執行組態和管理工作

Active IQ Unified Manager 9.10

NetApp
December 18, 2023

目錄

執行組態和管理工作 1
設定Active IQ Unified Manager 功能 1
設定Unified Manager備份 18
管理功能設定 18
使用維護主控台 21
管理使用者存取 33
管理SAML驗證設定 39
管理驗證 44
管理安全性憑證 51

執行組態和管理工作

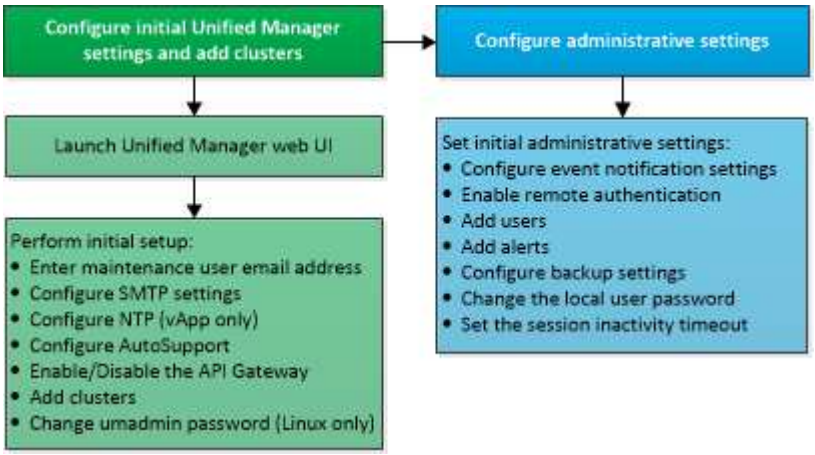
設定Active IQ Unified Manager 功能

安裝Active IQ Unified Manager 完整套功能（前身OnCommand 為「非統一化管理程式」）之後、您必須完成初始設定（也稱為「第一次使用體驗精靈」）、才能存取網路UI。然後您可以執行其他組態工作、例如新增叢集、設定遠端驗證、新增使用者及新增警示。

完成Unified Manager執行個體的初始設定時、需要執行本手冊中所述的部分程序。其他程序是建議的組態設定、有助於在新執行個體上設定、或是在您開始定期監控ONTAP 您的不二系統之前、先瞭解這些設定。

組態順序總覽

組態工作流程會說明您在使用Unified Manager之前必須執行的工作。



存取**Unified Manager Web UI**

安裝Unified Manager之後、您可以存取Web UI來設定Unified Manager、以便開始監控ONTAP 您的VMware系統。

您需要的是什麼

- 如果這是您第一次存取Web UI、則必須以維護使用者（或Linux安裝的umadmin使用者）的身分登入。
- 如果您打算允許使用者使用簡短名稱存取Unified Manager、而非使用完整網域名稱（FQDN）或IP位址、則網路組態必須將此簡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。您可以確認繼續存取的風險、或是安裝憑證授權單位（CA）簽署的數位憑證來進行伺服器驗證。

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位址或完整網域名稱（FQDN）。

   連結格式如下：「https://URL`」。

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

> 如果您連續三次嘗試登入Web UI失敗、一小時內您將會被鎖定在系統之外、並需要聯絡系統管理員。這僅適用於本機使用者。

執行**Unified Manager Web UI**的初始設定

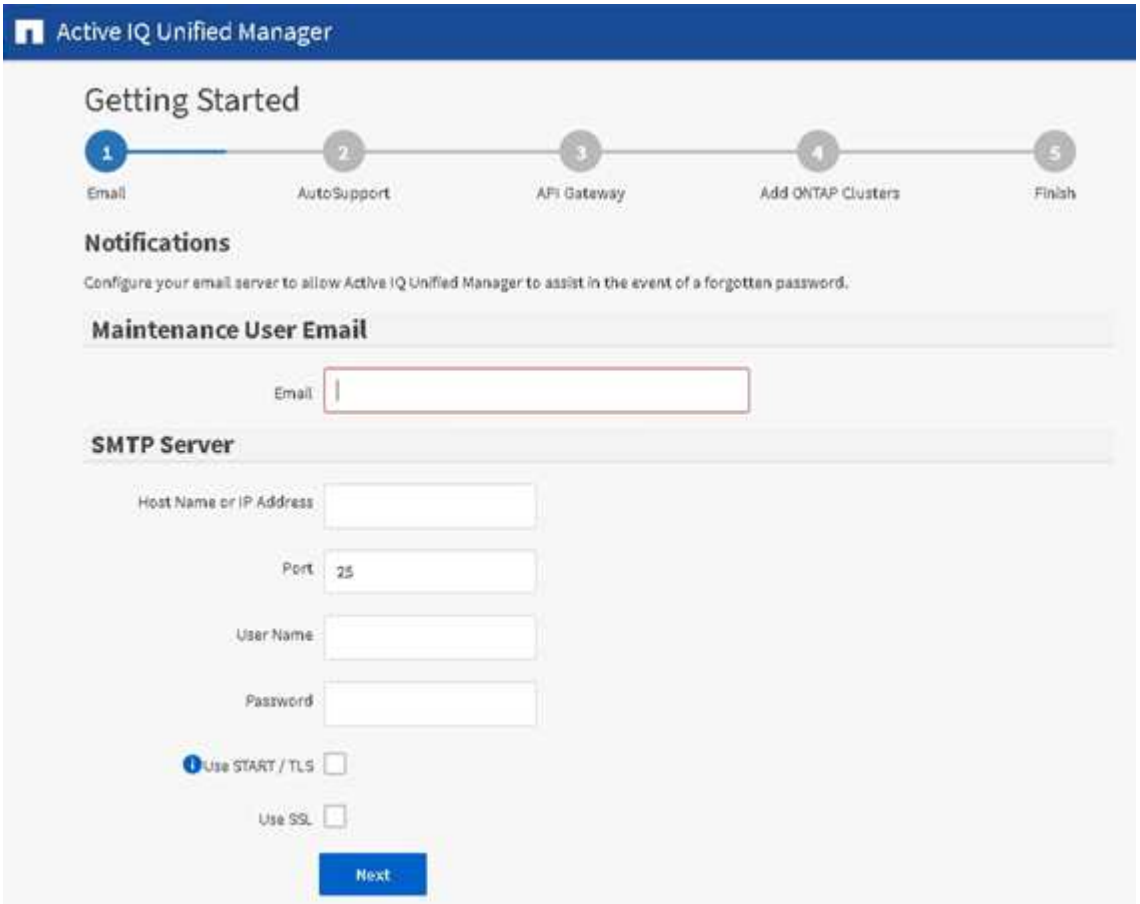
若要使用Unified Manager、您必須先設定初始設定選項、包括NTP伺服器、維護使用者電子郵件地址、SMTP伺服器主機、以及新增ONTAP 叢集。

您需要的是什麼

您必須執行下列作業：

- 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（適用於Linux安裝的umadmin使用者）登入

僅當您第一次存取Web UI時、才會顯示「《程式碼統一化管理程式入門」頁面。Active IQ以下頁面來自VMware的安裝。



如果您想要稍後變更這些選項、可以從Unified Manager左側導覽窗格的「一般」選項中選取您的選項。請注意、NTP設定僅適用於VMware安裝、稍後可使用Unified Manager維護主控台進行變更。

