Gestire syslog

SANtricity 11.8

NetApp
December 16, 2024

Sommario

Gestire syslog

Visualizzare l’attività del registro di audit

Visualizzando i registri di controllo, gli utenti con autorizzazioni di amministratore della sicurezza possono monitorare le azioni degli utenti, gli errori di autenticazione, i tentativi di accesso non validi e la durata della sessione utente.

Prima di iniziare

È necessario effettuare l’accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Registro audit**.

   L’attività del registro di controllo viene visualizzata in formato tabulare, che include le seguenti colonne di informazioni:

   - **Data/ora** — Timestamp di quando lo storage array ha rilevato l’evento (in GMT).
   - **Username** — Nome utente associato all’evento. Per qualsiasi azione non autenticata sull’array di storage, viene visualizzato "N/A" come nome utente. Le azioni non autenticate potrebbero essere attivate dal proxy interno o da qualche altro meccanismo.
   - **Status Code** — Codice di stato HTTP dell’operazione (200, 400, ecc.) e testo descrittivo associato all’evento.
   - **URL a cui si accede** — URL completo (incluso host) e stringa di query.
   - **Client IP Address** — Indirizzo IP del client associato all’evento.
   - **Origine** — origine di registrazione associata all’evento, che può essere System Manager, CLI, Web Services o Support Shell.
   - **Descrizione** — ulteriori informazioni sull’evento, se applicabile.
3. Utilizzare le selezioni nella pagina Registro audit per visualizzare e gestire gli eventi.

Dettagli della selezione

Selezione	Descrizione
Mostra gli eventi del…	Limita gli eventi visualizzati in base all'intervallo di date (ultime 24 ore, ultimi 7 giorni, ultimi 30 giorni o un intervallo di date personalizzato).
Filtro	Limita gli eventi visualizzati dai caratteri immessi nel campo. Utilizzare le virgolette ("") per una corrispondenza esatta tra parole, immettere `OR` per restituire una o più parole o immettere un trattino (—) per omettere le parole.
Aggiornare	Selezionare **Refresh** (Aggiorna) per aggiornare la pagina agli eventi più recenti.
Visualizza/Modifica impostazioni	Selezionare **Visualizza/Modifica impostazioni** per aprire una finestra di dialogo che consente di specificare un criterio di log completo e il livello di azioni da registrare.
Eliminare gli eventi	Selezionare **Elimina** per aprire una finestra di dialogo che consente di rimuovere gli eventi precedenti dalla pagina.
Mostra/Nascondi colonne	Fare clic sull'icona **Mostra/Nascondi** colonna per selezionare altre colonne da visualizzare nella tabella. Le colonne aggiuntive includono: • **Method** — il metodo HTTP (AD esempio, POST, GET, DELETE, ecc.). • **Comando CLI eseguito** — comando CLI (grammatica) eseguito per richieste CLI sicure. • **CLI Return Status** — un codice di stato CLI o una richiesta di file di input dal client. • **Symbol procedure** — procedura di simbolo eseguita. • **SSH Event Type** — tipo di eventi Secure Shell (SSH), come login, logout e login_fail. • **SSH Session PID** — numero ID del processo della sessione SSH. • **SSH Session Duration(s)** — il numero di secondi in cui l'utente ha effettuato l'accesso. • **Authentication Type** — i tipi possono includere Local user, LDAP, SAML e Access token. • **Authentication ID** — ID della sessione autenticata.
Attiva/disattiva filtri colonna	Fare clic sull'icona **Alterna** per aprire i campi di filtraggio per ciascuna colonna. Immettere i caratteri all'interno di un campo colonna per limitare gli eventi visualizzati da tali caratteri. Fare nuovamente clic sull'icona per chiudere i campi di filtraggio.
Annulla le modifiche	Fare clic sull'icona **Annulla** per ripristinare la configurazione predefinita della tabella.

