執行組態與管理工作

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

執行組態與管理工作 1
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
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
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 備份 19
管理功能設定 19
了解 Active IQ Unified Manager 中的功能設定 19
在 Active IQ Unified Manager 中啟用原則型儲存管理 19
了解 Active IQ Unified Manager 中的 API 閘道功能 20
在 Active IQ Unified Manager 中指定非活動逾時 20
在 Active IQ Unified Manager 中啟用 Active IQ 入口網站事件 20
在 Active IQ Unified Manager 中啟用和停用安全性設定以符合法規遵循 21
在 Active IQ Unified Manager 中啟用和停用指令碼上傳 21
在 Active IQ Unified Manager 中新增登入橫幅 22
使用維護主控台 22
了解 Active IQ Unified Manager 中的維護主控台 22
了解 Active IQ Unified Manager 中的維護使用者 22
Active IQ Unified Manager 中的診斷使用者功能 23
在 Active IQ Unified Manager 中存取維護主控台 23
在 Active IQ Unified Manager 中使用 vSphere VM 主控台存取維護主控台 23
維護主控台選單 24
在 Active IQ Unified Manager 中變更 Windows 上的維護使用者密碼 29
更改 Linux 系統上的 Active IQ Unified Manager umadmin 密碼 29
更改 Active IQ Unified Manager 用於 HTTP 和 HTTPS 協定的連接埠 30
將網路介面新增至 Active IQ Unified Manager 30
在 Active IQ Unified Manager 中重新產生用戶端憑證 31
新增磁碟空間 31
管理使用者存取 35
新增使用者 35
在 Active IQ Unified Manager 中編輯使用者設定 36

在 Active IQ Unified Manager 中檢視使用者 . . . 36
在 Active IQ Unified Manager 中刪除使用者或群組 . . . 37
了解 Active IQ Unified Manager 中的角色型存取控制 . . . 37
了解 Active IQ Unified Manager 中的使用者類型 . . . 37
了解 Active IQ Unified Manager 中的使用者角色 . . . 38
了解 Active IQ Unified Manager 中的使用者角色和功能 . . . 39
管理 SAML 驗證設定 . . . 40
在 Active IQ Unified Manager 中啟用 SAML 驗證 . . . 40
在 Active IQ Unified Manager 中使用身分供應商 . . . 40
在 Active IQ Unified Manager 中啟用 SAML 驗證 . . . 41
在 Active IQ Unified Manager 中變更 SAML 驗證身分供應商 . . . 42
在 Active IQ Unified Manager 安全性憑證變更後更新 SAML 驗證設定 . . . 43
在 Active IQ Unified Manager 中停用 SAML 驗證 . . . 44
從 Active IQ Unified Manager 維護主控台停用 SAML 驗證 . . . 44
在 Active IQ Unified Manager 中使用 SAML 驗證頁面 . . . 45
管理驗證 . . . 46
在 Active IQ Unified Manager 中編輯驗證伺服器 . . . 46
在 Active IQ Unified Manager 中刪除驗證伺服器 . . . 46
在 Active IQ Unified Manager 中使用 Active Directory 或 OpenLDAP 進行驗證 . . . 47
稽核記錄 . . . 47
使用 Active IQ Unified Manager 中的遠端身分驗證頁面 . . . 49
管理安全性證書 . . . 52
在 Active IQ Unified Manager 中檢視 HTTPS 安全性憑證 . . . 52
在 Active IQ Unified Manager 中下載 HTTPS 憑證簽署要求 . . . 52
在 Active IQ Unified Manager 中安裝由 CA 簽署的 HTTPS 憑證 . . . 53
了解 Active IQ Unified Manager Unified Manager 中如何使用外部工具產生 HTTPS 憑證 . . . 54
憑證管理頁面描述 . . . 56

執行組態與管理工作

設定 Active IQ Unified Manager

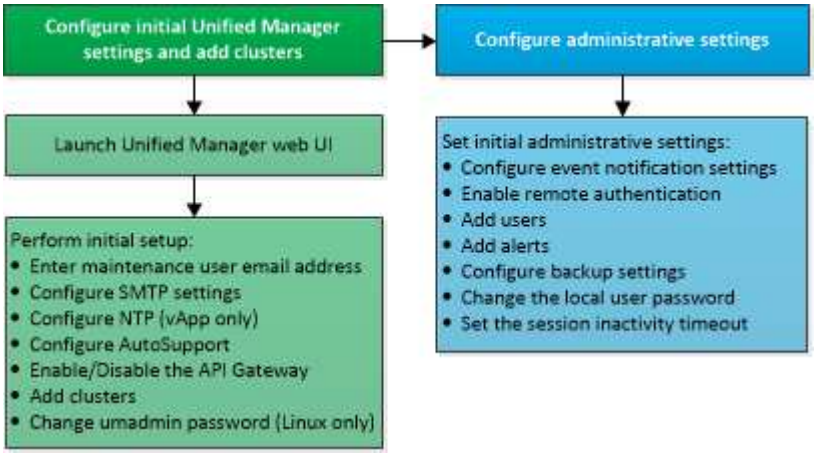
了解如何設定 Active IQ Unified Manager

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

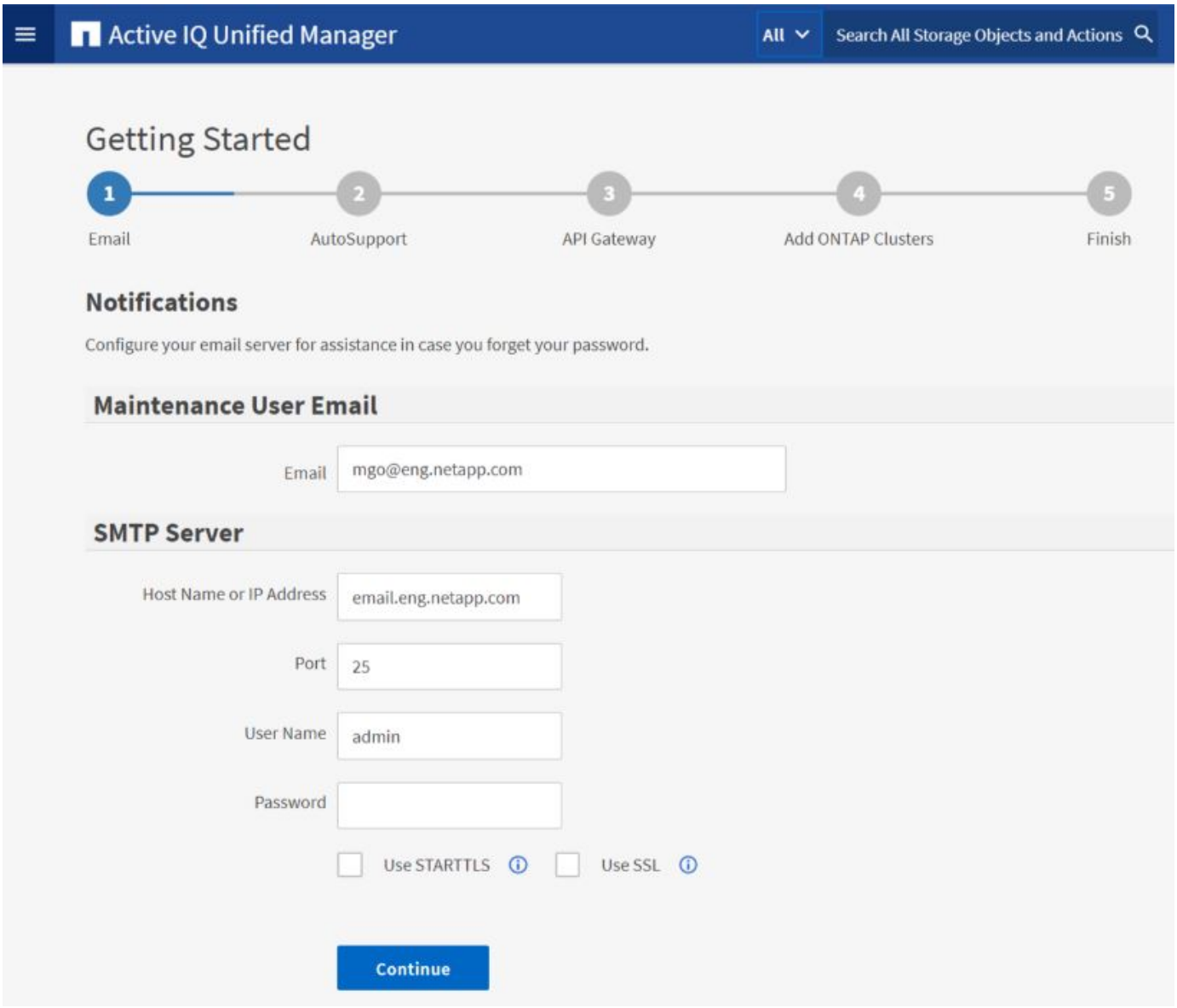
若要使用 Unified Manager，您必須先設定初始設定選項，包括 NTP 伺服器、維護使用者電子郵件地址、SMTP 伺服器主機，以及新增 ONTAP 叢集。

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。

設定 Active IQ Unified Manager 備份

您可以透過在主機系統上執行的一系列組態步驟以及透過維護主控台，在 Unified Manager 上設定備份功能。

有關組態步驟的資訊，請參閱"管理備份與恢復作業"。

管理功能設定

了解 Active IQ Unified Manager 中的功能設定

「功能設定」頁面可讓您啟用和停用 Active IQ Unified Manager 中的特定功能。這包括根據原則建立和管理儲存設備物件、啟用 API 閘道和登入橫幅、上傳用於管理警報的指令碼、根據閒置時間使 Web UI 工作階段逾時，以及停用接收 Active IQ 平台事件。

只有具有應用程式管理員角色的使用者才能存取「功能設定」頁面。

有關腳本上傳的資訊，請參閱 "啟用與停用指令碼上傳"。

在 Active IQ Unified Manager 中啟用原則型儲存管理

以原則為基礎的儲存管理 選項可根據服務層級目標（SLOs）進行儲存管理。此選項預設為啟用。

啟動此功能後，您可以在新增至 Active IQ Unified Manager 執行個體的 ONTAP 叢集上資源配置儲存設備工作負載，並根據指派的效能服務層級和儲存效率原則來管理這些工作負載。

您可以從 一般 > 功能設定 > 基於政策的儲存管理 中選擇啟動或停用此功能。啟動此功能後，以下頁面可用於操作和監控：

- 資源配置（儲存設備工作負載資源配置）
- 策略 > 效能服務層級
- 政策 > 儲存效率
- 叢集設定頁面上的「由效能服務層級管理的工作負載」欄
- *儀表板*上的「工作負載效能」面板