步驟

1. 在「支援初始設定」頁面中、輸入維護使用者電子郵件地址、SMTP伺服器主機名稱及任何其他的SMTP選項、以及NTP伺服器（僅限VMware安裝）Active IQ Unified Manager 。然後按一下 * 繼續 * 。
2. 在「支援」頁面中、按一下「同意並繼續」AutoSupport 、即可從AutoSupport Unified Manager將支援訊息傳送至NetAppActive IQ。

   如果您需要指定一個Proxy來提供網際網路存取、以便傳送AutoSupport 各種內容、或是想要停用AutoSupport 某些功能、請AutoSupport 從網路UI使用*一般*>* Swise*選項。

3. 在Red Hat和CentOS系統上、您可以將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、讓Unified Manager能夠管理ONTAP 您計畫使用ONTAP Isureest API監控的各個叢集。然後按一下 * 繼續 * 。

   您稍後可從*一般*>*功能設定*>* API閘道*的網路UI中啟用或停用此設定。如需API的詳細資訊、請參閱 "開始使用Active IQ Unified Manager 靜態API"。

5. 新增您要Unified Manager管理的叢集、然後按一下*下一步*。對於您打算管理的每個叢集、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認證、使用者必須具有「admin」角色。

   此步驟為選用步驟。您可以稍後在Web UI中從* Storage Management **>** Cluster Setup *新增叢集。

6. 在「摘要」頁面中、確認所有設定都正確無誤、然後按一下「完成」。

隨即關閉「使用入門」頁面、並顯示「Unified Manager儀表板」頁面。

新增叢集

您可以將叢集新增Active IQ Unified Manager 至支援功能、以便監控叢集。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）的能力、以便找出並解決可能發生的任何問題。

您需要的是什麼

- 您必須具有應用程式管理員或儲存管理員角色。
- 您必須具備下列資訊：
  - 主機名稱或叢集管理IP位址

    主機名稱是Unified Manager用來連線至叢集的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虛擬機器（SVM）的叢集管理LIF。如果使用節點管理LIF、則作業會失敗。

  - 叢集必須執行ONTAP 的是版本不穩定的9.1軟體或更新版本。
  - 系統管理員使用者名稱和密碼ONTAP

    此帳戶必須將「應用程式」存取權限設為_ontapi_、_ssh _和_http _的_admin_角色。

  - 使用HTTPS傳輸協定連線至叢集的連接埠號碼（通常為連接埠443）
  - 您擁有必要的憑證。需要兩種類型的憑證：

伺服器憑證：用於登錄。新增叢集需要有效的憑證。如果伺服器憑證過期、您應該重新產生該憑證、然後重新啟動Unified Manager、以便重新自動登錄服務。如需建立憑證的相關資訊、請參閱知識庫（KB）文章： "如何在ONTAP 更新SSL憑證的過程中進行更新9"

用戶端憑證：用於驗證。新增叢集需要有效的憑證。您無法將已過期憑證的叢集新增至Unified Manager、如果用戶端憑證已過期、則應在新增叢集之前重新產生叢集。不過、如果此憑證已新增且正由Unified Manager使用的叢集過期、則EMS訊息會繼續與過期的憑證搭配運作。您不需要重新產生用戶端憑證。

> 您可以使用Unified Manager NAT IP位址、新增位於NAT/防火牆後方的叢集。任何連線的Workflow Automation或SnapProtect 非功能性系統也必須位於NAT/防火牆之後、SnapProtect 而非功能性API呼叫則必須使用NAT IP位址來識別叢集。

- 您必須在Unified Manager伺服器上有足夠的空間。當資料庫目錄中超過90%的空間已耗用時、您將無法將叢集新增至伺服器。

若要進行支援、您必須同時新增本機和遠端叢集、而且叢集必須正確設定。MetroCluster

只要您已在叢集上設定第二個叢集管理LIF、讓Unified Manager的每個執行個體都透過不同的LIF連線、您就可以使用兩個Unified Manager執行個體來監控單一叢集。

步驟

1. 在左導覽窗格中、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IPv6變更為IPv6。下一個監控週期完成後、新的IP位址會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」以檢視叢集的憑證資訊。
6. 按一下「是」。

   Unified Manager只會在一開始新增叢集時檢查憑證。Unified Manager不會檢查每個API呼叫ONTAP 的認證資料以供參考。

在探索新叢集的所有物件之後、Unified Manager會開始收集前15天的歷史效能資料。這些統計資料是使用資料持續性收集功能來收集。此功能可在新增叢集之後、立即為叢集提供超過兩週的效能資訊。在資料持續性收集週期完成之後、系統會依預設每五分鐘收集一次即時叢集效能資料。

> 由於收集15天的效能資料會佔用大量CPU資源、因此建議您將新增的叢集重新分段、以使資料持續性收集輪詢不會同時在太多叢集上執行。此外、如果您在資料持續性收集期間重新啟動Unified Manager、收集作業將會暫停、而且效能圖表中會出現遺漏時間範圍的落差。

> 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、Unified Manager HTTPS憑證開始日期是否晚於叢集上的日期。您必須確保時鐘是使用NTP或類似服務來同步。

設定Unified Manager以傳送警示通知

您可以設定Unified Manager傳送通知、提醒您環境中的事件。在傳送通知之前、您必須先設定其他數個Unified Manager選項。

您需要的是什麼

您必須具有應用程式管理員角色。

部署Unified Manager並完成初始組態之後、您應該考慮設定環境、以觸發警示、並根據事件接收產生通知電子郵件或SNMP設陷。

步驟

1. "設定事件通知設定"

   如果您想要在環境中發生特定事件時傳送警示通知、您必須設定一個SMTP伺服器、並提供電子郵件地址、以便傳送警示通知。如果您要使用SNMP設陷、可以選取該選項並提供必要資訊。

2. "啟用遠端驗證"

   如果您想要遠端LDAP或Active Directory使用者存取Unified Manager執行個體並接收警示通知、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、讓驗證伺服器內的遠端使用者能夠存取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、您會指派使用者接收警示通知。

5. "新增警示"

   新增電子郵件地址以傳送通知、新增使用者以接收通知、設定網路設定、以及設定環境所需的SMTP和SNMP選項之後、即可指派警示。

設定事件通知設定

您可以設定Unified Manager在事件產生或事件指派給使用者時傳送警示通知。您可以設定用於傳送警示的SMTP伺服器、並設定各種通知機制、例如、警示通知可以以電子郵件或SNMP設陷傳送。

您需要的是什麼

您必須具備下列資訊：

- 傳送警示通知的電子郵件地址

  電子郵件地址會出現在「已傳送警示通知」的「寄件者」欄位中。如果由於任何原因而無法傳送電子郵件、此電子郵件地址也會作為無法傳送郵件的收件者。

- 用於存取伺服器的SMTP伺服器主機名稱、以及使用者名稱和密碼
- 接收SNMP設陷之設陷目的地主機的主機名稱或IP位址、以及SNMP版本、傳出設陷連接埠、社群及其他必要的SNMP組態值

  若要指定多個設陷目的地、請以逗號分隔每個主機。在此情況下、清單中所有主機的所有其他SNMP設定（例如版本和傳出陷阱連接埠）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*一般*>*通知*。
2. 在「通知」頁面中、設定適當的設定、然後按一下「儲存」。
   - 附註：*
     - 如果寄件者地址已預先填入「+ActiveIQUnifiedManager@localhost.com」地址、您應該將其變更為實際有效的電子郵件地址、以確保所有電子郵件通知都能順利傳送。
     - 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）、而非主機名稱。

