設定通知

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/active-iq-unified-manager-918/config/task_configure_unified_manager_to_send_alert_notifications.html on November 13, 2026. Always check docs.netapp.com for the latest.

目錄

設定通知 . . . 1
- 設定 Active IQ Unified Manager 以傳送警示通知 . . . 1
- 在 Active IQ Unified Manager 中設定事件通知設定 . . . 1
- 在 Active IQ Unified Manager 中啟用遠端驗證 . . . 2
- 在 Active IQ Unified Manager 中停用巢狀群組的遠端驗證 . . . 3
- 在 Active IQ Unified Manager 中設定驗證服務 . . . 4
- 將驗證伺服器新增至 Active IQ Unified Manager . . . 5
- 測試 Active IQ Unified Manager 中的驗證伺服器組態 . . . 6
- 在 Active IQ Unified Manager 中新增警報 . . . 6
  - 新增警報的範例 . . . 7

設定通知

設定 Active IQ Unified Manager 以傳送警示通知

您可以設定 Unified Manager 以傳送通知，提醒您環境中發生的事件。在傳送通知之前，您必須設定其他幾個 Unified Manager 選項。

開始之前

您必須擁有應用程式管理員角色。

部署 Unified Manager 並完成初始組態後，您應該考慮設定您的環境，以便在收到事件時觸發警報並產生通知電子郵件或 SNMP 陷阱。

步驟

1. "設定事件通知設定"。

   如果您希望在環境中發生特定事件時收到警報通知，則必須設定 SMTP 伺服器並提供用於傳送警報通知的電子郵件地址。如果您想使用 SNMP 陷阱，可以選擇該選項並提供必要的資訊。

2. "啟用遠端驗證"。

   如果您希望遠端 LDAP 或 Active Directory 使用者存取 Unified Manager 執行個體並接收警報通知，則必須啟用遠端驗證。

3. "新增驗證伺服器"。

   您可以新增驗證伺服器，以便驗證伺服器內的遠端使用者可以存取 Unified Manager。

4. "新增使用者"。

   您可以新增多種不同類型的本機或遠端使用者，並指派特定角色。建立警示時，您會指派一位使用者來接收警示通知。

5. "新增警示"。

   新增用於傳送通知的電子郵件地址、新增接收通知的使用者、設定網路設定以及設定環境所需的 SMTP 和 SNMP 選項後，即可指派警報。

在 Active IQ Unified Manager 中設定事件通知設定

您可以設定 Unified Manager，使其在產生事件或將事件指派給使用者時傳送警報通知。您可以設定用於傳送警報的 SMTP 伺服器，也可以設定各種通知機制——例如，警報通知可以透過電子郵件或 SNMP 陷阱的形式傳送。

開始之前

您必須具備以下資訊：

- 發送警報通知的電子郵件地址

此電子郵件地址會顯示在已傳送提醒通知的 “From” 欄位中。如果電子郵件因任何原因無法送達，此電子郵件地址也會做為無法送達郵件的收件者。

- SMTP 伺服器主機名稱，以及存取該伺服器的使用者名稱和密碼
- 接收 SNMP 陷阱的目的地主機的主機名稱或 IP 位址，以及 SNMP 版本、傳出陷阱連接埠、團體名稱和其他必要的 SNMP 組態值

  若要指定多個陷阱目的地，請用逗號分隔每個主機。在這種情況下，清單中所有其他 SNMP 設定（例如版本和傳出陷阱連接埠）對於所有主機都必須相同。

您必須擁有應用程式系統管理員或儲存系統管理員角色。

步驟

1. 在左側導覽窗格中，按一下 一般 > 通知。
2. 在「通知」頁面中，設定適當的設定。

   附註：

   - 如果「寄件者地址」預先填寫了地址「ActiveIQUnifiedManager@localhost.com」，則應將其變更為真實、有效的電子郵件地址，以確保所有電子郵件通知都能成功送達。
   - 如果無法解析 SMTP 伺服器的主機名稱，您可以指定 SMTP 伺服器的 IP 位址（IPv4 或 IPv6）而不是主機名稱。
3. 按一下 **Save** 。
4. 如果您選擇了 使用 **STARTTLS** 或 使用 **SSL** 選項，按一下 儲存 按鈕後會顯示憑證頁面。請驗證憑證詳細資料並接受憑證，以儲存通知設定。