Selezione	Descrizione
Esportare	Fare clic su **Export** (Esporta) per salvare i dati della tabella in un file CSV (comma Separated Value).

Definire i criteri del registro di controllo

È possibile modificare il criterio di sovrascrittura e i tipi di eventi registrati nel registro di controllo.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

A proposito di questa attività

Questa attività descrive come modificare le impostazioni del registro di controllo, che includono il criterio per la sovrascrittura degli eventi precedenti e il criterio per la registrazione dei tipi di evento.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Registro di controllo**.
3. Selezionare **Visualizza/Modifica impostazioni**.

   Viene visualizzata la finestra di dialogo Audit Log Settings (Impostazioni registro di controllo).

4. Modificare il criterio di sovrascrittura o i tipi di eventi registrati.

Dettagli del campo

Impostazione	Descrizione
Sovrascrivere il criterio	Determina il criterio per la sovrascrittura di eventi precedenti quando viene raggiunta la capacità massima: • **Consente di sovrascrivere gli eventi meno recenti nel registro di controllo quando il registro di controllo è pieno** — sovrascrive gli eventi precedenti quando il registro di controllo raggiunge 50,000 record. • **Richiedere l'eliminazione manuale degli eventi del registro di controllo** — specifica che gli eventi non verranno cancellati automaticamente; viene invece visualizzato un avviso di soglia in corrispondenza della percentuale impostata. Gli eventi devono essere cancellati manualmente. Se il criterio di sovrascrittura è disattivato e le voci del registro di controllo raggiungono il limite massimo, l'accesso a System Manager viene negato agli utenti senza autorizzazioni di amministratore della sicurezza. Per ripristinare l'accesso al sistema agli utenti senza autorizzazioni di amministratore della sicurezza, un utente assegnato al ruolo di amministratore della protezione deve eliminare i vecchi record di eventi. I criteri di sovrascrittura non si applicano se un server syslog è configurato per l'archiviazione dei registri di controllo.
Livello di azioni da registrare	Determina i tipi di eventi da registrare: • **Registra solo eventi di modifica** — Mostra solo gli eventi in cui un'azione dell'utente comporta la modifica del sistema. • **Registra tutti gli eventi di modifica e di sola lettura** — Mostra tutti gli eventi, inclusa un'azione dell'utente che comporta la lettura o il download delle informazioni.

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

Eliminare gli eventi dal registro di controllo

È possibile cancellare il registro di controllo degli eventi precedenti, rendendo più gestibile la ricerca tra gli eventi. È possibile salvare gli eventi precedenti in un file CSV (comma-Separated Values) al momento dell'eliminazione.

Prima di iniziare

È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di

sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Selezionare la scheda **Registro di controllo**.
3. Selezionare **Delete** (Elimina).

   Viene visualizzata la finestra di dialogo Delete Audit Log.

4. Selezionare o immettere il numero di eventi meno recenti che si desidera eliminare.
5. Se si desidera esportare gli eventi cancellati in un file CSV (scelta consigliata), mantenere la casella di controllo selezionata. Quando si fa clic su **Delete** (Elimina) nella fase successiva, viene richiesto di inserire un nome e una posizione per il file. In caso contrario, se non si desidera salvare gli eventi in un file CSV, fare clic sulla casella di controllo per deselezionarla.
6. Fare clic su **Delete** (Elimina).

   Viene visualizzata una finestra di dialogo di conferma.

7. Digitare `delete` nel campo, quindi fare clic su **Elimina**.

   Gli eventi meno recenti vengono rimossi dalla pagina Registro di controllo.

