設定 **Active IQ Unified Manager**

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/concept_configure_unified_manager.html on November 13, 2026. Always check docs.netapp.com for the latest.

目錄

設定 Active IQ Unified Manager . . . 1
- 了解如何設定 Active IQ Unified Manager . . . 1
- 了解 Active IQ Unified Manager 中的組態順序 . . . 1
- 在 Active IQ Unified Manager 中存取 Web UI . . . 1
- 執行 Active IQ Unified Manager Web UI 的初始設定 . . . 2
- 將叢集新增至 Active IQ Unified Manager . . . 4
- 設定通知 . . . 6
  - 設定 Active IQ Unified Manager 以傳送警示通知 . . . 6
  - 在 Active IQ Unified Manager 中設定事件通知設定 . . . 7
  - 在 Active IQ Unified Manager 中啟用遠端驗證 . . . 7
  - 在 Active IQ Unified Manager 中停用巢狀群組的遠端驗證 . . . 8
  - 在 Active IQ Unified Manager 中設定驗證服務 . . . 9
  - 將驗證伺服器新增至 Active IQ Unified Manager . . . 10
  - 測試 Active IQ Unified Manager 中的驗證伺服器組態 . . . 11
  - 在 Active IQ Unified Manager 中新增警報 . . . 12
- 在 Active IQ Unified Manager 中變更本機使用者密碼 . . . 13
- 在 Active IQ Unified Manager 中設定工作階段不活動逾時 . . . 14
- 使用 Active IQ Unified Manager 中的 CLI 設定工作階段逾時 . . . 14
- 變更 Unified Manager 主機名稱 . . . 15
  - 更改 Active IQ Unified Manager 虛擬應用裝置主機名稱 . . . 15
  - 在 Active IQ Unified Manager 中產生 HTTPS 安全性憑證 . . . 15
  - 重新啟動 Active IQ Unified Manager 虛擬機器 . . . 17
  - 在 Linux 系統上變更 Active IQ Unified Manager 主機名稱 . . . 17
- 在 Active IQ Unified Manager 中啟用並停用原則型儲存管理 . . . 18

設定 Active IQ Unified Manager

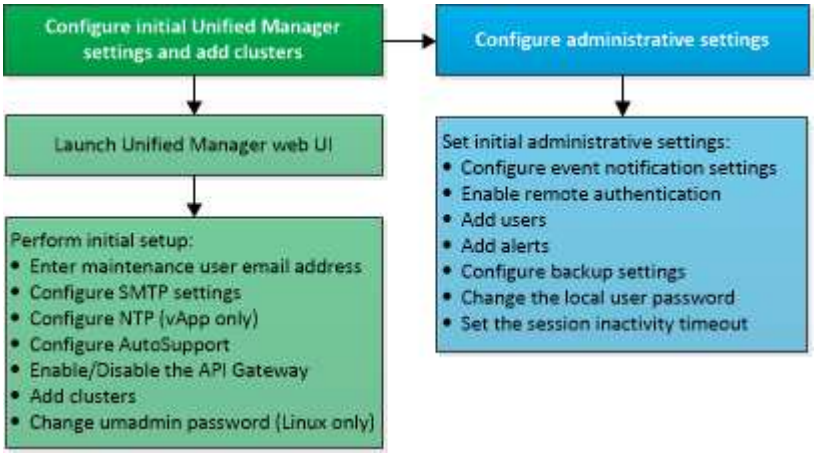
了解如何設定 Active IQ Unified Manager

安裝 Active IQ Unified Manager（原名 OnCommand Unified Manager）後，您必須完成初始設定（也稱為首次體驗精靈）才能存取 Web 使用者介面。然後，您可以執行其他組態任務，例如新增叢集、設定遠端驗證、新增使用者和新增警報。

本手冊中所述的某些步驟是完成 Unified Manager 執行個體初始設定所必需的。其他步驟則是建議的組態設定，有助於您在新執行個體上進行設定，或在開始對 ONTAP 系統進行常規監控之前了解這些設定。

