di 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** o selezionare un singolo cluster dal menu a discesa.
3. Fare clic sulla freccia destra nel pannello **Security**. Viene visualizzata la pagina Security (sicurezza).

Facendo clic sui grafici a barre, sui conteggi e *View Reports* | collegamenti consentono di accedere alla pagina Volumes (volumi), Clusters (Clusters) o Storage VM (Storage VM) per visualizzare i dettagli corrispondenti o generare report, in base alle esigenze.

La pagina Security (sicurezza) visualizza i seguenti pannelli:

- **Cluster Compliance:** Stato di sicurezza (numero di cluster conformi o non conformi) di tutti i cluster di un data center
- **Storage VM Compliance:** Lo stato di sicurezza (numero di storage VM conformi o non conformi) per tutte le storage VM del data center
- **Volume Encryption:** Stato della crittografia del volume (numero di volumi crittografati o non crittografati) di tutti i volumi dell'ambiente
- **Volume Anti-ransomware Status:** Stato di sicurezza (numero di volumi con anti-ransomware attivato o disattivato) di tutti i volumi nel tuo ambiente
- **Cluster Authentication and Certificates:** Numero di cluster che utilizzano ciascun tipo di metodo di autenticazione, ad esempio 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 tra 60 giorni.


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

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

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage > Clusters**.
2. Selezionare **Visualizza > sicurezza > tutti i cluster**.

Parametri di sicurezza predefiniti, come Global FIPS, Telnet, impostazioni SSH non sicure, banner di accesso, protocollo temporale di rete, Vengono visualizzati trasporto HTTPS AutoSupport e lo stato della scadenza del certificato del cluster.

Fare clic su  Pulsante More options (altre opzioni) e scegliere di visualizzare i dettagli di sicurezza nella pagina **Security** di Unified Manager o in System Manager. È necessario disporre di credenziali valide per visualizzare i dettagli in System Manager.



Se un cluster dispone di un certificato scaduto, fare clic su *expired* Sotto **Cluster Certificate Valid**, e rinnovarlo da System Manager (9.10.1 e versioni successive). Non è possibile fare clic su *expired* Se l'istanza di System Manager è di 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 VM / Security** consente di visualizzare lo stato di conformità della sicurezza a livello di storage VM.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage > Storage VM**.
2. Selezionare **Visualizza > sicurezza > tutte le macchine virtuali storage**. Viene visualizzato un elenco di cluster con i parametri di sicurezza.

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

Fare clic su  Pulsante More options (altre opzioni) e scegliere di visualizzare i dettagli di sicurezza nella pagina **Security** di Unified Manager o in System Manager. È necessario disporre di credenziali valide per visualizzare i dettagli in System Manager.

Per informazioni sulla sicurezza anti-ransomware per volumi e macchine virtuali storage, vedere ["Visualizzazione dello stato anti-ransomware di tutti i volumi e le VM di storage"](#).

Visualizzazione di eventi di sicurezza che potrebbero richiedere aggiornamenti software o firmware

Alcuni eventi di sicurezza hanno un'area di impatto di "Upgrade". Questi eventi vengono segnalati dalla piattaforma Active IQ e identificano i problemi in cui la risoluzione richiede l'aggiornamento del software ONTAP, del firmware del nodo o del software del sistema operativo (per gli avvisi di sicurezza).

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Potrebbe essere necessario eseguire un'azione correttiva immediata per alcuni di questi problemi, mentre altri

potrebbero essere in grado di attendere la successiva manutenzione pianificata. È possibile visualizzare tutti questi eventi e assegnarli agli utenti in grado di risolvere i problemi. Inoltre, se esistono alcuni eventi di aggiornamento della protezione che non si desidera ricevere notifiche, questo elenco può aiutare a identificare tali eventi in modo da poterli disattivare.

Fasi

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

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

2. Dal menu View (Visualizza), selezionare **Upgrade events** (Aggiorna eventi).

Nella pagina vengono visualizzati tutti gli eventi di protezione dell'aggiornamento attivi.

Visualizzazione del modo in cui viene gestita l'autenticazione dell'utente su tutti i cluster

La pagina Security (sicurezza) visualizza i tipi di autenticazione utilizzati per autenticare gli utenti su ciascun cluster e il numero di utenti che accedono al cluster utilizzando ciascun tipo. In questo modo è possibile verificare che l'autenticazione dell'utente venga eseguita in modo sicuro, come definito dall'organizzazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Dashboard**.
2. Nella parte superiore della dashboard, selezionare **tutti i cluster** dal menu a discesa.
3. Fare clic sulla freccia destra nel pannello **Security** (sicurezza) per visualizzare la pagina **Security** (protezione).
4. Visualizzare la scheda **Cluster Authentication** per visualizzare il numero di utenti che accedono al sistema utilizzando ciascun tipo di autenticazione.
5. Visualizzare 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 utilizzando un metodo non consigliato da NetApp, è possibile disattivare il metodo.

Visualizzazione dello stato di crittografia di tutti i volumi

È possibile visualizzare un elenco di tutti i volumi e il relativo stato di crittografia corrente per determinare se i dati presenti nei volumi sono adeguatamente protetti dall'accesso da parte di utenti non autorizzati.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

I tipi di crittografia che è possibile applicare 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 dalla crittografia software e hardware.
- None (Nessuno) - volumi non crittografati.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage > Volumes**.
2. Nel menu View (Visualizza), selezionare **Health > Volumes Encryption** (crittografia volumi)
3. Nella vista **Health: Volumes Encryption**, ordinare il campo **Encryption Type** oppure utilizzare il filtro per visualizzare i volumi con un tipo di crittografia specifico o che non sono crittografati (tipo di crittografia "None").