Configurare il server syslog per i registri di controllo

Se si desidera archiviare i registri di controllo su un server syslog esterno, è possibile configurare le comunicazioni tra tale server e lo storage array. Una volta stabilita la connessione, i registri di controllo vengono salvati automaticamente nel server syslog.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- L'indirizzo del server syslog, il protocollo e il numero di porta devono essere disponibili. L'indirizzo del server può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Se il server utilizza un protocollo sicuro (ad esempio TLS), è necessario che nel sistema locale sia disponibile un certificato dell'autorità di certificazione (CA). I certificati CA identificano i proprietari dei siti Web per connessioni sicure tra server e client.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Dalla scheda Registro di controllo, selezionare **Configura server Syslog**.

   Viene visualizzata la finestra di dialogo Configura server Syslog.

3. Fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo Add Syslog Server (Aggiungi server Syslog).

4. Inserire le informazioni relative al server, quindi fare clic su **Aggiungi**.

- **Indirizzo server** — immettere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- **Protocol** (protocollo) — selezionare un protocollo dall'elenco a discesa (ad esempio TLS, UDP o TCP).
- **Carica certificato (opzionale)** — se è stato selezionato il protocollo TLS e non è stato ancora caricato un certificato CA firmato, fare clic su **Sfoglia** per caricare un file di certificato. I registri di controllo non vengono archiviati in un server syslog senza un certificato attendibile.

> Se il certificato diventa non valido in un secondo momento, l'handshake TLS avrà esito negativo. Di conseguenza, un messaggio di errore viene inviato al registro di controllo e i messaggi non vengono più inviati al server syslog. Per risolvere questo problema, è necessario correggere il certificato sul server syslog e accedere al **Impostazioni › Registro audit › Configura server Syslog › Test tutti**.

- **Port** — inserire il numero di porta del ricevitore syslog. Dopo aver fatto clic su **Add** (Aggiungi), viene visualizzata la finestra di dialogo Configure Syslog Servers (Configura server Syslog) e il server syslog configurato.

5. Per verificare la connessione del server con lo storage array, selezionare **Test All**.

Risultati

Dopo la configurazione, tutti i nuovi registri di controllo vengono inviati al server syslog. I registri precedenti non vengono trasferiti. Per configurare ulteriormente le impostazioni syslog per gli avvisi, vedere "Configurare il server syslog per gli avvisi".

```
NOTE: If multiple syslog servers are configured, all configured syslog
servers will receive an audit log.
```

Modificare le impostazioni del server syslog per i record del registro di controllo

È possibile modificare le impostazioni del server syslog utilizzato per l'archiviazione dei registri di controllo e caricare un nuovo certificato CA per il server.

Prima di iniziare

- È necessario effettuare l'accesso con un profilo utente che includa le autorizzazioni di amministratore di sicurezza. In caso contrario, le funzioni di gestione degli accessi non vengono visualizzate.
- L'indirizzo del server syslog, il protocollo e il numero di porta devono essere disponibili. L'indirizzo del server può essere un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- Se si sta caricando un nuovo certificato CA, il certificato deve essere disponibile nel sistema locale.

Fasi

1. Selezionare **Impostazioni › Gestione accessi**.
2. Dalla scheda Registro di controllo, selezionare **Configura server Syslog**.

   I server syslog configurati vengono visualizzati nella pagina.

3. Per modificare le informazioni sul server, selezionare l'icona **Edit** (matita) a destra del nome del server, quindi apportare le modifiche desiderate nei seguenti campi:

- **Server Address** — inserire un nome di dominio completo, un indirizzo IPv4 o un indirizzo IPv6.
- **Protocol** (protocollo) — selezionare un protocollo dall'elenco a discesa (ad esempio TLS, UDP o TCP).
- **Port** — inserire il numero di porta del ricevitore syslog.

4. Se il protocollo è stato modificato nel protocollo TLS sicuro (da UDP o TCP), fare clic su **Import Trusted Certificate** (Importa certificato attendibile) per caricare un certificato CA.
5. Per verificare la nuova connessione con lo storage array, selezionare **Test All**.

Risultati

Dopo la configurazione, tutti i nuovi registri di controllo vengono inviati al server syslog. I registri precedenti non vengono trasferiti.