了解 Active IQ Unified Manager 中的組態順序

組態工作流程描述在使用 Unified Manager 之前必須執行的任務。



在 Active IQ Unified Manager 中存取 Web UI

安裝 Unified Manager 後，您可以存取 Web UI 來設定 Unified Manager，以便開始監控您的 ONTAP 系統。

開始之前

- 如果這是您第一次存取 Web UI，您必須以維護使用者（或 Linux 安裝的 umadmin 使用者）身分登入。
- 如果您打算允許使用者使用短名稱而不是使用完整網域（FQDN）或 IP 位址來存取 Unified Manager，則您的網路組態必須將此短名稱解析為有效的 FQDN。
- 如果伺服器使用自我簽署的數位憑證，瀏覽器可能會顯示警告，指出該憑證不受信任。您可以確認風險以繼續存取，或安裝憑證授權單位 （CA） 簽署的數位憑證以進行伺服器驗證。

步驟

1. 使用安裝結束時顯示的 URL，透過瀏覽器啟動 Unified Manager Web UI。該 URL 是 Unified Manager 伺服器的 IP 位址或完整網域名稱（FQDN）。

   連結格式如下： `https://URL`。

2. 使用您的維護使用者憑證登入 Unified Manager Web UI。

如果您在一小時內連續三次嘗試登入 Web UI 失敗，您將被鎖定在系統之外，需要聯絡系統管理員。這僅適用於本機使用者。

執行 **Active IQ Unified Manager Web UI** 的初始設定

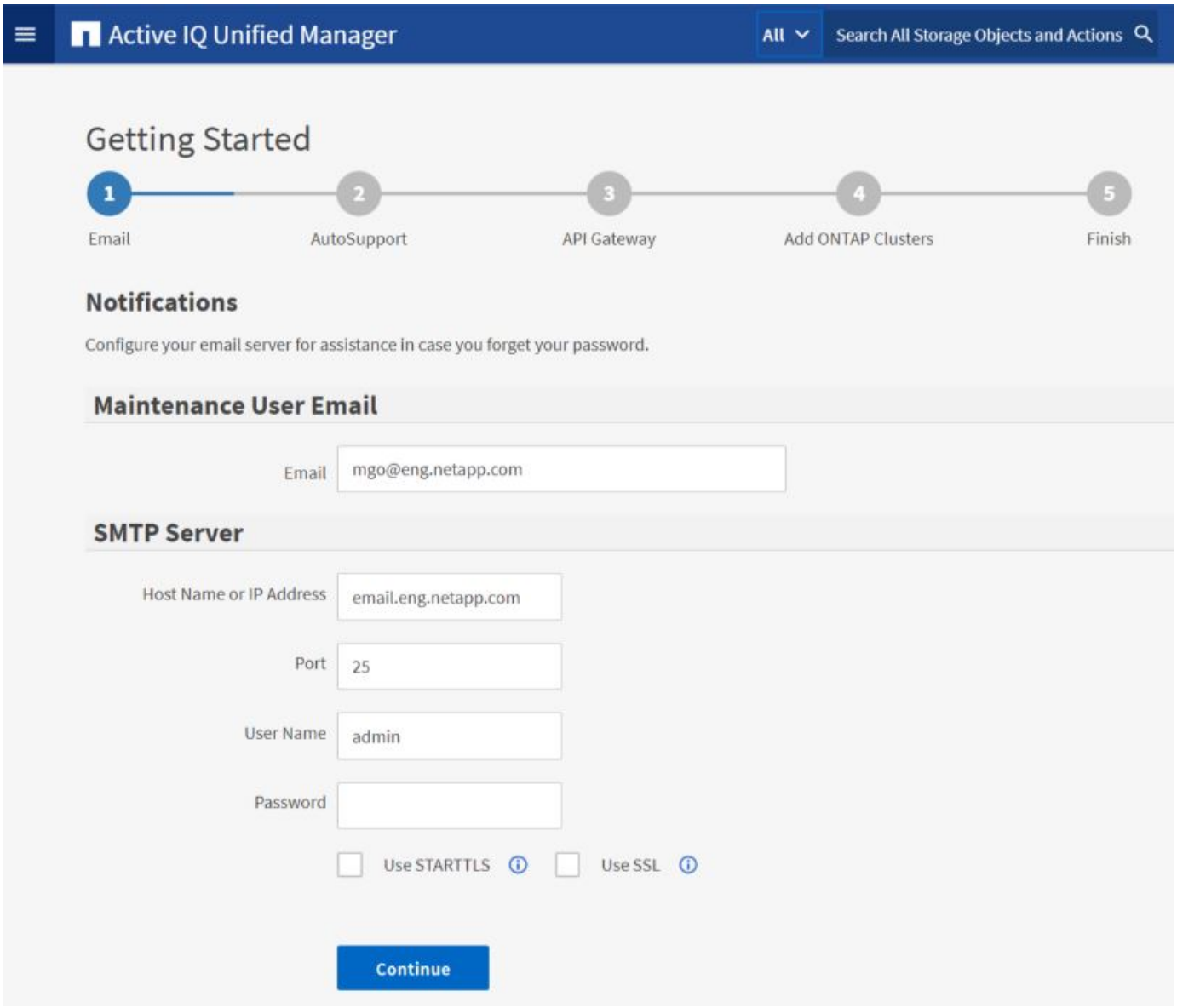
若要使用 Unified Manager，您必須先設定初始設定選項，包括 NTP 伺服器、維護使用者電子郵件地址、SMTP 伺服器主機，以及新增 ONTAP 叢集。

