



警示
SANtricity 11.8
NetApp
December 16, 2024

目錄

警示	1
警示總覽	1
概念	1
管理電子郵件警示	3
管理SNMP警示	6
管理系統記錄警示	13
常見問題集	15

警示

警示總覽

您可以設定System Manager以透過電子郵件、SNMP設陷和系統記錄訊息傳送儲存陣列警示。

什麼是警示？

alerts 通知系統管理員儲存陣列上發生的重要事件。事件可能包括電池故障、從最佳狀態移至離線狀態的元件、或是控制器中的備援錯誤等問題。所有重大事件都會被視為「警示」、以及一些警告和資訊事件。

深入瞭解：

- ["警示的運作方式"](#)
- ["警示術語"](#)

如何設定警示？

您可以將警示設定為以訊息形式傳送至一或多個電子郵件地址、作為SNMP設陷傳送至SNMP伺服器、或作為訊息傳送至syslog伺服器。警示組態可從功能表：設定[警示]取得。

深入瞭解：

- ["設定郵件伺服器和收件者的警示"](#)
- ["設定系統記錄伺服器以發出警示"](#)
- ["設定 SNMP 警示"](#)

相關資訊

深入瞭解警示相關概念：

- ["事件記錄總覽"](#)
- ["時間戳記不一致"](#)

概念

警示的運作方式

警示會通知系統管理員儲存陣列上發生的重要事件。警示可透過電子郵件、SNMP設陷和系統記錄傳送。

警示程序的運作方式如下：

1. 系統管理員可在System Manager中設定下列一或多種警示方法：

- 電子郵件-訊息會傳送至電子郵件地址。
 - * SNMP *- SNMP設陷會傳送至SNMP伺服器。
 - 系統日誌-訊息會傳送至系統日誌伺服器。
2. 儲存陣列的事件監視器偵測到問題時、會將該問題的相關資訊寫入事件記錄（可從功能表：Support[事件記錄]取得）。例如、問題可能包括電池故障、從最佳化移至離線的元件、或是控制器中的備援錯誤等事件。
 3. 如果事件監控器判定事件為「alertable」（警示表）、則會使用設定的警示方法（電子郵件、SNMP及/或系統記錄）傳送通知。所有重大事件都會被視為「警示」、以及一些警告和資訊事件。

警示組態

您可以從「初始設定」精靈（僅限電子郵件警示）或「警示」頁面設定警示。若要檢查目前的組態、請前往功能表：設定[警示]。

警示區塊會顯示警示組態、這可以是下列其中一項：

- 未設定。
- 已設定；至少已設定一種警示方法。若要判斷要設定哪些警示方法、請將游標指向方塊。

警示資訊

警示可包含下列類型的資訊：

- 儲存陣列名稱。
- 與事件記錄項目相關的事件錯誤類型。
- 事件發生的日期和時間。
- 活動的簡短說明。



Syslog 警示遵循 RFC 5424 訊息標準。

警示術語

瞭解警示條款如何適用於您的儲存陣列。

元件	說明
事件監控	事件監視器位於儲存陣列上、並作為背景工作執行。當事件監控器偵測到儲存陣列上的異常狀況時、會將有關問題的資訊寫入事件記錄。問題可能包括電池故障、從最佳狀態移至離線狀態的元件、或是控制器中的備援錯誤等事件。如果事件監控器判定事件為「alertable」（警示表）、則會使用設定的警示方法（電子郵件、SNMP及/或系統記錄）傳送通知。所有重大事件都會被視為「警示」、以及一些警告和資訊事件。
郵件伺服器	郵件伺服器用於傳送和接收電子郵件警示。伺服器使用簡易郵件傳輸傳輸協定（Simple Mail Transfer Protocol、簡稱SMTP）。

元件	說明
SNMP	簡易網路管理傳輸協定（SNMP）是一種網際網路標準傳輸協定、用於管理和共用IP網路上裝置之間的資訊。
SNMP設陷	SNMP設陷是傳送至SNMP伺服器的通知。陷阱包含儲存陣列重大問題的相關資訊。
SNMP設陷目的地	SNMP設陷目的地是執行SNMP服務之伺服器的IPv4或IPv6位址。
社群名稱	社群名稱是類似SNMP環境中網路伺服器密碼的字串。
mib檔案	管理資訊庫（mib）檔案定義儲存陣列中所監控及管理的資料。必須使用SNMP服務應用程式在伺服器上複製及編譯。支援網站上的System Manager軟體可提供此mib檔案。
mib變數	管理資訊庫（MIB）變數可傳回儲存陣列名稱、陣列位置、以及回應SNMP GetRequest的聯絡人等值。
系統記錄	syslog是網路裝置用來傳送事件訊息至記錄伺服器的傳輸協定。
UDP	使用者資料包傳輸協定（UDP）是傳輸層傳輸協定、可在其封包標頭中指定來源連接埠和目的地連接埠號碼。