啟用遠端驗證

您可以啟用遠端驗證、讓Unified Manager伺服器能夠與驗證伺服器通訊。驗證伺服器的使用者可以存取Unified Manager圖形介面、以管理儲存物件和資料。

您需要的是什麼

您必須具有應用程式管理員角色。

> Unified Manager伺服器必須直接連線至驗證伺服器。您必須停用任何本機LDAP用戶端、例如SSSD（系統安全服務精靈）或NSLCD（名稱服務LDAP快取精靈）。

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

LDAP和LDAPS（安全LDAP）支援遠端驗證。Unified Manager使用389作為非安全通訊的預設連接埠、而使用636作為安全通訊的預設連接埠。

> 用於驗證使用者的憑證必須符合X・509格式。

步驟

1. 在左導覽窗格中、按一下*一般*>*遠端驗證*。
2. 勾選「啟用遠端驗證...」方塊。
3. 在驗證服務欄位中、選取服務類型並設定驗證服務。

對於驗證類型...	輸入下列資訊...
Active Directory	• 驗證伺服器管理員名稱的格式如下： ◦ 「名稱\使用者名稱」 ◦ "username@domainname" ◦ 「Bind Distinguished Name」（連結辨別名稱）（使用適當的LDAP表示法） • 系統管理員密碼 • 基礎辨別名稱（使用適當的LDAP表示法）
開啟LDAP	• 連結辨別名稱（以適當的LDAP表示法） • 連結密碼 • 基礎辨別名稱

如果Active Directory使用者的驗證需要很長時間或逾時、驗證伺服器可能需要很長時間才能回應。停用Unified Manager中的巢狀群組支援、可能會縮短驗證時間。

如果您為驗證伺服器選取「使用安全連線」選項、Unified Manager就會使用安全通訊端層（SSL）傳輸協定與驗證伺服器通訊。

4. *選用：*新增驗證伺服器、並測試驗證。
5. 按一下「 * 儲存 * 」。

從遠端驗證停用巢狀群組

如果已啟用遠端驗證、您可以停用巢狀群組驗證、以便只有個別使用者（而非群組成員）可以遠端驗證Unified Manager。若要改善Active Directory驗證回應時間、您可以停用巢狀群組。

您需要的是什麼

- 您必須具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、且將遠端群組新增至Unified Manager、則個別使用者必須是遠端群組的成員、才能驗證Unified Manager。

步驟

1. 在左導覽窗格中、按一下*一般*>*遠端驗證*。
2. 選中*禁用嵌套組查找*複選框。
3. 按一下「 * 儲存 * 」。

設定驗證服務

驗證服務可在提供遠端使用者或遠端群組存取Unified Manager之前、先在驗證伺服器中驗證這些使用者或遠端群組。您可以使用預先定義的驗證服務（例如Active Directory或OpenLDAP）、或設定自己的驗證機制來驗證使用者。

您需要的是什麼

- 您必須啟用遠端驗證。
- 您必須具有應用程式管理員角色。

步驟

1. 在左導覽窗格中、按一下*一般*>*遠端驗證*。
2. 選取下列其中一項驗證服務：

如果您選取...	然後執行此動作...
Active Directory	a. 輸入管理員名稱和密碼。 b. 指定驗證伺服器的基礎辨別名稱。 例如、如果驗證伺服器的網域名稱是+ou@domain.com、則基礎辨別名稱是* CN=ou,DC=domain,DC=com*。
OpenLDAP	a. 輸入綁定辨別名稱和綁定密碼。 b. 指定驗證伺服器的基礎辨別名稱。 例如、如果驗證伺服器的網域名稱是+ou@domain.com、則基礎辨別名稱是* CN=ou,DC=domain,DC=com*。
其他	a. 輸入綁定辨別名稱和綁定密碼。 b. 指定驗證伺服器的基礎辨別名稱。 例如、如果驗證伺服器的網域名稱是+ou@domain.com、則基礎辨別名稱是* 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、群組成員資格、使用者群組和成員屬性。

若要修改驗證服務、您必須刪除任何現有的驗證伺服器、然後新增驗證伺服器。

3. 按一下「* 儲存 * 」。

新增驗證伺服器

您可以在管理伺服器上新增驗證伺服器並啟用遠端驗證、以便驗證伺服器內的遠端使用者存取Unified Manager。

您需要的是什麼

- 必須提供下列資訊：
  - 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
- 您必須啟用遠端驗證並設定驗證服務、以便管理伺服器能夠驗證驗證伺服器中的遠端使用者或群組。
- 您必須具有應用程式管理員角色。

如果您要新增的驗證伺服器是高可用度（HA）配對（使用相同的資料庫）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、與合作夥伴通訊。

步驟

1. 在左導覽窗格中、按一下*一般*>*遠端驗證*。
2. 啟用或停用*使用安全連線*選項：

如果您想要...	然後執行此動作...
啟用它	a. 選擇*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、確認憑證資訊、然後按一下「關閉」。 f. 在授權主機對話方塊中、按一下*是*。 ⓘ 當您啟用*使用安全連線驗證*選項時、Unified Manager會與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連接埠、而非安全通訊則使用389連接埠。

如果您想要...	然後執行此動作...
停用它	a. 清除*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. 按一下「 * 新增 * 」。

您新增的驗證伺服器會顯示在「伺服器」區域中。

3. 執行測試驗證、確認您可以在新增的驗證伺服器中驗證使用者。

測試驗證伺服器的組態

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。您可以從驗證伺服器搜尋遠端使用者或遠端群組、然後使用設定進行驗證、藉此驗證組態。

您需要的是什麼

- 您必須啟用遠端驗證、並設定驗證服務、Unified Manager伺服器才能驗證遠端使用者或遠端群組。
- 您必須新增驗證伺服器、以便管理伺服器從這些伺服器搜尋遠端使用者或遠端群組、並進行驗證。
- 您必須具有應用程式管理員角色。

如果驗證服務設定為Active Directory、而且您正在驗證屬於驗證伺服器主要群組的遠端使用者驗證、驗證結果中就不會顯示主要群組的相關資訊。

步驟

1. 在左導覽窗格中、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」。

   如果您正在驗證遠端群組、則不得輸入密碼。

新增警示

您可以設定警示、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示。您可以指定通知的頻率、並將指令碼與警示建立關聯。

您需要的是什麼

- 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設陷主機、才能讓Active IQ Unified Manager 此伺服器在產生事件時使用這些設定來傳送通知給使用者。
- 您必須知道要觸發警示的資源和事件、以及您要通知的使用者使用者名稱或電子郵件地址。

- 如果您想要根據事件執行指令碼、必須使用「指令碼」頁面將指令碼新增至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「警示設定」頁面建立警示之外、您也可以在收到事件後直接從「事件詳細資料」頁面建立警示、如以下所述。

步驟

1. 在左導覽窗格中、按一下*儲存管理*>*警示設定*。
2. 在「警示設定」頁面中、按一下*「新增*」。
3. 在「新增警示」對話方塊中、按一下*名稱*、然後輸入警示的名稱和說明。
4. 按一下*資源*、然後選取要納入警示或排除在警示範圍之外的資源。