開始之前

您必須已執行下列操作：

- 使用安裝後提供的 URL 啟動 Unified Manager Web UI
- 使用安裝期間建立的維護使用者名稱和密碼（Linux 安裝為 umadmin 使用者）登入

Active IQ Unified ManagerGetting Started 頁面僅在您首次存取 Web 使用者介面時顯示。以下頁面來自 VMware 上的安裝。



如果您稍後想要變更任何這些選項，可以從 Unified Manager 左側導覽窗格的「一般」選項中進行選擇。請注意，NTP 設定僅適用於 VMware 安裝，且稍後可使用 Unified Manager 維護主控台進行變更。

步驟

1. 在 Active IQ Unified Manager 的初始設定頁面中，輸入維護使用者的電子郵件地址、SMTP 伺服器主機名稱和任何其他 SMTP 選項，以及 NTP 伺服器（僅限 VMware 安裝）。然後按一下 繼續。

   如果您選擇了 使用 **STARTTLS** 或 使用 **SSL** 選項，按一下 繼續 按鈕後將顯示憑證頁面。請驗證憑證詳細資訊並接受憑證，以繼續進行 Web UI 的初始設定。

2. 在 AutoSupport 頁面上，按一下 同意並繼續 以啟用從 Unified Manager 傳送 AutoSupport 訊息至 NetAppActive IQ。

   如果您需要指定 Proxy 來提供網際網路存取以傳送 AutoSupport 內容，或者如果您想要停用 AutoSupport，請使用 Web UI 中的 一般 > **AutoSupport** 選項。

3. 在 Red Hat 系統中，將 umadmin 使用者密碼從預設的「`admin`」字串變更為個人化字串。

4. 在「設定 API 閘道」頁面中，選擇是否要使用 API 閘道功能，該功能可讓 Unified Manager 管理您規劃使用 ONTAP REST API 監控的 ONTAP 叢集。然後按一下 繼續。

   您稍後可以在 Web UI 中，從 一般 > 功能設定 > **API** 閘道 啟用或停用此設定。如需 API 的詳細資訊，請參閱 "Active IQ Unified Manager REST API 入門指南"。

5. 新增您希望 Unified Manager 管理的叢集，然後按一下 下一步。對於您計畫管理的每個叢集，您必須擁有主機名稱或叢集管理 IP 位址（IPv4 或 IPv6），以及使用者名稱和密碼憑證 - 該使用者必須具有 “admin” 角色。

   此步驟為選用。您稍後可以在 Web 使用者介面中從 儲存管理 > 叢集設定 新增叢集。

6. 在「摘要」頁面中，確認所有設定均正確，然後按一下 完成。

「入門指南」頁面關閉，並顯示「Unified Manager 儀表板」頁面。

將叢集新增至 **Active IQ Unified Manager**

您可以將叢集新增至 Active IQ Unified Manager 中，以便監控該叢集。這包括取得叢集資訊，例如叢集的健全狀況、容量、效能和組態，以便您找出並解決可能發生的任何問題。

開始之前

- 您必須擁有應用程式系統管理員或儲存系統管理員角色。
- 您必須具備以下資訊：
  - Unified Manager 支援內部部署 ONTAP 叢集、ONTAP Select 和 Cloud Volumes ONTAP。
  - 主機名稱或叢集管理 IP 位址