Visualizzazione dello stato anti-ransomware di tutti i volumi e le VM di storage

È possibile visualizzare un elenco di tutti i volumi e le VM di storage (SVM) e il relativo stato anti-ransomware corrente per determinare se i dati sui volumi e sulle SVM sono adeguatamente protetti da attacchi ransomware.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Per ulteriori informazioni sui diversi stati anti-ransomware, vedere "[ONTAP: Attiva l'anti-ransomware](#)".

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

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage > Volumes**.
2. Nel menu Visualizza, selezionare **Health > Security > Anti-ransomware**
3. Nella vista **Security: Anti-ransomware**, è possibile ordinare in base ai diversi campi o utilizzare il filtro.



L'anti-ransomware non è supportato per volumi offline, volumi limitati, volumi SnapLock, volumi FlexGroup, volumi FlexCache, Volumi solo SAN, volumi di macchine virtuali storage bloccate, volumi root di macchine virtuali storage o volumi di protezione dei dati.

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

Fasi

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



Il monitoraggio anti-ransomware non è supportato sulle macchine virtuali storage che non hanno attivato il protocollo NAS.

Visualizzazione di tutti gli eventi di sicurezza attivi

È possibile visualizzare tutti gli eventi di protezione attivi e assegnarli a un utente in grado di risolvere il problema. Inoltre, se alcuni eventi di protezione non si desidera ricevere, questo elenco può aiutare a identificare gli eventi che si desidera disattivare.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Fasi

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

Per impostazione predefinita, gli eventi nuovi e confermati vengono visualizzati nella pagina di inventario Gestione eventi.

2. Dal menu View (Visualizza), selezionare **Active Security events** (Eventi di sicurezza attivi).

La pagina visualizza tutti gli eventi New e Acknowledged Security generati negli ultimi 7 giorni.

Aggiunta di avvisi per eventi di sicurezza

È possibile configurare gli avvisi per singoli eventi di sicurezza come qualsiasi altro evento ricevuto da Unified Manager. Inoltre, se si desidera trattare tutti gli eventi di sicurezza allo stesso modo e inviare messaggi e-mail alla stessa persona, è possibile creare un singolo avviso per notificare l'attivazione di qualsiasi evento di sicurezza.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

L'esempio seguente mostra come creare un avviso per l'evento di protezione "Telnet Protocol enabled". In questo modo viene inviato un avviso se l'accesso Telnet è configurato per l'accesso amministrativo remoto al cluster. È possibile utilizzare questa stessa metodologia per creare avvisi per tutti gli eventi di sicurezza.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management > Alert Setup**.
2. Nella pagina **Alert Setup**, fare clic su **Add** (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 **Resources** (risorse) e selezionare il cluster o il cluster in cui si desidera attivare l'avviso.
5. Fare clic su **Eventi** ed eseguire le seguenti operazioni:
 - a. Nell'elenco gravità evento, selezionare **Avviso**.
 - b. Nell'elenco Eventi corrispondenti, selezionare **protocollo Telnet attivato**.
6. Fare clic su **azioni**, quindi selezionare il nome dell'utente che riceverà l'e-mail di avviso nel campo **Avvisa questi utenti**.
7. Configurare le altre opzioni di questa pagina per la frequenza di notifica, l'emissione di trap SNMP e l'esecuzione di uno script.

8. Fare clic su **Save** (Salva).

Disattivazione di eventi di sicurezza specifici

Tutti gli eventi sono attivati per impostazione predefinita. È possibile disattivare eventi specifici per impedire la generazione di notifiche per gli eventi che non sono importanti nel proprio ambiente. È possibile attivare gli eventi disattivati se si desidera riprendere la ricezione delle notifiche.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

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

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management > Event Setup**.
2. Nella pagina impostazione **evento**, disattivare o attivare gli eventi scegliendo una delle seguenti opzioni:

| Se si desidera... | Quindi... |
|------------------------|--|
| Disattivare gli eventi | <ol style="list-style-type: none">a. Fare clic su Disable (Disattiva).b. Nella finestra di dialogo Disable Events (Disattiva eventi), selezionare la severità Warning. Questa è la categoria per tutti gli eventi di sicurezza.c. Nella colonna Eventi corrispondenti, selezionare gli eventi di protezione che si desidera disattivare, quindi fare clic sulla freccia destra per spostarli nella colonna Disable Events (Disattiva eventi).d. Fare clic su Save and Close (Salva e chiudi).e. Verificare che gli eventi disattivati siano visualizzati nella vista elenco della pagina impostazione eventi. |
| Attivare gli eventi | <ol style="list-style-type: none">a. Dall'elenco degli eventi disattivati, selezionare la casella di controllo corrispondente all'evento o agli eventi che si desidera riabilitare.b. Fare clic su Enable (attiva). |

Eventi di sicurezza

Gli eventi di sicurezza forniscono informazioni sullo stato di sicurezza dei cluster ONTAP, delle macchine virtuali di storage e dei volumi in base ai parametri definiti nella *Guida al*

rafforzamento della sicurezza NetApp per ONTAP 9. Questi eventi notificano potenziali problemi in modo da poterne valutare la severità e, se necessario, risolvere il problema.

Gli eventi di sicurezza sono raggruppati per tipo di origine e includono il nome dell'evento e del trap, il livello di impatto e la severità. Questi eventi vengono visualizzati nelle categorie di eventi delle macchine virtuali del cluster e dello storage.

Informazioni sul copyright

Copyright © 2023 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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.