管理電子郵件警示

設定郵件伺服器和收件者的警示

若要設定電子郵件警示、您必須指定警示收件者的郵件伺服器位址和電子郵件位址。最多允許20個電子郵件地址。

開始之前

- 郵件伺服器的位址必須是可用的。位址可以是IPV4或IPV6位址、也可以是完整網域名稱。



若要使用完整網域名稱、您必須在兩個控制器上設定DNS伺服器。您可以從「硬體」頁面設定DNS伺服器。

- 必須提供電子郵件地址、才能作為警示傳送者使用。這是警示訊息「寄件者」欄位中顯示的位址。在SMTP傳輸協定中需要寄件者位址、否則會產生錯誤。
- 警示收件者的電子郵件地址必須可供使用。收件者通常是網路管理員或儲存管理員的位址。您最多可以輸入20個電子郵件地址。

關於這項工作

此工作說明如何設定郵件伺服器、輸入寄件者和收件者的電子郵件地址、以及測試從「警示」頁面輸入的所有電子郵件地址。



您也可以從初始設定精靈設定電子郵件警示。

步驟

1. 選取功能表：設定[警示]。
2. 選取*電子郵件*索引標籤。

如果尚未設定電子郵件伺服器、「電子郵件」標籤會顯示「設定郵件伺服器」。

3. 選擇*設定郵件伺服器*。

此時將打開Configure Mail Server（配置郵件服務器）對話框。

4. 輸入郵件伺服器資訊、然後按一下「儲存」。

◦ 郵件伺服器位址-輸入郵件伺服器的完整網域名稱、IPv4位址或IPv6位址。



若要使用完整網域名稱、您必須在兩個控制器上設定DNS伺服器。您可以從「硬體」頁面設定DNS伺服器。

- 電子郵件寄件者地址-輸入有效的電子郵件地址、作為電子郵件寄件者。此地址會出現在電子郵件訊息的「寄件者」欄位中。
- 加密-如果您要加密訊息、請選取*SMTP*或*STARTTLS*作為加密類型、然後選取加密訊息的連接埠號碼。否則、請選取*無*。
- 使用者名稱與密碼-如有需要、請輸入使用者名稱與密碼、以便與傳出傳送者和郵件伺服器進行驗證。
- 在電子郵件中加入聯絡資訊-若要在警示訊息中包含寄件者的聯絡資訊、請選取此選項、然後輸入姓名和電話號碼。