您可以使用這些畫面建立效能服務等級和儲存效率原則，並資源配置儲存設備工作負載。您也可以監控符合已指派效能服務等級的儲存設備工作負載，以及不符合的儲存設備工作負載。「工作負載效能」和「工作負載 IOPS」面板還可讓您根據在資料中心叢集上資源配置的儲存設備工作負載，評估叢集的總容量、可用容量、已使用容量及效能（IOPS）。

啟用此功能後，您可以從 功能表列 > 說明按鈕 > **API** 文件 > **storage-provider** 類別執行 Unified Manager REST API 來執行部分功能。或者，您可以輸入主機名稱或 IP 位址以及 URL 來存取 REST API 頁面，格式為 https://<hostname>/docs/api/

如需有關 API 的詳細資訊，請參閱"Active IQ Unified Manager REST API 入門指南"。

了解 **Active IQ Unified Manager** 中的 **API** 閘道功能

API 閘道功能使 Active IQ Unified Manager 成為單一控制平面，您可以從中管理多個 ONTAP 叢集，而無需個別登入它們。

您可以在首次登入 Unified Manager 時顯示的組態頁面中啟用此功能。或者，您也可以從 一般 > 功能設定 > **API** 閘道 啟用或停用此功能。

Unified Manager REST API 與 ONTAP REST API 不同，並非所有 ONTAP REST API 的功能都可以透過 Unified Manager REST API 實現。但是，如果您有特定的業務需求，需要存取 ONTAP API 來管理 Unified Manager 未公開的特定功能，則可以啟用 API 閘道功能並執行 ONTAP API。閘道充當 Proxy，透過保持標頭和主體請求的格式與 ONTAP API 相同來傳輸 API 請求。您可以使用 Unified Manager 憑證執行特定的 API 來存取和管理 ONTAP 叢集，而無需傳遞個別叢集的憑證。Unified Manager 作為管理的單點，用於在您的 Unified Manager 執行個體代管的 ONTAP 叢集上執行 API。API 傳回的回應與直接從 ONTAP 執行對應的 ONTAP REST API 傳回的回應相同。

啟用此功能後，您可以從 功能表列 > 說明 按鈕 > **API** 文件 > 閘道 類別執行 Unified Manager REST API。或者，您也可以以下列格式輸入主機名稱或 IP 位址以及 URL 來存取 REST API 頁面 `https://<hostname>/docs/api/`

如需有關 API 的詳細資訊，請參閱"Active IQ Unified Manager REST API 入門指南"。

在 **Active IQ Unified Manager** 中指定非活動逾時

您可以為 Active IQ Unified Manager 指定非活動逾時值。如果使用者在指定時間內沒有活動，應用程式將自動登出。此選項預設為啟用。

您可以從 一般 > 功能設定 > 不活動逾時 停用此功能或修改時間。啟動此功能後，您應該在 **LOGOUT AFTER** 欄位中指定不活動的時間限制（以分鐘為單位），之後系統會自動登出。預設值為 4320 分鐘（72 小時）。

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。

在 **Active IQ Unified Manager** 中啟用 **Active IQ** 入口網站事件

您可以指定是否要啟用或停用 Active IQ 入口網站事件。此設定可讓 Active IQ 入口網站發現並顯示有關係統組態、佈線等方面的其他事件。此選項預設為啟用。

啟用此功能後，Active IQ Unified Manager 將顯示由 Active IQ 入口網站發現的事件。這些事件是透過對所有受監控儲存設備系統產生的 AutoSupport 訊息執行一組規則所建立。這些事件與其他 Unified Manager 事件不同，它們可識別與系統組態、佈線、最佳實務做法和可用度問題相關的事件或風險。

您可以從 一般 > 功能設定 > **Active IQ Portal** 事件 中選擇啟動或停用此功能。在沒有外部網路存取的站台中，您必須從 儲存管理 > 事件設定 > 上傳規則 手動上傳規則。

此功能預設為啟用。停用此功能將阻止 Unified Manager 發現或顯示 Active IQ 事件。停用後，啟用此功能可使 Unified Manager 在叢集所在時區的預先定義時間 00:15 接收叢集上的 Active IQ 事件。

在 **Active IQ Unified Manager** 中啟用和停用安全性設定以符合法規遵循

透過使用「功能設定」頁面的 安全性儀表板 面板上的 自訂 按鈕，您可以啟用或停用 Unified Manager 上的法規遵循監控安全性參數。

本頁面啟用或停用的設定會治理 Unified Manager 上叢集和儲存 VM 的整體法規遵循狀態。根據選擇，對應的欄位會顯示在叢集清單頁面的 安全性：所有叢集 檢視和儲存 VM 清單頁面的 安全性：所有儲存 **VM** 檢視中。

只有具有系統管理員角色的使用者才能編輯這些設定。

系統會根據 "NetApp ONTAP 9 安全加固指南" 中定義的建議，評估您的 ONTAP 叢集、儲存設備虛擬機器和磁碟區的安全性準則。儀表板上的「安全性」面板和「安全性」頁面會顯示叢集、儲存設備虛擬機器和磁碟區的預設安全性法規遵循狀態。系統也會產生安全性事件，並對發生安全性違規的叢集和儲存設備虛擬機器啟用管理動作。

自訂安全性設定

若要根據您的 ONTAP 環境自訂法規遵循監控設定，請依照下列步驟操作：

步驟

1. 按一下 一般 **>** 功能設定 **>** 安全性儀表板 **>** 自訂。此時會顯示 自訂安全性儀表板設定 快顯視窗。

   您啟用或停用的安全性法規遵循參數會直接影響「叢集」和「儲存 VM」畫面上的預設安全性檢視、報告和排程報告。如果您在修改安全性參數之前已從這些畫面上傳過 Excel 報告，則下載的 Excel 報告可能有錯誤。

2. 若要啟用或停用 ONTAP 叢集的自訂設定，請在 叢集 下選取所需的一般設定。如需自訂叢集法規遵循選項的相關資訊，請參閱 "叢集法規遵循類別"。
3. 若要啟用或停用儲存設備虛擬機器的自訂設定，請在 **Storage VM** 下選取所需的一般設定。如需自訂儲存設備虛擬機器法規遵循選項的相關資訊，請參閱 "儲存虛擬機器法規遵循類別"。

自訂 **AutoSupport** 和驗證設定

在 **AutoSupport** 設定 區段中，您可以指定是否要使用 HTTPS 傳輸從 ONTAP 傳送 AutoSupport 訊息。

從 驗證設定 區段中，您可以啟用 Unified Manager 警報，以便為預設的 ONTAP 系統管理員使用者發出警報。

在 **Active IQ Unified Manager** 中啟用和停用指令碼上傳

預設情況下，上傳指令碼到 Unified Manager 並執行指令碼的功能已啟用。如果出於安全性原因，您的組織不希望允許此活動，您可以停用此功能。

開始之前

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 > 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指令碼：

如果您想要.....	然後這樣做.....
停用指令碼	在 指令碼上傳 面板中，將滑桿按鈕向左移動。
啟用指令碼	在 腳本上傳 面板中，將滑桿按鈕向右移動。

在 **Active IQ Unified Manager** 中新增登入橫幅

新增登入橫幅可以讓您的組織顯示任何訊息，例如誰有權存取系統以及登入和登出期間的使用條款和條件。

任何使用者，例如儲存設備操作員或管理員，都可以在登入、登出和工作階段逾時期間檢視此登入橫幅彈出視窗。

使用維護主控台

了解 **Active IQ Unified Manager** 中的維護主控台

Unified Manager 維護主控台可讓您維護 Unified Manager 系統上的設定，並進行任何必要的變更，以防止問題發生。

根據您安裝 Unified Manager 的作業系統，維護主控台提供下列功能：

- 疑難排解虛擬應用裝置的任何問題，尤其是在 Unified Manager Web 介面無法使用時
- 升級至較新版本的 Unified Manager
- 產生支援包以發送給技術支援
- 設定網路設定
- 變更維護使用者密碼
- 連線至外部資料供應商以傳送效能統計資料
- 變更內部效能資料收集
- 從先前備份的版本還原 Unified Manager 資料庫和組態設定。

了解 **Active IQ Unified Manager** 中的維護使用者

維護使用者是在 Red Hat Enterprise Linux 系統上安裝 Unified Manager 時建立的。維護使用者名稱是 “umadmin” 使用者。維護使用者在 Web UI 中擁有應用程式系統管理員角色，且該使用者可以建立後續使用者並為其指派角色。

維護使用者（或 umadmin 使用者）也可以存取 Unified Manager 維護主控台。

Active IQ Unified Manager 中的診斷使用者功能

診斷存取的目的是為了方便技術支援協助您進行疑難排解，您只能在技術支援的指導下使用它。

診斷使用者可以在技術支援的指導下執行作業系統層級的命令，以進行疑難排解。

在 Active IQ Unified Manager 中存取維護主控台

如果 Unified Manager 使用者介面無法運作，或者您需要執行使用者介面中沒有的功能，您可以存取維護主控台來管理您的 Unified Manager 系統。

開始之前

您必須已安裝並設定 Unified Manager。

閒置 15 分鐘後，維護主控台會將您登出。

在 VMware 上安裝時，如果您已經透過 VMware 控制台以維護使用者身分登入，則無法同時使用 Secure Shell 登入。

步驟

1. 請依照下列步驟存取維護主控台：

在這個作業系統上.....	請依照以下步驟操作.....
VMware	a. 使用 Secure Shell，連線至 Unified Manager 虛擬應用裝置的 IP 位址或完整網域名稱。 b. 使用您的維護使用者名稱和密碼登入維護主控台。
Linux	a. 使用 Secure Shell，連線至 Unified Manager 系統的 IP 位址或完整網域名稱。 b. 使用維護使用者（umadmin）名稱和密碼登入系統。 c. 輸入命令 `maintenance_console`並按下 Enter 鍵。
Windows	a. 使用系統管理員憑證登入 Unified Manager 系統。 b. 以 Windows 系統管理員身分啟動 PowerShell。 c. 輸入命令 `maintenance_console`並按下 Enter 鍵。

顯示 Unified Manager 維護主控台選單。

在 Active IQ Unified Manager 中使用 vSphere VM 主控台存取維護主控台

如果 Unified Manager 使用者介面無法運作，或者您需要執行使用者介面中無法使用的功

能，您可以存取維護主控台來重新設定您的虛擬應用裝置。

開始之前

- 您必須是維護使用者。
- 必須先啟動虛擬應用裝置才能存取維護主控台。

步驟

1. 在 vSphere 用戶端中，找到 Unified Manager 虛擬應用裝置。
2. 按一下 **Console** 索引標籤。
3. 點選控制台視窗內部進行登入。
4. 使用您的使用者名稱和密碼登入維護主控台。

