執行配置和管理任務

Active IQ Unified Manager

NetApp
October 15, 2025

目錄

執行配置和管理任務

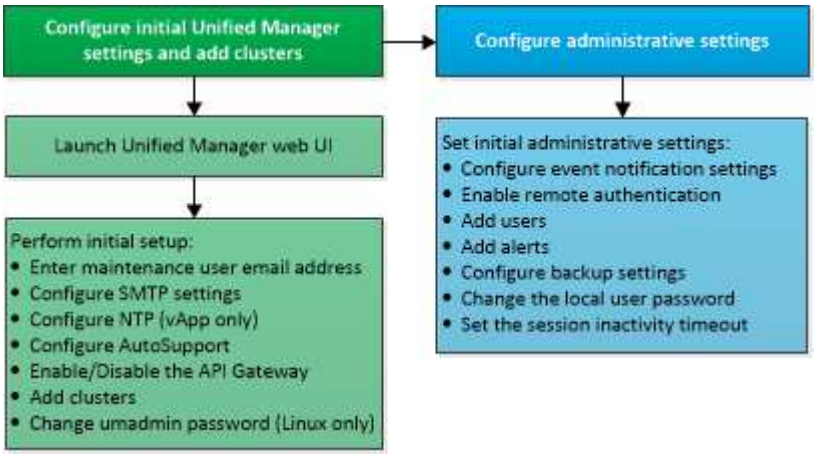
配置Active IQ Unified Manager

安裝Active IQ Unified Manager （以前稱為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 UI。然後，您可以執行其他配置任務，例如新增叢集、配置遠端身份驗證、新增使用者和新增警報。

本手冊中所述的一些步驟是完成 Unified Manager 實例的初始設定所必需的。其他程式是建議的配置設置，這些設置有助於在新實例上進行設置，或在您開始定期監控ONTAP系統之前了解這些設置。

配置序列概述

設定工作流程描述了您在使用 Unified Manager 之前必須執行的任務。



存取 **Unified Manager Web UI**

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

開始之前

- 如果這是您第一次造訪 Web UI，則必須以維護使用者（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全限定網域名稱 (FQDN) 或 IP 位址存取 Unified Manager，則您的網路設定必須將此短名稱解析為有效的 FQDN。
- 如果伺服器使用自簽名數位證書，瀏覽器可能會顯示警告，表示該證書不受信任。您可以承認風險並繼續訪問，或者安裝憑證授權單位 (CA) 簽署的數位憑證進行伺服器驗證。

步驟

1. 使用安裝結束時顯示的 URL 從瀏覽器啟動 Unified Manager Web UI。 URL 是 Unified Manager 伺服器的 IP 位址或完全限定網域名稱 (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，並且需要聯絡您的系統管理員。這僅適用於本地用戶。

執行 **Unified Manager Web UI** 的初始設置

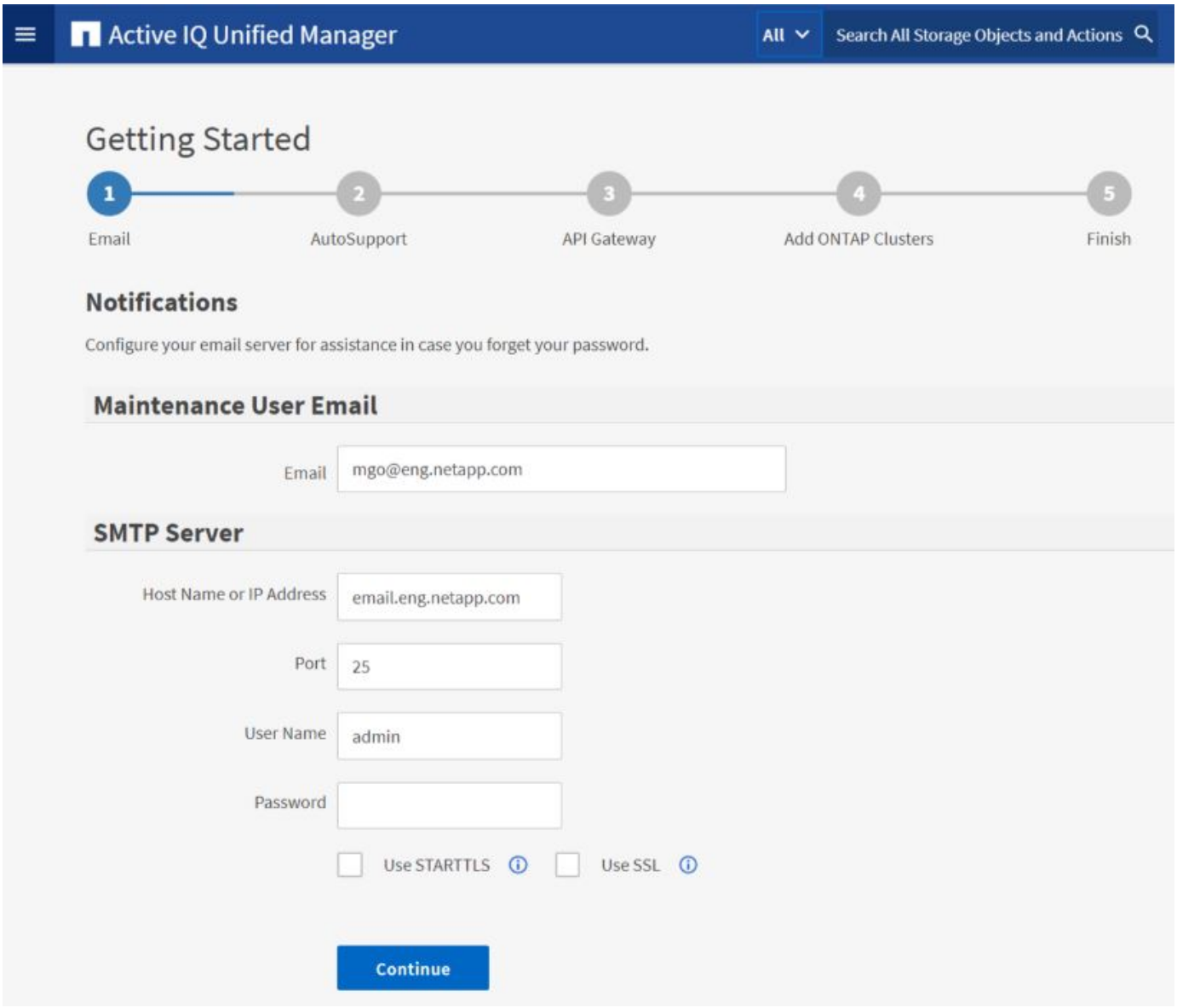
若要使用 Unified Manager，您必須先設定初始設定選項，包括 NTP 伺服器、維護使用者電子郵件地址、SMTP 伺服器主機以及新增ONTAP叢集。

開始之前

您必須已執行以下操作：

- 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 安裝的 umadmin 使用者）登入

只有在您第一次造訪 Web UI 時才會出現Active IQ Unified ManagerGetting Started 頁面。以下頁面來自 VMware 上的安裝。



如果您稍後想要變更這些選項中的任何一個，您可以從 Unified Manager 左側導覽窗格中的常規選項中選擇您的選擇。請注意，NTP 設定僅適用於 VMware 安裝，並且可以稍後使用 Unified Manager 維護控制台進行變更。

步驟

1. 在Active IQ Unified Manager初始設定頁面中，輸入維護使用者電子郵件地址、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）。然後點選“繼續”。

   如果您選擇了「使用 STARTTLS」或「使用 SSL」選項，則按一下「繼續」按鈕後將顯示憑證頁面。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頁面中，按一下 同意並繼續 以啟用從 Unified Manager 到 NetAppActive IQ 的AutoSupport訊息發送。

   如果您需要指定代理程式來提供網際網路存取以傳送AutoSupport內容，或您想要停用AutoSupport，請使用 Web UI 中的 **General** > * AutoSupport* 選項。

3. 在 Red Hat 系統上，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 管理您計畫使用ONTAP REST API 監控的ONTAP叢集。然後點選“繼續”。

   您可以稍後在 Web UI 中從 常規 > 功能設定 > **API** 網關 啟用或停用此設定。有關 API 的更多信息，請參閱"Active IQ Unified Manager REST API 入門"。

5. 新增您希望 Unified Manager 管理的集群，然後按一下「下一步」。對於您計劃管理的每個集群，您必須擁有主機名稱或集群管理 IP 位址（IPv4 或 IPv6）以及使用者名稱和密碼憑證 - 使用者必須具有「admin」角色。

   此步驟是可選的。您可以稍後在 Web UI 中從 儲存管理 > 叢集設定 新增叢集。

6. 在「摘要」頁面中，驗證所有設定是否正確，然後按一下「完成」。

“入門”頁面關閉並顯示“統一管理器儀表板”頁面。

新增集群

您可以將叢集新增至Active IQ Unified Manager，以便監控該叢集。這包括獲取叢集資訊的能力，例如叢集的健康狀況、容量、效能和配置，以便您可以發現並解決可能出現的任何問題。

開始之前

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須具有以下資訊：
  - Unified Manager 支援本機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 或短名稱。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虛擬機器 (SVM) 的叢集管理 LIF。如果您使用節點管理 LIF，操作將會失敗。

  - 叢集必須運行ONTAP 9.1 版軟體或更高版本。
  - ONTAP管理員使用者名稱和密碼

    此帳戶必須具有 *admin* 角色，並將應用程式存取權限設為 *ontapi*、*console* 和 *http*。

  - 使用 HTTPS 協定連接叢集的連接埠號碼（通常為連接埠 443）
  - 您擁有所需的證書：

    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章 SSL (HTTPS) 憑證。 NetApp建議您將其升級為 CA 簽章憑證以獲得更好的安全性。如果伺服器憑證過期，您應該重新產生它並重新啟動 Unified Manager，以便服務合併新憑證。有關重新產生 SSL 憑證的更多信息，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 通知進行身份驗證。

用於相互 **TLS** 通訊的憑證：在 Unified Manager 和ONTAP之間的相互 TLS 通訊期間使用。根據ONTAP版本，為叢集啟用基於憑證的身份驗證。如果執行ONTAP版本的叢集低於 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，則不會自動為叢集啟用基於憑證的驗證。但是，您可以透過修改和儲存叢集詳細資訊來啟用它。如果憑證過期，您應該重新產生它以包含新憑證。有關查看和重新生成證書的更多信息，請參閱"編輯集群"。

- 您可以從 Web UI 新增集群，並自動啟用基於憑證的身份驗證。
- 您可以透過 Unified Manager CLI 新增集群，預設不會啟用基於憑證的身份驗證。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。你可以看到"支援的 Unified Manager CLI 命令"使用 Unified Manager CLI 新增叢集。
- 如果為叢集啟用了基於憑證的驗證，並且您從伺服器備份 Unified Manager 並將其還原到主機名稱或 IP 位址已變更的另一個 Unified Manager 伺服器，則叢集的監控可能會失敗。為避免失敗，請編輯並儲存叢集詳細資訊。有關編輯集群詳細信息的更多信息，請參閱"編輯集群"。

+ 集群證書：此證書歸ONTAP擁有。您無法將憑證已過期的叢集新增至 Unified Manager，如果憑證已過期，則應在新增叢集之前重新產生憑證。有關證書產生的信息，請參閱知識庫 (KB) 文章 "如何在系統管理員使用者介面中續訂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，您將無法向伺服器新增叢集。

對於MetroCluster配置，您必須新增本地集群和遠端集群，並且必須正確配置集群。

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。下一個監控週期完成後，新的 IP 位址將反映在叢集網格和叢集設定頁面中。

4. 點選“提交”。
5. 在授權主機對話方塊中，按一下“檢視憑證”，查看叢集的憑證資訊。
6. 按一下“是”。

   儲存叢集詳細資料後，您可以看到叢集的 Mutual TLS 通訊憑證。

   如果未啟用基於憑證的驗證，Unified Manager 僅在最初新增叢集時檢查憑證。 Unified Manager 不會檢查對ONTAP的每個 API 呼叫的憑證。