   您可以在「名稱包含」欄位中指定文字字串、以選取一組資源、藉此設定篩選條件。根據您指定的文字字串、可用資源清單僅會顯示符合篩選規則的資源。您指定的文字字串區分大小寫。

   如果資源同時符合您所指定的「包含」和「排除」規則、則排除規則優先於「包含」規則、而且不會針對與排除資源相關的事件產生警示。

5. 按一下*事件*、然後根據您要觸發警示的事件名稱或事件嚴重性類型來選取事件。

   若要選取多個事件、請在選取時按Ctrl鍵。

6. 按一下「動作」、然後選取您要通知的使用者、選擇通知頻率、選擇是否要將SNMP設陷傳送到設陷接收器、並指派指令碼在產生警示時執行。

   如果您修改為使用者指定的電子郵件地址、然後重新開啟警示以進行編輯、則「名稱」欄位會顯示空白、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」頁面修改所選使用者的電子郵件地址、則所選使用者的修改電子郵件地址不會更新。

   您也可以選擇透過SNMP設陷通知使用者。

7. 按一下「 * 儲存 * 」。

新增警示的範例

本範例說明如何建立符合下列需求的警示：

- 警示名稱：HealthTest
- 資源：包括名稱包含「'abc'」的所有磁碟區、並排除名稱包含「'xyz'」的所有磁碟區
- 事件：包括所有重要的健全狀況事件
- 行動：包括「+sample@domain.com」、「Test」指令碼、使用者必須每15分鐘通知一次

在「新增警示」對話方塊中執行下列步驟：

步驟

1. 按一下*姓名*、然後在*警示名稱*欄位中輸入* HealthTest*。

2. 按一下「資源」、然後在「包含」索引標籤中、從下拉式清單中選取「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. 選取*<<All Volumes whose name contains 'abc'>>「可用資源」區域中的「*」、然後將其移至「選取的資源」區域。
   c. 按一下「排除」、然後在「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」欄位中選取「嚴重」。
4. 從「Matching Event（符合事件）」區域中選取* All Critical事件*、然後將其移至「Selected Event（選取的事件）」區域。
5. 按一下「動作」、然後在「警示這些使用者」欄位中輸入* sample@domain.com。
6. 選擇*每15分鐘提醒一次*、每15分鐘通知使用者一次。

   您可以設定警示、在指定時間內重複傳送通知給收件者。您應該決定警示的事件通知啟動時間。

7. 在Select Script to執行（選擇要執行的指令碼）功能表中、選取* Test*指令碼。
8. 按一下「 * 儲存 * 」。

變更本機使用者密碼

您可以變更本機使用者登入密碼、以避免潛在的安全風險。

您需要的是什麼

您必須以本機使用者的身分登入。

維護使用者和遠端使用者的密碼無法使用這些步驟加以變更。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 "使用維護主控台"。

步驟

1. 登入Unified Manager。
2. 從頂端功能表列按一下使用者圖示、然後按一下*變更密碼*。

   如果您是遠端使用者、則不會顯示*變更密碼*選項。

3. 在「變更密碼」對話方塊中、輸入目前密碼和新密碼。
4. 按一下「 * 儲存 * 」。

如果Unified Manager是以高可用度組態設定、您必須在設定的第二個節點上變更密碼。兩個執行個體都必須有相同的密碼。

設定工作階段閒置逾時

您可以指定Unified Manager的閒置逾時值、以便在一段時間後自動終止工作階段。依預設、逾時時間設為4、320分鐘（72小時）。

您需要的是什麼

您必須具有應用程式管理員角色。

此設定會影響所有登入的使用者工作階段。

> 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、選擇下列其中一個選項來指定閒置逾時：

如果您想要...	然後執行此動作...
未設定逾時、因此工作階段不會自動關閉	在「無活動逾時」面板中、將滑桿按鈕移至左側（關閉）、然後按一下「套用」。
將特定分鐘數設為逾時值	在「無活動逾時」面板中、將滑桿按鈕移到右側（開啟）、以分鐘為單位指定無活動逾時值、然後按一下「套用」。

變更**Unified Manager**主機名稱

有時候、您可能想要變更已安裝Unified Manager的系統主機名稱。例如、您可能想要重新命名主機、以便更輕鬆地依類型、工作群組或受監控的叢集群組識別Unified Manager伺服器。

變更主機名稱所需的步驟各不相同、視Unified Manager是在VMware ESXi伺服器、Red Hat或CentOS Linux伺服器或Microsoft Windows伺服器上執行而定。

變更**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、會為網路主機指派一個名稱。您可以在部署後變更主機名稱。如果變更主機名稱、也必須重新產生HTTPS憑證。

您需要的是什麼

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給您、才能執行這些工作。

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、則表示您已為網路主機指定名稱。如果使用DHCP設定網路、則主機名稱應取自DNS。如果未正確設定DHCP或DNS、系統會自動指派主機名稱「'Unified Manager'」、並與安全性憑證建立關聯。

無論主機名稱的指派方式為何、如果您變更主機名稱、並打算使用新的主機名稱來存取Unified Manager Web UI、您都必須產生新的安全性憑證。

如果您使用伺服器的IP位址而非主機名稱來存取Web UI、則如果變更主機名稱、就不需要產生新的憑證。不過、最好更新憑證、使憑證中的主機名稱與實際主機名稱相符。

如果您在Unified Manager中變更主機名稱、則必須手動更新OnCommand Workflow Automation BIOS（WFA）中的主機名稱。在WFA中不會自動更新主機名稱。

在Unified Manager虛擬機器重新啟動之前、新的憑證不會生效。

步驟

1. 產生HTTPS安全性憑證

   如果您想要使用新的主機名稱來存取Unified Manager Web UI、則必須重新產生HTTPS憑證、才能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憑證之後、您必須重新啟動Unified Manager虛擬機器。

產生**HTTPS**安全性憑證

首次安裝時、會安裝預設的HTTPS憑證。Active IQ Unified Manager您可能會產生新的HTTPS安全性憑證來取代現有的憑證。

您需要的是什麼

您必須具有應用程式管理員角色。

重新產生憑證可能有多種原因、例如您想要擁有更好的辨別名稱（DN）值、或是想要較高的金鑰大小、或是較長的過期期間、或是目前的憑證已過期。

如果您無法存取Unified Manager Web UI、可以使用維護主控台重新產生具有相同值的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。如果您從維護主控台使用「重設伺服器憑證」選項、則會建立新的HTTPS憑證、有效期為397天。此憑證的RSA金鑰大小為2048位元。

步驟

1. 在左導覽窗格中、按一下*一般*>* HTTPS憑證*。
2. 按一下*重新產生HTTPS憑證*。

   此時會顯示重新產生HTTPS憑證對話方塊。

3. 根據您要產生憑證的方式、選取下列其中一個選項：

如果您想要...	執行此動作...
以目前值重新產生憑證	按一下*使用目前的憑證屬性重新產生*選項。

如果您想要...	執行此動作...
使用不同的值產生憑證	按一下*更新目前的憑證屬性*選項。 如果您未輸入新值、「一般名稱」和「替代名稱」欄位會使用現有憑證的值。「Common Name」（一般名稱）應設定為主機的FQDN。其他欄位不需要值、但您可以輸入值、例如電子郵件、公司、部門、 城市、州/省和國家/地區（如果您希望在證書中填入這些值）。您也可以從可用的金鑰大小（金鑰演算法為「'rSA'」）和有效期間中進行選擇。 • 允許的金鑰大小值為「2048」、「3072」和「4096」。 • 有效期間最短為1天、最長為36500天。 即使允許使用36500天的有效期間、建議您使用不超過397天或13個月的有效期間。因為如果您選取超過3997天的有效期間、並計畫匯出此憑證的CSR並由已知的CA簽署、CA傳回給您的已簽署憑證的有效性將減至3997天。 • 如果您要從憑證的替代名稱欄位中移除本機識別資訊、可以選取「排除本機識別資訊（例如localhost）」核取方塊。選取此核取方塊時、替代名稱欄位中只會使用您在欄位中輸入的內容。如果保留空白、則產生的憑證將完全沒有替代名稱欄位。