   閒置 15 分鐘後，維護主控台會將您登出。

維護主控台選單

了解 **Active IQ Unified Manager** 中的維護主控台選單

維護主控台由不同的選單組成，可讓您維護與管理 Unified Manager 伺服器的特殊功能與組態設定。

根據您安裝 Unified Manager 的作業系統，維護主控台包含下列選單：

- 升級 Unified Manager（僅限 VMware）
- 網路組態（僅限 VMware）
- 系統組態（僅限 VMware）
  a. 支援/診斷
  b. 重設伺服器憑證
  c. 重新產生用戶端憑證
  d. 備份恢復
  e. 外部資料供應商
  f. 效能輪詢間隔組態
  g. 停用 SAML 驗證
  h. 檢視/變更應用程式連接埠
  i. 偵錯日誌組態
  j. 控制對 MySQL 連接埠 3306 的存取
  k. 結束

您可以從清單中選擇數字來存取特定的選單選項。例如，若要備份與恢復，請選擇 *4*。

Active IQ Unified Manager 中的網路組態選單

網路組態功能表可讓您管理網路設定。當 Unified Manager 使用者介面無法使用時，您應該使用此功能表。

如果 Unified Manager 安裝在 Red Hat Enterprise Linux 或 Microsoft Windows 上，則此功能表無法使用。

以下是可供選擇的選單選項。

- 顯示 **IP** 位址設定

  顯示虛擬應用裝置的目前網路設定，包括 IP 位址、網路、廣播位址、子網路遮罩、閘道和 DNS 伺服器。

- 更改 **IP** 位址設定

  可讓您變更虛擬應用裝置的任何網路設定，包括 IP 位址、網路遮罩、閘道或 DNS 伺服器。如果您使用維護主控台將網路設定從 DHCP 切換為靜態連網，則無法編輯主機名稱。您必須選取 提交變更 才能使變更生效。

- 顯示網域名稱搜尋設定

  顯示用於解析主機名稱的網域名稱搜尋清單。

- 變更網域名稱搜尋設定

  可讓您變更解析主機名稱時要搜尋的網域名稱。您必須選取 提交變更 才能使變更生效。

- 顯示靜態路由

  顯示目前靜態網路路由。

- 更改靜態路由

  允許您新增或刪除靜態網路路由。您必須選取 提交變更 才能使變更生效。

  - 新增路由

    允許您新增靜態路由。

  - 刪除路由

    允許您刪除靜態路由。

  - 返回

    返回*主選單*。

  - 離開

    退出維護主控台。

- 停用網路介面

  停用任何可用的網路介面。如果只有一個網路介面可用，則無法將其停用。您必須選取 提交變更 才能使變更生效。

- 啟用網路介面

  啟用可用的網路介面。您必須選取 提交變更 才能使變更生效。

- 提交變更

  套用對虛擬應用裝置網路設定所做的任何變更。您必須選取此選項才能使所做的任何變更生效，否則變更將不會生效。

- **Ping** 主機

  Ping 目標主機以確認 IP 位址變更或 DNS 組態。

- 恢復預設值

  將所有設定重設為出廠預設值。您必須選擇 提交變更 才能使變更生效。

- 返回

  返回*主選單*。

- 離開

  退出維護主控台。

使用 **Active IQ Unified Manager** 中的系統組態選單

系統組態選單可讓您透過提供各種選項來管理您的虛擬應用裝置，例如檢視伺服器狀態，以及重新啟動和關閉虛擬機器。

當 Unified Manager 安裝在 Linux 或 Microsoft Windows 系統上時，此功能表中僅提供 “從 Unified Manager 備份還原” 選項。

以下是可供選擇的選單選項：

- 顯示伺服器狀態

  顯示目前伺服器狀態。狀態選項包括「執行中」和「未執行」。

  如果伺服器未執行，您可能需要聯絡技術支援。

- 重新啟動虛擬機器

  重新啟動虛擬機器，停止所有服務。重新啟動後，虛擬機器和服務會重新啟動。

- 關閉虛擬機器

關閉虛擬機器，停止所有服務。

您只能從虛擬機器控制台選擇此選項。

- 更改**<logged in user>**使用者密碼

  更改目前登入使用者的密碼，該使用者只能是維護使用者。

- 增加資料磁碟容量

  增加虛擬機器中資料磁碟（磁碟 3）的大小。

- 增加交換磁碟容量

  增加虛擬機器中交換磁碟（磁碟 2）的大小。

- 更改時區

  將時區變更為您所在的位置。

- 更改 **NTP** 伺服器

  變更 NTP 伺服器設定，例如 IP 位址或完整網域名稱（FQDN）。

- 更改 **NTP** 服務

  在 `ntp`與 `systemd-timesyncd`服務之間切換。

- 從 **Unified Manager** 備份還原

  從先前備份的版本還原 Unified Manager 資料庫和組態設定。

- 重設伺服器憑證

  重設伺服器安全性憑證。

- 更改主機名稱

  變更安裝虛擬應用裝置的主機名稱。

- 返回

  退出系統組態選單並返回主選單。

- 離開

  退出維護主控台選單。

使用 **Active IQ Unified Manager** 中的「支援與診斷」選單

透過「支援和診斷」選單，您可以產生支援套裝組合，並將其發送給技術支援以獲得疑難排解協助。

以下是可供選擇的選單選項：

- 產生輕量級支援套裝組合

  讓您能夠產生輕量級的支援套裝組合，其中僅包含 30 天的日誌和組態資料庫記錄——不包含效能資料、擷取記錄檔案和伺服器堆積傾印。

- 產生支援套裝組合

  可讓您在診斷使用者的主目錄中建立包含診斷資訊的完整支援套裝組合（7-Zip 檔案）。如果您的系統已連線至網際網路，您也可以將支援套裝組合上傳至 NetApp。

  該檔案包含 AutoSupport 訊息產生的資訊、Unified Manager 資料庫的內容、有關 Unified Manager 伺服器內部的詳細資料，以及通常不包含在 AutoSupport 訊息或輕量級支援套裝組合中的詳細層級記錄。

了解 **Active IQ Unified Manager** 中的其他維護主控台選單選項

以下功能表選項可讓您在 Unified Manager 伺服器上執行各種管理任務。

以下是可供選擇的選單選項：

- 重設伺服器憑證

  重新產生 HTTPS 伺服器憑證。

  您可以在 Unified Manager GUI 中按一下 一般 > **HTTPS** 憑證 > 重新產生 **HTTPS** 憑證 來重新產生伺服器憑證。

- 停用 **SAML** 驗證

  停用 SAML 驗證，使身分供應商（IdP）不再為存取 Unified Manager GUI 的使用者提供登入驗證。當 IdP 伺服器或 SAML 組態出現問題導致使用者無法存取 Unified Manager GUI 時，通常會使用此主控台選項。

- 外部資料供應商

  提供將 Unified Manager 連接到外部資料供應商的選項。建立連線後，效能資料會傳送至外部伺服器，以便儲存效能專家使用第三方軟體繪製效能計量圖表。顯示下列選項：

  - 顯示伺服器組態——顯示外部資料供應商目前的連線和組態設定。
  - 新增 / 修改伺服器連線——可讓您輸入外部資料供應商的新連線設定，或變更現有設定。
  - 修改伺服器組態——可讓您為外部資料供應商輸入新的組態設定，或變更現有設定。
  - 刪除伺服器連線--刪除與外部資料供應商的連線。

    刪除連線後，Unified Manager 將失去與外部伺服器的連線。

- 備份還原

  如需詳細資訊，請參閱 "管理備份與恢復作業" 下的主題。

- 效能輪詢間隔組態

提供設定 Unified Manager 從叢集收集效能統計資料頻率的選項。預設收集間隔為 5 分鐘。

如果您發現大型叢集的收集未能按時完成，您可以將此間隔變更為 10 或 15 分鐘。

- 檢視/變更應用程式連接埠

  提供選項以變更 Unified Manager 用於 HTTP 和 HTTPS 協定的預設連接埠（若基於安全性考量有此需求）。HTTP 的預設連接埠為 80，HTTPS 的預設連接埠為 443。

- 控制對 **MySQL** 連接埠 **3306** 的存取

  控制主機對預設 MySQL 連接埠 3306 的存取。基於安全性考量，在 Linux、Windows 和 VMware vSphere 系統上全新安裝 Unified Manager 時，透過此連接埠的存取僅限於 localhost。此選項可讓您在 localhost 和遠端主機之間切換此連接埠的可見度，也就是說，如果您的環境中僅對 localhost 啟用此連接埠，您也可以將此連接埠開放給遠端主機。或者，當對所有主機啟用時，您可以將此連接埠的存取限制為僅限 localhost。如果之前已在遠端主機上啟用存取，則在升級情況下將保留此組態。切換連接埠可見度後，您應該檢查 Windows 系統上的防火牆設定，如果設定為限制對 MySQL 連接埠 3306 的存取，則應停用防火牆設定。

- 離開

  退出維護主控台選單。

在 **Active IQ Unified Manager** 中變更 **Windows** 上的維護使用者密碼

必要時，您可以變更 Unified Manager 維護使用者的密碼。

步驟

1. 在 Unified Manager Web UI 登入頁面上，按一下 忘記密碼。

   系統會顯示一個頁面，提示您輸入要重設密碼的使用者名稱。

2. 輸入使用者名稱並按一下 提交。

   系統會將包含重設密碼連結的電子郵件傳送至為該使用者名稱定義的電子郵件位址。

3. 按一下電子郵件中的 重設密碼連結，並設定新密碼。
4. 返回 Web 使用者介面，並使用新密碼登入 Unified Manager。

更改 **Linux** 系統上的 **Active IQ Unified Manager umadmin** 密碼

基於安全性考慮，您必須在完成安裝程序後立即變更 Unified Manager umadmin 使用者的預設密碼。如有必要，您可以稍後隨時再次變更密碼。

開始之前

- Unified Manager 必須安裝在 Red Hat Enterprise Linux 系統上。
- 您必須擁有安裝 Unified Manager 的 Linux 系統的 root 使用者憑證。

步驟

1. 以 root 使用者登入執行 Unified Manager 的 Linux 系統。

2. 更改 umadmin 密碼：

   ```
   passwd umadmin
   ```

   系統提示您為 umadmin 使用者輸入新密碼。

更改 **Active IQ Unified Manager** 用於 **HTTP** 和 **HTTPS** 協定的連接埠

如果基於安全性考量而有需要，可以在安裝後變更 Unified Manager 用於 HTTP 和 HTTPS 協定的預設連接埠。HTTP 的預設連接埠為 80，HTTPS 的預設連接埠為 443。

開始之前

您必須擁有授權的使用者 ID 和密碼才能登入 Unified Manager 伺服器的維護控制台。

> 使用 Mozilla Firefox 或 Google Chrome 瀏覽器時，某些連接埠被認為是不安全的。在為 HTTP 和 HTTPS 流量指派新的連接埠號碼之前，請務必檢查您的瀏覽器設定。選擇不安全的連接埠可能會導致系統無法存取，屆時您需要聯絡客戶支援尋求解決方案。