發現新叢集的所有物件後，Unified Manager 開始收集前 15 天的歷史效能資料。這些統計數據是使用數據連續性收集功能收集的。此功能可在新增叢集後立即為您提供該叢集超過兩週的效能資訊。資料連續性收集週期完成後，預設每五分鐘收集一次即時叢集效能資料。

由於收集 15 天的效能資料需要大量 CPU，因此建議您錯開新叢集的添加，以便資料連續性收集輪詢不會同時在太多叢集上運行。此外，如果您在資料連續性收集期間重新啟動 Unified Manager，則收集將停止，並且您將在效能圖表中看到缺失時間範圍的差距。

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不同步，以及 Unified Manager HTTPS 憑證的開始日期是否晚於叢集上的日期。您必須確保使用 NTP 或類似服務同步時鐘。

相關資訊

"安裝 CA 簽署並傳回的 HTTPS 憑證"

配置 **Unified Manager** 以發送警報通知

您可以設定 Unified Manager 來傳送有關您環境中的事件的警報通知。在傳送通知之前，您必須設定其他幾個 Unified Manager 選項。

開始之前

您必須具有應用程式管理員角色。

部署 Unified Manager 並完成初始設定後，您應該考慮設定您的環境以根據收到的事件觸發警報並產生通知電子郵件或 SNMP 陷阱。

步驟

1. "配置事件通知設定"。

   如果您希望在您的環境中發生某些事件時發送警報通知，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，您可以選擇該選項並提供必要的資訊。

2. "啟用遠端身份驗證"。

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

3. "新增身份驗證伺服器"。

   您可以新增身份驗證伺服器，以便身份驗證伺服器內的遠端使用者可以存取 Unified Manager。

4. "新增用戶"。

   您可以新增幾種不同類型的本機或遠端使用者並指派特定的角色。建立警報時，您會指定一個使用者來接收警報通知。

5. "添加警報"。

   新增了用於發送通知的電子郵件地址、新增了用於接收通知的使用者、配置了網路設定以及配置了環境所需的 SMTP 和 SNMP 選項後，您就可以指派警報了。

配置事件通知設定

您可以設定 Unified Manager 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，並且可以設定各種通知機制 - 例如，警報通知可以作為電子郵件或 SNMP 陷阱傳送。

開始之前

您必須具有以下資訊：

- 發送警報通知的電子郵件地址

  電子郵件地址出現在已發送警報通知的「寄件者」欄位中。如果電子郵件因任何原因無法送達，則該電子郵件地址也將用作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
- 將接收 SNMP 陷阱的陷阱目標主機的主機名稱或 IP 位址，以及 SNMP 版本、出站陷阱連接埠、社群和其他所需的 SNMP 設定值

  若要指定多個陷阱目標，請用逗號分隔每個主機。在這種情況下，清單中所有主機的所有其他 SNMP 設定（例如版本和出站陷阱連接埠）必須相同。

您必須具有應用程式管理員或儲存管理員角色。

步驟

1. 在左側導覽窗格中，按一下「常規」>「通知」。
2. 在通知頁面中，配置適當的設定。

   筆記：

   - 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成功送達。
   - 如果無法解析 SMTP 伺服器的主機名，則可以指定 SMTP 伺服器的 IP 位址（IPv4 或 IPv6）來取代主機名稱。
3. 點選“儲存”。
4. 如果您選擇了「使用 STARTTLS」或「使用 SSL」選項，則按一下「儲存」按鈕後將顯示憑證頁面。驗證證書詳細資訊並接受證書以保存通知設定。

   您可以點擊*查看證書詳情*按鈕來查看證書詳情。如果現有憑證已過期，請取消選取 使用 **STARTTLS** 或 使用 **SSL** 框，儲存通知設置，然後再次選取 使用 **STARTTLS** 或 使用 **SSL** 框以查看新憑證。

啟用遠端身份驗證

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

開始之前

您必須具有應用程式管理員角色。

Unified Manager 伺服器必須直接與驗證伺服器連線。您必須停用任何本機 LDAP 用戶端，例如 SSSD（系統安全服務守護程式）或 NSLCD（名稱服務 LDAP 快取守護程式）。

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。

透過 LDAP 和 LDAPS（安全 LDAP）支援遠端身份驗證。 Unified Manager 使用 389 作為非安全通訊的預設端口，使用 636 作為安全通訊的預設端口。

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「常規」>「遠端驗證」。
2. 選取“啟用遠端身份驗證…”複選框。
3. 在身分驗證服務欄位中，選擇服務類型並配置身分驗證服務。

對於身份驗證類型...	輸入以下資訊...
活動目錄	• 認證伺服器管理員名稱採用以下格式之一： ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name`（使用適當的 LDAP 符號） • 管理者密碼 • 基本可分辨名稱（使用適當的 LDAP 符號）
開啟 LDAP	• 綁定可分辨名稱（以適當的 LDAP 符號表示） • 綁定密碼 • 基本可分辨名稱

如果 Active Directory 使用者的驗證花費很長時間或逾時，則驗證伺服器可能需要很長時間才能回應。停用 Unified Manager 中對嵌套群組的支援可能會減少身份驗證時間。

如果您為身分驗證伺服器選擇「使用安全連線」選項，則 Unified Manager 將使用安全通訊端層 (SSL) 協定與身分驗證伺服器進行通訊。

4. *可選：*新增身份驗證伺服器，並測試身份驗證。
5. 點選“儲存”。

禁用嵌套群組的遠端身份驗證

如果您啟用了遠端驗證，則可以停用巢狀群組驗證，以便只有個人使用者（而不是群組成

員）可以遠端向 Unified Manager 進行驗證。當您想要提高 Active Directory 驗證回應時間時，可以停用巢狀群組。

開始之前

- 您必須具有應用程式管理員角色。
- 停用嵌套群組僅適用於使用 Active Directory 時。

停用 Unified Manager 中對嵌套群組的支援可能會減少身份驗證時間。如果嵌套群組支援已停用，且如果將遠端群組新增至 Unified Manager，則個別使用者必須是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「常規」>「遠端驗證」。
2. 選取「停用巢狀組查找」複選框。
3. 點選“儲存”。

設定身份驗證服務

身份驗證服務可在身份驗證伺服器中對遠端使用者或遠端群組進行身份驗證，然後才允許他們存取 Unified Manager。您可以使用預先定義的驗證服務（例如 Active Directory 或 OpenLDAP）或透過設定您自己的驗證機制來對使用者進行身份驗證。

開始之前

- 您必須啟用遠端身份驗證。
- 您必須具有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下「常規」>「遠端驗證」。
2. 選擇以下身份驗證服務之一：

如果您選擇...	然後這樣做...
活動目錄	a. 輸入管理員名稱和密碼。 b. 指定身份驗證伺服器的基本可分辨名稱。 例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。
OpenLDAP	a. 輸入綁定可分辨名稱和綁定密碼。 b. 指定身份驗證伺服器的基本可分辨名稱。 例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。

如果您選擇...	然後這樣做...
其他的	a. 輸入綁定可分辨名稱和綁定密碼。 b. 指定身份驗證伺服器的基本可分辨名稱。 例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。 c. 指定認證伺服器支援的LDAP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。

如果要修改身份驗證服務，則必須刪除任何現有的身份驗證伺服器，然後新增的身份驗證伺服器。

3. 點選“儲存”。

新增身份驗證伺服器

您可以在管理伺服器上新增身份驗證伺服器並啟用遠端身份驗證，以便身份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：
  - 認證伺服器的主機名稱或IP位址
  - 認證伺服器的連接埠號
- 您必須啟用遠端身份驗證並設定身份驗證服務，以便管理伺服器可以對身份驗證伺服器中的遠端使用者或群組進行身份驗證。
- 您必須具有應用程式管理員角色。

如果您要新增的身份驗證伺服器是高可用性 (HA) 對的一部分（使用相同的資料庫），那麼您也可以新增合作夥伴驗證伺服器。當其中一個身份驗證伺服器無法存取時，這使得管理伺服器能夠與合作夥伴進行通訊。

步驟

1. 在左側導覽窗格中，按一下「常規」>「遠端驗證」。
2. 啟用或停用*使用安全連線*選項：

如果你想...	然後這樣做...
啟用它	a. 選擇*使用安全連線*選項。 b. 在身份驗證伺服器區域，按一下「新增」。 c. 在新增認證伺服器對話方塊中，輸入伺服器的認證名稱或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「檢視證書」對話方塊中，驗證證書訊息，然後按一下「關閉」。 f. 在授權主機對話方塊中，按一下「是」。 當您啟用*使用安全連線驗證*選項時，Unified Manager 會與身分驗證伺服器通訊並顯示憑證。Unified Manager 使用 636 作為安全通訊的預設端口，使用連接埠號碼 389 作為非安全通訊的預設連接埠。
禁用它	a. 清除*使用安全連線*選項。 b. 在身份驗證伺服器區域，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）以及連接埠詳細資訊。 d. 按一下“新增”。

您新增的身份驗證伺服器將顯示在伺服器區域。

3. 執行測試身份驗證以確認您可以在新增的身份驗證伺服器中對使用者進行身份驗證。

測試身份驗證伺服器的配置

您可以驗證身份驗證伺服器的配置，以確保管理伺服器能夠與它們通訊。您可以透過從身份驗證伺服器搜尋遠端使用者或遠端群組並使用配置的設定對其進行身份驗證來驗證配置。

開始之前

- 您必須啟用遠端身份驗證，並設定身份驗證服務，以便 Unified Manager 伺服器可以對遠端使用者或遠端群組進行身份驗證。
- 您必須新增身份驗證伺服器，以便管理伺服器可以從這些伺服器搜尋遠端使用者或遠端群組並對其進行身份驗證。
- 您必須具有應用程式管理員角色。

如果將身分驗證服務設定為 Active Directory，且您正在驗證屬於身分驗證伺服器主要群組的遠端使用者的驗證

，則身分驗證結果中不會顯示有關主要群組的資訊。

步驟

1. 在左側導覽窗格中，按一下「常規」>「遠端驗證」。
2. 按一下“測試身份驗證”。
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，然後按一下*測試*。

   如果您正在驗證遠端群組，則不得輸入密碼。

添加警報

您可以設定警報，以便在產生特定事件時通知您。您可以為單一資源、一組資源或特定嚴重性類型的事件設定警報。您可以指定接收通知的頻率並將腳本與警報關聯。

開始之前

- 您必須設定通知設置，例如使用者電子郵件地址、SMTP 伺服器和 SNMP 陷阱主機，以便Active IQ Unified Manager伺服器能夠在產生事件時使用這些設定向使用者傳送通知。
- 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腳本，則必須使用腳本頁面將腳本新增至 Unified Manager。
- 您必須具有應用程式管理員或儲存管理員角色。

除了從警報設定頁面建立警報之外，您還可以在收到事件後直接從事件詳細資訊頁面建立警報，如此處所述。

步驟

1. 在左側導覽窗格中，按一下「儲存管理」>「警報設定」。
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描述。
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*欄位中指定文字字串來設定過濾器，以選擇一組資源。根據您指定的文字字串，可用資源清單僅顯示符合過濾規則的資源。您指定的文字字串區分大小寫。

   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，並且不會針對與排除的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型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. 點選*操作*，選擇要通知的用戶，選擇通知頻率，選擇是否將 SNMP 陷阱傳送至陷阱接收器，並指派在產生警報時執行的腳本。

如果您修改為使用者指定的電子郵件地址並重新開啟警報進行編輯，則「名稱」欄位將顯示為空白，因為修改後的電子郵件地址不再對應到先前選取的使用者。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，則所選使用者的修改後的電子郵件地址不會更新。

您也可以選擇透過 SNMP 陷阱通知使用者。

7. 點選“儲存”。

新增警報的範例

此範例顯示如何建立滿足以下要求的警報：

- 警示名稱：HealthTest
- 資源：包括名稱包含「`abc`」的所有捲，並排除名稱包含「`xyz`」的所有捲
- 事件：包括所有重大健康事件
- 操作：包括“sample@domain.com”和“`Test`”腳本，並且每 15 分鐘通知一次用戶