    主機名稱是 Unified Manager 用於連接叢集的 FQDN 或簡稱。主機名稱必須解析為叢集管理 IP 位址。

    叢集管理 IP 位址必須是管理儲存設備虛擬機器（SVM）的叢集管理 LIF。如果使用節點管理 LIF，則操作會失敗。

  - 叢集必須執行 ONTAP 版本 9.1 或更高版本的軟體。
  - ONTAP 系統管理員使用者名稱和密碼

    此帳戶必須具有 *admin* 角色，且應用程式存取設定為 *ontapi*、*amqp*、*console* 和 *http*。

  - 使用 HTTPS 協定連接到叢集的連接埠號碼（通常為連接埠 443）
  - 您擁有所需的憑證：

    SSL (HTTPS) 憑證：此憑證歸 Unified Manager 所有。全新安裝 Unified Manager 時會產生預設的自簽 SSL (HTTPS) 憑證。NetApp 建議您將其升級為 CA 簽署憑證以提高安全性。如果伺服器憑證過期，您應該重新產生憑證並重新啟動 Unified Manager，以便服務套用新憑證。如需重新產生 SSL 憑證的詳細資訊，請參閱 "產生 HTTPS 安全性憑證"。

    EMS 憑證：此憑證歸 Unified Manager 所有。它用於對從 ONTAP 接收的 EMS 通知進行驗證。

    雙向 **TLS** 通訊憑證：用於 Unified Manager 和 ONTAP 之間的雙向 TLS 通訊。基於憑證的驗證是否針對

叢集啟用，取決於 ONTAP 版本。如果叢集執行的 ONTAP 版本低於 9.5，則不會啟用基於憑證的驗證。

如果您正在更新舊版的 Unified Manager，則叢集不會自動啟用以憑證為基礎的驗證。不過，您可以透過修改並儲存叢集詳細資料來啟用它。如果憑證過期，您應該重新產生憑證以納入新憑證。如需檢視與重新產生憑證的詳細資訊，請參閱 "編輯叢集"。

- 您可以從 Web UI 新增叢集，並且會自動啟用基於憑證的驗證。
- 您可以透過 Unified Manager CLI 新增叢集，預設未啟用基於憑證的驗證。如果您使用 Unified Manager CLI 新增叢集，則需要使用 Unified Manager UI 編輯該叢集。您可以查看 "支援的 Unified Manager CLI 命令" 了解如何使用 Unified Manager CLI 新增叢集。
- 如果叢集啟用了基於憑證的驗證，且您從一部伺服器備份 Unified Manager 並還原到另一部主機名稱或 IP 位址已變更的 Unified Manager 伺服器，則叢集監控可能會失敗。為避免此故障，請編輯並儲存叢集詳細資料。如需編輯叢集詳細資料的詳細資訊，請參閱 "編輯叢集"。

+ 叢集憑證：此憑證歸 ONTAP 所有。您無法使用已過期的憑證將叢集新增至 Unified Manager；如果憑證已過期，則應在新增叢集之前重新產生該憑證。如需憑證產生的相關資訊，請參閱知識庫（KB）文章 "如何在 System Manager 使用者介面中續約 ONTAP 自簽名憑證"。

- Unified Manager 伺服器上必須有足夠的空間。當資料庫目錄中超過 90% 的空間已被佔用時，您將無法將叢集新增至伺服器。

對於 MetroCluster 組態，您必須同時新增本機和遠端叢集，而且叢集必須正確設定。

步驟

1. 在左側導覽窗格中，按一下 儲存管理 > 叢集設定。
2. 在叢集設定頁面上，按一下 新增。
3. 在「新增叢集」對話方塊中，指定所需的值，例如叢集的主機名稱或 IP 位址、使用者名稱、密碼和連接埠號碼。

   您可以將叢集管理 IP 位址從 IPv6 變更為 IPv4，或從 IPv4 變更為 IPv6。新的 IP 位址將在下一個監控週期結束後反映在叢集網格和叢集組態頁面中。
4. 按一下 提交。
5. 在「授權主機」對話方塊中，按一下 檢視憑證 以檢視有關叢集的憑證資訊。
6. 點選 **Yes** 。

   儲存叢集詳細資料後，您可以看到叢集的相互 TLS 通訊憑證。

   如果未啟用以憑證為基礎的驗證， Unified Manager 僅在最初新增叢集時檢查憑證。Unified Manager 不會針對每次對 ONTAP 的 API 呼叫檢查憑證。