更改連接埠後，Unified Manager 執行個體會自動重新啟動，因此請確保此時是讓系統停機一小段時間的好時機。

1. 使用 SSH 以維護使用者身分登入 Unified Manager 主機。

   顯示 Unified Manager 維護主控台提示。

2. 輸入標記為 檢視/變更應用程式連接埠 的選單選項編號，然後按 Enter 鍵。
3. 如果出現提示，請再次輸入維護使用者密碼。
4. 輸入 HTTP 和 HTTPS 連接埠的新連接埠號碼，然後按 Enter 鍵。

   連接埠號碼留空將指定協定的預設連接埠。

   系統會提示您是否要變更連接埠並立即重新啟動 Unified Manager。

5. 輸入 **y** 變更連接埠並重新啟動 Unified Manager。
6. 退出維護主控台。

更改後，使用者必須在 URL 中包含新的連接埠號碼才能存取 Unified Manager Web UI，例如 https://host.company.com:1234、https://12.13.14.15:1122 或 https://[2001:db8:0:1]:2123。

將網路介面新增至 **Active IQ Unified Manager**

如果需要分隔網路流量，您可以新增新的網路介面。

開始之前

您必須使用 vSphere 將網路介面新增至虛擬應用裝置。

虛擬應用裝置必須開啟電源。

如果 Unified Manager 安裝在 Red Hat Enterprise Linux 或 Microsoft Windows 上，則無法執行此操作。

步驟

1. 在 vSphere 主控台主選單中，選擇 系統組態 > 重新啟動作業系統。

   重新啟動後，維護主控台可以偵測到新增的網路介面。

2. 存取維護控制台。
3. 選取 網路組態 > 啟用網路介面。
4. 選擇新的網路介面，然後按 **Enter** 鍵。

   選擇 **eth1** 並按 **Enter**。

5. 輸入 **y** 以啟用網路介面。
6. 輸入網路設定。

   如果使用靜態介面，或未偵測到 DHCP，系統會提示您輸入網路設定。

   輸入網路設定後，會自動返回 網路組態 選單。

7. 選取 提交變更。

   您必須提交變更才能新增網路介面。

在 **Active IQ Unified Manager** 中重新產生用戶端憑證

您可以使用維護主控台重新產生 Unified Manager 用戶端憑證。您的憑證有五年的延長有效期限。

步驟

1. 以維護使用者登入。
2. 選擇 重新產生用戶端憑證，然後按 **Enter**。
3. 如果系統提示進行驗證，請輸入所需的憑證。
4. 選擇 確認重新產生 並按下 **Enter**。
5. 憑證重新產生後，重新啟動 Unified Manager 服務以套用變更。
6. 若要驗證更新後的憑證，請登入 ONTAP。檢視用戶端憑證狀態和有效性狀態。

相關資訊 "使用 System Manager 管理 ONTAP 憑證"

新增磁碟空間

為 **Active IQ Unified Manager** 資料庫目錄新增磁碟空間

Unified Manager 資料庫目錄包含從 ONTAP 系統收集的所有健全狀況和效能資料。在某些

情況下，您可能需要增加資料庫目錄的大小。

例如，如果 Unified Manager 從大量叢集（每個叢集包含多個節點）收集資料，則資料庫目錄可能會被填滿。當資料庫目錄已滿 90% 時，您將收到警告事件；當目錄已滿 95% 時，您將收到關鍵事件。

在目錄達到 95% 滿之後，不會從叢集中收集其他資料。

根據 Unified Manager 是在 VMware ESXi 伺服器、Red Hat 伺服器或 Microsoft Windows 伺服器上執行，為資料目錄新增容量所需的步驟有所不同。

在 **Active IQ Unified Manager** 中為 **Linux** 主機上的資料目錄新增空間

如果您在最初設定 Linux 主機並安裝 Unified Manager 時，分配給 `/opt/netapp/data`目錄的磁碟空間不足以支援 Unified Manager，您可以在安裝後透過增加 `/opt/netapp/data`目錄的磁碟空間來新增磁碟空間。

開始之前

您必須擁有安裝了 Unified Manager 的 Red Hat Enterprise Linux 機器的 root 使用者存取權。

我們建議您在增加資料目錄大小之前備份 Unified Manager 資料庫。

步驟

1. 以 root 使用者身分登入要新增磁碟空間的 Linux 機器。
2. 依所示順序停止 Unified Manager 服務和相關的 MySQL 軟體：

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. 建立一個臨時備份資料夾（例如 `/backup-data`），並預留足夠的磁碟空間來容納目前 `/opt/netapp/data` 目錄中的資料。
4. 將現有 `/opt/netapp/data`目錄的內容和權限組態複製到備份資料目錄：

   ```
   cp -arp /opt/netapp/data/* /backup-data
   ```

5. 如果啟用 SE Linux：

   a. 取得現有 `/opt/netapp/data`資料夾中資料夾的 SE Linux 類型：

      ```
      se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
      head -1
      ```

      系統傳回類似如下的確認訊息：

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. 執行 chcon 命令為備份目錄設定 SE Linux 類型：

```
chcon -R --type=mysqld_db_t /backup-data
```

6. 移除 `/opt/netapp/data`目錄的內容：
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. 透過 LVM 命令或新增額外磁碟，將 `/opt/netapp/data` 目錄的大小擴充至至少 150 GB。

> 如果您已從磁碟建立 `/opt/netapp/data`，則不應嘗試將 `/opt/netapp/data`裝載為 `NFS` 或 `CIFS` 共用區。因為在這種情況下，如果您嘗試擴充磁碟空間，某些 `LVM` 命令（例如 `resize`和 `extend`）可能無法如預期運作。

8. 確認 `/opt/netapp/data`目錄擁有者（mysql）和群組（根目錄）未更改：

   `ls -ltr /opt/netapp/ | grep data`

   系統傳回類似如下的確認訊息：

```
drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
```

9. 如果啟用了 SE Linux，請確認 `/opt/netapp/data` 目錄的內容仍然設定為 mysqld_db_t：
   a. `touch /opt/netapp/data/abc`
   b. `ls -Z /opt/netapp/data/abc`

      系統傳回類似如下的確認訊息：

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. 刪除檔案 abc，以免該多餘檔案將來導致資料庫錯誤。
11. 將 backup-data 中的內容複製回擴充後的 `/opt/netapp/data` 目錄：

    `cp -arp /backup-data/* /opt/netapp/data/`

12. 如果已啟用 SE Linux，請執行以下命令：

    `chcon -R --type=mysqld_db_t /opt/netapp/data`

13. 啟動 MySQL 服務：

    `systemctl start mysqld`

14. MySQL 服務啟動後，依所示順序啟動 ocie 和 ocieau 服務：

    `systemctl start ocie ocieau`

15. 所有服務啟動完畢後，刪除備份資料夾 `/backup-data`：

```
rm -rf /backup-data
```

在 **Active IQ Unified Manager** 中為 **VMware** 虛擬機器的資料磁碟新增空間

如果您需要增加 Unified Manager 資料庫的資料磁碟空間，可以在安裝後使用 Unified Manager 維護主控台增加磁碟空間來增加容量。

開始之前

- 您必須有權存取 vSphere 用戶端。
- 虛擬機器本機不得儲存任何快照。
- 您必須擁有維護使用者憑證。

我們建議您在增加虛擬磁碟大小之前備份您的虛擬機器。

步驟

1. 在 vSphere 用戶端中，選取 Unified Manager 虛擬機器，然後將更多磁碟容量新增至資料 `disk 3`。如需詳細資訊，請參閱 VMware 文件。

   在極少數情況下，Unified Manager 部署會使用 “硬碟 2” 而不是 “硬碟 3” 作為資料磁碟。如果您的部署中出現了這種情況，請增加較大磁碟的空間。資料磁碟的空間始終大於其他磁碟。

2. 在 vSphere 用戶端中，選擇 Unified Manager 虛擬機器，然後選擇 **Console** 標籤。
3. 按一下主控台視窗，然後使用您的使用者名稱和密碼登入維護主控台。
4. 在主選單中，輸入 系統組態 選項的編號。
5. 在系統組態選單中，輸入 增加資料磁碟大小 選項的編號。

在 **Active IQ Unified Manager** 中為 **Windows** 伺服器上的邏輯磁碟機新增空間

如果您需要增加 Unified Manager 資料庫的磁碟空間，您可以為安裝 Unified Manager 的邏輯磁碟機新增容量。

開始之前

您必須擁有 Windows 系統管理員權限。

我們建議您在新增磁碟空間之前備份 Unified Manager 資料庫。

步驟

1. 以系統管理員登入要新增磁碟空間的 Windows 伺服器。
2. 請按照您想要使用的方法對應的步驟進行操作，以增加更多空間：

選項	說明
在實體伺服器上，為安裝 Unified Manager 伺服器的邏輯磁碟機新增容量。	請依照 Microsoft 主題中的步驟操作： "擴充基本磁碟區"

選項	說明
在實體伺服器上，新增硬碟機。	請依照 Microsoft 主題中的步驟操作： "新增硬碟磁碟機"
在虛擬機器上，增加磁碟分割的大小。	請依照 VMware 主題中的步驟操作： "增加磁碟分割區的大小"

管理使用者存取

新增使用者

在 **Active IQ Unified Manager** 中新增使用者

您可以使用「使用者」頁面新增本機使用者或資料庫使用者。您也可以新增屬於驗證伺服器的遠端使用者或使用者群組。您可以為這些使用者指派角色，並且根據角色的權限，使用者可以使用 Unified Manager 管理儲存設備物件和資料，或檢視資料庫中的資料。

開始之前

- 您必須擁有應用程式管理員角色。
- 若要新增遠端使用者或群組，您必須啟用遠端驗證並設定驗證伺服器。
- 如果您打算設定 SAML 驗證，以便身分供應商（IdP）對存取圖形介面的使用者進行驗證，請確保將這些使用者定義為 “remote” 使用者。

  啟用 SAML 驗證時，類型為 “local” 或 “maintenance” 的使用者無權存取 UI。

如果從 Windows Active Directory 新增群組，則所有直接成員和巢狀子群組都可以向 Unified Manager 驗證，除非巢狀子群組已停用。如果從 OpenLDAP 或其他驗證服務新增群組，則只有該群組的直接成員才能向 Unified Manager 驗證。

步驟

1. 在左側導覽窗格中，按一下 一般 > 使用者。
2. 在「使用者」頁面上，按一下 新增。
3. 在「新增使用者」對話方塊中，選擇要新增的使用者類型，並輸入所需資訊。