   您可以按一下 **View Certificate Details** 按鈕來檢視憑證詳細資料。如果現有憑證已過期，請取消勾選 **Use STARTTLS** 或 **Use SSL** 方塊，儲存通知設定，然後再次勾選 **Use STARTTLS** 或 **Use SSL** 方塊以檢視新憑證。

在 **Active IQ Unified Manager** 中啟用遠端驗證

您可以啟用遠端驗證，以便 Unified Manager 伺服器可以與您的驗證伺服器通訊。驗證伺服器的使用者可以存取 Unified Manager 圖形介面來管理儲存設備物件和資料。

開始之前

您必須擁有應用程式管理員角色。

> Unified Manager 伺服器必須直接連接至驗證伺服器。您必須停用任何本機 LDAP 用戶端，例如 SSSD（System Security Services Daemon）或 NSLCD（Name Service LDAP Caching Daemon）。

您可以使用 Open LDAP 或 Active Directory 啟用遠端驗證。如果停用遠端驗證，遠端使用者將無法存取 Unified Manager。

支援透過 LDAP 和 LDAPS（Secure LDAP）進行遠端驗證。Unified Manager 使用 389 作為非安全通訊的預設連接埠，並使用 636 作為安全通訊的預設連接埠。

用於驗證使用者身分的憑證必須符合 X.509 格式。

步驟

1. 在左側導覽窗格中，按一下 一般 > 遠端驗證。
2. 勾選 啟用遠端驗證..... 核取方塊。
3. 在「驗證服務」欄位中，選擇服務類型並設定驗證服務。

對於驗證類型.....	請輸入以下資訊.....
Active Directory	• 驗證伺服器系統管理員名稱，採用下列其中一種格式： ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name`（使用適當的 LDAP 表示法） • 管理員密碼 • 基本辨別名稱（使用適當的 LDAP 表示法）
Open LDAP	• 綁定辨別名稱（採用適當的 LDAP 表示法） • 綁定密碼 • 基本辨識名稱

如果 Active Directory 使用者驗證耗時過長或逾時，則可能是驗證伺服器回應速度過慢。停用 Unified Manager 中的巢狀群組支援可能會縮短驗證時間。

如果為驗證伺服器選擇「使用安全連線」選項，則 Unified Manager 將使用安全通訊端層 (SSL) 協定與驗證伺服器通訊。

4. *可選：*新增驗證伺服器，並測試驗證。
5. 按一下 **Save** 。

在 **Active IQ Unified Manager** 中停用巢狀群組的遠端驗證

如果您已啟用遠端驗證，您可以停用巢狀群組驗證，這樣只有個別使用者（而非群組成員）才能遠端向 Unified Manager 進行驗證。當您想要改善 Active Directory 驗證回應時間時，可以停用巢狀群組。

開始之前

- 您必須擁有應用程式管理員角色。
- 停用巢狀群組僅適用於使用 Active Directory 的情況。

停用 Unified Manager 中的巢狀群組支援可能會縮短驗證時間。如果停用巢狀群組支援，並且在 Unified Manager 新增了遠端群組，則個別使用者必須是該遠端群組的成員，才能向 Unified Manager 進行驗證。

步驟

1. 在左側導覽窗格中，按一下 一般 > 遠端驗證。
2. 勾選 停用巢狀群組查詢 的核取方塊。
3. 按一下 **Save** 。

在 **Active IQ Unified Manager** 中設定驗證服務

驗證服務允許在提供遠端使用者或遠端群組存取 Unified Manager 之前，先在驗證伺服器中對其進行驗證。您可以使用預先定義的驗證服務（例如 Active Directory 或 OpenLDAP ）來驗證使用者，或是設定您自己的驗證機制。

開始之前

- 您必須已啟用遠端驗證。
- 您必須擁有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下 一般 > 遠端驗證。
2. 請選擇以下驗證服務之一：

