Syslog managen

SANtricity 11.7

NetApp
February 12, 2024

Inhalt

Syslog managen

Zeigen Sie die Aktivität des Prüfprotokolls an

Durch die Anzeige von Prüfprotokollen können Benutzer mit Sicherheitsadministratorberechtigungen Benutzeraktionen, Authentifizierungsfehler, ungültige Anmeldeversuche und die Lebensdauer der Benutzersitzung überwachen.

Bevor Sie beginnen

Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **Überwachungsprotokoll** aus.

   Die Aktivität des Überwachungsprotokolls wird im Tabellenformat angezeigt, das die folgenden Informationspalten enthält:

   - **Datum/Uhrzeit** — Zeitstempel, wann das Speicherarray das Ereignis erkannt hat (in GMT).
   - **Benutzername** — der Benutzername, der dem Ereignis zugeordnet ist. Bei nicht authentifizierten Aktionen im Speicher-Array wird „N/A“ als Benutzername angezeigt. Nicht authentifizierte Aktionen können vom internen Proxy oder einem anderen Mechanismus ausgelöst werden.
   - **Statuscode** — HTTP-Statuscode der Operation (200, 400 usw.) und beschreibenden Text, der dem Ereignis zugeordnet ist.
   - **URL abgerufen** — vollständige URL (einschließlich Host) und Abfragezeichenfolge.
   - **Client-IP-Adresse** — IP-Adresse des Clients, der dem Ereignis zugeordnet ist.
   - **Quelle** — Logging-Quelle, die mit dem Ereignis verknüpft ist, kann System Manager, CLI, Web Services oder Support Shell sein.
   - **Beschreibung** — zusätzliche Informationen über die Veranstaltung, falls zutreffend.
3. Verwenden Sie die Auswahl auf der Seite „Überwachungsprotokoll“, um Ereignisse anzuzeigen und zu verwalten.

Auswahldetails

Auswahl	Beschreibung
Zeigt Ereignisse aus dem…	Grenzwerte für Ereignisse, die nach Datumsbereich angezeigt werden (letzte 24 Stunden, letzte 7 Tage, letzte 30 Tage oder ein benutzerdefinierter Datumsbereich).
Filtern	Begrenzungsereignisse, die durch die in das Feld eingegebenen Zeichen angezeigt werden. Verwenden Sie Anführungszeichen (") für eine genaue Wortabgleiche, geben Sie ein `OR` Um ein oder mehrere Wörter zurückzugeben, oder geben Sie einen Strich (—) ein, um Wörter auszulassen.
Aktualisierung	Wählen Sie **Aktualisieren**, um die Seite auf die aktuellen Ereignisse zu aktualisieren.
Einstellungen Anzeigen/Bearbeiten	Wählen Sie **Einstellungen anzeigen/bearbeiten** aus, um ein Dialogfeld zu öffnen, in dem Sie eine vollständige Protokollrichtlinie und eine Ebene der zu protokollierenden Aktionen festlegen können.
Löschen von Ereignissen	Wählen Sie **Löschen** aus, um ein Dialogfeld zu öffnen, in dem Sie alte Ereignisse von der Seite entfernen können.
Spalten ein-/ausblenden	Klicken Sie auf das Spaltensymbol **ein-/ausblenden** So wählen Sie zusätzliche Spalten aus, die in der Tabelle angezeigt werden sollen. Weitere Spalten sind: • **Methode** — die HTTP-Methode (z. B. POST, GET, DELETE usw.). • **CLI Befehl ausgeführt** — der CLI-Befehl (Grammatik) ausgeführt für Secure CLI Anfragen. • **CLI Rückgabestatus** — Ein CLI-Statuscode oder eine Anforderung für Eingabedateien vom Client. • **Symbol-Verfahren** — das Symbol-Verfahren ausgeführt. • **SSH Event Type** — Secure Shell (SSH) Ereignistyp, wie Login, Logout und Login_fail. • **SSH Session PID** — Prozess-ID-Nummer der SSH-Sitzung. • **SSH Sitzungsdauer(en)** — die Anzahl der Sekunden, die der Benutzer angemeldet war. • **Authentifizierungstyp** — Typen können lokalen Benutzer, LDAP, SAML und Access Token enthalten. • **Authentifizierungs-ID** — ID der authentifizierten Sitzung.
Spaltenfilter ein- oder ausschalten	Klicken Sie auf das Symbol **Umschalten** Zum Öffnen von Filterfeldern für jede Spalte. Geben Sie in ein Spaltenfeld Zeichen ein, um die durch diese Zeichen angezeigten Ereignisse einzuschränken. Klicken Sie erneut auf das Symbol, um die Filterfelder zu schließen.