按一下「儲存」之後、電子郵件地址會出現在「警示」頁面的「電子郵件」索引標籤中。

5. 選取*新增電子郵件*。

「新增電子郵件」對話方塊隨即開啟。

6. 輸入警示收件者的一或多個電子郵件地址、然後按一下*「Add*（新增*）」。

電子郵件地址會顯示在「警示」頁面上。

7. 如果您想確定電子郵件地址有效、請按一下*測試所有電子郵件*、將測試訊息傳送給收件者。

結果

設定電子郵件警示之後、每當發生警示事件時、事件監視器都會將電子郵件訊息傳送給指定的收件者。

編輯警示的電子郵件地址

您可以變更接收電子郵件警示的收件者電子郵件地址。

開始之前

您要編輯的電子郵件地址必須在「警示」頁面的「電子郵件」標籤中定義。

步驟

1. 選取功能表：設定[警示]。
2. 選取*電子郵件*索引標籤。
3. 從*電子郵件地址*表格中、選取您要變更的地址、然後按一下最右側的*編輯*（鉛筆）圖示。

該列會變成可編輯的欄位。

4. 輸入新地址、然後按一下*「Save*（勾號）」圖示。



如果您要取消變更、請選取*取消*（X）圖示。

結果

「警示」頁面的「電子郵件」索引標籤會顯示更新的電子郵件地址。

新增警示的電子郵件地址

您最多可新增20個電子郵件警示收件者。

步驟

1. 選取功能表：設定[警示]。
2. 選取*電子郵件*索引標籤。
3. 選取*新增電子郵件*。

「新增電子郵件」對話方塊隨即開啟。

4. 在空白欄位中、輸入新的電子郵件地址。如果您要新增多個地址、請選取*新增其他電子郵件*以開啟另一個欄位。
5. 按一下「*新增*」。

結果

「警示」頁面的「電子郵件」索引標籤會顯示新的電子郵件地址。

刪除郵件伺服器或電子郵件地址以取得警示

您可以移除先前定義的郵件伺服器、使警示不再傳送至電子郵件地址、或是移除個別的電子郵件地址。

步驟

1. 選取功能表：設定[警示]。
2. 選取*電子郵件*索引標籤。
3. 從表格中、執行下列其中一項：
 - 若要移除郵件伺服器、使警示不再傳送至電子郵件地址、請選取郵件伺服器的列。
 - 若要移除電子郵件地址、使警示不再傳送至此地址、請選取您要刪除之電子郵件地址的列。表右上角的*刪除*按鈕可供選擇。

4. 按一下*刪除*、然後確認作業。

編輯郵件伺服器以取得警示

您可以變更用於電子郵件警示的郵件伺服器位址和電子郵件寄件者位址。

開始之前

您要變更的郵件伺服器位址必須是可用的。位址可以是IPV4或IPV6位址、也可以是完整網域名稱。



若要使用完整網域名稱、您必須在兩個控制器上設定DNS伺服器。您可以從「硬體」頁面設定DNS伺服器。

步驟

1. 選取功能表：設定[警示]。
2. 選取*電子郵件*索引標籤。
3. 選擇*設定郵件伺服器*。

此時將打開Configure Mail Server（配置郵件服務器）對話框。

4. 編輯郵件伺服器位址、寄件者資訊及聯絡資訊。

- 郵件伺服器位址-編輯郵件伺服器的完整網域名稱、IPv4位址或IPv6位址。



若要使用完整網域名稱、您必須在兩個控制器上設定DNS伺服器。您可以從「硬體」頁面設定DNS伺服器。

- 電子郵件寄件者地址-編輯電子郵件地址、以作為電子郵件寄件者。此地址會出現在電子郵件訊息的「寄件者」欄位中。
- 在電子郵件中加入聯絡資訊-若要編輯寄件者的聯絡資訊、請選取此選項、然後編輯姓名和電話號碼。

5. 按一下「*儲存*」。

管理SNMP警示

設定 SNMP 警示

若要設定簡單網路管理傳輸協定（SNMP）警示、您必須至少識別一部伺服器、讓儲存陣列的事件監控器能夠傳送SNMP設陷。此組態需要社群名稱或使用者名稱、以及伺服器的IP位址。

開始之前

- 網路伺服器必須設定SNMP服務應用程式。您需要此伺服器的網路位址（無論是IPv4或IPv6位址）、事件監控器才能將陷阱訊息傳送到該位址。您可以使用多部伺服器（最多允許10部伺服器）。
- 管理資訊庫（mib）檔案已複製並使用SNMP服務應用程式在伺服器上編譯。此mib檔案定義要監控和管理的資料。

如果您沒有mib檔案、可以從NetApp支援網站取得：

- 前往 "NetApp支援"。
- 單擊* Downloads (下載) 選項卡，然後選擇 Downloads (下載)。
- 按一下「* E系列SANtricity」 「作業系統控制器軟體*」。
- 選擇*下載最新版本*。
- 登入。
- 接受「注意」聲明和授權合約。
- 向下捲動、直到您看到控制器類型的mib檔案、然後按一下連結下載檔案。