如果您選擇.....	然後這樣做.....
Active Directory	a. 請輸入系統管理員名稱和密碼。 b. 指定驗證伺服器的基本辨別名稱。 例如，如果驗證伺服器的網域名稱為 ou@domain.com，則基本可分辨名稱為 **cn=ou,dc=domain,dc=com**。
OpenLDAP	a. 輸入連結專有名稱和連結密碼。 b. 指定驗證伺服器的基本辨別名稱。 例如，如果驗證伺服器的網域名稱為 ou@domain.com，則基本可分辨名稱為 **cn=ou,dc=domain,dc=com**。
其他	a. 輸入連結專有名稱和連結密碼。 b. 指定驗證伺服器的基本辨別名稱。 例如，如果驗證伺服器的網域名稱為 ou@domain.com，則基本可分辨名稱為 **cn=ou,dc=domain,dc=com**。 c. 指定驗證伺服器支援的 LDAP 傳輸協定版本。 d. 輸入使用者名稱、群組成員身分、使用者群組和成員屬性。

如果要修改驗證服務，必須先刪除所有現有的驗證伺服器，然後再新增新的驗證伺服器。

3. 按一下 **Save** 。

將驗證伺服器新增至 **Active IQ Unified Manager**

您可以新增驗證伺服器並在管理伺服器上啟用遠端驗證，以便驗證伺服器內的遠端使用者可以存取 Unified Manager。

開始之前

- 必須提供以下資訊：
  - 驗證伺服器的主機名稱或 IP 位址
  - 驗證伺服器的連接埠號碼
- 您必須已啟用遠端驗證並設定驗證服務，以便管理伺服器可以對驗證伺服器中的遠端使用者或群組進行驗證。
- 您必須擁有應用程式管理員角色。

如果您新增的驗證伺服器是高可用性 (HA) 配對的一部分（使用相同的資料庫），您也可以新增合作夥伴驗證伺服器。這可讓管理伺服器在其中一部驗證伺服器無法連線時，與合作夥伴通訊。

步驟

1. 在左側導覽窗格中，按一下 一般 > 遠端驗證。
2. 啟用或停用 使用安全的連線 選項：

如果您想要.....	然後這樣做.....
啟用	a. 選取 使用安全連線 選項。 b. 在「驗證伺服器」區域中，按一下 新增。 c. 在「新增驗證伺服器」對話方塊中，輸入伺服器的驗證名稱或 IP 位址（IPv4 或 IPv6）。 d. 在「授權主機」對話方塊中，按一下「檢視憑證」。 e. 在「檢視憑證」對話方塊中，驗證憑證資訊，然後按一下 關閉。 f. 在「授權主機」對話方塊中，按一下 是。 啟用 **Use Secure Connection authentication** 選項後， Unified Manager 將與驗證伺服器通訊並顯示憑證。Unified Manager 預設使用 636 連接埠進行安全的通訊，並使用 389 連接埠進行非安全通訊。

如果您想要.....	然後這樣做.....
停用它	a. 取消勾選 使用安全連線 選項。 b. 在「驗證伺服器」區域中，按一下 新增。 c. 在「新增驗證伺服器」對話方塊中，指定伺服器的主機名稱或 IP 位址（IPv4 或 IPv6）以及連接埠詳細資料。 d. 點擊 **Add** 。

您新增的驗證伺服器將顯示在「伺服器」區域中。

3. 執行測試驗證，以確認您可以在新增的驗證伺服器中驗證使用者。

測試 **Active IQ Unified Manager** 中的驗證伺服器組態

您可以驗證驗證伺服器的組態，以確保管理伺服器能夠與其通訊。您可以透過從驗證伺服器搜尋遠端使用者或遠端群組，並使用已設定的設定對其進行驗證，藉此驗證組態。

開始之前

- 您必須啟用遠端驗證，並設定您的驗證服務，以便 Unified Manager 伺服器可以驗證遠端使用者或遠端群組。
- 您必須新增驗證伺服器，以便管理伺服器可以從這些伺服器中搜尋遠端使用者或遠端群組並對其驗證。
- 您必須擁有應用程式管理員角色。

如果驗證服務設定為 Active Directory，且您正在驗證屬於驗證伺服器主群組的遠端使用者的驗證，則驗證結果中不會顯示有關主群組的資訊。

步驟

1. 在左側導覽窗格中，按一下 一般 > 遠端驗證。
2. 按一下 測試驗證。
3. 在「測試使用者」對話方塊中，指定遠端使用者的使用者名稱和密碼或遠端群組的使用者名稱，然後按一下測試。