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“包含”標籤中，從下拉清單中選擇“磁碟區”。
   a. 在“名稱包含”欄位中輸入“**abc**”，顯示名稱中包含“`abc`”的磁碟區。
   b. 選擇 **+[All Volumes whose name contains 'abc']** + 從可用資源區域，並將其移至選定資源區域。
   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”，然後從“事件嚴重性”欄位中選擇“嚴重”。
4. 從符合事件區域選擇“所有關鍵事件”，並將其移至選定事件區域。
5. 按一下“操作”，然後在“警報這些使用者”欄位中輸入“**sample@domain.com**”。
6. 選擇*每 15 分鐘提醒一次*，每 15 分鐘通知一次使用者。

   您可以設定警報以在指定時間內重複向收件人發送通知。您應該確定事件通知對於警報生效的時間。

7. 在選擇要執行的腳本選單中，選擇*測試*腳本。
8. 點選“儲存”。

更改本機用戶密碼

您可以修改本機使用者登入密碼，以避免潛在的安全風險。

開始之前

您必須以本機使用者登入。

無法使用這些步驟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，請聯絡您的密碼管理員。若

要變更維護使用者密碼，請參閱"使用維護控制台"。

步驟

1. 登入 Unified Manager。
2. 從頂部選單列中，點擊使用者圖標，然後點擊*更改密碼*。

   如果您是遠端用戶，則不會顯示「更改密碼」選項。

3. 在「更改密碼」對話方塊中，輸入目前密碼和新密碼。
4. 點選“儲存”。

如果 Unified Manager 是在高可用性設定中進行設定的，則必須變更設定的第二個節點上的密碼。兩個實例必須具有相同的密碼。

設定會話不活動逾時

您可以指定 Unified Manager 的不活動逾時值，以便在一定時間不活動後會自動終止。預設情況下，超時設定為 4,320 分鐘（72 小時）。

開始之前

您必須具有應用程式管理員角色。

此設定會影響所有已登入的使用者會話。

如果您啟用了安全性斷言標記語言 (SAML) 驗證，則此選項不可用。

步驟

1. 在左側導覽窗格中，按一下「常規」>「功能設定」。
2. 在「功能設定」頁面中，透過選擇以下選項之一來指定不活動逾時：

如果你想...	然後這樣做...
沒有設定超時，這樣會話就不會自動關閉	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超時值	在「不活動逾時」面板中，將滑桿按鈕向右移動（開啟），以分鐘為單位指定不活動逾時值，然後按一下「套用」。

透過 CLI 設定會話逾時

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

關於此任務

您必須具有應用程式管理員角色。

會話逾時設定會影響所有已登入的使用者會話。

步驟

1. 透過輸入 `um cli login`命令。使用有效的使用者名稱和密碼進行身份驗證。
2. 輸入 `um option set max.session.timeout.value=<in mins>`命令修改會話逾時值。

更改 **Unified Manager** 主機名

在某些時候，您可能會想要變更已安裝 Unified Manager 的系統的主機名稱。例如，您可能想要重新命名主機，以便更輕鬆地按類型、工作群組或受監控的叢集群組識別 Unified Manager 伺服器。

更改主機名稱所需的步驟有所不同，取決於 Unified Manager 是在 VMware ESXi 伺服器、Red Hat Linux 伺服器還是 Microsoft Windows 伺服器上執行。

更改 **Unified Manager** 虛擬設備主機名

首次部署 Unified Manager 虛擬設備時，會為網路主機指派名稱。您可以在部署後變更主機名稱。如果變更主機名，也必須重新產生 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配置了靜態 IP 位址，那麼您將為網路主機指定名稱。如果您使用 DHCP 配置網絡，則主機名稱應從 DNS 中取得。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。

無論主機名稱為何分配，如果您變更主機名，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，則變更主機名稱時無需產生新憑證。但是，最佳做法是更新證書，以便證書中的主機名稱與實際主機名稱相符。

如果您在 Unified Manager 中變更主機名，則必須在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。

直到 Unified Manager 虛擬機器重新啟動後，新憑證才會生效。

步驟

1. 產生 HTTPS 安全性憑證

   如果您想要使用新的主機名稱存取 Unified Manager Web UI，則必須重新產生 HTTPS 憑證以將其與新的主機名稱關聯。

2. 重新啟動 Unified Manager 虛擬機

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

首次安裝Active IQ Unified Manager時，會安裝預設 HTTPS 憑證。您可以產生一個新的 HTTPS 安全性憑證來取代現有的憑證。

開始之前

您必須具有應用程式管理員角色。

重新產生憑證的原因可能有多種，例如，如果您想要更好的可分辨名稱 (DN) 值，或者您想要更大的金鑰大小，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，則可以使用維護控制台重新產生具有相同值的 HTTPS 憑證。在重新產生憑證時，您可以定義金鑰大小和金鑰的有效期限。如果您使用 `Reset Server Certificate`選項，則會建立一個有效期為 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「常規」>「**HTTPS** 憑證」。
2. 按一下「重新產生 HTTPS 憑證」。

   系統彈出「重新產生HTTPS證書」對話框。

3. 根據您想要產生憑證的方式選擇以下選項之一：

如果你想...	這樣做...
使用當前值重新產生證書	按一下「使用目前憑證屬性重新產生」選項。

如果你想...	這樣做...
使用不同的值產生證書	按一下“更新目前憑證屬性”選項。 如果您不輸入新值，則通用名稱和備用名稱欄位將使用現有憑證中的值。 “通用名稱”應設定為主機的 FQDN。其他欄位不需要值，但您可以輸入值，例如，如果您希望在憑證中填入這些值，則為 EMAIL 、COMPANY、DEPARTMENT、City、State 和 Country 輸入這些值。您也可以從可用的金鑰大小（金鑰演算法為「RSA」）和有效期限中進行選擇。 • 密鑰大小的允許值為 2048，3072`和 `4096。 • 有效期限最短1天，最長36500天。 儘管允許有效期為 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，併計劃匯出此憑證的 CSR 並由知名 CA 進行簽名，則 CA 返回給您的簽名憑證的有效期將減少到 397 天。 • 如果您想要從憑證中的備用名稱欄位中刪除本機識別訊息，可以勾選「排除本機識別資訊（例如 localhost）」複選框。選取此核取方塊後，只有您在欄位中輸入的內容才會在備用名稱欄位中使用。當留空時，產生的憑證將根本沒有備用名稱欄位。

4. 按一下「是」重新產生憑證。
5. 重新啟動 Unified Manager 伺服器，以使新憑證生效。
6. 透過查看HTTPS證書來驗證新的證書資訊。

重新啟動 **Unified Manager** 虛擬機

您可以從 Unified Manager 的維護控制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

虛擬設備已啟動。

您以維護使用者登入維護控制台。

您也可以使用「重新啟動客戶機」選項從 vSphere 重新啟動虛擬機器。有關詳細信息，請參閱 VMware 文件。

步驟

1. 存取維護控制台。
2. 選擇*系統設定*>*重新啟動虛擬機器*。

在 **Linux** 系統上變更 **Unified Manager** 主機名

在某些時候，您可能會想要變更已安裝 Unified Manager 的 Red Hat Enterprise Linux 機器的主機名稱。例如，您可能想要重新命名主機，以便在列出 Linux 機器時更輕鬆地按類型、工作群組或受監控的叢集群組識別 Unified Manager 伺服器。

開始之前

您必須具有安裝 Unified Manager 的 Linux 系統的 root 使用者存取權限。

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配置了靜態 IP 位址，那麼您將為網路主機指定名稱。如果您使用 DHCP 設定網絡，則主機名稱應從 DNS 伺服器中取得。

無論主機名稱為何分配，如果您變更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，則變更主機名稱時無需產生新憑證。但是，最佳做法是更新證書，以便證書中的主機名稱與實際主機名稱相符。直到 Linux 機器重新啟動後，新憑證才會生效。

如果您在 Unified Manager 中變更主機名，則必須在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. 輸入以下指令停止 Unified Manager 軟體和相關的 MySQL 軟體：

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. 使用 Linux 更改主機名 `hostnamectl`命令：

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. 為伺服器重新產生HTTPS憑證：

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

5. 重啟網路服務：

   ```
   systemctl restart NetworkManager.service
   ```

6. 服務重啟後，驗證新的主機名稱是否能ping通自己：

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

此命令應傳回先前為原始主機名稱設定的相同 IP 位址。

7. 完成並驗證主機名稱變更後，輸入以下命令重新啟動 Unified Manager：

```
systemctl start mysqld ocie ocieau
```

啟用和停用基於策略的儲存管理

從 Unified Manager 9.7 開始，您可以在ONTAP叢集上設定儲存工作負載（磁碟區和 LUN），並根據指派的效能服務等級管理這些工作負載。此功能類似於在ONTAP系統管理員中建立工作負載並附加 QoS 策略，但使用 Unified Manager 應用程式時，您可以設定和管理 Unified Manager 實例正在監控的所有叢集中的工作負載。

您必須具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 設定和管理工作負載，則可以停用它。

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
配置新工作負載的頁面	可從「常見任務」>「配置」取得
建立效能服務等級策略的頁面	可從 設定 > 策略 > 效能服務等級 取得
建立效能儲存效率策略的頁面	可從“設定”>“策略”>“儲存效率”存取
描述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信息，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「常規」>「功能設定」。
2. 在「功能設定」頁面中，透過選擇以下選項之一來停用或啟用基於政策的儲存管理：

如果你想...	然後這樣做...
禁用基於策略的儲存管理	在*基於策略的儲存管理*面板中，將滑桿按鈕向左移動。
啟用基於策略的儲存管理	在*基於策略的儲存管理*面板中，將滑桿按鈕向右移動。

設定 Unified Manager 備份

您可以透過在主機系統和維護控制台上執行的一組設定步驟來設定 Unified Manager 上的備份功能。

有關配置步驟的信息，請參閱"管理備份和復原作業"。

管理功能設定

透過「功能設定」頁面，您可以啟用和停用Active IQ Unified Manager中的特定功能。這包括根據策略建立和管理儲存物件、啟用 API 閘道和登入橫幅、上傳用於管理警報的腳本、根據不活動時間逾時 Web UI 會話以及停用接收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使用「功能設定」頁面。

有關腳本上傳的信息，請參閱"啟用和停用腳本上傳"。

啟用基於策略的儲存管理

*基於策略的儲存管理*選項允許基於服務等級目標 (SLO) 進行儲存管理。預設情況下啟用此選項。

啟動此功能後，您可以在新增至Active IQ Unified Manager實例的ONTAP叢集上設定儲存工作負載，並根據指派的效能服務等級和儲存效率原則管理這些工作負載。

您可以從*常規* > 功能設定 > *基於政策的儲存管理*選擇啟用或停用此功能。啟動此功能後，以下頁面可供操作和監控：

- 配置（儲存工作負載配置）
- 政策 > 效能服務水準
- 政策 > 儲存效率
- 在叢集設定頁面上按效能服務等級管理的工作負載列
- *儀表板*上的工作負載效能面板

您可以使用這些畫面來建立效能服務等級和儲存效率策略，並配置儲存工作負載。您也可以監控符合指定效能服務等級的儲存工作負載以及不符合規定的儲存工作負載。工作負載效能和工作負載 IOPS 面板還可讓您根據資料中心內叢集所配置的儲存工作負載來評估叢集的總容量、可用容量和已使用容量及效能 (IOPS)。

啟動此功能後，您可以執行 Unified Manager REST API 來從 功能表列 > 說明按鈕 > **API** 文件 > 儲存提供者 類別執行其中一些功能。或者，您可以輸入主機名稱或 IP 位址以及存取 REST API 頁面的 URL，格式為 https://<hostname>/docs/api/