關於這項工作

本工作說明如何識別SNMP伺服器的設陷目的地、然後測試您的組態。

步驟

1. 選取功能表：設定[警示]。
2. 選取* SNMP *索引標籤。

初次設定時、SNMP索引標籤會顯示「Configure Communities / Users」 (設定社群/使用者)。

3. 選擇*設定社群/使用者*。

「選取SNMP版本」對話方塊隨即開啟。

4. 選取警示的SNMP版本：* SNMPv2c*或* SNMPv3 *。

視您的選擇而定、「設定社群」對話方塊或「設定v3使用者」對話方塊會開啟。

5. 請遵循適當的SNMP v2c (社群) 或v3 (使用者) 指示：

- * SNMP v2c (社群) -在「設定社群」對話方塊中、輸入網路伺服器的一或多個社群字串。社群名稱是用來識別已知管理站組的字串、通常是由網路管理員所建立。它僅包含可列印的**Ascii**字元。您最多可以新增**256**個社群。完成後、請按一下「Save (儲存)」*。
- * v3 (使用者) -在「設定v3使用者」對話方塊中、按一下「*新增」、然後輸入下列資訊：
 - 使用者名稱-輸入名稱以識別使用者、最多31個字元。
 - 引擎ID-選取用來產生訊息驗證和加密金鑰的引擎ID、而且必須在管理網域上是唯一的。在大多數情況下、您應該選取*本機*。如果您使用的是非標準組態、請選取* Custom*；此時會出現另一個欄位、您必須輸入驗證引擎ID做為一個十六進位字串、其中的偶數字元長度介於10到32個字元之間。
 - 驗證認證資料-選取驗證傳輸協定、以確保使用者的身分識別。接著、輸入驗證密碼、這是設定或變更驗證傳輸協定時所需的密碼。密碼長度必須介於8到128個字元之間。
 - 隱私權認證-選取用於加密訊息內容的隱私權傳輸協定。接著、輸入隱私權密碼、這是設定或變更隱私權傳輸協定時所需的密碼。密碼長度必須介於8到128個字元之間。完成後、按一下*「Add* (新增*)」*、然後按一下「* Close (關閉)」*。

6. 在「警示」頁面中選取「SNMP」索引標籤、按一下「新增設陷目的地」。

「新增設陷目的地」對話方塊隨即開啟。

7. 輸入一個或多個陷阱目的地、選取其相關的社群名稱或使用者名稱、然後按一下*「Add* (新增*)」*。

- 陷阱目的地-輸入執行SNMP服務之伺服器的IPv4或IPv6位址。
 - 社群名稱或使用者名稱-從下拉式清單中、選取此設陷目的地的社群名稱（SNMPv2c）或使用者名稱（v3）。（如果您只定義了一個名稱、則該名稱已出現在此欄位中。）
 - 傳送驗證失敗Trap *-如果您想要在SNMP要求因無法辨識的社群名稱或使用者名稱而遭拒時、發出警示陷阱目的地、請選取此選項（核取方塊）。單擊 Add（添加）後，陷阱目標和相關名稱將顯示在 alert*（警告）頁面的* SNMP*（SNMP）選項卡中。
8. 若要確定設陷有效、請從表格中選取設陷目的地、然後按一下*測試設陷目的地*、將測試設陷傳送到設定的位址。

結果

每當發生警示事件時、事件監視器會將SNMP設陷傳送至伺服器。

新增SNMP警示的設陷目的地

您最多可以新增10部伺服器來傳送SNMP設陷。

開始之前

- 您要新增的網路伺服器必須使用SNMP服務應用程式進行設定。您需要此伺服器的網路位址（無論是IPv4或IPv6位址）、事件監控器才能將陷阱訊息傳送到該位址。您可以使用多部伺服器（最多允許10部伺服器）。
- 管理資訊庫（mib）檔案已複製並使用SNMP服務應用程式在伺服器上編譯。此mib檔案定義要監控和管理的資料。

如果您沒有mib檔案、可以從NetApp支援網站取得：

- 前往 "[NetApp支援](#)"。
- 單擊* Downloads（下載），然後選擇* Downloads（下載）。
- 按一下「* E系列SANtricity」 「作業系統控制器軟體*」。
- 選擇*下載最新版本*。
- 登入。
- 接受「注意」聲明和授權合約。
- 向下捲動、直到您看到控制器類型的mib檔案、然後按一下連結下載檔案。

步驟

1. 選取功能表：設定[警示]。
2. 選取* SNMP *索引標籤。

目前定義的設陷目的地會出現在表格中。

3. 選取*新增設陷的設計*。

「新增設陷目的地」對話方塊隨即開啟。

4. 輸入一個或多個陷阱目的地、選取其相關的社群名稱或使用者名稱、然後按一下*「Add*（新增*）」。
- 陷阱目的地-輸入執行SNMP服務之伺服器的IPv4或IPv6位址。