4. 按一下「是」以重新產生憑證。
5. 重新啟動Unified Manager伺服器、使新的憑證生效。

檢視HTTPS憑證來驗證新的憑證資訊。

重新啟動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。您必須在產生新的安全性憑證之後重新啟動、或是虛擬機器發生問題時重新啟動。

您需要的是什麼

虛擬應用裝置已開啟電源。

您會以維護使用者的身分登入維護主控台。

您也可以使用*重新啟動客戶*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. 存取維護主控台。
2. 選擇*系統組態*>*重新開機虛擬機器*。

變更**Linux**系統上的**Unified Manager**主機名稱

有時候、您可能想要變更已安裝Unified Manager的Red Hat Enterprise Linux或CentOS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、更輕鬆地依類型、工作群組或受監控的叢集群組識別Unified Manager伺服器。

您需要的是什麼

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

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、則表示您已為網路主機指定名稱。如果使用DHCP設定網路、則主機名稱應取自DNS伺服器。

無論主機名稱的指派方式為何、如果您變更主機名稱並打算使用新的主機名稱來存取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位址而非主機名稱來存取Web UI、則如果變更主機名稱、就不需要產生新的憑證。不過、更新憑證是最佳實務做法、以便憑證中的主機名稱與實際主機名稱相符。新的憑證在Linux機器重新啟動之前不會生效。

如果您在Unified Manager中變更主機名稱、則必須手動更新OnCommand Workflow Automation BIOS（WFA）中的主機名稱。在WFA中不會自動更新主機名稱。

步驟

1. 以root使用者身分登入您要修改的Unified Manager系統。
2. 輸入下列命令、停止Unified Manager軟體及相關的MySQL軟體：

   《神祕世界》

3. 使用Linux "hostnamel"命令變更主機名稱：

   「hostnamel Set-hostnamenew_FQDN」

   「hostnamel Set-hostnamenuhost.corp.widget.com」

4. 重新產生伺服器的HTTPS憑證：

   /`opt/NetApp/inapp/inapp/cert.sh cree'

5. 重新啟動網路服務：

   '服務網路重新啟動'

6. 重新啟動服務之後、請確認新的主機名稱是否能夠ping通自己：

"ping new_hostname"

"ping nuhost"

此命令應傳回先前針對原始主機名稱所設定的相同IP位址。

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

《神祕世界》（Mystemcl start mysqld ocie ocieau）

啟用及停用原則型儲存管理

從Unified Manager 9.7開始、您可以在ONTAP 您的VMware叢集上配置儲存工作負載（Volume和LUN）、並根據指派的效能服務層級來管理這些工作負載。這項功能類似ONTAP 於在《S21系統管理程式》中建立工作負載、並附加QoS原則、但當您使用Unified Manager套用時、您可以在Unified Manager執行個體所監控的所有叢集上配置及管理工作負載。

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來配置及管理工作負載、則可以停用此選項。

啟用時、此選項會在使用者介面中提供許多新項目：

新內容	位置
提供新工作負載的頁面	可從*一般工作*>*資源配置*取得
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
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
說明您目前工作負載效能與工作負載IOPS的面板	可從儀表板取得

請參閱產品的線上說明、以取得這些頁面及此功能的詳細資訊。

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、選擇下列其中一個選項來停用或啟用原則型儲存管理：

如果您想要...	然後執行此動作...
停用原則型儲存管理	在「原則型儲存管理」面板中、將滑桿按鈕移到左邊。
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Unified Manager備份

您可以透過一組設定步驟、在Unified Manager上設定備份功能、以便在主機系統上執行、並透過維護主控台執行。

如需組態步驟的相關資訊、請參閱 "管理備份與還原作業"。

管理功能設定

「功能設定」頁面可讓您啟用及停用Active IQ Unified Manager 功能。這包括根據原則建立及管理儲存物件、啟用API閘道和登入橫幅、上傳用於管理警示的指令碼、根據閒置時間逾時網路UI工作階段、以及停用接收Active IQ 到的更新平台事件。

> 「功能設定」頁面僅適用於具有應用程式管理員角色的使用者。

如需指令碼上傳的相關資訊、請參閱 "啟用及停用指令碼上傳"。

實現原則型儲存管理

*原則型儲存管理*選項可根據服務層級目標（SLO）進行儲存管理。此選項預設為啟用。

啟用此功能時、您可以在ONTAP 新增Active IQ Unified Manager 至您的物件執行個體的物件叢集上配置儲存工作負載、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*>*原則型儲存管理*選擇啟動或停用此功能。啟動此功能時、下列頁面可供操作及監控：

- 資源配置（儲存工作負載資源配置）
- 原則>*效能服務層級*
- 原則>*儲存效率*
- 「叢集設定」頁面上的「依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

您可以使用畫面來建立效能服務層級和儲存效率原則、以及配置儲存工作負載。您也可以監控符合指派之效能服務層級的儲存工作負載、以及不符合的工作負載。「工作負載效能與工作負載IOPS」面板也可讓您根據資料中心上所配置的儲存工作負載、評估整個資料中心叢集的總容量、可用容量及已使用容量與效能（IOPS）。

啟動此功能之後、您可以執行Unified Manager REST API、從*功能表列*>*說明按鈕*>* API Documentation *>*儲存設備供應商*類別執行部分功能。或者、您也可以輸入主機名稱或IP位址和URL、以+https://<hostname>/docs/api/+格式存取REST API頁面

如需API的詳細資訊、請參閱 "開始使用Active IQ Unified Manager 靜態API"

啟用**API**閘道

API閘道功能可Active IQ Unified Manager 讓支援不ONTAP 需個別登入即可從單一控制面

板管理多個支援叢集。

您可以從第一次登入Unified Manager時出現的組態頁面啟用此功能。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 R靜止API不同、ONTAP 並非所有的功能都能透過Unified Manager REST API使用。不過、如果您有特定的業務需求、需要存取ONTAP 不公開給Unified Manager的各項功能、以管理特定功能的各項功能、您可以啟用API閘道功能並執行ONTAP IsfAPI。閘道會做為Proxy、以ONTAP 相同格式維護介面標頭和實體要求、使API要求通道化。您可以使用Unified Manager認證資料並執行特定API來存取及管理ONTAP 等功能、而無需傳遞個別的叢集認證資料。Unified Manager可做為單一管理點、在ONTAP 由Unified Manager執行個體管理的整個叢集上執行API。API傳回的回應與直接ONTAP 從ONTAP 原地執行的個別REST API所傳回的回應相同。

啟用此功能之後、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、您也可以輸入主機名稱或IP位址和URL、以「https://<hostname>/docs/api/`」格式存取REST API頁面