   輸入所需的使用者資訊時，您必須指定該使用者獨有的電子郵件地址。您必須避免指定多個使用者共享的電子郵件地址。

4. 點擊 **Add** 。

在 **Active IQ Unified Manager** 中建立資料庫使用者

若要支援 Workflow Automation 與 Unified Manager 之間的連線，或存取資料庫檢視，您必須先在 Unified Manager Web UI 中建立具有 Integration Schema 或 Report Schema 角色的資料庫使用者。

開始之前

您必須擁有應用程式管理員角色。

資料庫使用者提供與 Workflow Automation 的整合，並可存取報表專屬的資料庫檢視。資料庫使用者無法存取 Unified Manager Web UI 或維護主控台，也無法執行 API 呼叫。

步驟

1. 在左側導覽窗格中，按一下 一般 > 使用者。
2. 在使用者頁面中，按一下 新增。
3. 在「新增使用者」對話方塊中，在 類型 下拉清單中選擇 資料庫使用者。
4. 輸入資料庫使用者的名稱和密碼。
5. 在 角色 下拉清單中，選擇適當的角色。

如果您是.....	選擇此角色
將 Unified Manager 與 Workflow Automation 連接	整合結構描述
存取報表和其他資料庫視圖	報表架構

6. 點擊 **Add** 。

在 **Active IQ Unified Manager** 中編輯使用者設定

您可以編輯為每位使用者指定的使用者設定，例如電子郵件地址和角色。例如，您可能需要變更身為儲存設備營運者的使用者角色，並為該使用者指派儲存管理員權限。

開始之前

您必須擁有應用程式管理員角色。

當您修改指派給使用者的角色時，下列任一操作發生時，變更才會生效：

- 使用者登出並重新登入 Unified Manager。
- 已達到 24 小時的工作階段逾時。

步驟

1. 在左側導覽窗格中，按一下 一般 > 使用者。
2. 在「使用者」頁面中，選取您要編輯設定的使用者，然後按一下 編輯。
3. 在「編輯使用者」對話方塊中，編輯為該使用者指定的相應設定。
4. 按一下 **Save** 。

在 **Active IQ Unified Manager** 中檢視使用者

您可以使用「使用者」頁面檢視使用 Unified Manager 管理儲存設備物件和資料的使用者清單。您可以檢視使用者的詳細資訊，例如使用者名稱、使用者類型、電子郵件地址以及指派給使用者的角色。

開始之前

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 > 使用者。

在 **Active IQ Unified Manager** 中刪除使用者或群組

您可以從管理伺服器資料庫中刪除一個或多個使用者，以防止特定使用者存取 Unified Manager。您也可以刪除群組，這樣群組中的所有使用者都將無法再存取管理伺服器。

開始之前

- 刪除遠端群組時，您必須重新指派已指派給遠端群組使用者的事件。

  如果您要刪除本機使用者或遠端使用者，則指派給這些使用者的事件將自動取消指派。

- 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 > 使用者。
2. 在「使用者」頁面中，選擇要刪除的使用者或群組，然後按一下 刪除。
3. 按一下 是 確認刪除。

了解 **Active IQ Unified Manager** 中的角色型存取控制

RBAC（角色型存取控制）提供控制誰能存取 Active IQ Unified Manager 伺服器中各種功能與資源的能力。RBAC 可讓系統管理員透過定義角色來管理使用者群組。如果您需要將特定功能的存取權限限制在選定的系統管理員，則必須為他們設定系統管理員帳戶。如果您想要限制系統管理員可以檢視的資訊以及他們可以執行的作業，則必須將角色套用至您建立的系統管理員帳戶。

管理伺服器使用 RBAC 進行使用者登入和角色權限。如果您尚未變更管理伺服器的管理使用者存取預設設定，則無需登入即可檢視這些設定。

當您發起需要特定權限的操作時，管理伺服器會提示您登入。例如，若要建立系統管理員帳戶，您必須使用應用程式管理員帳戶存取來登入。

了解 **Active IQ Unified Manager** 中的使用者類型

使用者類型指定使用者所持有的帳戶類型，包括遠端使用者、遠端群組、本機使用者、資料庫使用者和維護使用者。每種類型都有其自身的角色，該角色由具有系統管理員角色的使用者指派。

Unified Manager 使用者類型如下：

- 維護使用者

在 Unified Manager 的初始組態期間建立。然後，維護使用者會建立其他使用者並指派角色。維護使用者也是唯一有權存取維護主控台的使用者。當 Unified Manager 安裝在 Red Hat Enterprise Linux 系統上時，維護使用者會被賦予使用者名稱 “umadmin.”。

- 本機使用者

  存取 Unified Manager 介面，並根據維護使用者或具有應用程式系統管理員角色的使用者所賦予的角色執行功能。

- 遠端群組

  使用儲存在驗證伺服器上的憑證來存取 Unified Manager UI 的一組使用者。此帳戶的名稱應與儲存在驗證伺服器上的群組名稱相符。遠端群組中的所有使用者都可以使用各自的使用者憑證存取 Unified Manager UI。遠端群組可以根據其指派的角色執行功能。

- 遠端使用者

  使用儲存在驗證伺服器上的憑證存取 Unified Manager UI。遠端使用者根據維護使用者或具有應用程式管理員角色的使用者所指派的角色執行相應的功能。

- 資料庫使用者

  對 Unified Manager 資料庫中的資料具有唯讀存取權，無法存取 Unified Manager Web 介面或維護主控台，也無法執行 API 呼叫。

了解 **Active IQ Unified Manager** 中的使用者角色

維護使用者或應用程式管理員會為每個使用者指派一個角色。每個角色都包含特定的權限。您在 Unified Manager 中可以執行的活動範圍，取決於指派給您的角色以及該角色包含的權限。

Unified Manager 包含以下預先定義的使用者角色：

- 營運者

  檢視儲存系統資訊以及 Unified Manager 收集的其他資料，包括歷史記錄和容量趨勢。此角色允許儲存設備營運者檢視、指派、確認、解決事件並新增備註。

- 儲存管理員

  在 Unified Manager 中設定儲存管理作業。此角色可讓儲存管理員設定臨界值，並建立警報及其他儲存管理專屬的選項與原則。

- 應用程式管理員

  設定與儲存管理無關的設定。此角色可管理使用者、安全性憑證、資料庫存取及管理選項，包括驗證、SMTP、連網與 AutoSupport。

> 當 Unified Manager 安裝在 Linux 系統上時，具有應用程式管理員角色的初始使用者會自動命名為「umadmin」。

- 整合結構描述

  此角色允許對 Unified Manager 資料庫檢視進行唯讀存取，以便將 Unified Manager 與 OnCommand Workflow Automation （WFA） 整合。

- 報告架構

  此角色允許直接從 Unified Manager 資料庫唯讀存取報告和其他資料庫檢視。可檢視的資料庫包括：

  - netapp_model_view
  - netapp_performance
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - scalemonitor

了解 **Active IQ Unified Manager** 中的使用者角色和功能

根據您被指派的使用者角色，您可以決定在 Unified Manager 中可以執行哪些操作。

下表顯示每個使用者角色可執行的功能：

功能	操作員	儲存管理員	應用程式管理員	整合結構描述	報表架構
查看儲存系統資訊	•	•	•	•	•
查看其他資料，例如歷史記錄和容量趨勢	•	•	•	•	•
檢視、指派與解決事件	•	•	•		
檢視儲存設備服務物件，例如 SVM 關聯和資源池	•	•	•		
檢視臨界值原則	•	•	•		
管理儲存設備服務物件，例如 SVM 關聯和資源池		•	•		
定義警報		•	•		
管理儲存管理選項		•	•		
管理儲存管理原則		•	•		

功能	操作員	儲存管理員	應用程式管理員	整合結構描述	報表架構
管理使用者			•		
管理系統管理選項			•		
定義臨界值策略			•		
管理資料庫存取			•		
管理與 WFA 的整合並提供對資料庫視圖的存取				•	
排程與儲存報告		•	•		
從管理動作執行 “Fix It” 作業		•	•		
提供資料庫檢視表的唯讀存取					•

管理 SAML 驗證設定

在 Active IQ Unified Manager 中啟用 SAML 驗證

設定遠端驗證設定後，您可以啟用安全性聲明標記語言 (SAML) 驗證，以便遠端使用者在存取 Unified Manager Web UI 之前，透過安全的身分供應商 (IdP) 進行驗證。

請注意，啟用 SAML 驗證後，只有遠端使用者才能存取 Unified Manager 圖形化使用者介面。本機使用者和維護使用者將無法存取 UI。此組態不會影響存取維護主控台的使用者。

在 Active IQ Unified Manager 中使用身分供應商

設定 Unified Manager 使用身分供應商（IdP）為所有遠端使用者執行 SAML 驗證時，您需要感知一些必要的組態設定，以便成功連線到 Unified Manager。

您必須將 Unified Manager URI 和中繼資料輸入到 IdP 伺服器中。您可以從 Unified Manager SAML 驗證頁面複本此資訊。Unified Manager 在安全性聲明標記語言 (SAML) 標準中被視為服務供應商 (SP)。

支援的加密標準

- 進階加密標準（AES）：AES-128 和 AES-256
- 安全雜湊演算法（SHA）：SHA-1 和 SHA-256

已驗證的身分供應商

- Shibboleth
- Active Directory Federation Services (ADFS)

ADFS 組態要求

- 您必須依照下列順序定義三個宣告規則，這些規則是 Unified Manager 解析此信賴憑證者信任項目的 ADFS 安全性聲明標記語言 (SAML) 回應時所需的。

宣告規則	價值
SAM-account-name	名稱 ID
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
權杖群組 — 非限定名稱	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- 您必須將身分驗證方法設定為 “Forms Authentication”，否則使用者在登出 Unified Manager 時可能會收到錯誤。請依照以下步驟操作：
  a. 開啟 ADFS 管理控制台。
  b. 點選左側樹狀檢視中的「驗證策略」資料夾。
  c. 在右側的「動作」下，按一下「編輯全域主要驗證原則」。
  d. 將 Intranet 身分驗證方法設定為 “表單驗證”，而不是預設的 “Windows 驗證”。
- 在某些情況下，當 Unified Manager 安全性憑證由 CA 簽署時，透過身分提供者 (IdP) 登入會被拒絕。有兩種方法可以解決此問題：
  - 請依照連結中的說明，停用 ADFS 伺服器上與鏈結 CA 憑證關聯之信賴方的撤銷檢查：

    "停用依賴方信任的撤銷檢查"

  - 讓 CA 伺服器位於 ADFS 伺服器內，以便對 Unified Manager 伺服器憑證要求進行簽署。

其他組態要求

- Unified Manager 的時鐘偏差設定為 5 分鐘，因此 IdP 伺服器和 Unified Manager 伺服器之間的時間差不能超過 5 分鐘，否則驗證會失敗。