- 社群名稱或使用者名稱-從下拉式清單中、選取此設陷目的地的社群名稱 (SNMPv2c) 或使用者名稱 (v3)。(如果您只定義了一個名稱、則該名稱已出現在此欄位中。)
 - 傳送驗證失敗**Trap** *-如果您想要在**SNMP**要求因無法辨識的社群名稱或使用者名稱而遭拒時、發出警示陷阱目的地、請選取此選項 (核取方塊)。按一下「*新增」之後、陷阱目的地和相關的社群名稱或使用者名稱會出現在表格中。
5. 若要確定設陷有效、請從表格中選取設陷目的地、然後按一下*測試設陷目的地*、將測試設陷傳送到設定的位址。

結果

每當發生警示事件時、事件監視器會將SNMP設陷傳送至伺服器。

設定SNMP mib變數

對於SNMP警示、您可以選擇性地設定出現在SNMP設陷中的管理資訊庫 (MIB) 變數。這些變數可傳回儲存陣列名稱、陣列位置及聯絡人。

開始之前

必須使用SNMP服務應用程式在伺服器上複製及編譯mib檔案。

如果您沒有MIBA檔案、可以取得如下：

- 前往 "[NetApp支援](#)"。
- 單擊* Downloads (下載) ，然後選擇* Downloads (下載) 。
- 按一下「* E系列SANtricity 」 「作業系統控制器軟體*」。
- 選擇*下載最新版本*。
- 登入。
- 接受「注意」聲明和授權合約。
- 向下捲動、直到您看到控制器類型的mib檔案、然後按一下連結下載檔案。

關於這項工作

本工作說明如何定義SNMP設陷的mib變數。這些變數可傳回下列值以回應SNMP GetRequest：

- sysName (儲存陣列的名稱)
- sysLocation (儲存陣列的位置)
- sysContact (管理員姓名)

步驟

1. 選取功能表：設定[警示]。
2. 選取* SNMP *索引標籤。
3. 選擇*設定SNMP mib變數*。

此時將打開Configure SNMP mib Variables (配置SNMP mib變量) 對話框。

4. 輸入下列一或多個值、然後按一下*「Save (儲存)」*。

- **Name** — MIB 變量的值 `sysName`。例如、輸入儲存陣列的名稱。
- ***Location]** — MIB 變量的值 `sysLocation`。例如、輸入儲存陣列的位置。
- **Contact** — MIB 變量的值 `sysContact`。例如、輸入負責儲存陣列的管理員。

結果

這些值會出現在儲存陣列警示的SNMP設陷訊息中。

編輯SNMP v2c設陷的社群

您可以編輯SNMP v2c設陷的社群名稱。

開始之前

必須建立社群名稱。

步驟

1. 選取功能表：設定[警示]。
2. 選取* SNMP *索引標籤。

陷阱目的地和社群名稱會出現在表格中。

3. 選擇*設定社群*。
4. 輸入新的社群名稱、然後按一下「儲存」。社群名稱只能由可列印的Ascii字元組成。

結果

「警示」頁面的「SNMP」索引標籤會顯示更新的社群名稱。

編輯使用者設定的v3設陷

您可以編輯v3設陷的使用者定義。

開始之前

必須為v3設陷建立使用者。

步驟

1. 選取功能表：設定[警示]。
2. 選取* SNMP *索引標籤。

陷阱目的地和使用者名稱會出現在表格中。

3. 若要編輯使用者定義、請在表格中選取使用者、然後按一下「設定使用者」。
4. 在對話方塊中、按一下*檢視/編輯設定*。
5. 編輯下列資訊：
 - 使用者名稱-變更識別使用者的名稱、最長可達31個字元。
 - 引擎ID-選取用來產生訊息驗證和加密金鑰的引擎ID、而且必須在管理網域上是唯一的。在大多數情況

下、您應該選取*本機*。如果您使用的是非標準組態、請選取* Custom*；此時會出現另一個欄位、您必須輸入驗證引擎ID做為一個十六進位字串、其中的偶數字元長度介於10到32個字元之間。

- 驗證認證資料-選取驗證傳輸協定、以確保使用者的身分識別。接著、輸入驗證密碼、這是設定或變更驗證傳輸協定時所需的密碼。密碼長度必須介於8到128個字元之間。
- 隱私權認證-選取用於加密訊息內容的隱私權傳輸協定。接著、輸入隱私權密碼、這是設定或變更隱私權傳輸協定時所需的密碼。密碼長度必須介於8到128個字元之間。