有關 API 的更多信息，請參閱"Active IQ Unified Manager REST API 入門"。

啟用 **API** 網關

API 閘道功能可讓Active IQ Unified Manager作為單一控制平面，您可以從中管理多個ONTAP叢集，而無需單獨登入它們。

您可以從首次登入 Unified Manager 時出現的設定頁面啟用此功能。或者，您可以從*常規* > 功能設定 > *API 網關*啟用或停用此功能。

Unified Manager REST API 與ONTAP REST API 不同，並且並非所有ONTAP REST API 的功能都可以透過使用 Unified Manager REST API 來實現。但是，如果您有特定的業務需求，需要存取ONTAP API 來管理未向 Unified Manager 公開的特定功能，則可以啟用 API 閘道功能並執行ONTAP API。網關充當代理，透過維護與ONTAP API 相同的格式的標頭和正文請求來傳輸 API 請求。您可以使用 Unified Manager 憑證並執行特定的 API 來存取和管理ONTAP叢集，而無需傳遞單獨的叢集憑證。 Unified Manager 作為單一管理點，在由 Unified Manager 實例管理的ONTAP叢集中執行 API。 API 傳回的回應與直接從ONTAP執行的對應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 > 網關 類別執行 Unified Manager REST API。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，格式如下 `https://<hostname>/docs/api/`

有關 API 的更多信息，請參閱"Active IQ Unified Manager REST API 入門"。

指定不活動逾時

您可以指定Active IQ Unified Manager的不活動逾時值。在指定時間不活動後，應用程式將自動登出。預設情況下啟用此選項。

您可以從*常規* > 功能設定 > 不活動逾時*停用此功能或修改時間。一旦啟動此功能，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），之後系統將自動登出。預設值為 4320 分鐘（72 小時）。

如果您啟用了安全性斷言標記語言 (SAML) 驗證，則此選項不可用。

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。此設定允許Active IQ入口網站發現並顯示有關係統配置、佈線等的其他事件。預設情況下啟用此選項。

啟用此功能後， Active IQ Unified Manager將顯示Active IQ網站發現的事件。這些事件是透過針對所有受監控的儲存系統產生的AutoSupport訊息執行一組規則而建立的。這些事件與其他 Unified Manager 事件不同，它們識別與系統配置、佈線、最佳實踐和可用性問題相關的事件或風險。

您可以從 常規 > 功能設定 > 活動**Active IQ**入口網站事件*選擇啟用或停用此功能。在沒有外部網路存取的網站中，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。停用此功能將阻止在 Unified Manager 上發現或顯示Active IQ事件。停用此功能後，啟用此功能可允許 Unified Manager 在該叢集時區的預先定義時間 00:15 接收叢集上的Active IQ事件。

啟用和停用安全設定以實現合規性

透過使用「功能設定」頁面的「安全儀表板」面板上的「自訂」按鈕，您可以啟用或停用 Unified Manager 上的合規性監控的安全性參數。

從此頁面啟用或停用的設定控制 Unified Manager 上叢集和儲存虛擬機器的整體合規性狀態。根據選擇，對應的列將顯示在叢集清單頁面的*安全性：所有叢集*視圖和儲存虛擬機器清單頁面的*安全性：所有儲存虛擬機器*視圖中。

只有具有管理員角色的使用者才能編輯這些設定。

您的ONTAP叢集、儲存虛擬機器和磁碟區的安全標準將根據"NetApp ONTAP 9 安全強化指南"。儀表板上的安全面板和安全性頁面顯示叢集、儲存虛擬機器和磁碟區的預設安全合規狀態。也會產生安全事件並針對存在安全違規的叢集和儲存虛擬機器啟用管理操作。

自訂安全設定

若要根據您的ONTAP環境自訂合規性監控設置，請依照下列步驟操作：

步驟

1. 點選*常規>功能設定>安全儀表板>自訂*。出現「自訂安全儀表板設定」彈出視窗。

   您啟用或停用的安全性合規性參數會直接影響叢集和儲存虛擬機器畫面上的預設安全性視圖、報表和排程報告。如果您在修改安全參數之前從這些畫面上傳了 Excel 報告，則下載的 Excel 報告可能有錯誤。

2. 若要啟用或停用ONTAP叢集的自訂設置，請在 叢集 下選擇所需的常規設定。有關自訂叢集合規性的選項的信息，請參閱"集群合規性類別"。
3. 若要啟用或停用儲存虛擬機器的自訂設置，請在「儲存虛擬機器」下選擇所需的常規設定。有關自訂儲存虛擬機器合規性的選項的信息，請參閱"儲存虛擬機器合規性類別"。

自訂**AutoSupport**和身份驗證設置

在 * AutoSupport設定* 部分，您可以指定是否使用 HTTPS 傳送從ONTAP傳送AutoSupport訊息。

從「驗證設定」部分，您可以啟用 Unified Manager 警報來向預設ONTAP管理員使用者發出警報。

啟用和停用腳本上傳

預設情況下，將腳本上傳到 Unified Manager 並執行它們的功能是啟用的。如果您的組織出於安全原因不想允許此活動，您可以停用此功能。

開始之前

您必須具有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下「常規」>「功能設定」。

2. 在「功能設定」頁面中，透過選擇以下選項之一來停用或啟用腳本：

如果你想...	然後這樣做...
停用腳本	在*腳本上傳*面板中，將滑桿按鈕向左移動。
啟用腳本	在*腳本上傳*面板中，將滑桿按鈕向右移動。

新增登入橫幅

新增登入橫幅使您的組織能夠顯示任何訊息，例如，誰被允許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（例如儲存操作員或管理員）都可以在登入、登出和會話逾時期間查看此登入橫幅彈出視窗。

使用維護控制台

您可以使用維護控制台設定網路設定、設定和管理安裝了 Unified Manager 的系統，以及執行其他維護任務以協助您預防和排除可能出現的問題。

維護控制台提供哪些功能

Unified Manager 維護控制台可讓您維護 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。

根據安裝 Unified Manager 的作業系統，維護控制台提供以下功能：

- 排除虛擬設備的任何問題，尤其是在 Unified Manager Web 介面不可用的情況下
- 升級到較新版本的 Unified Manager
- 產生支援包以發送給技術支持
- 設定網路設定
- 修改維護用戶密碼
- 連接到外部數據提供者以發送效能統計數據
- 更改性能數據收集內部
- 從先前備份的版本還原 Unified Manager 資料庫和設定。

維護用戶做什麼

維護使用者是在 Red Hat Enterprise Linux 系統上安裝 Unified Manager 期間建立的。維護用戶名是“umadmin”用戶。維護使用者在 Web UI 中具有應用程式管理員角色，並且該使用者可以建立後續使用者並為他們指派角色。

維護使用者或 umadmin 使用者也可以存取 Unified Manager 維護控制台。

診斷使用者功能

診斷存取的目的是使技術支援能夠幫助您進行故障排除，並且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級命令，以進行故障排除。

存取維護控制台

如果 Unified Manager 使用者介面未執行，或者您需要執行使用者介面中不可用的功能，則可以存取維護控制台來管理 Unified Manager 系統。

開始之前

您必須已安裝並設定 Unified Manager。

15 分鐘不活動後，維護控制台將註銷您。

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錄，則無法同時使用安全外殼登入。

步

1. 請依照下列步驟存取維護控制台：

在此作業系統上...	請依照以下步驟操作...
VMware	a. 使用安全性外殼連接到 Unified Manager 虛擬設備的 IP 位址或完全限定網域名稱。 b. 使用您的維護使用者名稱和密碼登入維護控制台。
Linux	a. 使用安全性外殼連接到 Unified Manager 系統的 IP 位址或完全限定網域名稱。 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`然後按 Enter 鍵。
視窗	a. 使用管理員憑證登入 Unified Manager 系統。 b. 以 Windows 管理員身分啟動 PowerShell。 c. 輸入命令 `maintenance_console`然後按 Enter 鍵。

顯示 Unified Manager 維護控制台選單。

使用 **vSphere VM** 控制台存取維護控制台

如果 Unified Manager 使用者介面未執行，或者您需要執行使用者介面中不可用的功能，則可以存取維護控制台來重新設定虛擬設備。

開始之前

- 您必須是維護使用者。
- 必須開啟虛擬設備才能存取維護控制台。

步驟

1. 在 vSphere Client 中，找到 Unified Manager 虛擬設備。
2. 按一下「控制台」標籤。
3. 按一下控制台視窗內部即可登入。
4. 使用您的使用者名稱和密碼登入維護控制台。

   15 分鐘不活動後，維護控制台將註銷您。

維護控制台選單

維護控制台由不同的選單組成，可讓您維護和管理 Unified Manager 伺服器的特殊功能和設定設定。

根據安裝 Unified Manager 的作業系統，維護控制台包含下列選單：

- 升級 Unified Manager（僅限 VMware）
- 網路配置（僅限 VMware）
- 系統配置（僅限 VMware）
  a. 支持/診斷
  b. 重置伺服器憑證
  c. 外部資料提供者
  d. 備份還原
  e. 效能輪詢間隔配置
  f. 禁用 SAML 身份驗證
  g. 查看/更改應用程式端口
  h. 偵錯日誌配置
  i. 控制對 MySQL 連接埠 3306 的訪問
  j. 出口

您從清單中選擇數字來存取特定的選單選項。例如，對於備份和恢復，您選擇_4_。

網路配置選單可讓您管理網路設定。當 Unified Manager 使用者介面不可用時，您應該使用此功能表。

如果 Unified Manager 安裝在 Red Hat Enterprise Linux 或 Microsoft Windows 上，則此功能表不可用。

有以下選單選項可供選擇。

- 顯示 **IP** 位址設定

  顯示虛擬設備的目前網路設置，包括 IP 位址、網路、廣播位址、網路遮罩、網關和 DNS 伺服器。

- 更改 **IP** 位址設定

  使您能夠更改虛擬設備的任何網路設置，包括 IP 位址、網路遮罩、網關或 DNS 伺服器。如果您使用維護控制台將網路設定從 DHCP 切換到靜態網絡，則無法編輯主機名稱。您必須選擇“提交更改”才能使更改生效。

- 顯示網域搜尋設定

  顯示用於解析主機名稱的網域搜尋清單。

- 更改網域搜尋設定

  使您能夠變更解析主機名稱時要搜尋的網域名稱。您必須選擇“提交更改”才能使更改生效。

- 顯示靜態路由

  顯示目前靜態網路路由。

- 更改靜態路由

  使您能夠新增或刪除靜態網路路由。您必須選擇“提交更改”才能使更改生效。

  - 新增路線

    使您能夠新增靜態路由。

  - 刪除路線

    使您能夠刪除靜態路由。

  - 後退

    帶您返回*主選單*。

  - 出口

    退出維護控制台。

- 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，則無法停用它。您必須選擇“提交更改”才能使更改生效。

- 啟用網路介面

  啟用可用的網路介面。您必須選擇“提交更改”才能使更改生效。

- 提交更改

  應用對虛擬設備的網路設定所做的任何變更。您必須選擇此選項才能實施所做的任何更改，否則不會發生更改。

- **Ping** 主機

  對目標主機執行 ping 操作以確認 IP 位址變更或 DNS 配置。

- 恢復預設值

  將所有設定重設為出廠預設值。您必須選擇“提交更改”才能使更改生效。

- 後退

  帶您返回*主選單*。

- 出口

  退出維護控制台。

系統配置選單

系統配置選單提供各種選項，例如查看伺服器狀態以及重新啟動和關閉虛擬機，使您能夠管理虛擬設備。

當 Unified Manager 安裝在 Linux 或 Microsoft Windows 系統上時，此功能表中只有「從 Unified Manager 備份還原」選項可用。