在發現新叢集的所有物件後，Unified Manager 會開始收集過去 15 天的歷史效能資料。這些統計資料是透過資料連續性收集功能收集的。此功能可在叢集新增後立即提供超過兩週的效能資訊。資料連續性收集週期完成後，預設情況下，系統會每五分鐘收集即時叢集效能資料。

由於收集 15 天的效能資料會佔用大量 CPU 資源，建議您錯開新增叢集的時間，以避免同時在過多叢集上執行資料連續性收集輪詢。此外，如果在資料連續性收集期間重新啟動 Unified Manager

，收集工作將會停止，您將在效能圖表中看到缺少時間段的資料空白。

如果您收到無法新增叢集的錯誤訊息，請檢查兩個系統上的時鐘是否未同步，以及 Unified Manager HTTPS 憑證的起始日期是否晚於叢集上的日期。您必須確保使用 NTP 或類似服務來同步時鐘。

相關資訊

"安裝 CA 簽署並傳回的 HTTPS 憑證"

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**。

如果您選擇.....	然後這樣做.....
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。
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** 。

在 **Active IQ Unified Manager** 中變更本機使用者密碼

您可以變更本機使用者登入密碼以防止潛力的安全性風險。

開始之前

您必須以本機使用者登入。

使用這些步驟無法變更維護使用者和遠端使用者的密碼。若要變更遠端使用者密碼，請聯絡您的密碼系統管理員。若要變更維護使用者密碼，請參閱 "使用維護主控台"。

步驟

1. 登入 Unified Manager。
2. 從頂部功能表列中，按一下使用者圖示，然後按一下 更改密碼。

   如果您是遠端使用者，則不會顯示 變更密碼 選項。

3. 在「更改密碼」對話方塊中，輸入目前密碼和新密碼。
4. 按一下 **Save** 。

如果 Unified Manager 設定為高可用性組態，則必須變更設定中第二個節點的密碼。兩個執行個體必須具有相同的密碼。

在 **Active IQ Unified Manager** 中設定工作階段不活動逾時

您可以為 Unified Manager 指定閒置逾時值，以便在一段時間未活動後自動終止工作階段。預設逾時設為 4,320 分鐘（72 小時）。

開始之前

您必須擁有應用程式管理員角色。

此設定會影響所有已登入使用者工作階段。

如果您已啟用安全性聲明標記語言 (SAML) 驗證，則無法使用此選項。

步驟

1. 在左側導覽窗格中，按一下 一般 > 功能設定。
2. 在 功能設定 頁面中，選擇下列選項之一來指定不活動逾時：

如果您想要.....	然後這樣做.....
未設定逾時，因此工作階段永遠不會自動關閉	在 不活動逾時 面板中，將滑桿按鈕向左移動（關閉），然後按一下 套用。
設定特定的分鐘數作為逾時值	在 閒置逾時 面板中，將滑桿按鈕向右移動（開啟），以分鐘為單位指定閒置逾時值，然後按一下 套用。

使用 **Active IQ Unified Manager** 中的 **CLI** 設定工作階段逾時

您可以使用 CLI 為 Unified Manager 設定最大工作階段逾時值，以便在一定時間後自動終止工作階段。預設情況下，您的工作階段逾時設定為最大值，即 4,320 分鐘（72 小時）。這表示即使您已登入並正在使用 Unified Manager，您的工作階段也會在 72 小時後自動結束。

關於此任務

您必須擁有應用程式管理員角色。

工作階段逾時設定會影響所有已登入使用者的工作階段。

步驟

1. 輸入 `um cli login` 命令以登入 Unified Manager CLI。使用有效的使用者名稱和密碼進行驗證。
2. 輸入 `um option set max.session.timeout.value=<in mins>` 命令以修改工作階段逾時值。

變更 Unified Manager 主機名稱

更改 Active IQ Unified Manager 虛擬應用裝置主機名稱

首次部署 Unified Manager 虛擬應用裝置時，系統會為網路主機指派名稱。部署後，您可以變更主機名稱。如果變更主機名稱，則必須重新產生 HTTPS 憑證。

開始之前

您必須以維護使用者身分登入 Unified Manager，或被指派應用程式管理員角色才能執行這些任務。

您可以使用主機名稱（或主機 IP 位址）存取 Unified Manager Web UI。如果您在部署期間為網路設定了靜態 IP 位址，則需要為網路主機指定名稱。如果您使用 DHCP 設定網路，則主機名稱應取自 DNS。如果 DHCP 或 DNS 設定不正確，則會自動指派主機名稱 “Unified Manager”，並將其與安全性憑證關聯。