結果

「警示」頁面的「SNMP」索引標籤會顯示更新的設定。

新增SNMP v2c設陷的社群

您最多可以新增256個SNMP v2c設陷的社群名稱。

步驟

1. 選取功能表：設定[警示]。
2. 選取* SNMP *索引標籤。

陷阱目的地和社群名稱會出現在表格中。

3. 選擇*設定社群*。

「設定社群」對話方塊隨即開啟。

4. 選取*新增其他社群*。
5. 輸入新的社群名稱、然後按一下「儲存」。

結果

新的社群名稱會出現在「警示」頁面的SNMP索引標籤中。

新增使用者以使用v3設陷

您最多可以新增256位使用者來使用v3設陷。

步驟

1. 選取功能表：設定[警示]。
2. 選取* SNMP *索引標籤。

陷阱目的地和使用者名稱會出現在表格中。

3. 選取*設定使用者*。

此時將打開Configure v3 Users（配置v3用戶）對話框。

4. 選取*「Add*」。
5. 輸入下列資訊、然後按一下「新增」。

- 使用者名稱-輸入名稱以識別使用者、最多31個字元。
- 引擎ID-選取用來產生訊息驗證和加密金鑰的引擎ID、而且必須在管理網域上是唯一的。在大多數情況下、您應該選取*本機*。如果您使用的是非標準組態、請選取* Custom*；此時會出現另一個欄位、您必須輸入驗證引擎ID做為一個十六進位字串、其中的偶數字元長度介於10到32個字元之間。
- 驗證認證資料-選取驗證傳輸協定、以確保使用者的身分識別。接著、輸入驗證密碼、這是設定或變更驗證傳輸協定時所需的密碼。密碼長度必須介於8到128個字元之間。
- 隱私權認證-選取用於加密訊息內容的隱私權傳輸協定。接著、輸入隱私權密碼、這是設定或變更隱私權傳輸協定時所需的密碼。密碼長度必須介於8到128個字元之間。