有以下選單選項可供選擇：

- 顯示伺服器狀態

  顯示目前伺服器狀態。狀態選項包括“正在運行”和“未運行”。

  如果伺服器沒有運行，您可能需要聯絡技術支援。

- 重啟虛擬機器

  重新啟動虛擬機，停止所有服務。重啟後，虛擬機器和服務重新啟動。

- 關閉虛擬機器

  關閉虛擬機，停止所有服務。

您只能從虛擬機器控制台選擇此選項。

- 更改<登入使用者>的使用者密碼

  更改目前登入使用者的密碼，該使用者只能是維護使用者。

- 增加資料磁碟大小

  增加虛擬機器中資料磁碟（磁碟 3）的大小。

- *增加交換磁碟大小

  增加虛擬機器中交換磁碟（磁碟 2）的大小。

- 更改時區

  將時區變更為您的位置。

- 更改 **NTP** 伺服器

  變更 NTP 伺服器設置，例如 IP 位址或完全限定網域名稱 (FQDN)。

- 更改 **NTP** 服務

  在 `ntp`和 `systemd-timesyncd`服務。

- 從統一管理器備份還原

  從先前備份的版本還原 Unified Manager 資料庫和設定。

- 重置伺服器憑證

  重置伺服器安全性憑證。

- 更改主機名稱

  變更安裝虛擬設備的主機的名稱。

- 後退

  退出系統配置選單並返回主選單。

- 出口

  退出維護控制台選單。

支援和診斷選單

透過「支援和診斷」選單，您可以產生支援包，然後將其發送給技術支援以獲得故障排除幫助。

有以下選單選項可用：

- 產生輕量級支援包

  使您能夠產生僅包含 30 天的日誌和設定資料庫記錄的輕量級支援包 - 它不包括效能資料、擷取記錄檔和伺服器堆轉儲。

- 產生支援包

  使您能夠在診斷使用者的主目錄中建立包含診斷資訊的完整支援包（7-Zip 檔案）。如果您的系統已連接到互聯網，您也可以將支援包上傳到NetApp。

  該檔案包括由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AutoSupport訊息或輕量級支援套件中通常不包含的詳細等級日誌。

附加選單選項

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。

有以下選單選項可供選擇：

- 重置伺服器憑證

  重新產生 HTTPS 伺服器憑證。

  您可以透過點選 常規 > **HTTPS** 憑證 > 重新產生 **HTTPS** 憑證 在 Unified Manager GUI 中重新產生伺服器憑證。

- 停用 **SAML** 驗證

  停用 SAML 驗證，以便身分提供者 (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 設定問題阻止使用者存取 Unified Manager GUI 時，通常會使用此控制台選項。

- 外部資料提供者

  提供將 Unified Manager 連接到外部資料提供者的選項。建立連接後，效能數據將發送到外部伺服器，以便儲存效能專家可以使用第三方軟體繪製效能指標圖表。將顯示以下選項：

  - 顯示伺服器配置－顯示外部資料提供者的目前連線和設定。
  - 新增/修改伺服器連線－使您能夠為外部資料提供者輸入新的連線設置，或變更現有設定。
  - 修改伺服器配置－使您能夠為外部資料提供者輸入新的配置設置，或變更現有設定。
  - 刪除伺服器連線－刪除與外部資料提供者的連線。

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

- 備份還原

  有關信息，請參閱以下主題"管理備份和復原作業"。

- 效能輪詢間隔配置

  提供一個選項來設定 Unified Manager 從叢集收集效能統計資料的頻率。預設收集間隔為5分鐘。

如果您發現大型叢集的收集沒有按時完成，則可以將此間隔變更為 10 或 15 分鐘。

- 查看/更改應用程式連接埠

  如果出於安全考慮，提供一個選項來更改 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。

- 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。基於安全性原因，在 Linux、Windows 和 VMware vSphere 系統上全新安裝 Unified Manager 期間，透過此連接埠的存取僅限於本機。此選項使您能夠在本地主機和遠端主機之間切換此端口的可見性，也就是說，如果僅在您的環境中為本地主機啟用了該端口，那麼您也可以使該端口對遠端主機可用。或者，當為所有主機啟用時，您可以將此連接埠的存取權限限制為僅限本機主機。如果之前在遠端主機上啟用了訪問，則在升級場景中將保留該配置。切換連接埠可見性後，您應該檢查 Windows 系統上的防火牆設置，如果設定配置為限制對 MySQL 連接埠 3306 的訪問，則應停用防火牆設置。

- 出口

  退出維護控制台選單。

在 **Windows** 上變更維護使用者密碼

您可以在需要時變更 Unified Manager 維護使用者密碼。

步驟

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

   將顯示一個頁面，提示您輸入要重設密碼的使用者的姓名。

2. 輸入使用者名稱並點擊*提交*。

   一封包含重設密碼連結的電子郵件將傳送至為該使用者名稱定義的電子郵件地址。

3. 點擊電子郵件中的*重設密碼連結*並定義新密碼。
4. 返回 Web UI 並使用新密碼登入 Unified Manager。

在 **Linux** 系統上變更 **umadmin** 密碼

出於安全原因，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。如果需要，您可以隨時再次變更密碼。

開始之前

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

步驟

1. 以 root 使用者身分登入執行 Unified Manager 的 Linux 系統。
2. 更改 umadmin 密碼：

```
passwd umadmin
```

系統提示您輸入 umadmin 使用者的新密碼。

更改 **Unified Manager** 用於 **HTTP** 和 **HTTPS** 協定的端口

如果出於安全性考慮，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

您必須擁有授權登入 Unified Manager 伺服器維護控制台的使用者 ID 和密碼。

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，請先檢查您的瀏覽器。選擇不安全的連接埠可能會導致系統無法存取，這需要您聯絡客戶支援尋求解決方案。

變更連接埠後，Unified Manager 實例會自動重新啟動，因此請確保這是一個短時間關閉系統的好時機。

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

   將顯示 Unified Manager 維護控制台提示。

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

   將連接埠號留空將為協定分配預設連接埠。

   系統會提示您是否要立即變更連接埠並重新啟動 Unified Manager。

5. 鍵入 **y** 以變更連接埠並重新啟動 Unified Manager。
6. 退出維護控制台。

完成此變更後，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+或 https://[2001:db8:0:1]:2123。

新增網路介面

如果需要分離網路流量，可以新增新的網路介面。

開始之前

您必須已使用 vSphere 將網路介面新增至虛擬設備。

虛擬設備必須已開啟電源。

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 控制台主選單中，選擇 系統配置 > 重新啟動作業系統。

   重新啟動後，維護控制台可以偵測到新新增的網路介面。

2. 存取維護控制台。
3. 選擇*網路設定* > 啟用網路介面。
4. 選擇新的網路介面並按 **Enter**。

   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，系統將提示您輸入網路設定。

   進入網路設定後，自動返回*網路設定*選單。

7. 選擇*提交更改*。

   您必須提交變更才能新增網路介面。

向 **Unified Manager** 資料庫目錄新增磁碟空間

Unified Manager 資料庫目錄包含從ONTAP系統收集的所有健康和效能資料。某些情況下可能需要您增加資料庫目錄的大小。

例如，如果 Unified Manager 從大量叢集（每個叢集都有許多節點）收集數據，則資料庫目錄可能會已滿。當資料庫目錄已滿 90% 時，您將收到警告事件；當資料庫目錄已滿 95% 時，您將收到嚴重事件。

當目錄達到 95% 滿度後，將不再從群集收集其他資料。

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

為**Linux**主機的資料目錄新增空間

如果您分配的磁碟空間不足 `/opt/netapp/data`目錄以支援 Unified Manager，當您最初設定 Linux 主機然後安裝 Unified Manager 時，您可以在安裝後透過增加 `/opt/netapp/data`目錄。

開始之前

您必須具有安裝了 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的大小之前備份 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. 以所示順序停止 Unified Manager 服務和相關的 MySQL 軟體：

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. 建立臨時備份資料夾（例如， `/backup-data` ）具有足夠的磁碟空間來包含當前 `/opt/netapp/data`目錄。
4. 複製現有 `/opt/netapp/data`目錄到備份資料目錄：

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

5. 如果啟用了 SE Linux：

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

      ```
      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 指令設定備份目錄的 SE Linux 類型：

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

6. 刪除 `/opt/netapp/data`目錄：

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. 擴大規模 `/opt/netapp/data`透過 LVM 指令或新增額外的磁碟將目錄大小增加到至少 150 GB。

   > 如果您已經創建 `/opt/netapp/data`從磁碟，那麼您不應該嘗試安裝 `/opt/netapp/data`作為 NFS 或 CIFS 共享。因為在這種情況下，如果您嘗試擴展磁碟空間，則一些 LVM 命令，例如 `resize`和 `extend`可能無法如預期工作。

8. 確認 `/opt/netapp/data`目錄擁有者（mysql）和群組（root）保持不變：

   ```
   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，以便這個無關的檔案將來不會導致資料庫錯誤。
11. 將備份資料中的內容複製回擴充的 `/opt/netapp/data`目錄：

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

12. 如果啟用了 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，依照所示順序啟動ocie和ocieau服務：