在 **Active IQ Unified Manager** 中啟用 **SAML** 驗證

您可以啟用安全性聲明標記語言 (SAML) 驗證，以便遠端使用者在存取 Unified Manager Web UI 之前，先透過安全的身分供應商 (IdP) 進行驗證。

開始之前

- 您必須已設定遠端驗證並驗證其已成功。
- 您必須至少建立一個具有應用程式管理員角色的遠端使用者或遠端群組。
- 身分供應商（IdP）必須受 Unified Manager 支援，並且必須進行設定。
- 您必須擁有 IdP URL 和中繼資料。
- 您必須能夠存取 IdP 伺服器。

在 Unified Manager 中啟用 SAML 驗證後，使用者必須先使用 Unified Manager 伺服器主機資訊設定身分提供者（IdP），才能存取圖形化使用者介面。因此，您必須準備好在開始組態程序之前完成連線的兩個部分。IdP 可以在設定 Unified Manager 之前或之後進行設定。

啟用 SAML 驗證後，只有遠端使用者才能存取 Unified Manager 圖形化使用者介面。本機使用者和維護使用者將無法存取 UI。此組態不會影響存取維護主控台、Unified Manager 命令或 ZAPI 的使用者。

完成此頁面上的 SAML 組態後，Unified Manager 將自動重新啟動。

步驟

1. 在左側導覽窗格中，按一下 一般 > **SAML** 驗證。
2. 選取 啟用 **SAML** 驗證 核取方塊。

   顯示設定 IdP 連線所需的欄位。

3. 輸入將 Unified Manager 伺服器連接至 IdP 伺服器所需的 IdP URI 與 IdP 中繼資料。

   如果可以從 Unified Manager 伺服器直接存取 IdP 伺服器，您可以在輸入 IdP URI 後按一下 取得 **IdP** 中繼資料 按鈕，自動填入 IdP 中繼資料欄位。

4. 複製 Unified Manager 主機中繼資料 URI，或將主機中繼資料儲存到 XML 文字檔案。

   現在您可以使用此資訊設定 IdP 伺服器。

5. 按一下 **Save** 。

   系統會顯示訊息方塊，確認您要完成組態並重新啟動 Unified Manager。

6. 按一下 確認並登出 ， Unified Manager 將重新啟動。

下次獲得授權的遠端使用者嘗試存取 Unified Manager 圖形介面時，他們將在 IdP 登入頁面而不是 Unified Manager 登入頁面輸入他們的憑證。

如果尚未完成，請存取您的 IdP 並輸入 Unified Manager 伺服器 URI 和中繼資料以完成組態。

當使用 ADFS 作為身分供應商時，Unified Manager GUI 不會遵循 ADFS 逾時設定，而是會持續運作，直到達到 Unified Manager 工作階段逾時為止。您可以按一下 一般 > 功能設定 > 閒置逾時來變更 GUI 工作階段逾時。

在 **Active IQ Unified Manager** 中變更 **SAML** 驗證身分供應商

您可以變更 Unified Manager 用來驗證遠端使用者的身份供應商（IdP）。

開始之前

- 您必須擁有 IdP URL 和中繼資料。
- 您必須能夠存取 IdP。

新的 IdP 可以在設定 Unified Manager 之前或之後進行設定。

步驟

1. 在左側導覽窗格中，按一下 一般 > **SAML** 驗證。
2. 輸入新的 IdP URI 和將 Unified Manager 伺服器連接到 IdP 所需的 IdP 中繼資料。

如果可以從 Unified Manager 伺服器直接存取 IdP，您可以在輸入 IdP URL 後按一下 取得 **IdP** 中繼資料 按鈕，自動填入 IdP 中繼資料欄位。

3. 複製 Unified Manager 中繼資料 URI，或將中繼資料儲存到 XML 文字檔案。
4. 按一下 儲存組態。

   螢幕上會顯示訊息方塊，確認您要變更組態。

5. 按一下 **OK** 。

存取新的 IdP 並輸入 Unified Manager 伺服器 URI 和中繼資料以完成組態。

下次獲得授權的遠端使用者嘗試存取 Unified Manager 圖形介面時，他們將在新的 IdP 登入頁面而不是舊的 IdP 登入頁面中輸入其憑證。

在 **Active IQ Unified Manager** 安全性憑證變更後更新 **SAML** 驗證設定

對 Unified Manager 伺服器上安裝的 HTTPS 安全性憑證的任何變更都需要更新 SAML 驗證組態設定。如果您重新命名主機系統、為主機系統指派新的 IP 位址或手動變更系統的安全性憑證，則憑證會更新。

更改安全性憑證並重新啟動 Unified Manager 伺服器後，SAML 驗證將無法運作，使用者將無法存取 Unified Manager 圖形介面。您必須在 IdP 伺服器和 Unified Manager 伺服器上更新 SAML 驗證設定，才能重新啟用使用者介面存取。

步驟

1. 登入維護主控台。
2. 在*主選單*中，輸入*停用 SAML 驗證*選項的編號。

   螢幕上會顯示一則訊息，確認您是否要停用 SAML 驗證並重新啟動 Unified Manager。

3. 使用更新的 FQDN 或 IP 位址啟動 Unified Manager 使用者介面，在瀏覽器中接受更新後的伺服器憑證，並使用維護使用者憑證登入。
4. 在 設定/驗證 頁面中，選擇 **SAML** 驗證 標籤並設定 IdP 連線。
5. 複製 Unified Manager 主機中繼資料 URI，或將主機中繼資料儲存到 XML 文字檔案。
6. 按一下 **Save** 。

   系統會顯示訊息方塊，確認您要完成組態並重新啟動 Unified Manager。

7. 按一下 確認並登出 ， Unified Manager 將重新啟動。
8. 存取您的 IdP 伺服器，並輸入 Unified Manager 伺服器 URI 和中繼資料，以完成設定。

身分供應商	設定步驟
ADFS	a. 在 ADFS 管理 GUI 中刪除現有的信賴方信任項目。 b. 使用更新後 Unified Manager 伺服器的 `saml_sp_metadata.xml`新增依賴方信任項目。 c. 定義 Unified Manager 解析此信賴方信任項目的 ADFS SAML 回應所需的三個宣告規則。 d. 重新啟動 ADFS Windows 服務。
Shibboleth	a. 將 Unified Manager 伺服器的新 FQDN 更新至 `attribute-filter.xml` 和 `relying-party.xml` 檔案中。 b. 重新啟動 Apache Tomcat Web 伺服器，並等待 8005 連接埠上線。

9. 登入 Unified Manager 並驗證 SAML 驗證是否透過您的身分提供者（IdP）如預期運作。

在 **Active IQ Unified Manager** 中停用 **SAML** 驗證

如果您想要在遠端使用者登入 Unified Manager Web UI 之前，停止透過安全的身分供應商（IdP）對其進行驗證，您可以停用 SAML 驗證。停用 SAML 驗證後，已設定的目錄服務供應商（例如 Active Directory 或 LDAP）將執行登入驗證。

停用 SAML 驗證後，除了已設定的遠端使用者外，本機使用者和維護使用者也將能夠存取圖形化使用者介面。

如果您無法存取圖形化使用者介面，也可以使用 Unified Manager 維護主控台停用 SAML 驗證。

停用 SAML 驗證後，Unified Manager 將自動重新啟動。

步驟

1. 在左側導覽窗格中，按一下 一般 > **SAML** 驗證。
2. 取消勾選 啟用 **SAML** 驗證 核取方塊。
3. 按一下 **Save** 。

   系統會顯示訊息方塊，確認您要完成組態並重新啟動 Unified Manager。

4. 按一下 確認並登出 ， Unified Manager 將重新啟動。

下次遠端使用者嘗試存取 Unified Manager 圖形介面時，他們將在 Unified Manager 登入頁面而非 IdP 登入頁面輸入其憑證。

存取您的 IdP 並刪除 Unified Manager 伺服器 URI 和中繼資料。

從 **Active IQ Unified Manager** 維護主控台停用 **SAML** 驗證

當無法存取 Unified Manager 介面（GUI）時，您可能需要從維護控制台停用 SAML 驗

證。這種情況可能發生在組態錯誤或身分提供者（IdP）無法存取時。

開始之前

您必須以維護使用者的身分存取維護控制台。

停用 SAML 驗證後，已設定的目錄服務供應商（例如 Active Directory 或 LDAP）將執行登入驗證。除了已設定的遠端使用者外，本機使用者和維護使用者也將能夠存取圖形化使用者介面。

您也可以在使用者介面中的「設定/驗證」頁面停用 SAML 驗證。

停用 SAML 驗證後，Unified Manager 將自動重新啟動。

步驟

1. 登入維護主控台。
2. 在*主選單*中，輸入*停用 SAML 驗證*選項的編號。

   螢幕上會顯示一則訊息，確認您是否要停用 SAML 驗證並重新啟動 Unified Manager。

3. 輸入 **y**，然後按 Enter 鍵，Unified Manager 將重新啟動。

下次遠端使用者嘗試存取 Unified Manager 圖形介面時，他們將在 Unified Manager 登入頁面而非 IdP 登入頁面輸入其憑證。

如有需要，存取您的 IdP 並刪除 Unified Manager 伺服器 URL 和中繼資料。

在 **Active IQ Unified Manager** 中使用 **SAML** 驗證頁面

您可以使用 SAML 驗證頁面設定 Unified Manager，以便在遠端使用者登入 Unified Manager Web UI 之前，透過安全的身分供應商 (IdP) 使用 SAML 對其進行驗證。

- 您必須擁有應用程式管理員角色才能建立或修改 SAML 組態。
- 您必須設定遠端驗證。
- 您必須至少設定一個遠端使用者或遠端群組。

設定遠端驗證和遠端使用者後，您可以選取「啟用 SAML 驗證」核取方塊，以啟用透過安全的身分供應商進行驗證。

- **IdP URI**

  從 Unified Manager 伺服器存取 IdP 的 URI。範例 URI 如下所示。

  ADFS 範例 URI：

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Shibboleth 範例 URI：

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **IdP** 中繼資料

  XML 格式的 IdP 中繼資料。

  如果可以從 Unified Manager 伺服器存取 IdP URL，則可以按一下 取得 **IdP** 中繼資料 按鈕來填入此欄位。

- 主機系統（**FQDN**）

  安裝期間所定義的 Unified Manager 主機系統的完整網域名稱（FQDN）。如有必要，您可以變更此值。

- 主機 **URI**

  從身分識別提供者（IdP）存取 Unified Manager 主機系統的 URI。

- 主機中繼資料

  XML 格式的主機系統中繼資料。

管理驗證

在 **Active IQ Unified Manager** 中編輯驗證伺服器

您可以變更 Unified Manager 伺服器與驗證伺服器通訊時使用的連接埠。

開始之前
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. 勾選 停用巢狀群組查閱 核取方塊。
3. 在 驗證伺服器 區域中，選擇您要編輯的驗證伺服器，然後按一下 編輯。
4. 在 編輯驗證伺服器 對話方塊中，編輯連接埠詳細資訊。
5. 按一下 **Save** 。