如需API的詳細資訊、請參閱 "開始使用Active IQ Unified Manager 靜態API"。

指定不活動逾時

您可以指定Active IQ Unified Manager 不活動逾時值以供使用。在指定時間內無活動之後、應用程式會自動登出。此選項預設為啟用。

您可以停用此功能、或從*一般*>*功能設定*>*無活動逾時*修改時間。啟動此功能後、您應該在*登出時間*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。

啟用**Active IQ** 入口網站活動

您可以指定是否要啟用或停用Active IQ 入口網站的功能。此設定可讓Active IQ 入口網站探索及顯示有關系統組態、纜線等的其他事件。此選項預設為啟用。

啟用此功能時Active IQ Unified Manager 、支援的功能會顯示Active IQ 由這個入口網站發現的事件。這些事件是透過針對AutoSupport 所有受監控儲存系統產生的各種資訊、執行一組規則來建立。這些事件與其他Unified Manager事件不同、可識別與系統組態、佈線、最佳實務做法和可用度相關的事件或風險。

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。在無法存取外部網路的站台中、您必須從* Storage Management **>** Event Setup *>*上傳規則*手動上傳規則。

此功能預設為啟用。停用此功能可停止Active IQ 在Unified Manager上發現或顯示不實的事件。停用時、啟用此功能可讓Unified Manager在Active IQ 叢集時區的預先定義時間00：15接收叢集上的各種事件。

啟用及停用安全性設定以符合法規要求

使用「功能設定」頁面的「安全性儀表板」面板上的*自訂*按鈕、即可在Unified Manager上啟用或停用法規遵循監控的安全參數。

此頁面啟用或停用的設定、會管理Unified Manager上叢集和儲存VM的整體法規遵循狀態。根據所選內容、對應的欄位可在「叢集」清單頁面的「安全性：所有叢集」檢視和「儲存VM」目錄頁的「安全性：所有儲存**VM**」檢

視中看到。

> 只有具備系統管理員角色的使用者才能編輯這些設定。

根據中定義的建議、評估您的叢集、儲存VM和Volume的安全性條件ONTAP "《NetApp ONTAP 安全強化指南》9"。儀表板和「安全性」頁面上的「安全性」面板會顯示叢集、儲存VM和磁碟區的預設安全性法規遵循狀態。也會針對發生安全性違規的叢集和儲存VM、產生安全性事件並啟用管理動作。

自訂安全性設定

若要根據ONTAP 您的需求自訂法規遵循監控的設定、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*。「自訂安全性儀表板設定」快顯視窗隨即出現。

> 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Excel報告、則下載的Excel報告可能有問題。

2. 若要啟用或停用ONTAP 您的還原叢集的自訂設定、請在*叢集*下選取所需的一般設定。如需自訂叢集規範選項的相關資訊、請參閱 "叢集規範類別"
3. 若要啟用或停用儲存VM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VM法規遵循選項的相關資訊、請參閱 "儲存VM法規遵循類別"。

自訂**AutoSupport** 功能與驗證設定

在* AutoSupport 《》「設定」區段中、您可以指定是否要使用HTTPS傳輸來傳送AutoSupport 來自該區域的訊息ONTAP 。

從*驗證設定*區段、您可以針對預設ONTAP 的管理員使用者、啟用Unified Manager警示。

啟用及停用指令碼上傳

預設會啟用將指令碼上傳至Unified Manager並執行的功能。如果貴組織因為安全理由而不想允許此活動、您可以停用此功能。

您需要的是什麼

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*一般*>*功能設定*。
2. 在「功能設定」頁面中、選擇下列其中一個選項來停用或啟用指令碼：

如果您想要...	然後執行此動作...
停用指令碼	在「指令碼上傳」面板中、將滑桿按鈕移到左邊。
啟用指令碼	在「指令碼上傳」面板中、將滑桿按鈕移到右側。

新增登入橫幅

新增登入橫幅可讓貴組織顯示任何資訊、例如允許存取系統的人員、以及登入和登出期間的使用條款與條件。

任何使用者（例如儲存設備操作員或系統管理員）都可以在登入、登出及工作階段逾時期間檢視此登入橫幅快顯視窗。

使用維護主控台

您可以使用維護主控台來設定網路設定、設定及管理安裝Unified Manager的系統、以及執行其他維護工作、以協助您預防及疑難排解可能的問題。

維護主控台提供哪些功能

Unified Manager維護主控台可讓您維護Unified Manager系統上的設定、並進行必要的變更、以避免發生問題。

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Unified Manager網路介面無法使用時
- 升級至較新版本的Unified Manager
- 產生支援服務組合以傳送給技術支援人員
- 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
- 變更內部的效能資料收集
- 從先前備份的版本還原Unified Manager資料庫和組態設定。

維護使用者的功能

維護使用者是在Red Hat Enterprise Linux或CentOS系統上安裝Unified Manager時建立。維護使用者名稱為「umadmin」使用者。維護使用者在Web UI中具有應用程式管理員角色、而且該使用者可以建立後續的使用者並指派角色。

維護使用者或umadmin使用者也可以存取Unified Manager維護主控台。

診斷使用者功能

診斷存取的目的是讓技術支援人員協助您進行疑難排解、您只能在技術支援人員的指示下使用。

診斷使用者可在技術支援指示下執行OS層級命令、以進行疑難排解。

存取維護主控台

如果Unified Manager使用者介面未運作、或是您需要執行使用者介面中未提供的功能、您可以存取維護主控台來管理Unified Manager系統。

您需要的是什麼

您必須已安裝並設定Unified Manager。

在閒置15分鐘後、維護主控台會將您登出。

> 安裝在VMware上時、如果您已透過VMware主控台以維護使用者身分登入、則無法使用Secure Shell同時登入。

步驟

1. 請依照下列步驟存取維護主控台：

在此作業系統上...	請遵循下列步驟...
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「maintainess_Console」、然後按Enter。
Windows	a. 以系統管理員認證登入Unified Manager系統。 b. 以Windows系統管理員身分啟動PowerShell。 c. 輸入命令「maintainess_Console」、然後按Enter。

此時會顯示Unified Manager維護主控台功能表。

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、或是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重新設定虛擬應用裝置。

您需要的是什麼

- 您必須是維護使用者。
- 必須開啟虛擬應用裝置電源、才能存取維護主控台。

步驟

1. 在vSphere Client中、找出Unified Manager虛擬應用裝置。
2. 按一下*主控台*索引標籤。
3. 按一下主控台視窗內的即可登入。
4. 使用您的使用者名稱和密碼登入維護主控台。

   在閒置15分鐘後、維護主控台會將您登出。

維護主控台功能表

維護主控台包含不同的功能表、可讓您維護及管理Unified Manager伺服器的特殊功能和組態設定。

根據您安裝Unified Manager的作業系統、維護主控台包含下列功能表：

- 升級Unified Manager（僅限VMware）
- 網路組態（僅限VMware）
- 系統組態（僅限VMware）
- 支援/診斷
- 重設伺服器憑證
- 外部資料提供者
- 效能輪詢時間間隔組態

網路組態功能表

「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、CentOS或Microsoft Windows上、則無法使用此功能表。

下列功能表選項可供使用。

- 顯示**IP**位址設定

顯示虛擬應用裝置目前的網路設定、包括IP位址、網路、廣播位址、網路遮罩、閘道、 和DNS伺服器。

- 變更**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切換為靜態網路、則無法編輯主機名稱。您必須選取*提交變更*、變更才會生效。