```
systemctl start ocie ocieau
```

15. 所有服務啟動後，刪除備份資料夾 `/backup-data`：

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

為**VMware**虛擬機器資料盤新增空間

如果需要增加 Unified Manager 資料庫的資料磁碟空間量，則可以在安裝後使用 Unified Manager 維護控制台增加磁碟空間來增加容量。

開始之前

- 您必須具有 vSphere Client 的存取權限。
- 虛擬機器一定不能有本地儲存的快照。
- 您必須擁有維護使用者憑證。

我們建議您在增加虛擬磁碟的大小之前備份虛擬機器。

步驟

1. 在 vSphere 用戶端中，選擇 Unified Manager 虛擬機，然後在資料中新增更多磁碟容量 `disk 3`。有關詳細信息，請參閱 VMware 文件。

   在極少數情況下，Unified Manager 部署使用「硬碟 2」而不是「硬碟 3」作為資料磁碟。如果您的部署中出現這種情況，請增加較大磁碟的空間。資料磁碟的空間總是比其他磁碟大。

2. 在 vSphere 用戶端中，選擇 Unified Manager 虛擬機，然後選擇「控制台」標籤。
3. 按一下控制台窗口，然後使用您的使用者名稱和密碼登入維護控制台。
4. 在主選單中，輸入*系統配置*選項的編號。
5. 在系統設定選單中，輸入「增加資料磁碟大小」選項的數字。

為 **Microsoft Windows** 伺服器的邏輯磁碟機新增空間

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

開始之前

您必須具有 Windows 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. 以管理員身分登入要新增磁碟空間的 Windows 伺服器。
2. 按照與您想要使用的方法相對應的步驟來增加更多空間：

選項	描述
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： "擴充基本捲"
在實體伺服器上，新增硬碟。	請依照 Microsoft 主題中的步驟操作： "新增硬碟驅動器"
在虛擬機器上，增加磁碟分割的大小。	請按照 VMware 主題中的步驟操作： "增加磁碟分割區的大小"

管理用戶訪問

您可以建立角色並指派功能來控制使用者對Active IQ Unified Manager 的存取。您可以識別具有存取 Unified Manager 中選取物件所需權限的使用者。只有擁有這些角色和功能的使用者才能管理 Unified Manager 中的物件。

新增用戶

您可以使用「使用者」頁面新增本機使用者或資料庫使用者。您也可以新增屬於身份驗證伺服器的遠端使用者或群組。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 管理儲存物件和數據，或查看資料庫中的資料。

開始之前

- 您必須具有應用程式管理員角色。
- 若要新增遠端使用者或群組，您必須啟用遠端身份驗證並設定身份驗證伺服器。
- 如果您打算設定 SAML 驗證，以便身分提供者 (IdP) 對存取圖形介面的使用者進行身份驗證，請確保這些使用者被定義為「遠端」使用者。

  啟用 SAML 身份驗證時，「本機」或「維護」類型的使用者無法存取 UI。

如果您從 Windows Active Directory 新增一個群組，則所有直接成員和巢狀子群組都可以向 Unified Manager 進行驗證，除非巢狀子群組已停用。如果您從 OpenLDAP 或其他驗證服務新增一個群組，則只有該群組的直接成員才能向 Unified Manager 進行驗證。

步驟

1. 在左側導覽窗格中，按一下「常規」>「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，然後輸入所需的資訊。

   輸入所需的使用者資訊時，您必須指定該使用者唯一的電子郵件地址。您必須避免指定由多個使用者共用的電子郵件地址。

4. 按一下“新增”。

建立資料庫用戶

若要支援工作流程自動化和 Unified Manager 之間的連接，或存取資料庫視圖，您必須先在 Unified Manager Web UI 中建立具有整合模式或報表模式角色的資料庫使用者。

開始之前

您必須具有應用程式管理員角色。

資料庫使用者提供與工作流程自動化的整合以及對特定於報告的資料庫視圖的存取。資料庫使用者無權存取 Unified Manager Web UI 或維護控制台，也無法執行 API 呼叫。

步驟

1. 在左側導覽窗格中，按一下「常規」>「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 Union Manager 與工作流程自動化連接起來	整合模式
存取報告和其他資料庫視圖	報告架構

6. 按一下“新增”。

編輯用戶設定

您可以編輯每個使用者指定的使用者設置，例如電子郵件地址和角色。例如，您可能想要變更儲存操作員使用者的角色，並為該使用者指派儲存管理員權限。

開始之前

您必須具有應用程式管理員角色。

修改指派給使用者的角色時，發生下列任一操作時都會套用變更：

- 使用者登出並重新登入 Unified Manager。
- 會話逾時已達 24 小時。

步驟

1. 在左側導覽窗格中，按一下「常規」>「使用者」。
2. 在「用戶」頁面中，選擇要編輯設定的用戶，然後按一下「編輯」。
3. 在「編輯使用者」對話方塊中，編輯為使用者指定的適當設定。
4. 點選“儲存”。

查看用戶

您可以使用「使用者」頁面查看使用 Unified Manager 管理儲存物件和資料的使用者清單。您可以查看有關使用者的詳細信息，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

您必須具有應用程式管理員角色。

步

1. 在左側導覽窗格中，按一下「常規」>「使用者」。

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用戶，以防止特定用戶存取 Unified Manager。您也可以刪除群組，以便群組中的所有使用者都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。

  如果您刪除本機用戶或遠端用戶，則指派給這些用戶的事件將自動取消指派。

- 您必須具有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下「常規」>「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. 點選“是”確認刪除。

什麼是 **RBAC**

RBAC（基於角色的存取控制）可以控制誰有權存取Active IQ Unified Manager伺服器中的各種功能和資源。

基於角色的存取控制的作用

基於角色的存取控制 (RBAC) 使管理員能夠透過定義角色來管理使用者群組。如果您需要限制選定管理員對特定功能的訪問，則必須為他們設定管理員帳戶。如果您想要限制管理員可以查看的資訊和可以執行的操作，您必須將角色套用到您建立的管理員帳戶。

管理伺服器使用RBAC進行使用者登入和角色權限。如果您沒有更改管理伺服器的管理用戶存取的預設設置，則無需登入即可查看它們。

當您啟動需要特定權限的操作時，管理伺服器會提示您登入。例如，要建立管理員帳戶，您必須使用應用程式管理員帳戶存取權限登入。

使用者類型的定義

使用者類型指定使用者持有的帳戶類型，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。每種類型都有自己的角色，由具有管理員角色的使用者分配。

Unified Manager 使用者類型如下：

- 維護使用者

  在 Unified Manager 的初始設定期間建立。然後，維護使用者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控制台的使用者。當 Unified Manager 安裝在 Red Hat Enterprise Linux 系統上時，維護使用者的使用者名稱為「umadmin」。

- 本地用戶

  存取 Unified Manager UI 並根據維護使用者或具有應用程式管理員角色的使用者授予的角色執行功能。

- 遠端組

  使用儲存在驗證伺服器上的憑證存取 Unified Manager UI 的一組使用者。該帳戶的名稱應與身份驗證伺服器上儲存的群組的名稱相符。遠端群組內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賦予的角色執行功能。

- 資料庫使用者

  對 Unified Manager 資料庫中的資料具有唯讀存取權限，但無法存取 Unified Manager Web 介面或維護控制台，也無法執行 API 呼叫。

使用者角色的定義

維護使用者或應用程式管理員為每個使用者指派一個角色。每個角色都包含一定的權限。您可以在 Unified Manager 中執行的活動範圍取決於您被指派的角色以及該角色所包含的權限。

Unified Manager 包含以下預先定義使用者角色：

- 操作員

  查看儲存系統資訊和 Unified Manager 收集的其他數據，包括歷史記錄和容量趨勢。此角色使儲存操作員能夠查看、指派、確認、解決事件並新增註釋。

- 存儲管理員

  在 Unified Manager 中設定儲存管理操作。此角色使儲存管理員能夠配置閾值並建立警報和其他特定於儲存管理的選項和策略。

- 應用程式管理員

  配置與儲存管理無關的設定。此角色可以管理使用者、安全性憑證、資料庫存取和管理選項，包括身份驗證、SMTP、網路和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將自動命名為「umadmin」。

- 整合模式

  此角色允許對 Unified Manager 資料庫視圖進行唯讀訪問，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 資料庫對報表和其他資料庫視圖進行唯讀存取。可以查看的資料庫包括：

  - netapp_model_view
  - netapp_效能
  - 奧庫姆
  - ocum_報告
  - ocum_report_birt
  - 操作
  - 規模監控器

Unified Manager 使用者角色和功能

根據您指派的使用者角色，您可以決定可以在 Unified Manager 中執行哪些操作。

下表顯示了每個使用者角色可以執行的功能：

功能	操作員	儲存管理員	應用程式管理員	整合模式	報告架構
查看儲存系統資訊	•	•	•	•	•
查看其他數據，例如歷史記錄和容量趨勢	•	•	•	•	•
查看、分配和解決事件	•	•	•		
檢視儲存服務對象，例如 SVM 關聯和資源池	•	•	•		
查看閾值策略	•	•	•		
管理儲存服務對象，例如 SVM 關聯和資源池		•	•		
定義警報		•	•		
管理儲存管理選項		•	•		
管理儲存管理策略		•	•		
管理用戶			•		
管理管理選項			•		
定義閾值策略			•		
管理資料庫訪問			•		
管理與 WFA 的整合並提供對資料庫視圖的訪問				•	

功能	操作員	儲存管理員	應用程式管理員	整合模式	報告架構
安排和保存報告		•	•		
從管理操作執行「修復」操作		•	•		
提供對資料庫視圖的唯讀存取權限					•

管理 SAML 身份驗證設定

設定遠端驗證設定後，您可以啟用安全性斷言標記語言 (SAML) 驗證，以便遠端使用者在存取 Unified Manager Web UI 之前由安全性身分提供者 (IdP) 進行驗證。

請注意，啟用 SAML 身份驗證後，只有遠端使用者才能存取 Unified Manager 圖形使用者介面。本機用戶和維護用戶將無法存取 UI。此配置不會影響存取維護控制台的使用者。

身份提供者要求

當設定 Unified Manager 使用身分提供者 (IdP) 為所有遠端使用者執行 SAML 驗證時，您需要了解一些必要的設定設置，以便成功連線到 Unified Manager。

您必須將 Unified Manager URI 和元資料輸入到 IdP 伺服器中。您可以從 Unified ManagerSAML 驗證頁面複製此資訊。 Unified Manager 被視為安全斷言標記語言 (SAML) 標準中的服務提供者 (SP)。

支援的加密標準

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

經過驗證的身份提供者

- 口令
- Active Directory 聯合驗證服務 (ADFS)

ADFS 設定要求

- 您必須依照下列順序定義三個宣告規則，Unified Manager 需要這些規則來解析此依賴方信任項目的 ADFS SAML 回應。

聲明規則	價值
SAM 帳戶名稱	姓名 ID

聲明規則	價值
SAM 帳戶名稱	urn:oid:0.9.2342.19200300.100.1.1
令牌組——非限定名稱	urn：oid：1.3.6.1.4.1.5923.1.5.1.1

- 您必須將身份驗證方法設定為“表單驗證”，否則使用者在退出 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. 點選左側樹狀視圖上的身份驗證策略資料夾。
  c. 在右側的操作下，按一下編輯全域主要驗證策略。
  d. 將 Intranet 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 IdP 登入會被拒絕。有兩種解決方法可以解決此問題：
  - 依照連結中的說明，停用 ADFS 伺服器上與鍊式 CA 憑證關聯的信賴方的撤銷檢查：

    "停用每個依賴方信任的撤銷檢查"

  - 讓 CA 伺服器駐留在 ADFS 伺服器內以簽署 Unified Manager 伺服器憑證要求。

其他配置要求

- Unified Manager 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。

啟用 **SAML** 身份驗證

您可以啟用安全性斷言標記語言 (SAML) 驗證，以便遠端使用者在存取 Unified Manager Web UI 之前先透過安全性身分提供者 (IdP) 進行驗證。

開始之前

- 您必須已配置遠端身份驗證並驗證其是否成功。
- 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。
- 身分提供者 (IdP) 必須受 Unified Manager 支持，並且必須進行設定。
- 您必須擁有 IdP URL 和元資料。
- 您必須有權存取 IdP 伺服器。

從 Unified Manager 啟用 SAML 驗證後，使用者無法存取圖形使用者介面，直到使用 Unified Manager 伺服器主機資訊設定 IdP。因此，您必須準備好在開始設定程序之前完成連接的兩個部分。可以在設定 Unified Manager 之前或之後設定 IdP。

啟用 SAML 身份驗證後，只有遠端使用者才能存取 Unified Manager 圖形使用者介面。本機用戶和維護用戶將無法存取 UI。此配置不會影響存取維護控制台、Unified Manager 命令或 ZAPI 的使用者。

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

步驟

1. 在左側導覽窗格中，按一下「常規」>「**SAML** 驗證」。
2. 選取「啟用 SAML 身份驗證」複選框。

   顯示配置 IdP 連線所需的欄位。

3. 輸入將 Unified Manager 伺服器連接到 IdP 伺服器所需的 IdP URI 和 IdP 元資料。

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

4. 複製 Unified Manager 主機元資料 URI，或將主機元資料儲存到 XML 文字檔案。

   現在您可以使用此資訊來設定 IdP 伺服器。

5. 點選“儲存”。

   將顯示一個訊息框，確認您是否要完成設定並重新啟動 Unified Manager。

6. 點選*確認並登出*，Unified Manager 將重新啟動。

下次授權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 登入頁面中輸入其憑證。

如果尚未完成，請造訪您的 IdP 並輸入 Unified Manager 伺服器 URI 和元資料以完成設定。

當使用 ADFS 作為身分提供者時，Unified Manager GUI 不遵守 ADFS 逾時，並將繼續運作，直到達到 Unified Manager 會話逾時。您可以透過點擊 常規 > 功能設定 > 不活動逾時 來變更 GUI 會話逾時。

更改用於 **SAML** 身份驗證的身份提供者

您可以變更 Unified Manager 用於對遠端使用者進行身份驗證的身分提供者 (IdP)。

開始之前

- 您必須擁有 IdP URL 和元資料。
- 您必須有權存取 IdP。

可以在設定 Unified Manager 之前或之後設定新的 IdP。

步驟

1. 在左側導覽窗格中，按一下「常規」>「**SAML** 驗證」。
2. 輸入新的 IdP URI 以及將 Unified Manager 伺服器連接到 IdP 所需的 IdP 元資料。

   如果可以直接從 Unified Manager 伺服器存取 IdP，則可以在輸入 IdP URL 後按一下 取得 **IdP** 元資料 按鈕以自動填入 IdP 元資料欄位。

3. 複製 Unified Manager 元資料 URI，或將元資料儲存到 XML 文字檔案。
4. 按一下“儲存配置”。

   將顯示一個訊息框來確認您是否要變更配置。

5. 按一下“確定”。

存取新的 IdP 並輸入 Unified Manager 伺服器 URI 和元資料以完成設定。

下次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。

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會要求您更新 SAML 驗證設定。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證書，則證書會更新。

變更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。您必須更新 IdP 伺服器和 Unified Manager 伺服器上的 SAML 驗證設定才能重新啟用對使用者介面的存取。

步驟

1. 登入維護控制台。
2. 在*主選單*中，輸入*停用 SAML 驗證*選項的號碼。

   將顯示一則訊息，確認您要停用 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，將更新後的伺服器憑證接受到瀏覽器中，然後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 主機元資料 URI，或將主機元資料儲存到 XML 文字檔案。
6. 點選“儲存”。

   將顯示一個訊息框，確認您是否要完成設定並重新啟動 Unified Manager。

7. 點選*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 和元資料以完成設定。

身分提供者	設定步驟
ADFS	a. 刪除 ADFS 管理 GUI 中現有的依賴方信任條目。 b. 使用 `saml_sp_metadata.xml`來自更新的 Unified Manager 伺服器。 c. 定義 Unified Manager 解析此依賴方信任條目的 ADFS SAML 回應所需的三個聲明規則。 d. 重新啟動 ADFS Windows 服務。