Auswahl	Beschreibung
Änderungen rückgängig machen	Klicken Sie auf das Symbol **Rückgängig** Um die Tabelle auf die Standardkonfiguration zurückzugeben.
Exportieren	Klicken Sie auf **Exportieren**, um die Tabellendaten in einer kommagetrennten Datei (CSV) zu speichern.

Richtlinien für Prüfprotokolle definieren

Sie können die Überschreibungsrichtlinie und die im Audit-Protokoll aufgezeichneten Ereignistypen ändern.

Bevor Sie beginnen

Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.

Über diese Aufgabe

Dieser Task beschreibt, wie die Einstellungen für das Überwachungsprotokoll geändert werden, einschließlich der Richtlinie zum Überschreiben alter Ereignisse und der Richtlinie für die Aufzeichnung von Ereignistypen.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **Prüfprotokoll** aus.
3. Wählen Sie **Einstellungen Anzeigen/Bearbeiten**.

   Das Dialogfeld Einstellungen für das Überwachungsprotokoll wird geöffnet.

4. Ändern Sie die Überschreibungsrichtlinie oder die Arten der aufgezeichneten Ereignisse.

Felddetails

Einstellung	Beschreibung
Überschreibungsrichtlinie	Legt die Richtlinie zum Überschreiben alter Ereignisse fest, wenn die maximale Kapazität erreicht ist: • **Die ältesten Ereignisse im Audit-Protokoll können überschrieben werden, wenn das Audit-Protokoll voll ist** — überschreibt die alten Ereignisse, wenn das Audit-Protokoll 50,000 Datensätze erreicht. • **Das manuelle Löschen von Audit-Protokollereignissen ist erforderlich** — gibt an, dass Ereignisse nicht automatisch gelöscht werden; stattdessen erscheint eine Schwellenwertwarnung im festgelegten Prozentsatz. Ereignisse müssen manuell gelöscht werden. Wenn die Überschreibungsrichtlinie deaktiviert ist und die Einträge des Prüfprotokolls die maximale Grenze erreichen, wird Benutzern der Zugriff auf System Manager ohne die Berechtigung des Sicherheitsadministrators verweigert. Um den Systemzugriff für Benutzer ohne Sicherheitsadministrator-Berechtigungen wiederherzustellen, muss ein Benutzer, der der Rolle Sicherheitsadministrator zugewiesen ist, die alten Ereignisdatensätze löschen. Überschreibungsrichtlinien gelten nicht, wenn ein Syslog-Server für die Archivierung von Audit-Protokollen konfiguriert ist.
Level der zu protokollierenden Aktionen	Legt die Arten von zu protokollierenden Ereignissen fest: • **Änderungsereignisse aufzeichnen** — zeigt nur Ereignisse an, bei denen eine Benutzeraktion eine Systemänderung beinhaltet. • **Alle Änderungen und schreibgeschützten Ereignisse** — zeigt alle Ereignisse an, einschließlich einer Benutzeraktion, die das Lesen oder Herunterladen von Informationen beinhaltet.

5. Klicken Sie Auf **Speichern**.

Löschen von Ereignissen aus dem Auditprotokoll

Sie können das Audit-Protokoll von alten Ereignissen löschen, wodurch das Suchen durch Ereignisse leichter zu verwalten ist. Sie haben die Möglichkeit, alte Ereignisse beim Löschen in einer CSV-Datei (kommagetrennte Werte) zu speichern.

Bevor Sie beginnen

Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie die Registerkarte **Prüfprotokoll** aus.
3. Wählen Sie **Löschen**.

   Das Dialogfeld Prüfprotokoll löschen wird geöffnet.

4. Wählen Sie oder geben Sie die Anzahl der ältesten Ereignisse ein, die Sie löschen möchten.
5. Wenn Sie die gelöschten Ereignisse in eine CSV-Datei exportieren möchten (empfohlen), lassen Sie das Kontrollkästchen aktiviert. Sie werden aufgefordert, einen Dateinamen und Speicherort einzugeben, wenn Sie im nächsten Schritt auf **Löschen** klicken. Wenn Sie keine Ereignisse in einer CSV-Datei speichern möchten, aktivieren Sie das Kontrollkästchen, um die Auswahl aufzuheben.
6. Klicken Sie Auf **Löschen**.

   Ein Bestätigungsdialogfeld wird geöffnet.

7. Typ `delete` Klicken Sie im Feld auf **Löschen**.

   Die ältesten Ereignisse werden von der Seite „Überwachungsprotokoll“ entfernt.