- 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*、變更才會生效。

- 顯示靜態路由

  顯示目前的靜態網路路由。

- 變更靜態路由

  可讓您新增或刪除靜態網路路由。您必須選取*提交變更*、變更才會生效。

  - 新增路由

    可讓您新增靜態路由。

  - 刪除路由

    可讓您刪除靜態路由。

  - 返回

    返回*主功能表*。

  - 退出

    結束維護主控台。

- 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、您就無法停用它。您必須選取*提交變更*、變更才會生效。

- 啟用網路介面

  啟用可用的網路介面。您必須選取*提交變更*、變更才會生效。

- 提交變更

  套用對虛擬應用裝置的網路設定所做的任何變更。您必須選取此選項、才能執行任何變更、或是變更不會發生。

- * Ping主機*

  Ping目標主機以確認IP位址變更或DNS組態。

- 還原為預設設定

  將所有設定重設為原廠預設值。您必須選取*提交變更*、變更才會生效。

- 返回

  返回*主功能表*。

- 退出

  結束維護主控台。

系統組態功能表

System Configuration（系統組態）功能表可讓您提供各種選項來管理虛擬應用裝置、例如檢視伺服器狀態、以及重新開機和關閉虛擬機器。

> 當Unified Manager安裝在Linux或Microsoft Windows系統上時、此功能表僅提供「從Unified Manager Backup還原」選項。

以下是可用的功能表選項：

- 顯示伺服器狀態

  顯示目前的伺服器狀態。狀態選項包括「執行中」和「未執行中」。

  如果伺服器未執行、您可能需要聯絡技術支援部門。

- 重新啟動虛擬機器

  重新啟動虛擬機器、停止所有服務。重新開機之後、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。

  您只能從虛擬機器主控台選取此選項。

- 變更<登入使用者>使用者密碼

  變更目前登入的使用者密碼、只能是維護使用者。

- 增加資料磁碟大小

  增加虛擬機器中的資料磁碟（磁碟3）大小。

- 增加交換磁碟大小

增加虛擬機器中的交換磁碟（磁碟2）大小。

- 變更時區

  將時區變更為您所在的位置。

- 變更**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）。

- 變更**NTP**服務

  在「NTP」和「系統時間yncdd」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。

- 變更主機名稱

  變更安裝虛擬應用裝置的主機名稱。

- 返回

  退出系統組態功能表、然後返回主功能表。

- 退出

  結束維護主控台功能表。

支援與診斷功能表

「支援與診斷」功能表可讓您產生支援服務組合、以便傳送給技術支援人員以取得疑難排解協助。

下列功能表選項可供使用：

- 產生輕度支援產品組合

  可讓您產生一個輕量級支援套件、其中僅包含30天的記錄和組態資料庫記錄、不包括效能資料、擷取記錄檔和伺服器堆疊傾印。

- 產生支援產品組合

  可讓您建立完整的支援套裝組合（7-Zip檔案）、其中包含診斷使用者主目錄中的診斷資訊。如果您的系統已連線至網際網路、您也可以將支援服務組合上傳至NetApp。

  此檔案包含AutoSupport 由下列項目所產生的資訊：消息內容、Unified Manager資料庫內容、Unified

Manager伺服器內部環境的詳細資料、AutoSupport 以及通常不包含在消息中或輕量級支援組合中的詳細層級記錄。

其他功能表選項

下列功能表選項可讓您在Unified Manager伺服器上執行各種管理工作。

以下是可用的功能表選項：

- 重設伺服器憑證

  重新產生HTTPS伺服器憑證。

  您可以按一下「一般」>「* 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、使身分識別供應商（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組態問題阻礙使用者存取Unified Manager GUI時、通常會使用此主控台選項。

- 外部資料提供者

  提供將Unified Manager連線至外部資料供應商的選項。建立連線之後、效能資料會傳送至外部伺服器、讓儲存效能專家能夠使用協力廠商軟體來記錄效能指標。畫面會顯示下列選項：

  - 顯示伺服器組態-顯示外部資料提供者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提供者的新連線設定、或是變更現有的設定。
  - 修改伺服器組態-可讓您輸入外部資料提供者的新組態設定、或是變更現有的設定。
  - 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會失去與外部伺服器的連線。

- 效能輪詢時間間隔組態

  提供選項、可設定Unified Manager從叢集收集效能統計資料的頻率。預設收集時間間隔為5分鐘。

  如果發現大型叢集的集合未準時完成、您可以將此時間間隔變更為10或15分鐘。

- 檢視/變更應用程式連接埠

  提供選項、可變更Unified Manager用於HTTP和HTTPS傳輸協定的預設連接埠（若安全性需要）。HTTP預設連接埠為80、HTTPS預設連接埠為443。

- 退出

  結束維護主控台功能表。

變更Windows上的維護使用者密碼

您可以視需要變更Unified Manager維護使用者密碼。

步驟

1. 在Unified Manager Web UI登入頁面中、按一下*忘記密碼*。

   畫面會顯示一個頁面、提示您輸入要重設密碼的使用者名稱。

2. 輸入使用者名稱、然後按一下*提交*。

   含有重設密碼連結的電子郵件會傳送至針對該使用者名稱所定義的電子郵件地址。

3. 按一下電子郵件中的*重設密碼連結*、然後定義新密碼。
4. 返回網路UI、然後使用新密碼登入Unified Manager。

變更Linux系統上的umadmin密碼

基於安全考量、您必須在完成安裝程序之後、立即變更Unified Manager umadmin使用者的預設密碼。如有必要、您可以稍後再變更密碼。

您需要的是什麼

- Unified Manager必須安裝在Red Hat Enterprise Linux或CentOS Linux系統上。
- 您必須擁有安裝Unified Manager的Linux系統的root使用者認證資料。

步驟

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

   「passwdadmin umadmin」

   系統會提示您輸入umadmin使用者的新密碼。

變更Unified Manager用於HTTP和HTTPS傳輸協定的連接埠

Unified Manager用於HTTP和HTTPS傳輸協定的預設連接埠、可在安裝後視安全性需求加以變更。HTTP預設連接埠為80、HTTPS預設連接埠為443。

您需要的是什麼

您必須擁有授權使用者ID和密碼、才能登入Unified Manager伺服器的維護主控台。

> 有些連接埠在使用Mozilla Firefox或Google Chrome瀏覽器時被視為不安全。在為HTTP和HTTPS流量指派新的連接埠號碼之前、請先查看瀏覽器。選取不安全的連接埠可能會使系統無法存取、因此您必須聯絡客戶支援部門以取得解決方案。

變更連接埠後、Unified Manager執行個體會自動重新啟動、因此請務必在短時間內讓系統停機。

1. 以SSH作為維護使用者登入Unified Manager主機。

   此時會顯示Unified Manager維護主控台提示。

2. 輸入標有*檢視/變更應用程式連接埠*的功能表選項編號、然後按Enter。
3. 如果出現提示、請再次輸入維護使用者密碼。
4. 輸入HTTP和HTTPS連接埠的新連接埠號碼、然後按Enter。