口令	a. 將 Unified Manager 伺服器的新 FQDN 更新到 `attribute-filter.xml`和 `relying-party.xml`文件。 b. 重新啟動 Apache Tomcat Web 伺服器並等待連接埠 8005 上線。

9. 登入 Unified Manager 並透過您的 IdP 驗證 SAML 身份驗證是否如預期運作。

禁用 **SAML** 身份驗證

當您想要在遠端使用者登入 Unified Manager Web UI 之前停止透過安全性身分提供者 (IdP) 對其進行驗證時，可以停用 SAML 驗證。當停用 SAML 驗證時，設定的目錄服務提供者（例如 Active Directory 或 LDAP）將執行登入驗證。

停用 SAML 身份驗證後，除了配置的遠端使用者之外，本機使用者和維護使用者也將能夠存取圖形使用者介面。

如果您無法存取圖形使用者介面，您也可以使用 Unified Manager 維護控制台停用 SAML 驗證。

停用 SAML 驗證後，Unified Manager 會自動重新啟動。

步驟

1. 在左側導覽窗格中，按一下「常規」>「**SAML** 驗證」。
2. 取消選取*啟用 SAML 驗證*複選框。
3. 點選“儲存”。

   將顯示一個訊息框，確認您是否要完成設定並重新啟動 Unified Manager。

4. 點選*確認並登出*，Unified Manager 將重新啟動。

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

存取您的 IdP 並刪除 Unified Manager 伺服器 URI 和元資料。

從維護控制台停用 **SAML** 驗證

當無法存取 Unified Manager GUI 時，您可能需要從維護控制台停用 SAML 驗證。如果配置錯誤或無法存取 IdP，則可能會發生這種情況。

開始之前

您必須以維護使用者身分存取維護控制台。

當停用 SAML 驗證時，設定的目錄服務提供者（例如 Active Directory 或 LDAP）將執行登入驗證。除了配置的遠端使用者之外，本機使用者和維護使用者也能夠存取圖形使用者介面。

您也可以從 UI 中的設定/身份驗證頁面停用 SAML 身份驗證。

停用 SAML 驗證後，Unified Manager 會自動重新啟動。

步驟

1. 登入維護控制台。
2. 在*主選單*中，輸入*停用 SAML 驗證*選項的號碼。

   將顯示一則訊息，確認您要停用 SAML 驗證並重新啟動 Unified Manager。

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

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

如果需要，請造訪您的 IdP 並刪除 Unified Manager 伺服器 URL 和元資料。

SAML 身份驗證頁面

您可以使用 SAML 驗證頁面設定 Unified Manager，以便透過安全身分提供者 (IdP) 使用 SAML 對遠端使用者進行驗證，然後他們才能登入 Unified Manager Web UI。

- 您必須具有應用程式管理員角色才能建立或修改 SAML 設定。
- 您必須已設定遠端身份驗證。
- 您必須至少配置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，您可以勾選啟用 SAML 驗證核取方塊以使用安全性身分提供者啟用身分驗證。

- **IdP URI**

  從 Unified Manager 伺服器存取 IdP 的 URI。下面列出了範例 URI。

  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** 元資料

  XML 格式的 IdP 元資料。

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

- 主機系統（**FQDN**）

  安裝期間定義的 Unified Manager 主機系統的 FQDN。如果需要的話，您可以更改該值。

- 主機 **URI**

  從 IdP 存取 Unified Manager 主機系統的 URI。

- 主機元資料

  XML 格式的主機系統元資料。

管理身份驗證

您可以在 Unified Manager 伺服器上使用 LDAP 或 Active Directory 啟用身份驗證，並將其設定為與您的伺服器協同工作以對遠端使用者進行身份驗證。

若要啟用遠端身分驗證、設定身分驗證服務和新增身分驗證伺服器，請參閱上一節「設定 Unified Manager 以傳送警報通知」。

編輯身份驗證伺服器

您可以變更 Unified Manager 伺服器用於與身分驗證伺服器通訊的連接埠。

開始之前

您必須具有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下「常規」>「遠端驗證」。
2. 勾選“停用巢狀組查找”方塊。
3. 在「驗證伺服器」區域中，選擇要編輯的驗證伺服器，然後按一下「編輯」。
4. 在「編輯身份驗證伺服器」對話方塊中，編輯連接埠詳細資訊。
5. 點選“儲存”。

刪除身份驗證伺服器

如果您想要封鎖 Unified Manager 伺服器與身份驗證伺服器通信，您可以刪除該身份驗證伺服器。例如，如果您想要變更管理伺服器正在與之通訊的身份驗證伺服器，您可以刪除

該驗證伺服器並新增新的身份驗證伺服器。

開始之前

您必須具有應用程式管理員角色。

當您刪除身份驗證伺服器時，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「常規」>「遠端驗證」。
2. 選擇一個或多個要刪除的身份驗證伺服器，然後按一下「刪除」。
3. 按一下“是”確認刪除請求。

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

使用 **Active Directory** 或 **OpenLDAP** 進行驗證

您可以在管理伺服器上啟用遠端身份驗證，並將管理伺服器設定為與您的身份驗證伺服器通信，以便身份驗證伺服器內的使用者可以存取 Unified Manager。

您可以使用下列預先定義身分驗證服務之一，也可以指定您自己的身分驗證服務：

- 微軟活動目錄

  您不能使用 Microsoft 輕量級目錄服務。

- OpenLDAP

您可以選擇所需的身份驗證服務並新增適當的身份驗證伺服器，以使身份驗證伺服器中的遠端使用者能夠存取 Unified Manager。遠端使用者或群組的憑證由身份驗證伺服器維護。管理伺服器使用輕量級目錄存取協定 (LDAP) 對配置的驗證伺服器內的遠端使用者進行驗證。

對於在 Unified Manager 中建立的本機用戶，管理伺服器維護自己的用戶名稱和密碼資料庫。管理伺服器執行身份驗證，且不使用 Active Directory 或 OpenLDAP 進行身份驗證。

審計日誌

您可以使用稽核日誌偵測稽核日誌是否已外洩。使用者執行的所有活動都受到監控並記錄在稽核日誌中。審核針對Active IQ Unified Manager的所有使用者介面和公開的 API 功能進行。

您可以使用*稽核日誌：檔案檢視*來檢視和存取Active IQ Unified Manager中可用的所有稽核日誌檔案。審計日誌：文件視圖中的文件根據其建立日期列出。此視圖顯示從安裝或升級到系統中現在捕獲的所有審計日誌的資訊。每當您在 Unified Manager 中執行操作時，資訊都會更新並可在日誌中取得。使用「檔案完整性狀態」屬性擷取每個日誌檔案的狀態，該屬性受到主動監控以偵測日誌檔案的篡改或刪除。當系統中有稽核日誌時，稽核日誌可以具有下列狀態之一：

狀態	描述
積極的	目前正在記錄日誌的檔案。
普通的	系統中處於非活動狀態、壓縮並儲存的檔案。
被竄改	該文件已被手動編輯過的使用者破壞。
手動刪除	已被授權使用者刪除的檔案。
滾動刪除	根據滾動配置策略，由於滾動而被刪除的檔案。
意外刪除	由於未知原因而被刪除的檔案。

審計日誌頁麵包括以下命令按鈕：

- 配置
- 刪除
- 下載

使用 **DELETE** 按鈕可以刪除稽核日誌檢視中所列的任何稽核日誌。您可以刪除審計日誌，並可選擇提供刪除檔案的原因，這有助於將來確定有效的刪除。 REASON 欄位列出了原因以及執行刪除操作的使用者的姓名。

刪除日誌檔案將導致檔案從系統中刪除，但資料庫表中的條目不會被刪除。

您可以使用稽核日誌部分中的 **DOWNLOAD** 按鈕從Active IQ Unified Manager下載稽核日誌並匯出稽核日誌檔案。標記為“正常”或“篡改”的檔案以壓縮檔案形式下載 `.gzip`格式。

審計日誌檔案定期歸檔並保存到資料庫以供參考。在存檔之前，審計日誌經過數位簽章以維護安全性和完整性。

產生完整的AutoSupport套件時，支援包將包括存檔和活動審計日誌檔案。但是，當產生輕量級支援包時，它僅包含活動審計日誌。不包括存檔的稽核日誌。

配置審計日誌

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捲動策略，並為稽核日誌啟用遠端日誌記錄。

您可以根據要在系統中儲存的資料量和頻率設定*MAX FILE SIZE*和*AUDIT LOG RETENTION DAYS*中的值。欄位 **TOTAL AUDIT LOG SIZE** 中的值是系統中存在的稽核日誌資料的總大小。捲動原則由欄位 **AUDIT LOG RETENTION DAYS**、**MAX FILE SIZE** 和 **TOTAL AUDIT LOG SIZE** 中的值決定。當稽核日誌備份的大小達到*TOTAL AUDIT LOG SIZE*中配置的值時，將刪除第一個已存檔的檔案。這意味著最舊的檔案被刪除。但文件條目仍然在資料庫中可用，並被標記為“`Rollover Delete`”。 **AUDIT LOG RETENTION DAYS** 值表示稽核日誌檔案保留的天數。任何比此欄位中設定的值更舊的檔案都會被翻轉。

步驟

1. 點選*審計日誌*>>*配置*。

2. 在 **MAX FILE SIZE**、**TOTAL AUDIT LOG SIZE** 和 **AUDIT LOG RETENTION DAYS** 中輸入數值。

   如果您想啟用遠端日誌記錄，那麼您應該選擇*啟用遠端日誌記錄*。 /// 2025-6-11，OTHERDOC-133

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「啟用遠端日誌記錄」核取方塊來啟用遠端稽核日誌記錄。您可以使用此功能將稽核日誌傳輸到遠端 Syslog 伺服器。這將使您能夠在空間受限的情況下管理稽核日誌。

稽核日誌的遠端記錄提供了防篡改備份，以防Active IQ Unified Manager伺服器上的稽核日誌檔案被篡改。

步驟

1. 在*設定稽核日誌*對話方塊中，選取*啟用遠端日誌記錄*複選框。

   顯示用於配置遠端日誌記錄的附加欄位。

2. 輸入您想要連接的遠端伺服器的 **HOSTNAME** 和 **PORT**。
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共憑證。

   證書應上傳至 `.pem`格式。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「主機名稱」作為 `SubjectAltName`（SAN）屬性。

4. 輸入以下欄位的值：**CHARSET**、**CONNECTION TIMEOUT**、**RECONNECTION DELAY**。

   這些欄位的值應以毫秒為單位。

5. 在 **FORMAT** 和 **PROTOCOL** 欄位中選擇所需的 Syslog 格式和 TLS 協定版本。
6. 如果目標 Syslog 伺服器需要基於憑證的驗證，請勾選「啟用用戶端驗證」複選框。

   在儲存審計日誌配置之前，您需要下載用戶端身份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份驗證憑證的雜湊值。

   範例：syslog-ng 需要使用下列命令建立憑證的 <hash> `openssl x509 -noout -hash -in cert.pem`，然後您應該將客戶端身份驗證憑證符號連結到以 <hash> .0 命名的檔案。

7. 按一下「儲存」以設定與伺服器的連線並啟用遠端日誌記錄。

   您將被重新導向到稽核日誌頁面。

   *連線逾時*值會影響配置。如果配置回應的時間比定義值長，則可能會因連線錯誤而導致配置失敗。若要建立成功的連接，請增加*連接逾時*值，然後再次嘗試配置。

遠端身份驗證頁面

您可以使用遠端身份驗證頁面設定 Unified Manager 與您的身份驗證伺服器通信，以對嘗試登入 Unified Manager Web UI 的遠端使用者進行身份驗證。

您必須具有應用程式管理員或儲存管理員角色。

選取啟用遠端身份驗證複選框後，您可以使用身份驗證伺服器啟用遠端身份驗證。

- 認證服務

  使您能夠設定管理伺服器以在目錄服務提供者（例如 Active Directory、OpenLDAP）中對使用者進行驗證，或指定您自己的驗證機制。只有當您啟用了遠端身份驗證時，您才可以指定身份驗證服務。

  - 活動目錄
    - 管理員姓名

      指定認證伺服器的管理員名稱。

    - 密碼

      指定存取認證伺服器的密碼。

    - 基本可分辨名稱

      指定遠端使用者在認證伺服器中的位置。例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。

    - 禁用嵌套組查找

      指定是否啟用或停用嵌套組查找選項。預設此選項是禁用的。如果您使用 Active Directory，則可以透過停用對嵌套群組的支援來加快身份驗證速度。

    - 使用安全連接

      指定用於與身份驗證伺服器通訊的身份驗證服務。

  - **OpenLDAP**
    - 綁定可分辨名稱

      指定與基本可分辨名稱一起使用的綁定可分辨名稱，以在身份驗證伺服器中尋找遠端使用者。

    - 綁定密碼

      指定存取認證伺服器的密碼。

    - 基本可分辨名稱

      指定遠端使用者在認證伺服器中的位置。例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。

    - 使用安全連接

      指定使用安全 LDAP 與 LDAP 驗證伺服器進行通訊。

  - 其他的

- 綁定可分辨名稱

  指定綁定可分辨名稱，該名稱與基本可分辨名稱一起使用，以在您配置的身份驗證伺服器中尋找遠端使用者。

- 綁定密碼

  指定存取認證伺服器的密碼。

- 基本可分辨名稱

  指定遠端使用者在認證伺服器中的位置。例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。

- 協議版本

  指定您的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協定版本或將版本設定為 2 或 3。

- 使用者名稱屬性

  指定驗證伺服器中的屬性名稱，該屬性包含要由管理伺服器進行驗證的使用者登入名稱。

- 群組成員身分屬性

  指定一個值，該值根據使用者的身份驗證伺服器中指定的屬性和值為遠端使用者指派管理伺服器群組成員身分。

- UGID

  如果遠端使用者作為身分驗證伺服器中 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。

- 禁用嵌套組查找

  指定是否啟用或停用嵌套組查找選項。預設此選項是禁用的。如果您使用 Active Directory，則可以透過停用對嵌套群組的支援來加快身份驗證速度。

- 成員

  指定身份驗證伺服器用於儲存有關群組的各個成員的資訊的屬性名稱。

- 使用者物件類別

  指定遠端認證伺服器中使用者的物件類別。

- 群組物件類別

  指定遠端認證伺服器中所有群組的物件類別。

> 您為_Member_、*User Object Class* 和 *Group Object Class* 屬性輸入的值應與在 Active Directory、OpenLDAP 和 LDAP 配置中新增的值相同。否則，身份驗證可能會失敗。

- 使用安全連接

  指定用於與身份驗證伺服器通訊的身份驗證服務。

  如果要修改身份驗證服務，請確保刪除所有現有的身份驗證伺服器並新增新的身份驗證伺服器。

身份驗證伺服器區域

身份驗證伺服器區域顯示管理伺服器與之通訊以尋找和驗證遠端使用者的身份驗證伺服器。遠端使用者或群組的憑證由身份驗證伺服器維護。

- 命令按鈕

  使您能夠新增、編輯或刪除身份驗證伺服器。

  - 添加

    使您能夠新增身份驗證伺服器。

  如果您要新增的身份驗證伺服器是高可用性對的一部分（使用相同的資料庫），那麼您也可以新增合作夥伴驗證伺服器。當其中一個身份驗證伺服器無法存取時，這使得管理伺服器能夠與合作夥伴進行通訊。

  - 編輯

    使您能夠編輯選定身份驗證伺服器的設定。

  - 刪除

    刪除選定的認證伺服器。

- 姓名或 **IP** 位址

  顯示用於在管理伺服器上驗證使用者的驗證伺服器的主機名稱或 IP 位址。

- 港口

  顯示認證伺服器的連接埠號碼。

- 測試認證

  此按鈕透過驗證遠端使用者或群組來驗證您的身份驗證伺服器的配置。

  測試時，如果僅指定用戶名，管理伺服器會在認證伺服器中搜尋遠端用戶，但不會對用戶進行認證。如果您同時指定使用者名稱和密碼，管理伺服器將搜尋並驗證遠端使用者。

  如果遠端身份驗證已停用，則您無法測試身份驗證。

管理安全證書

您可以在 Unified Manager 伺服器中設定 HTTPS，以透過安全連線監控和管理您的叢集。

查看**HTTPS**安全證書

您可以將 HTTPS 憑證詳細資訊與瀏覽器中檢索到的憑證進行比較，以確保瀏覽器與 Unified Manager 的加密連線不會被攔截。

開始之前

您必須具有操作員、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的內容，或檢視可以從中存取 Unified Manager 的主題備用名稱 (SAN)。

步

1. 在左側導覽窗格中，按一下「常規」>「**HTTPS** 憑證」。

   HTTPS憑證顯示在頁面頂部

如果您需要查看比 HTTPS 憑證頁面上顯示的更多有關安全憑證的詳細信息，您可以在瀏覽器中查看連接憑證。

下載 **HTTPS** 憑證簽署請求

您可以下載目前 HTTPS 安全性憑證的認證簽章要求，以便將該檔案提供給憑證授權單位進行簽署。 CA 簽章憑證有助於防止中間人攻擊，並提供比自簽章憑證更好的安全保護。

開始之前

您必須具有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下「常規」>「**HTTPS** 憑證」。
2. 按一下「下載 HTTPS 憑證簽署請求」。
3. 儲存 `<hostname>.csr`文件。

您可以將該文件提供給證書頒發機構進行簽名，然後安裝已簽署的證書。

安裝 **CA** 簽署並傳回的 **HTTPS** 憑證

您可以在證書頒發機構簽署並返回安全證書後上傳並安裝該證書。您上傳並安裝的檔案必須是現有自簽名憑證的簽章版本。 CA 簽章憑證有助於防止中間人攻擊，並提供比自簽章憑證更好的安全保護。

*開始之前

您必須完成以下操作：

- 下載憑證簽署請求文件並由憑證授權單位簽名
- 以 PEM 格式儲存憑證鏈
- 包含鏈中的所有證書，從 Unified Manager 伺服器證書到根簽名證書，包括任何存在的中間證書

您必須具有應用程式管理員角色。

如果建立 CSR 的憑證有效期超過 397 天，則 CA 會在簽署並傳回憑證之前將有效期縮短至 397 天

步驟

1. 在左側導覽窗格中，按一下「常規」>「**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. 選擇文件，然後按一下*安裝*來安裝該文件。

   有關信息，請參閱"安裝使用外部工具產生的 HTTPS 憑證"。

證書鏈範例

以下範例顯示了憑證鏈檔案的可能外觀：