Syslog-Server für Audit-Protokolle konfigurieren

Wenn Sie Auditprotokolle auf einem externen Syslog-Server archivieren möchten, können Sie die Kommunikation zwischen diesem Server und dem Speicher-Array konfigurieren. Nach der Verbindungsherstellung werden Audit-Protokolle automatisch auf dem Syslog-Server gespeichert.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Die Syslog-Serveradresse, das Protokoll und die Portnummer müssen verfügbar sein. Bei der Serveradresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
- Wenn Ihr Server ein sicheres Protokoll verwendet (z. B. TLS), muss auf Ihrem lokalen System ein Zertifikat für Zertifizierungsstellen (CA) verfügbar sein. CA-Zertifikate identifizieren Website-Eigentümer für sichere Verbindungen zwischen Servern und Clients.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie auf der Registerkarte Audit Log die Option **Configure Syslog Servers** aus.

   Das Dialogfeld Configure Syslog Servers wird geöffnet.

3. Klicken Sie Auf **Hinzufügen**.

   Das Dialogfeld Syslog Server hinzufügen wird geöffnet.

4. Geben Sie Informationen für den Server ein, und klicken Sie dann auf **Hinzufügen**.
   - **Server-Adresse** — Geben Sie einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse ein.
   - **Protokoll** — Wählen Sie aus der Dropdown-Liste ein Protokoll aus (z. B. TLS, UDP oder TCP).
   - **Zertifikat hochladen (optional)** — Wenn Sie das TLS-Protokoll ausgewählt haben und noch kein signiertes CA-Zertifikat hochgeladen haben, klicken Sie auf **Durchsuchen**, um eine Zertifikatdatei hochzuladen. Audit-Protokolle werden nicht ohne vertrauenswürdiges Zertifikat auf einem Syslog-Server archiviert.

     Wenn das Zertifikat später ungültig wird, schlägt der TLS-Handshake fehl. Als Ergebnis wird eine Fehlermeldung in das Auditprotokoll geschrieben und Meldungen werden nicht mehr an den Syslog-Server gesendet. Um dieses Problem zu lösen, müssen Sie das Zertifikat auf dem Syslog-Server beheben und dann zum Menü:Einstellungen[Audit-Protokoll > Syslog-Server konfigurieren > Alle testen] wechseln.

   - **Port** — Geben Sie die Portnummer für den Syslog-Empfänger ein. Nachdem Sie auf **Hinzufügen** geklickt haben, wird das Dialogfeld Configure Syslog Servers geöffnet und der konfigurierte Syslog Server auf der Seite angezeigt.
5. Um die Serververbindung mit dem Speicher-Array zu testen, wählen Sie **Alle testen**.

Ergebnisse

Nach der Konfiguration werden alle neuen Audit-Protokolle an den Syslog-Server gesendet. Frühere Protokolle werden nicht übertragen.

Bearbeiten Sie die Syslog-Servereinstellungen für Audit-Protokolldatensätze

Sie können die Einstellungen für den Syslog-Server ändern, der für die Archivierung von Audit-Protokollen verwendet wird, und auch ein neues Zertifikat für die Zertifizierungsstelle (Certificate Authority, CA) für den Server hochladen.

Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Die Syslog-Serveradresse, das Protokoll und die Portnummer müssen verfügbar sein. Bei der Serveradresse kann es sich um einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse oder eine IPv6-Adresse handeln.
- Wenn Sie ein neues CA-Zertifikat hochladen, muss das Zertifikat auf Ihrem lokalen System verfügbar sein.

Schritte

1. Wählen Sie Menü:Einstellungen[Zugriffsverwaltung].
2. Wählen Sie auf der Registerkarte Audit Log die Option **Configure Syslog Servers** aus.

   Konfigurierte Syslog-Server werden auf der Seite angezeigt.
3. Um die Serverinformationen zu bearbeiten, wählen Sie rechts neben dem Servernamen das Symbol **Bearbeiten** (Bleistift) aus und nehmen Sie die gewünschten Änderungen in den folgenden Feldern vor:
   - **Server-Adresse** — Geben Sie einen vollständig qualifizierten Domänennamen, eine IPv4-Adresse

oder eine IPv6-Adresse ein.

- **Protokoll** — Wählen Sie aus der Dropdown-Liste ein Protokoll aus (z. B. TLS, UDP oder TCP).
- **Port** — Geben Sie die Portnummer für den Syslog-Empfänger ein.

4. Wenn Sie das Protokoll in das sichere TLS-Protokoll (entweder von UDP oder TCP) geändert haben, klicken Sie auf **Vertrautes Zertifikat importieren**, um ein CA-Zertifikat hochzuladen.
5. Um die neue Verbindung mit dem Speicher-Array zu testen, wählen Sie **Alle testen**.

Ergebnisse

Nach der Konfiguration werden alle neuen Audit-Protokolle an den Syslog-Server gesendet. Frühere Protokolle werden nicht übertragen.