Registrazione dell'audit

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

Sommario

Registrazione dell'audit

È possibile rilevare se i registri di controllo sono stati compromessi con l'utilizzo dei registri di controllo. Tutte le attività eseguite da un utente vengono monitorate e registrate nei registri di controllo. I controlli vengono eseguiti per tutte le funzionalità dell'interfaccia utente e delle API` esposte pubblicamente di Active IQ Unified Manager.

È possibile utilizzare il registro di controllo: Visualizzazione file* per visualizzare e accedere a tutti i file di registro di controllo disponibili in Active IQ Unified Manager. I file nella visualizzazione file del registro di controllo sono elencati in base alla data di creazione. Questa vista visualizza le informazioni di tutti i log di controllo acquisiti dall'installazione o dall'aggiornamento al presente nel sistema. Ogni volta che si esegue un'azione in Unified Manager, le informazioni vengono aggiornate e sono disponibili nei registri. Lo stato di ciascun file di log viene acquisito utilizzando l'attributo "file Integrity Status", che viene monitorato attivamente per rilevare la manomissione o l'eliminazione del file di log. I registri di controllo possono avere uno dei seguenti stati quando i registri di controllo sono disponibili nel sistema:

Stato	Descrizione
ATTIVO	File in cui vengono attualmente registrati i log.
NORMALE	File inattivo, compresso e memorizzato nel sistema.
MANOMESSO	File che è stato compromesso da un utente che ha modificato manualmente il file.
MANUAL_DELETE	File eliminato da un utente autorizzato.
ROLLOVER_DELETE	File che è stato eliminato a causa dell'annullamento in base a criteri di configurazione a rotazione.
UNEXPECTED_DELETE	File eliminato per motivi sconosciuti.

La pagina Registro di controllo include i seguenti pulsanti di comando:

- Configurare
- Eliminare
- Scarica

Il pulsante **DELETE** consente di eliminare qualsiasi registro di controllo elencato nella vista registri di controllo. È possibile eliminare un registro di controllo e, facoltativamente, fornire un motivo per eliminare il file, in modo da poter determinare un'eliminazione valida in futuro. La colonna REASON (MOTIVO) elenca il motivo insieme al nome dell'utente che ha eseguito l'operazione di eliminazione.

L'eliminazione di un file di log causerà l'eliminazione del file dal sistema, ma la voce nella tabella DB non verrà eliminata.

È possibile scaricare i registri di controllo da Active IQ Unified Manager utilizzando il pulsante **DOWNLOAD** nella sezione registri di controllo ed esportare i file di registro di controllo. I file contrassegnati con "NORMAL" o "MANOMESSI" vengono scaricati in un file compresso `.gzip` formato.

I file di log di audit vengono archiviati periodicamente e salvati nel database per riferimento. Prima dell'archiviazione, i registri di controllo sono dotati di firma digitale per garantire la sicurezza e l'integrità.

Quando viene generato un bundle AutoSupport completo, il bundle di supporto include file di log di audit sia archiviati che attivi. Tuttavia, quando viene generato un bundle di supporto leggero, include solo i registri di controllo attivi. I registri di controllo archiviati non sono inclusi.

Configurazione dei registri di audit

È possibile utilizzare il pulsante **Configura** nella sezione registri di controllo per configurare i criteri di rolling per i file di registro di controllo e per attivare la registrazione remota per i registri di controllo.

