管理系統記錄
SANtricity 11.8

NetApp
June 24, 2024

目錄

管理系統記錄

檢視稽核記錄活動

透過檢視稽核記錄、具有「安全性管理」權限的使用者可以監控使用者動作、驗證失敗、無效的登入嘗試、以及使用者工作階段壽命。

開始之前

您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。

步驟

1. 選取功能表：設定[Access Management（存取管理）]。
2. 選取「稽核記錄」索引標籤。

   稽核記錄活動會以表格格式顯示、其中包含下列資訊欄：

   - 日期/時間-儲存陣列偵測到事件的時間戳記（以GMT[時間]為準）。
   - 使用者名稱：與事件相關的使用者名稱。對於儲存陣列上的任何未驗證動作、「N/A」會顯示為使用者名稱。未驗證的動作可能會由內部Proxy或其他機制觸發。
   - 狀態代碼-作業的HTTP狀態代碼（200、400等）、以及與事件相關的說明文字。
   - * URL access*-完整URL（包括主機）和查詢字串。
   - 用戶端**IP**位址-與事件相關聯之用戶端的IP位址。
   - 來源：與事件相關的記錄來源、可以是System Manager、CLI、Web Services或Support Shell。
   - 說明：事件的其他相關資訊（若適用）。
3. 使用「稽核記錄」頁面上的選項來檢視及管理事件。

選擇詳細資料

選擇	說明
從…顯示事件	限制依日期範圍（過去24小時、過去7天、過去30天或自訂日期範圍）顯示的事件。
篩選器	限制以欄位中輸入的字元顯示的事件。請使用引號（""）表示完全相符的字詞、輸入「OR」以傳回一或多個字詞、或輸入破折號（-）以省略字詞。
重新整理	選擇* Refresh*（重新整理*）、將頁面更新為最新的事件。
檢視/編輯設定	選取*檢視/編輯設定*以開啟對話方塊、讓您指定要記錄的完整記錄原則和行動層級。
刪除事件	選取*刪除*可開啟對話方塊、讓您從頁面移除舊事件。
顯示/隱藏欄	按一下*顯示/隱藏*欄圖示 可選擇要在表格中顯示的其他列。其他欄位包括： • 方法：HTTP方法（例如POST、GET、DELETE等）。 • **CLI**命令已執行—針對安全CLI要求執行的CLI命令（語法）。 • * CLI傳回狀態*：CLI狀態代碼或用戶端輸入檔的要求。 • 符號程序-執行的符號程序。 • * SSH事件類型*-安全Shell（SSH）事件類型、例如登入、登出及login_fail。 • * SSH工作階段PID*- SSH工作階段的處理序ID編號。 • * SSH工作階段持續時間*-使用者登入的秒數。 • 驗證類型：類型可以包括本機使用者、LDAP、SAML及存取權杖。 • 驗證**ID**-已驗證工作階段的ID。
切換欄篩選條件	按一下*切換*圖示 開啟每欄的篩選欄位。在欄位中輸入字元、以限制這些字元所顯示的事件。再按一下圖示以關閉篩選欄位。
復原變更	按一下「復原」圖示 可將表恢復爲默認配置。
匯出	按一下「匯出」、將表格資料儲存至以逗號分隔的值（CSV）檔案。

定義稽核記錄原則

您可以變更覆寫原則及稽核記錄中記錄的事件類型。

開始之前

您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。

關於這項工作

此工作說明如何變更稽核記錄設定、包括覆寫舊事件的原則、以及記錄事件類型的原則。

步驟

1. 選取功能表：設定[Access Management（存取管理）]。
2. 選取*稽核記錄*索引標籤。
3. 選取*檢視/編輯設定*。

   「稽核記錄設定」對話方塊隨即開啟。

4. 變更覆寫原則或記錄的事件類型。

   欄位詳細資料

設定	說明
覆寫原則	決定當達到最大容量時覆寫舊事件的原則： • *當稽核日誌已滿*時、允許覆寫稽核日誌中最舊的事件；當稽核日誌達到50、000筆記錄時、會覆寫舊事件。 • 要求手動刪除稽核記錄事件-指定不會自動刪除事件、而是在設定的百分比顯示臨界值警告。必須手動刪除事件。 如果停用覆寫原則、且稽核記錄項目達到上限、則沒有「安全性管理」權限的使用者將無法存取System Manager。若要將系統存取權限還原給沒有「安全性管理」權限的使用者、則指派給「安全性管理」角色的使用者必須刪除舊的事件記錄。 如果將syslog伺服器設定為歸檔稽核記錄、則不適用覆寫原則。
要記錄的行動層級	決定要記錄的事件類型： • 僅記錄修改事件-僅顯示使用者動作涉及變更系統的事件。 • 記錄所有修改和唯讀事件-顯示所有事件、包括需要讀取或下載資訊的使用者動作。