移除SNMP v2c設陷的社群

您可以移除SNMP v2c設陷的社群名稱。

步驟

1. 選取功能表：設定[警示]。
2. 選取* SNMP *索引標籤。

陷阱目的地和社群名稱會顯示在*警示*頁面上。

3. 選擇*設定社群*。

「設定社群」對話方塊隨即開啟。

4. 選取您要刪除的社群名稱、然後按一下最右側的*移除* (X) 圖示。

如果設陷目的地與此社群名稱相關聯、「確認移除社群」對話方塊會顯示受影響的設陷目的地地址。

5. 確認操作、然後按一下*移除*。

結果

社群名稱及其相關的陷阱目的地會從警示頁面中移除。

移除使用者的v3設陷

您可以移除使用者的v3設陷。

步驟

1. 選取功能表：設定[警示]。
2. 選取* SNMP *索引標籤。

設陷目的地和使用者名稱會出現在警示頁面上。

3. 選取*設定使用者*。

此時將打開Configure v3 Users（配置v3用戶）對話框。

4. 選取您要刪除的使用者名稱、然後按一下*刪除*。

5. 確認操作、然後按一下*刪除*。

結果

使用者名稱及其相關的設陷目的地會從警示頁面中移除。

刪除設陷目的地

您可以刪除設陷目的地位址、使儲存陣列的事件監視器不再將SNMP設陷傳送到該位址。

步驟

1. 選取功能表：設定[警示]。
2. 選取* SNMP *索引標籤。

陷阱目的地位址會出現在表格中。

3. 選取設陷目的地、然後按一下頁面右上角的*刪除*。
4. 確認操作、然後按一下*刪除*。

目的地位址不再出現在「警示」頁面上。

結果

刪除的設陷目的地不再從儲存陣列的事件監視器接收SNMP設陷。

管理系統記錄警示

設定系統記錄伺服器以發出警示

若要設定syslog警示、您必須輸入syslog伺服器位址和udp連接埠。最多允許五部syslog伺服器。

開始之前

- 系統記錄伺服器位址必須可用。此位址可以是完整網域名稱、IPv4位址或IPv6位址。
- 系統記錄伺服器的udp連接埠號碼必須可用。此連接埠通常為514。

關於這項工作

此工作說明如何輸入syslog伺服器的位址和連接埠、然後測試您輸入的位址。

步驟

1. 選取功能表：設定[警示]。
2. 選取「系統記錄」索引標籤。

如果尚未定義syslog伺服器、「警示」頁面會顯示「新增Syslog伺服器」。

3. 按一下「新增**Syslog**伺服器」。

此時會開啟「新增Syslog伺服器」對話方塊。

4. 輸入一或多個syslog伺服器的資訊（最多五個）、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。
 - * udp Port*-通常syslog的udp連接埠為514。下表顯示已設定的syslog伺服器。
5. 若要傳送測試警示至伺服器位址、請選取*測試所有Syslog伺服器*。

結果

每當發生警示事件時、事件監控器都會傳送警示至syslog伺服器。若要進一步設定稽核記錄的 Syslog 設定，請參閱 ["設定系統記錄伺服器進行稽核記錄"](#)。



如果設定多個 Syslog 伺服器、所有設定的 Syslog 伺服器都會收到稽核記錄。

編輯系統記錄伺服器以取得警示

您可以編輯用於接收系統記錄警示的伺服器位址。

步驟

1. 選取功能表：設定[警示]。
2. 選取「系統記錄」索引標籤。
3. 從表中選取syslog伺服器位址、然後按一下最右側的*編輯*（鉛筆）圖示。

該列會變成可編輯的欄位。

4. 編輯伺服器位址和udp連接埠號碼、然後按一下*「Save*（勾選）」圖示。

結果

更新的伺服器位址會出現在表格中。

新增系統記錄伺服器以供警示

您最多可以新增五部伺服器來執行系統記錄警示。

開始之前

- 系統記錄伺服器位址必須可用。此位址可以是完整網域名稱、IPv4位址或IPv6位址。
- 系統記錄伺服器的udp連接埠號碼必須可用。此連接埠通常為514。

步驟

1. 選取功能表：設定[警示]。
2. 選取「系統記錄」索引標籤。
3. 選擇* Add Syslog Servers*（添加Syslog服務器*）。

此時會開啟「新增Syslog伺服器」對話方塊。

4. 選取*新增其他syslog伺服器*。
5. 輸入syslog伺服器的資訊、然後按一下*「Add*（新增*）」。

- 系統記錄伺服器位址-輸入完整網域名稱、IPv4位址或IPv6位址。

- * udp Port*-通常syslog的udp連接埠為514。



最多可設定五部syslog伺服器。

結果

系統記錄伺服器位址會出現在表格中。

刪除系統記錄伺服器以取得警示

您可以刪除syslog伺服器、使其不再接收警示。

步驟

1. 選取功能表：設定[警示]。
2. 選取「系統記錄」索引標籤。
3. 選取syslog伺服器位址、然後按一下右上角的*移除*。

「確認刪除Syslog伺服器」對話方塊隨即開啟。

4. 確認操作、然後按一下*刪除*。

結果

您移除的伺服器不再從事件監視器接收警示。

常見問題集

停用警示時該怎麼辦？

如果您希望系統管理員收到儲存陣列中發生重要事件的通知、您必須設定警示方法。

若為SANtricity 以《支援系統管理程式》管理的儲存陣列、您可從「警示」頁面設定警示。警示通知可透過電子郵件、SNMP設陷或系統記錄訊息傳送。此外、您也可以從初始設定精靈設定電子郵件警示。

如何設定SNMP或syslog警示？

除了電子郵件警示之外、您也可以設定要透過簡單網路管理傳輸協定（SNMP）設陷或透過系統記錄訊息傳送的警示。

若要設定SNMP或syslog警示、請前往功能表：設定[警示]。

為什麼陣列與警示之間的時間戳記不一致？

當儲存陣列傳送警示時、對於接收警示的目標伺服器或主機所在的時區而言、它不正確。相反地、儲存陣列會使用本機時間（GMT）來建立警示記錄所用的時間戳記。因此、您可能看到儲存陣列與收到警示的伺服器或主機之間的時間戳記不一致。

由於儲存陣列在傳送警示時區不正確、因此警示上的時間戳記為相對於GMT-的時間區偏移值為零。若要計算適合您當地時區的時間戳記、您應該決定小時與時間的時差、然後從時間戳記中新增或減去該值。

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。