在 **Active IQ Unified Manager** 中刪除驗證伺服器

如果您想要阻止 Unified Manager 伺服器與某個驗證伺服器通訊，可以刪除該驗證伺服器。例如，如果您想要變更管理伺服器正在通訊的驗證伺服器，可以刪除該驗證伺服器並新增新的驗證伺服器。

開始之前
您必須擁有應用程式管理員角色。

刪除驗證伺服器後，該驗證伺服器的遠端使用者或群組將無法再存取 Unified Manager。

步驟

1. 在左側導覽窗格中，按一下 一般 > 遠端驗證。

2. 選擇一個或多個要刪除的驗證伺服器，然後按一下 刪除。
3. 點擊 是 確認刪除請求。

   如果啟用 使用安全連線 選項，則與驗證伺服器關聯的憑證將隨驗證伺服器一起刪除。

在 **Active IQ Unified Manager** 中使用 **Active Directory** 或 **OpenLDAP** 進行驗證

您可以在管理伺服器上啟用遠端驗證，並將管理伺服器設定為與您的驗證伺服器通訊，以便驗證伺服器中的使用者可以存取 Unified Manager。

您可以使用以下預先定義的驗證服務之一，也可以指定您自己的驗證服務：

- Microsoft Active Directory

  您無法使用 Microsoft Lightweight Directory Services。

- OpenLDAP

您可以選取所需的驗證服務並新增適當的驗證伺服器，以讓驗證伺服器中的遠端使用者存取 Unified Manager。遠端使用者或群組的認證由驗證伺服器維護。管理伺服器使用輕量型目錄存取通訊協定 （LDAP） 在已設定的驗證伺服器中驗證遠端使用者。

對於在 Unified Manager 中建立的本機使用者，管理伺服器會維護自己的使用者名稱和密碼資料庫。管理伺服器會執行驗證，且不使用 Active Directory 或 OpenLDAP 進行驗證。

稽核記錄

了解 **Active IQ Unified Manager** 中的稽核日誌

您可以使用稽核日誌來偵測稽核日誌是否已遭到竄改。使用者執行的所有活動都會受到監控，並記錄在稽核日誌中。稽核涵蓋 Active IQ Unified Manager 的所有使用者介面及公開 API 的功能。

您可以使用 **Audit Log: File View** 檢視和存取 Active IQ Unified Manager 中所有可用的稽核日誌檔。Audit Log: File View 中的檔案會依其建立日期列出。此檢視會顯示從安裝或升級到目前系統中所擷取的所有稽核日誌資訊。每當您在 Unified Manager 中執行行動時，資訊就會更新並提供於日誌中。每個日誌檔的狀態會使用 “File Integrity Status” 屬性來擷取，該屬性會受到主動監控，以偵測日誌檔是否遭到竄改或刪除。當稽核日誌在系統中可用時，稽核日誌可能具有下列其中一種狀態：

狀態	說明
作用中	目前正在記錄日誌的檔案。
正常	系統中儲存的非作用中、已壓縮的檔案。
已竄改	已被使用者手動編輯而遭到破壞的檔案。
MANUAL_DELETE	被授權使用者刪除的檔案。
ROLLOVER_DELETE	因基於滾動組態原則進行滾動而遭刪除的檔案。
UNEXPECTED_DELETE	因不明原因被刪除的檔案。

稽核日誌頁面包含下列命令按鈕：

- 設定
- 刪除
- 下載

DELETE 按鈕可讓您刪除「稽核日誌」檢視中所列的任何稽核日誌。您可以刪除稽核日誌，並可選擇提供刪除檔案的原因，以便未來判斷刪除是否有效。REASON 欄會列出原因以及執行刪除作業的使用者名稱。

刪除日誌檔會將檔案從系統中刪除，但不會刪除資料庫表格中的項目。

您可以使用 Active IQ Unified Manager 中「稽核日誌」區段的 **DOWNLOAD** 按鈕下載稽核日誌，並匯出稽核日誌檔案。標記為 “NORMAL” 或 “TAMPERED” 的檔案將以壓縮 `.gzip`格式下載。

稽核日誌檔會定期歸檔並儲存到資料庫中以供參考。歸檔前，稽核日誌會進行數位簽章，以維護安全性和完整性。

產生完整的 AutoSupport 套裝組合時，支援套裝組合包含已歸檔和作用中的稽核日誌檔案。但產生精簡支援套裝組合時，僅包含作用中的稽核日誌。不包含已歸檔的稽核日誌。

設定 **Active IQ Unified Manager** 稽核日誌

您可以使用「稽核日誌」部分中的 設定 按鈕來設定稽核日誌檔案的輪替原則，並啟用稽核日誌的遠端記錄。

您可以根據您希望在系統中儲存的資料量和頻率，設定 **MAX FILE SIZE** 和 **AUDIT LOG RETENTION DAYS** 的值。**TOTAL AUDIT LOG SIZE** 欄位的值表示系統中存在的稽核日誌資料總量。滾動原則由 **AUDIT LOG RETENTION DAYS** 、 **MAX FILE SIZE** 和 **TOTAL AUDIT LOG SIZE** 欄位的值決定。當稽核日誌備份的大小達到 **TOTAL AUDIT LOG SIZE** 中設定的值時，系統會刪除最先歸檔的檔案。這意味著最舊的檔案將被刪除。但該檔案條目仍保留在資料庫中，並標記為 “Rollover Delete”。**AUDIT LOG RETENTION DAYS** 的值表示稽核日誌檔案的保留天數。任何早於此欄位中設定值的檔案將被滾動刪除。

步驟

1. 按一下 稽核日誌 > > 設定。
2. 在 最大檔案大小、稽核日誌總大小 和 稽核日誌保留天數 中輸入數值。

   若要啟用遠端記錄，請選擇 啟用遠端記錄。

在 **Active IQ Unified Manager** 中啟用稽核日誌的遠端記錄

您可以在「設定稽核日誌」對話方塊中選取 啟用遠端記錄 核取方塊來啟用遠端稽核記錄。您可以使用此功能將稽核日誌傳輸到遠端 Syslog 伺服器。這可讓您在有空間限制時管理稽核日誌。

遠端記錄稽核日誌可在 Active IQ Unified Manager 伺服器上的稽核日誌檔案被篡改時提供防篡改備份。

步驟

1. 在 設定稽核日誌 對話方塊中，選取 啟用遠端記錄 核取方塊。

顯示用於設定遠端記錄的其他欄位。

2. 輸入要連線的遠端伺服器的*主機名稱*和*連接埠*。
3. 在 伺服器 **CA** 憑證 欄位中，按一下 瀏覽 以選擇目標伺服器的公開憑證。

   憑證應以 `.pem`格式上傳。此憑證應從目標 `Syslog` 伺服器取得，且不應過期。憑證應包含所選的 "`hostname`" 作為 `SubjectAltName`（SAN）屬性的一部分。

4. 請輸入下列欄位的值：**CHARSET**、**CONNECTION TIMEOUT**、**RECONNECTION DELAY**。

   這些欄位的值應以毫秒為單位。

5. 請在 **FORMAT** 和 **PROTOCOL** 欄位中選擇所需的 Syslog 格式和 TLS 傳輸協定版本。
6. 如果目標 Syslog 伺服器需要以憑證為基礎的驗證，請選取 啟用用戶端身分驗證 核取方塊。

   您需要在儲存稽核記錄組態之前下載用戶端身分驗證憑證並將其上傳到 Syslog 伺服器，否則連線將失敗。根據 Syslog 伺服器的類型，您可能需要建立用戶端身分驗證憑證的雜湊值。

   範例：syslog-ng 需要使用命令 `openssl x509 -noout -hash -in cert.pem`建立憑證的<hash>，然後您應將用戶端身分驗證憑證以符號連結的方式連結至以<hash> .0 命名的檔案。

7. 點擊 儲存 以設定與伺服器的連線並啟用遠端記錄。

   您將被重新導向至稽核日誌頁面。

   連線逾時 值會影響組態。如果組態回應時間超過定義的值，則可能會因連線錯誤而導致組態故障。若要成功建立連線，請增加 連線逾時 值，然後重試組態。

使用 **Active IQ Unified Manager** 中的遠端身分驗證頁面

您可以使用遠端驗證頁面設定 Unified Manager 與您的驗證伺服器通訊，以驗證嘗試登入 Unified Manager Web UI 的遠端使用者。

您必須擁有應用程式系統管理員或儲存系統管理員角色。

選取「啟用遠端驗證」核取方塊後，即可使用驗證伺服器啟用遠端驗證。

- 驗證服務

  允許您設定管理伺服器，使其能夠透過目錄服務供應商（例如 Active Directory 、 OpenLDAP ）驗證使用者，或指定您自己的驗證機制。只有在啟用遠端驗證後，才能指定驗證服務。

  - **Active Directory**
    - 系統管理員姓名

      指定驗證伺服器的系統管理員名稱。

    - 密碼

      指定存取驗證伺服器的密碼。

- 基本辨識名稱

  指定遠端使用者在驗證伺服器中的位置。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**。

- 停用巢狀群組查詢

  指定是否啟用或停用巢狀群組查閱選項。預設情況下，此選項處於停用狀態。如果您使用 Active Directory，則可以透過停用對巢狀群組的支援來加快驗證速度。

- 使用安全的連線

  指定用於與驗證伺服器通訊的驗證服務。

◦ **OpenLDAP**

- 連結辨別名稱

  指定與基本可分辨名稱一起使用的連結可分辨名稱，以便在驗證伺服器中尋找遠端使用者。

- 連結密碼

  指定存取驗證伺服器的密碼。

- 基本辨識名稱

  指定遠端使用者在驗證伺服器中的位置。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**。

- 使用安全的連線

  指定使用安全 LDAP 與 LDAP 驗證伺服器通訊。

◦ 其他

- 連結辨別名稱

  指定與基本可分辨名稱一起使用的連結可分辨名稱，以便在您設定的驗證伺服器中尋找遠端使用者。

- 連結密碼

  指定存取驗證伺服器的密碼。

- 基本辨識名稱

  指定遠端使用者在驗證伺服器中的位置。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**。

- 傳輸協定版本

  指定驗證伺服器支援的輕量級目錄存取協定 (LDAP) 版本。您可以指定是否必須自動偵測傳輸協定版本，也可以將版本設定為 2 或 3。

- 使用者名稱屬性

  指定驗證伺服器中包含要由管理伺服器進行驗證的使用者登入名稱的屬性名稱。

- 群組成員屬性

  指定一個值，該值根據使用者驗證伺服器中指定的屬性和值，將管理伺服器群組成員身分指派給遠端使用者。

- UGID

  如果遠端使用者在驗證伺服器中被包含為 GroupOfUniqueNames 物件的成員，則此選項可讓您根據該 GroupOfUniqueNames 物件中的指定屬性，將管理伺服器群組成員身分指派給遠端使用者。

