Gestione degli obiettivi di sicurezza del cluster

Active IQ Unified Manager 9.7

NetApp
April 17, 2024

Sommario

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.

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.

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.	Nessuna raccomandazione	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.	Nessuna raccomandazione	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.	Nessuna raccomandazione	No
Utenti certificati	Indica se un utente certificato è configurato per accedere al cluster.	Nessuna raccomandazione	No
Utenti locali	Indica se gli utenti locali sono configurati per l'accesso al cluster.	Nessuna raccomandazione	No

Categorie di conformità SVM

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 `cbc*`.	No	Sì

Parametro	Descrizione	Consiglio	Influisce sulla conformità SVM
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

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).

Parametro	Descrizione
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 del cluster di alto livello

Il pannello Security (sicurezza) di Unified ManagerDashboard mostra lo stato di sicurezza di alto livello per tutti i cluster o per un singolo cluster, a seconda della vista corrente.

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. Visualizzare il pannello **Security** per visualizzare lo stato generale.

   Questo pannello visualizza:

   - un elenco degli eventi di sicurezza ricevuti nelle ultime 24 ore
   - Un link da ciascuno di questi eventi alla pagina dei dettagli dell'evento
   - Un collegamento che consente di visualizzare tutti gli eventi di sicurezza attivi nella pagina dell'inventario di gestione degli eventi
   - lo stato di sicurezza del cluster (numero di cluster conformi o non conformi)
   - Lo stato di sicurezza SVM (numero di SVM conformi o non conformi)

- lo stato di crittografia del volume (numero di volumi crittografati o non crittografati)

4. Fare clic sulla freccia destra nella parte superiore del pannello per visualizzare i dettagli relativi alla sicurezza nella pagina **sicurezza**.

Visualizzazione dettagliata dello stato di sicurezza per cluster e SVM

La pagina Security (sicurezza) mostra lo stato di sicurezza di alto livello per tutti i cluster e lo stato di sicurezza dettagliato per i singoli cluster. Lo stato dettagliato del cluster include la conformità del cluster, la conformità SVM e la conformità alla crittografia dei volumi.

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**.

   La pagina Security (sicurezza) visualizza le seguenti informazioni:

   - lo stato di sicurezza del cluster (numero di cluster conformi o non conformi)
   - Lo stato di sicurezza SVM (numero di SVM conformi o non conformi)
   - lo stato di crittografia del volume (numero di volumi crittografati o non crittografati)
   - i metodi di autenticazione del cluster utilizzati su ciascun cluster
4. Fare riferimento a. "Guida al rafforzamento della sicurezza di NetApp per ONTAP 9" Per istruzioni su come rendere tutti i cluster, le SVM e i volumi conformi alle raccomandazioni di sicurezza NetApp.

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).

Prima di iniziare

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

A proposito di questa attività

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.

Risultati

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.

Prima di iniziare

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

A proposito di questa attività

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**, selezionare **Health** > **Volumes Encryption**
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 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.

Prima di iniziare

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.

Prima di iniziare

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

A proposito di questa attività

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 tap 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.

Prima di iniziare

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

A proposito di questa attività

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 **Setup evento**, disattivare o attivare gli eventi scegliendo una delle seguenti opzioni:

Se si desidera…	Quindi…
Disattivare gli eventi	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	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.