配置Active IQ Unified Manager

Active IQ Unified Manager

NetApp
October 15, 2025

目錄

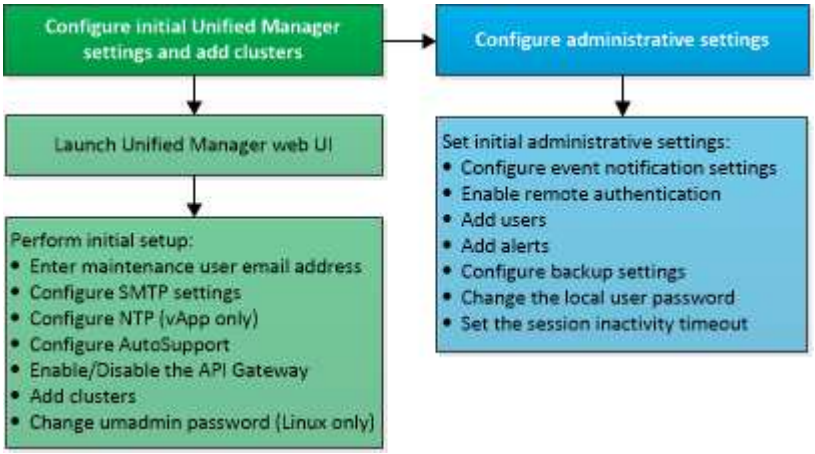
配置Active IQ Unified Manager

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

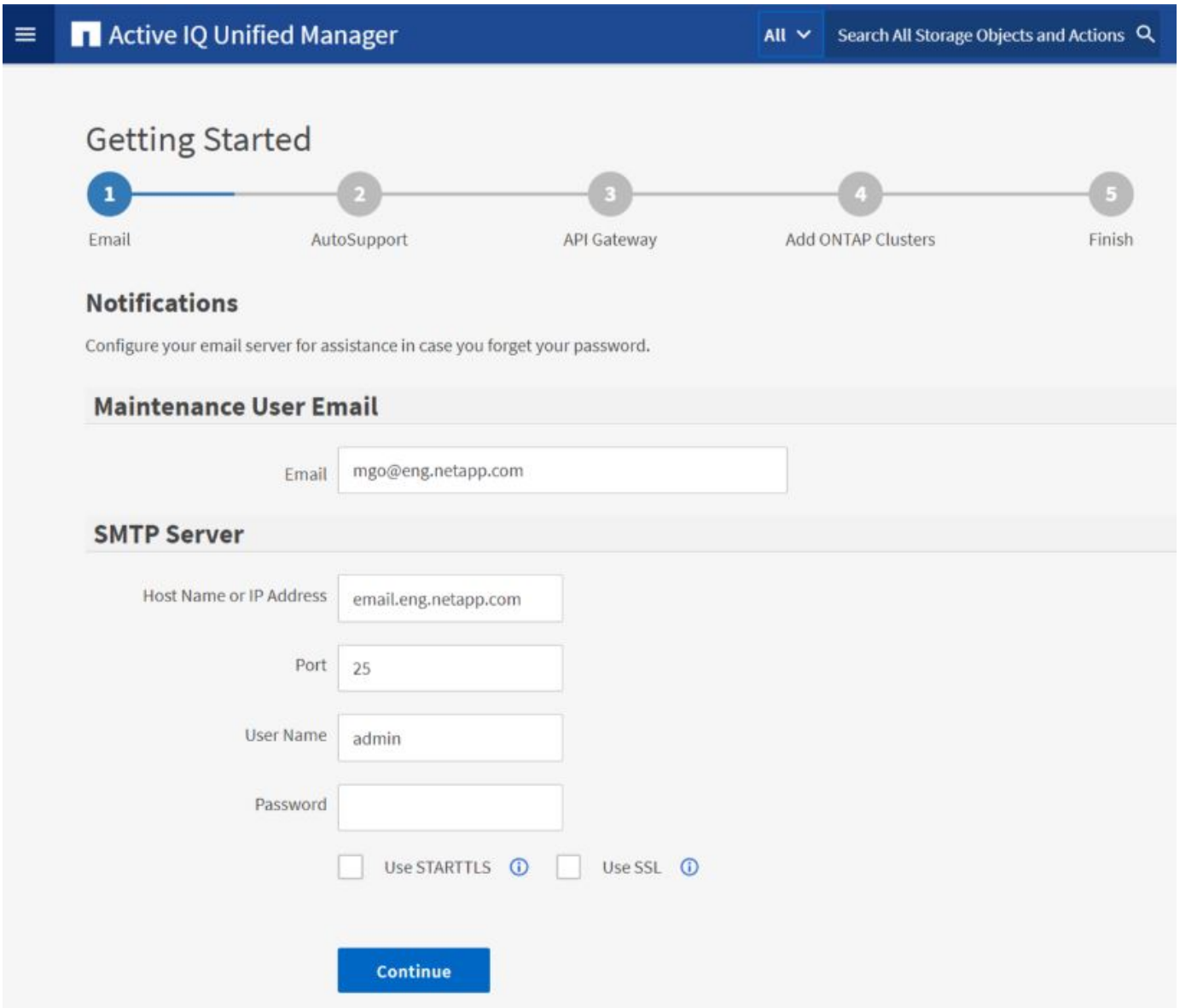
若要使用 Unified Manager，您必須先設定初始設定選項，包括 NTP 伺服器、維護使用者電子郵件地址、SMTP 伺服器主機以及新增ONTAP叢集。

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）

對於身份驗證類型...	輸入以下資訊...
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*。
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。

產生**HTTPS**安全證書

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。