È possibile impostare i valori nei CAMPI **MAX FILE SIZE** e **AUDIT LOG RETENTION DAYS** in base alla quantità e alla frequenza desiderate dei dati che si desidera memorizzare nel sistema. Il valore nel campo **TOTAL AUDIT LOG SIZE** (DIMENSIONE TOTALE REGISTRO DI CONTROLLO) è la dimensione dei dati totali del registro di controllo presenti nel sistema. La policy di rollover è determinata dai valori nel campo **GIORNI DI CONSERVAZIONE DEL REGISTRO DI CONTROLLO**, **dimensione DEL FILE MAX** e **DIMENSIONE TOTALE DEL REGISTRO DI CONTROLLO**. Quando la dimensione del backup del registro di controllo raggiunge il valore configurato in **TOTAL AUDIT LOG SIZE**, il file archiviato per primo viene cancellato. Ciò significa che il file meno recente viene cancellato. Tuttavia, la voce del file continua a essere disponibile nel database ed è contrassegnata come "Elimina rollover". Il valore **GIORNI di CONSERVAZIONE del REGISTRO DI CONTROLLO** corrisponde al numero di giorni in cui i file di registro di controllo vengono conservati. Viene eseguito il rollover di qualsiasi file precedente al valore impostato in questo campo.

Fasi

1. Fare clic su **Audit Logs** > > **Configure**.
2. Inserire i valori nelle voci **MAX FILE SIZE**, **TOTAL AUDIT LOG SIZE** e **AUDIT LOG RETENTION DAYS**.

   Se si desidera attivare la registrazione remota, selezionare **Enable Remote Logging** (attiva registrazione remota).

Abilitazione della registrazione remota dei registri di controllo

È possibile selezionare la casella di controllo **Enable Remote Logging** (attiva registrazione remota) nella finestra di dialogo Configure Audit Logs (Configura registri di controllo) per attivare la registrazione remota dell'audit. È possibile utilizzare questa funzione per trasferire i registri di controllo a un server Syslog remoto. In questo modo, è possibile gestire i registri di controllo in caso di limiti di spazio.

La registrazione remota dei registri di controllo fornisce un backup a prova di manomissione nel caso in cui i file di registro di controllo sul server Active IQ Unified Manager vengano manomessi.

Fasi

1. Nella finestra di dialogo **Configura registri di controllo**, selezionare la casella di controllo **attiva registrazione remota**.

   Vengono visualizzati ulteriori campi per configurare la registrazione remota.

2. Immettere il **NOME HOST** e la **PORTA** del server remoto a cui si desidera connettersi.
3. Nel campo **CERTIFICATO CA DEL SERVER**, fare clic su **SFOGLIA** per selezionare un certificato pubblico del server di destinazione.

   Il certificato deve essere caricato in `.pem` formato. Questo certificato deve essere ottenuto dal server Syslog di destinazione e non deve essere scaduto. Il certificato deve contenere il "hostname" selezionato come parte di `SubjectAltName` (SAN).

4. Immettere i valori per i seguenti campi: **CHARSET**, **TIMEOUT CONNESSIONE**, **RITARDO DI RICONNESSIONE**.

   I valori devono essere espressi in millisecondi per questi campi.

5. Selezionare il formato Syslog e la versione del protocollo TLS richiesti nei campi **FORMAT** e **PROTOCOL**.
6. Selezionare la casella di controllo **Enable Client Authentication** (attiva autenticazione client) se il server Syslog di destinazione richiede l'autenticazione basata su certificato.

   Prima di salvare la configurazione del registro di controllo, sarà necessario scaricare il certificato di autenticazione del client e caricarlo sul server Syslog, altrimenti la connessione non avrà esito positivo. A seconda del tipo di server Syslog, potrebbe essere necessario creare un hash del certificato di autenticazione del client.

   Esempio: Syslog-ng richiede la creazione di un <hash> del certificato utilizzando il comando `openssl x509 -noout -hash -in cert.pem`, quindi collegare simbolicamente il certificato di autenticazione del client a un file denominato dopo <hash> .0.

7. Fare clic su **Save** (Salva) per configurare la connessione con il server e attivare la registrazione remota.

   Verrà reindirizzato alla pagina Audit Logs (registri di controllo).

> Il valore **Timeout connessione** può influire sulla configurazione. Se la risposta della configurazione richiede più tempo rispetto al valore definito, potrebbe verificarsi un errore di configurazione a causa di un errore di connessione. Per stabilire una connessione corretta, aumentare il valore **Timeout connessione** e riprovare a eseguire la configurazione.

Informazioni sul copyright

Informazioni sul marchio commerciale