無論主機名稱是如何指派的，如果您變更了主機名稱，並且打算使用新的主機名稱存取 Unified Manager Web UI，則必須產生新的安全性憑證。

如果您使用伺服器的 IP 位址而不是主機名稱存取 Web 使用者介面，則變更主機名稱時無需產生新憑證。但是，最佳實務做法是更新憑證，使憑證中的主機名稱與實際主機名稱相符。

如果在 Unified Manager 中變更主機名稱，您必須在 OnCommand Workflow Automation (WFA) 中手動更新主機名稱。主機名稱不會在 WFA 中自動更新。

新憑證只有在 Unified Manager 虛擬機器重新啟動後才會生效。

步驟

1. 產生 HTTPS 安全性憑證

   如果您要使用新的主機名稱存取 Unified Manager Web UI，則必須重新產生 HTTPS 憑證，將其與新的主機名稱建立關聯。

2. 重新啟動 Unified Manager 虛擬機器

   重新產生 HTTPS 憑證後，必須重新啟動 Unified Manager 虛擬機器。

在 Active IQ Unified Manager 中產生 HTTPS 安全性憑證

首次安裝 Active IQ Unified Manager 時，系統會安裝預設的 HTTPS 憑證。您可以產生新的 HTTPS 安全性憑證來取代現有憑證。

開始之前

您必須擁有應用程式管理員角色。

重新產生憑證的原因有很多，例如，如果您想要更好的可分辨名稱（DN）值，或想要更大的金鑰長度，或更長

的有效期，或目前憑證已過期。

如果您無法存取 Unified Manager Web UI，您可以使用維護主控台以相同的值重新產生 HTTPS 憑證。重新產生憑證時，您可以定義金鑰大小和金鑰的有效期間。如果您使用維護主控台中的 `Reset Server Certificate` 選項，則會建立有效期限為 397 天的新 HTTPS 憑證。此憑證將具有大小為 2048 位元的 RSA 金鑰。

步驟

1. 在左側導覽窗格中，按一下 一般 > **HTTPS** 憑證。
2. 點選 重新產生 **HTTPS** 憑證。

   隨即顯示「重新產生 HTTPS 憑證」對話方塊。
3. 根據您希望產生憑證的方式，選擇以下選項之一：

如果您想要.....	這樣做.....
使用目前值重新產生憑證	按一下 使用目前憑證屬性重新產生 選項。
使用不同的值產生憑證	點選 更新目前憑證屬性 選項。 如果您不輸入新值， Common Name 和 Alternative Names 欄位將使用現有憑證中的值。"`Common Name`" 應設定為主機的 FQDN。其他欄位不需要值，但如果您希望憑證中填入這些值，則可以輸入值，例如 EMAIL、COMPANY、DEPARTMENT、City、State 和 Country。您也可以從可用的 KEY SIZE（金鑰演算法為 "`RSA`"）和 VALIDITY PERIOD 中進行選擇。 • 金鑰大小允許的值為 `2048`、`3072` 和 `4096`。 • 有效期限最短為 1 天，最長為 36500 天。 儘管允許的有效期為 36500 天，但建議您使用不超過 397 天或 13 個月的有效期。因為如果您選擇的有效期超過 397 天，並且計畫為此憑證匯出 CSR 並由知名 CA 簽署，則 CA 傳回給您的已簽署憑證的有效期將縮短至 397 天。 • 如果您希望從憑證的「備用名稱」欄位移除本機識別資訊，可以選取「排除本機識別資訊（例如 localhost）」核取方塊。選取此核取方塊後，「備用名稱」欄位將僅使用您在此欄位中輸入的內容。如果留空，產生的憑證將完全不包含「備用名稱」欄位。