   如果您要驗證遠端群組，則不得輸入密碼。

在 **Active IQ Unified Manager** 中新增警報

您可以設定警報，以便在產生特定事件時收到通知。您可以為單一資源、一組資源或特定嚴重性類別的事件設定警報。您可以指定接收通知的頻率，並將指令碼關聯至警報。

開始之前

- 您必須設定通知設定，例如使用者電子郵件地址、SMTP 伺服器和 SNMP trap 主機，才能使 Active IQ Unified Manager 伺服器使用這些設定，在產生事件時傳送通知給使用者。
- 您必須知道要觸發警報的資源和事件，以及要通知的使用者的使用者名稱或電子郵件地址。

- 如果您希望根據事件執行指令碼，則必須使用「指令碼」頁面將指令碼新增至 Unified Manager。
- 您必須擁有應用程式系統管理員或儲存系統管理員角色。

除了可以按照此處所述從「警報設定」頁面建立警報外，您還可以在收到事件後直接從「事件詳情」頁面建立警報。

步驟

1. 在左側導覽窗格中，按一下 儲存設備管理 > 警示設定。
2. 在「警報設定」頁面中，按一下 新增。
3. 在「新增警報」對話方塊中，按一下 名稱，然後輸入警報的名稱和執行摘要。
4. 按一下 資源，然後選擇要包含在警報中或從警報中排除的資源。

   您可以透過在 名稱包含 欄位中指定字串來設定篩選條件，從而選擇一組資源。根據您指定的字串，可用資源清單將僅顯示符合篩選規則的資源。您指定的字串區分大小寫。

   如果資源同時符合您指定的包含規則和排除規則，則排除規則優先於包含規則，並且不會為與排除資源相關的事件產生警報。

5. 按一下 事件，然後根據事件名稱或事件嚴重性類別選擇要觸發警報的事件。

   若要選擇多個事件，請在選擇時按住 Ctrl 鍵。

6. 按一下 **Actions** ，選擇要通知的使用者，選擇通知頻率，選擇是否將 SNMP trap 傳送至 trap 接收器，並指派在產生警報時要執行的指令碼。

   如果您修改了為使用者指定的電子郵件地址，並重新開啟警示以進行編輯，則「名稱」欄位會顯示為空白，因為修改後的電子郵件地址不再對應至先前選取的使用者。此外，如果您從「使用者」頁面修改了所選使用者的電子郵件地址，則修改後的電子郵件地址不會為所選使用者更新。

   您也可以選擇透過 SNMP 陷阱通知使用者。

7. 按一下 **Save** 。

新增警報的範例

本範例展示如何建立滿足以下要求的警報：

- 警報名稱：HealthTest
- 資源：包括名稱中包含「`abc`」的所有磁碟區，並排除名稱中包含「`xyz`」的所有磁碟區
- 事件：包括所有關鍵健全狀況事件
- 動作：包括 "sample@domain.com"、一個 “Test” 指令碼，並且必須每 15 分鐘通知使用者

在「新增警報」對話方塊中執行以下步驟：

步驟

1. 按一下 名稱，然後在 警報名稱 欄位中輸入 **HealthTest**。

2. 按一下 資源 ，然後在 Include 索引標籤中，從下拉清單中選取 磁碟區 。
   a. 在 名稱包含 欄位中輸入 **abc**，以顯示名稱包含 “abc” 的磁碟區。
   b. 從「可用資源」區域選取 **<<All Volumes whose name contains 'abc'>>**，並將其移至「已選資源」區域。
   c. 按一下 排除，在 名稱包含 欄位中輸入 **xyz**，然後按一下 新增。
3. 按一下 事件，然後在「事件嚴重性」欄位中選擇 關鍵。
4. 從相符事件區域中選取 所有關鍵事件，並將其移至選取的事件區域。
5. 按一下 動作 ，然後在「通知這些使用者」欄位中輸入 **sample@domain.com** 。
6. 選擇 每 **15** 分鐘提醒一次 即可每 15 分鐘通知使用者一次。

   您可以設定警報，使其在指定時間內重複向收件人發送通知。您應該決定警報的事件通知開始作用中的時間。

7. 在「選擇要執行的指令碼」功能表中，選擇 **Test** 指令碼。
8. 按一下 **Save** 。

版權資訊

Copyright © 2026 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。