```
-----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-----
```

安裝使用外部工具產生的 **HTTPS** 憑證

您可以安裝自簽名或 CA 簽署的證書，並使用外部工具（如 OpenSSL、BoringSSL、LetsEncrypt）產生。

您應該將私鑰與憑證鏈一起加載，因為這些憑證是外部產生的公鑰-私鑰對。允許的金鑰對演算法是“RSA”和“EC”。在「常規」部分下的「HTTPS 憑證」頁面中提供了「安裝 **HTTPS** 憑證」選項。您上傳的文件應採用以下輸入格式。

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. 反向直到根的 CA 證書，用於簽署上述證書

載入帶有 **EC** 金鑰對的憑證的格式

允許的曲線是“prime256v1”和“secp384r1”。具有外部產生的 EC 對的憑證樣本：

```
 -----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-----
```

使用 **RSA** 金鑰對載入憑證的格式

屬於主機憑證的 RSA 金鑰對允許的金鑰大小為 2048、3072 和 4096。具有外部產生的 **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-----
```

上傳憑證後，您應該重新啟動Active IQ Unified Manager實例以使變更生效。

上傳外部產生的憑證時進行檢查

系統在上傳使用外部工具產生的憑證時執行檢查。如果任何檢查失敗，則證書被拒絕。還包括產品內 CSR 產生的憑證和使用外部工具產生的憑證的驗證。

- 輸入中的私鑰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) 與主機的 FQDN 進行檢查。
- 主機憑證的通用名稱（CN）不能為空或空白，且不能設定為localhost。
- 證書的有效期限起始日期不應為日後日期，且證書的有效期限到期日不應為過去日期。
- 如果存在中級 CA 或 CA，則憑證的有效期開始日期不應在未來，有效期到期日不應在過去。

輸入中的私鑰不應該被加密。如果有任何私鑰被加密，那麼系統就會拒絕它們。

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"^]

證書管理的頁面描述

您可以使用 HTTPS 憑證頁面查看目前的安全性憑證並產生新的 HTTPS 憑證。

HTTPS 憑證頁面

HTTPS 憑證頁面可讓您查看目前安全性憑證、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名 HTTPS 證書，則此頁面上顯示的證書是安裝期間產生的證書。

命令按鈕

命令按鈕使您能夠執行以下操作：

- 下載 **HTTPS** 憑證簽署請求

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

- 安裝 **HTTPS** 憑證

  使您能夠在證書頒發機構簽署並返回安全證書後上傳並安裝該證書。重新啟動管理伺服器後，新憑證將生效。

- 重新產生 **HTTPS** 憑證

  使您能夠產生新的自簽名 HTTPS 證書，以取代目前的安全性證書。重新啟動 Unified Manager 後，新憑證將生效。

重新產生 **HTTPS** 憑證對話框

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

當前證書資訊出現在此頁面上。

「使用目前憑證屬性重新產生」和「更新目前憑證屬性」選擇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

  必需的。您希望保護的完全限定網域名稱 (FQDN)。

  在 Unified Manager 高可用性設定中，使用虛擬 IP 位址。

- 電子郵件

  選修的。用於聯絡您組織的電子郵件地址；通常是憑證管理員或 IT 部門的電子郵件地址。

- 公司

  選修的。通常是您公司的註冊名稱。

- 部門

選修的。貴公司部門的名稱。

- 城市

  選修的。貴公司所在的城市。

- 狀態

  選修的。貴公司所在的州或省位置（不縮寫）。

- 國家

  選修的。貴公司所在的國家。這通常是該國家的兩個字母的 ISO 代碼。

- 其他名稱

  必需的。除了現有的本地主機或其他網路位址之外，還可用於存取此伺服器的附加非主要網域名稱。用逗號分隔每個備用名稱。

  如果您想要從憑證中的備用名稱欄位中刪除本機識別訊息，請勾選「排除本機識別資訊（例如 localhost）」複選框。選取此核取方塊後，只有您在欄位中輸入的內容才會在備用名稱欄位中使用。當留空時，產生的憑證將根本沒有備用名稱欄位。

- 金鑰大小（金鑰演算法：**RSA**）

  金鑰演算法設定為RSA。您可以從下列密鑰大小中選擇一個：2048、3072 或 4096 位元。預設密鑰大小設定為 2048 位元。

- 有效期限

  預設有效期為397天。如果您從先前的版本升級，您可能會看到先前的憑證有效性保持不變。

有關詳細信息，請參閱 "產生 HTTPS 憑證"。