4. 按一下 是 以重新產生憑證。

5. 重新啟動 Unified Manager 伺服器，使新憑證生效。
6. 透過檢視 HTTPS 憑證來驗證新的憑證資訊。

重新啟動 **Active IQ Unified Manager** 虛擬機器

您可以從 Unified Manager 的維護主控台重新啟動虛擬機器。產生新的安全性憑證後，或虛擬機器出現問題時，必須重新啟動。

開始之前

虛擬應用裝置已啟動。

您已以維護使用者的身分登入維護主控台。

您也可以使用 **Restart Guest** 選項從 vSphere 重新啟動虛擬機器。如需詳細資訊，請參閱 VMware 文件。

步驟

1. 存取維護控制台。
2. 選擇 系統組態 > 重新啟動虛擬機器。

在 **Linux** 系統上變更 **Active IQ Unified Manager** 主機名稱

在某些情況下，您可能需要變更已安裝 Unified Manager 的 Red Hat Enterprise Linux 機器主機名稱。例如，當您列出 Linux 機器時，您可能希望重新命名主機，以便依類型、工作群組或受監控的叢集群組更輕鬆地識別 Unified Manager 伺服器。

開始之前

您必須擁有安裝 Unified Manager 的 Linux 系統的 root 使用者存取權。

您可以使用主機名稱（或主機 IP 位址）存取 Unified Manager web UI。如果您在部署期間為網路設定了靜態 IP 位址，則您應該已經為網路主機指定了名稱。如果您使用 DHCP 設定網路，則主機名稱應取自 DNS 伺服器。

無論主機名稱是如何指派的，如果您變更了主機名稱並打算使用新主機名稱存取 Unified Manager Web UI，則必須產生新的安全性憑證。

如果您使用伺服器的 IP 位址而不是主機名稱存取 Web UI，則變更主機名稱後無需產生新憑證。但是，最佳實務做法是更新憑證，使憑證中的主機名稱與實際主機名稱相符。新憑證需要重新啟動 Linux 機器後才能生效。

如果在 Unified Manager 中變更主機名稱，您必須在 OnCommand Workflow Automation (WFA) 中手動更新主機名稱。主機名稱不會在 WFA 中自動更新。

步驟

1. 以 root 使用者身分登入要修改的 Unified Manager 系統。
2. 輸入以下命令停止 Unified Manager 軟體及其關聯的 MySQL 軟體：

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. 使用 Linux `hostnamectl` 命令更改主機名稱：

```
hostnamectl set-hostname new_FQDN

hostnamectl set-hostname nuhost.corp.widget.com
```

4. 重新產生伺服器的 HTTPS 憑證：

```
/opt/netapp/essentials/bin/cert.sh create
```

5. 重新啟動網路服務：

```
systemctl restart NetworkManager.service
```

6. 服務重新啟動後，驗證新的主機名稱是否能夠 ping 通自身：

```
ping new_hostname

ping nuhost
```

此命令應傳回與先前為原始主機名稱設定相同的 IP 位址。

7. 完成並驗證主機名稱變更後，請輸入下列命令重新啟動 Unified Manager：

```
systemctl start mysqld ocie ocieau
```

在 **Active IQ Unified Manager** 中啟用並停用原則型儲存管理

從 Unified Manager 9.7 開始，您可以在 ONTAP 叢集上資源配置儲存設備工作負載（磁碟區和 LUN），並根據指派的效能服務層級管理這些工作負載。此功能類似於在 ONTAP System Manager 中建立工作負載並附加 QoS 原則，但使用 Unified Manager 套用時，您可以跨您的 Unified Manager 執行個體監控的所有叢集資源配置和管理工作負載。

您必須擁有應用程式管理員角色。

此選項預設為啟用，但如果您不想使用 Unified Manager 來資源配置和管理工作負載，則可以將其停用。

啟用後，此選項會在使用者介面中提供許多新項目：

新內容	地點
用於資源配置新工作負載的頁面	可從 常用任務 > 資源配置 中取得
用於建立效能服務層級原則的頁面	可從 設定 > 原則 > 效能服務層級 取得
用於建立效能儲存效率原則的頁面	可從 設定 > 原則 > 儲存效率 取得
顯示目前工作負載效能和工作負載 IOPS 的面板	可從儀表板取得

有關這些頁面和此功能的更多資訊，請參閱產品中的線上說明。

步驟

1. 在左側導覽窗格中，按一下 一般 > 功能設定。

2. 在 功能設定 頁面中，選擇下列選項之一來停用或啟用原則型儲存管理：

如果您想要.....	然後這樣做.....
停用原則型儲存管理	在 原則型儲存管理 面板中，將滑桿按鈕向左移動。
啟用原則型儲存管理	在 原則型儲存管理 面板中，將滑桿按鈕向右移動。

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。