- 停用巢狀群組查詢

  指定是否啟用或停用巢狀群組查閱選項。預設情況下，此選項處於停用狀態。如果您使用 Active Directory，則可以透過停用對巢狀群組的支援來加快驗證速度。

- 成員

  指定驗證伺服器用於儲存有關群組內各個成員資訊的屬性名稱。

- 使用者物件類別

  指定遠端驗證伺服器中使用者的物件類別。

- 群組物件類別

  指定遠端驗證伺服器中所有群組的物件類別。

  您為 *Member*、*User Object Class* 和 *Group Object Class* 屬性輸入的值應與您的 Active Directory、OpenLDAP 和 LDAP 組態中新增的值相同。否則，驗證可能會失敗。

- 使用安全的連線

  指定用於與驗證伺服器通訊的驗證服務。

如果您要修改驗證服務，請務必刪除任何現有的驗證伺服器，並新增新的驗證伺服器。

驗證伺服器區域

「驗證伺服器」區域顯示管理伺服器用於尋找和驗證遠端使用者的驗證伺服器。遠端使用者或群組的憑證由驗證伺服器維護。

- 命令按鈕

  允許您新增、編輯或刪除驗證伺服器。

  - 新增

    允許您新增驗證伺服器。

如果您新增的驗證伺服器是高可用性配對（使用相同資料庫）的一部分，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個驗證伺服器無法連線時，與合作夥伴進行通訊。

◦ 編輯

允許您編輯所選驗證伺服器的設定。

◦ 刪除

刪除選定的驗證伺服器。

- 名稱或 **IP** 位址

顯示用於在管理伺服器上驗證使用者身分的驗證伺服器的主機名稱或 IP 位址。

- 連接埠

顯示驗證伺服器的連接埠號碼。

- 測試驗證

此按鈕透過驗證遠端使用者或群組來驗證您的驗證伺服器組態。

測試時，如果僅指定使用者名稱，管理伺服器會在驗證伺服器中搜尋遠端使用者，但不會驗證該使用者。如果同時指定使用者名稱和密碼，管理伺服器會搜尋並驗證遠端使用者。

如果停用遠端驗證，則無法測試驗證。

管理安全性證書

在 **Active IQ Unified Manager** 中檢視 **HTTPS** 安全性憑證

您可以將 HTTPS 憑證詳細資訊與瀏覽器中擷取的憑證進行比較，以確保瀏覽器與 Unified Manager 的加密連線沒有被攔截。

開始之前

您必須擁有操作員、應用程式管理員或儲存管理員角色。

檢視憑證可讓您驗證重新產生的憑證內容，或檢視可從中存取 Unified Manager 的主題備用名稱（SAN）。

步驟

1. 在左側導覽窗格中，按一下 一般 > **HTTPS** 憑證。

HTTPS 憑證顯示在頁面頂部

如果您需要檢視比 HTTPS 憑證頁面上所顯示更詳細的安全性憑證資訊，您可以在瀏覽器中檢視連線憑證。

在 **Active IQ Unified Manager** 中下載 **HTTPS** 憑證簽署要求

您可以下載目前 HTTPS 安全性憑證的認證簽署要求，以便將該檔案提供給憑證授權單位（CA）進行簽署。由 CA 簽署的憑證有助於防止中間人攻擊，並提供比自簽名憑證更好的

安全性保護。

開始之前

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 > **HTTPS** 憑證。
2. 按一下 下載 **HTTPS** 憑證簽章請求。
3. 儲存 `<hostname>.csr`檔案。

您可以將檔案提供給憑證授權單位進行簽署，然後安裝已簽署的憑證。

在 **Active IQ Unified Manager** 中安裝由 **CA** 簽署的 **HTTPS** 憑證

在憑證授權單位（CA）簽署並傳回憑證後，您可以上傳並安裝安全性憑證。您上傳並安裝的檔案必須是現有自簽憑證的簽署版本。CA 簽署的憑證有助於防止中間人攻擊，並提供比自簽憑證更好的安全性保護。

*什麼。開始之前

您必須完成以下操作：

- 已下載憑證簽署要求檔案，並由憑證授權單位簽署
- 已將憑證鏈儲存為 PEM 格式
- 包含憑證鏈中的所有憑證，從 Unified Manager 伺服器憑證到根目錄簽署憑證，包括任何存在的中繼憑證

您必須擁有應用程式管理員角色。

如果已建立 CSR 的憑證有效期超過 397 天，則 CA 在簽署並傳回憑證之前，會將憑證有效期縮短至 397 天

步驟

1. 在左側導覽窗格中，按一下 一般 > **HTTPS** 憑證。
2. 按一下 安裝 **HTTPS** 憑證。
3. 在顯示的對話方塊中，按一下 選擇檔案**.....** 以找到要上傳的檔案。
4. 選擇檔案，然後按一下 安裝 來安裝檔案。

   如需相關資訊，請參閱 "安裝使用外部工具產生的 HTTPS 憑證"。

憑證鏈範例

以下範例顯示憑證鏈檔案的可能格式：

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
```

```
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

了解 **Active IQ Unified Manager Unified Manager** 中如何使用外部工具產生 **HTTPS** 憑證

您可以安裝自我簽署或 CA 簽署的憑證，這些憑證是使用 OpenSSL、BoringSSL、LetsEncrypt 等外部工具所產生。

您應該將私鑰與憑證鏈一起載入，因為這些憑證是外部產生的公私鑰對。允許使用的金鑰對演算法為 “RSA” 和 “EC”。安裝 **HTTPS** 憑證 選項位於「一般」區段下的「HTTPS 憑證」頁面中。您上傳的檔案應採用下列輸入格式。

1. 屬於 Active IQ Unified Manager 主機的伺服器的私鑰
2. 與私鑰匹配的伺服器憑證
3. 用於簽署上述憑證的 CA 憑證（反向排列直至根目錄 CA）

用於載入包含 **EC** 金鑰對的憑證的格式

允許的曲線為「`prime256v1`」和「`secp384r1`」。包含外部產生 EC 對的憑證範例：

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
```

```
-----END CERTIFICATE-----
```

用於載入包含 **RSA** 金鑰對的憑證的格式

屬於主機憑證的 RSA 金鑰對允許的金鑰長度為 2048、3072 和 4096。具有外部產生之 **RSA** 金鑰對 的憑證：

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

憑證上傳後，您應該重新啟動 Active IQ Unified Manager 執行個體，以使變更生效。

上傳外部產生的憑證時的檢查

系統在上傳使用外部工具產生的憑證時會進行檢查。如果任何一項檢查失敗，則憑證將被拒絕。此外，系統也會對產品內部從 CSR 產生的憑證以及使用外部工具產生的憑證進行驗證。

- 輸入中的私鑰會根據輸入中的主機憑證進行驗證。
- 主機憑證中的通用名稱（CN）會與主機的 FQDN 進行比對。
- 主機憑證的通用名稱（CN）不應為空，也不應設定為 localhost。
- 憑證的有效期限起始日期不應在未來，有效期限終止日期也不應在過去。
- 如果存在中繼 CA 或 CA，憑證的有效起始日期不應在未來，且有效到期日期不應在過去。

輸入的私鑰不應加密。如果存在任何加密的私鑰，系統將拒絕該私鑰。

範例 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

範例 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

範例 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

如果憑證安裝失敗，請參閱知識庫（KB）文章：https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager 無法安裝外部產生的憑證"^]

憑證管理頁面描述

了解 **Active IQ Unified Manager** 中的 **HTTPS** 憑證頁面

HTTPS 憑證頁面可讓您檢視目前安全性憑證、下載憑證簽署要求、產生新的自簽名 HTTPS 憑證或安裝新的 HTTPS 憑證。

如果您尚未產生新的自簽署 HTTPS 憑證，則此頁面上顯示的憑證是安裝期間所產生的憑證。

命令按鈕

命令按鈕可用於執行以下操作：

- 下載 **HTTPS** 憑證簽署請求

  下載目前已安裝的 HTTPS 憑證的認證請求。瀏覽器會提示您儲存 <hostname>.csr 檔案，以便您可以將該檔案提供給憑證授權單位進行簽署。

- 安裝 **HTTPS** 憑證

  允許您在憑證授權單位簽署並返回安全性憑證後上傳並安裝該憑證。新憑證將在您重新啟動管理伺服器後生效。

- 重新產生 **HTTPS** 憑證

  允許您產生新的自簽名 HTTPS 憑證，以取代目前的安全性憑證。重新啟動 Unified Manager 後，新憑證將生效。

在 **Active IQ Unified Manager** 中重新產生 **HTTPS** 憑證對話方塊

「重新產生 HTTPS 憑證」對話方塊可讓您自訂安全性資訊，然後使用該資訊產生新的 HTTPS 憑證。

此頁面顯示目前的憑證資訊。

"\`使用目前憑證屬性重新產生\`" 和 "\`更新目前憑證屬性\`" 選項可讓您使用目前資訊重新產生憑證，或使用新資訊產生憑證。

- 通用名稱

  必填。您希望安全的完整網域名稱（FQDN）。

  在 Unified Manager 高可用度組態中，使用虛擬 IP 位址。

- 電子郵件

  選用。用於聯絡貴組織的電子郵件地址；通常是憑證系統管理員或 IT 部門的電子郵件地址。

- 公司

  選填。通常為貴公司的法定名稱。

- 部門

  選用。貴公司的部門名稱。

- 城市

  選用。貴公司所在的城市。

- 狀態

  選用。貴公司所在的州或省份位置，請勿縮寫。

- 國家

  選用。貴公司所在的國家。這通常是該國家的兩個字母 ISO 代碼。

- 別名

  必填。除了現有的 localhost 或其他網路位址之外，可用來存取此伺服器的其他非主要網域名稱。請以逗號分隔每個替代名稱。

  如果您想要從憑證的「備用名稱」欄位移除本機識別資訊，請選取 “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，則產生的憑證將完全不包含「備用名稱」欄位。

- 金鑰長度（金鑰演算法：**RSA**）

  金鑰演算法設定為 RSA。您可以從下列金鑰長度中選擇：2048 位元、3072 位元或 4096 位元。預設金鑰長度設定為 2048 位元。

- 有效期限

  預設有效期為 397 天。如果您是從舊版本升級而來，則可能會發現先前的憑證有效期未變更。

如需詳細資訊，請參閱 "產生 HTTPS 憑證"。

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。