5. 按一下「 * 儲存 * 」。

從稽核記錄刪除事件

您可以清除舊事件的稽核記錄、以便更容易管理事件搜尋。您可以選擇在刪除時將舊事件儲存至CSV（以逗號分隔的值）檔案。

開始之前

您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。

步驟

1. 選取功能表：設定[Access Management（存取管理）]。
2. 選取*稽核記錄*索引標籤。
3. 選擇*刪除*。

   「刪除稽核記錄」對話方塊隨即開啟。
4. 選取或輸入您要刪除的最舊事件數目。
5. 如果您要將刪除的事件匯出至CSV檔案（建議）、請保持核取方塊為選取狀態。在下一步中按一下「刪除」時、系統會提示您輸入檔案名稱和位置。否則、如果您不想將事件儲存至CSV檔案、請按一下核取方塊加以取消選取。
6. 按一下*刪除*。

   隨即開啟確認對話方塊。
7. 在欄位中輸入「刪除」、然後按一下「刪除」。

   最舊的事件會從「稽核記錄」頁面移除。

設定系統記錄伺服器進行稽核記錄

如果您想要將稽核記錄歸檔到外部syslog伺服器、可以設定該伺服器與儲存陣列之間的通訊。建立連線之後、稽核記錄會自動儲存至syslog伺服器。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。
- 系統記錄伺服器位址、傳輸協定和連接埠號碼必須可用。伺服器位址可以是完整網域名稱、IPv4位址或IPv6位址。
- 如果您的伺服器使用安全傳輸協定（例如TLS）、則您的本機系統必須具備憑證授權單位（CA）憑證。CA憑證可識別網站擁有者、以確保伺服器與用戶端之間的安全連線。

步驟

1. 選取功能表：設定[Access Management（存取管理）]。
2. 從「稽核記錄」索引標籤、選取*「設定Syslog伺服器」*。

   此時將打開Configure Syslog Servers（配置Syslog服務器）對話框。

3. 按一下「 * 新增 * 」。

   此時會開啟「新增Syslog伺服器」對話方塊。

4. 輸入伺服器的資訊、然後按一下*「Add*（新增*）」。

   - 伺服器位址-輸入完整網域名稱、IPv4位址或IPv6位址。
   - 傳輸協定-從下拉式清單中選取傳輸協定（例如TLS、udp或TCP）。
   - 上傳憑證（選用）-如果您選取TLS傳輸協定、但尚未上傳簽署的CA憑證、請按一下*瀏覽*上傳憑證檔案。稽核記錄不會歸檔至沒有信任憑證的syslog伺服器。

     如果憑證稍後失效、TLS交握將會失敗。因此、系統會在稽核記錄中張貼錯誤訊息、而不會再將訊息傳送到syslog伺服器。若要解決此問題、您必須先修正syslog伺服器上的憑證、然後前往功能表：設定[稽核記錄>設定Syslog伺服器>全部測試]。

   - * Port*（連接埠）-輸入syslog接收器的連接埠號碼。按一下「新增」之後、「設定Syslog伺服器」對話方塊隨即開啟、並在頁面上顯示您設定的syslog伺服器。

5. 若要測試伺服器與儲存陣列的連線、請選取* Test All*。

結果

設定完成後、所有新的稽核記錄都會傳送到syslog伺服器。不會傳輸先前的記錄。若要進一步設定警示的Syslog 設定、請參閱 "設定系統記錄伺服器以發出警示"。

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

編輯稽核記錄的**syslog**伺服器設定

您可以變更用於歸檔稽核記錄的syslog伺服器設定、也可以上傳伺服器的新憑證授權單位（CA）憑證。

開始之前

- 您必須以包含安全管理員權限的使用者設定檔登入。否則、就不會顯示存取管理功能。
- 系統記錄伺服器位址、傳輸協定和連接埠號碼必須可用。伺服器位址可以是完整網域名稱、IPv4位址或IPv6位址。
- 如果您要上傳新的CA憑證、則必須在本機系統上提供該憑證。

步驟

1. 選取功能表：設定[Access Management（存取管理）]。
2. 從「稽核記錄」索引標籤、選取*「設定Syslog伺服器」*。

   已設定的syslog伺服器會顯示在頁面上。

3. 若要編輯伺服器資訊、請選取伺服器名稱右側的*編輯*（鉛筆）圖示、然後在下列欄位中進行所需的變更：

   - 伺服器位址-輸入完整網域名稱、IPv4位址或IPv6位址。

- 傳輸協定-從下拉式清單中選取傳輸協定（例如TLS、udp或TCP）。
- * Port*（連接埠）-輸入syslog接收器的連接埠號碼。

4. 如果您將傳輸協定變更為安全TLS傳輸協定（從UDP或TCP）、請按一下*匯入信任的憑證*上傳CA憑證。
5. 若要測試與儲存陣列的新連線、請選取*「Test All（測試全部）」*。

結果

設定完成後、所有新的稽核記錄都會傳送到syslog伺服器。不會傳輸先前的記錄。