   將連接埠號碼保留空白、會指派該傳輸協定的預設連接埠。

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

5. 輸入* y*以變更連接埠、然後重新啟動Unified Manager。
6. 離開維護主控台。

變更完成後、使用者必須在URL中加入新的連接埠號碼、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。

新增網路介面

如果需要分隔網路流量、您可以新增網路介面。

您需要的是什麼

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、則無法執行此作業。

步驟

1. 在vSphere主功能表中、選取*系統組態*>*重新開機作業系統*。

   重新開機後、維護主控台即可偵測新增的網路介面。

2. 存取維護主控台。
3. 選擇*網路組態*>*啟用網路介面*。
4. 選擇新的網路介面、然後按* Enter *。

   選擇* eth1*並按* Enter *。

5. 鍵入* 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。

   輸入網路設定之後、您會自動返回*網路組態*功能表。

7. 選擇*提交變更*。

   您必須提交變更以新增網路介面。

將磁碟空間新增至**Unified Manager**資料庫目錄

Unified Manager資料庫目錄包含ONTAP 從VMware系統收集到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從大量叢集收集資料、而每個叢集都有許多節點、則資料庫目錄可能會滿。當資料庫目錄已滿90%時、您將會收到警告事件、而當目錄已滿95%時、您將會收到重大事件。

> 在目錄達到95%滿量後、不會從叢集收集其他資料。

新增容量至資料目錄所需的步驟各不相同、取決於Unified Manager是在VMware ESXi伺服器、Red Hat或CentOS Linux伺服器、還是在Microsoft Windows伺服器上執行。

將空間新增至**Linux**主機的資料目錄

如果您在最初設定Linux主機並安裝Unified Manager時、將磁碟空間不足分配給「/opt/NetApp/data」目錄以支援Unified Manager、則可在安裝後增加磁碟空間、方法是在「/opt/NetApp/data」目錄中增加磁碟空間。

您需要的是什麼

您必須擁有root使用者存取權、才能存取安裝Unified Manager的Red Hat Enterprise Linux或CentOS Linux機器。

建議您先備份Unified Manager資料庫、再增加資料目錄的大小。

步驟

1. 以root使用者身分登入您要新增磁碟空間的Linux機器。
2. 依照下列順序停止Unified Manager服務及相關的MySQL軟體：

   《神祕世界》

3. 建立具有足夠磁碟空間的暫用備份資料夾（例如：「/backup-data」）、以將資料包含在目前的「/opt/NetApp/data」目錄中。
4. 將現有的「/opt/NetApp/data（選擇/ NetApp）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. 如果已啟用SE Linux：

   a. 在現有的「/opt/NetApp/data」資料夾中取得資料夾的SE Linux類型：

      「ls-Z /opt/netapp/data」| awk「｛print $4｝」| awk -F：「｛print $3｝」|標頭-1

      系統會傳回類似下列的確認訊息：

```
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（選擇/ NetApp /資料）目錄的內容：
   a. 「CD /opt/NetApp/data」
   b. 「rm -RF *」
7. 透過LVM命令或新增額外的磁碟、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了「/opt/NetApp/data」、則不應嘗試將「/ops/NetApp/data」掛載為NFS或CIFS共用。在這種情況下、如果您嘗試擴充磁碟空間、某些LVM命令（例如「大小」和「擴充」）可能無法如預期般運作。

8. 確認「/opt/NetApp/data'目錄擁有者（mySQL）和群組（root）沒有變更：

「ls -ltr /opt/netapp/| grep data」

系統會傳回類似下列的確認訊息：

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

9. 如果已啟用SE Linux、請確認「/opt/netapp/data'」目錄的內容仍設定為mysqld_db_t:
   a. 「Touch /opt/NetApp/data/abc」
   b. 「ls -Z /opt/NetApp/data/abc」

   系統會傳回類似下列的確認訊息：

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

10. 刪除abc檔案、以避免此無關檔案在未來造成資料庫錯誤。
11. 將內容從備份資料複製回擴充的「/ope/NetApp/data'目錄：

「cp -arp /backup-data/*/opt/NetApp/data/」

12. 如果已啟用SE Linux、請執行下列命令：

「chcon -R --type=mysqld_db_t /opp/netapp/data'

13. 啟動MySQL服務：

《stystemctl start mysqld》

14. MySQL服務啟動後、請依下列順序啟動ocie和ocieau服務：

    《神祕之星》

15. 所有服務啟動後、請刪除備份資料夾「/backup-data」：

    「rm -rf /backup-data」

為**VMware**虛擬機器的資料磁碟增加空間

如果您需要增加Unified Manager資料庫的資料磁碟空間、可以使用Unified Manager維護主控台增加磁碟空間、在安裝後新增容量。

您需要的是什麼

- 您必須擁有vSphere Client的存取權。
- 虛擬機器不得在本機儲存任何快照。
- 您必須擁有維護使用者認證資料。

建議您在增加虛擬磁碟大小之前先備份虛擬機器。

步驟

1. 在vSphere用戶端中、選取Unified Manager虛擬機器、然後在資料「磁碟3」中新增更多磁碟容量。如需詳細資料、請參閱VMware文件。

   在某些罕見的情況下、Unified Manager部署會使用「硬碟2」作為資料磁碟、而非「硬碟3」。如果您的部署發生這種情況、請增加任何較大磁碟的空間。資料磁碟的空間永遠會比其他磁碟更多。

2. 在vSphere用戶端中、選取Unified Manager虛擬機器、然後選取*主控台*索引標籤。
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. 在主功能表中、輸入*系統組態*選項的編號。
5. 在System Configuration Menu（系統組態功能表）中、輸入「增加資料磁碟大小」選項的編號。

為**Microsoft Windows**伺服器的邏輯磁碟機增加空間

如果您需要增加Unified Manager資料庫的磁碟空間量、可以將容量新增至安裝Unified Manager的邏輯磁碟機。

您需要的是什麼

您必須擁有Windows系統管理員權限。

建議您在新增磁碟空間之前先備份Unified Manager資料庫。

步驟

1. 以系統管理員身分登入您要新增磁碟空間的Windows伺服器。

2. 依照您要用來新增更多空間的方法所對應的步驟進行：

選項	說明
在實體伺服器上、新增容量至安裝Unified Manager伺服器的邏輯磁碟機。	請依照Microsoft主題中的步驟進行： "擴充基本Volume"
在實體伺服器上、新增硬碟機。	請依照Microsoft主題中的步驟進行： "新增硬碟機"
在虛擬機器上、增加磁碟分割區的大小。	請遵循VMware主題中的步驟： "增加磁碟分割區的大小"

管理使用者存取

您可以建立角色並指派功能、以控制使用者對所選叢集物件的存取。您可以識別擁有所需功能的使用者、以存取叢集內的選定物件。只有這些使用者可以存取、以管理叢集物件。

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群組。您可以指派角色給這些使用者、並根據角色權限、使用者可以使用Unified Manager管理儲存物件和資料、或是檢視資料庫中的資料。

您需要的是什麼

- 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、您必須啟用遠端驗證並設定驗證伺服器。
- 如果您打算設定SAML驗證、讓身分識別供應商（IDP）驗證存取圖形介面的使用者、請確定這些使用者定義為「即時」使用者。

  啟用SAML驗證時、不允許「'local'」或「maintenfiting'」類型的使用者存取UI。

如果您從Windows Active Directory新增群組、則除非停用巢狀子群組、否則所有的直接成員和巢狀子群組都可以驗證Unified Manager。如果您從OpenLDAP或其他驗證服務新增群組、則只有該群組的直接成員可以驗證Unified Manager。

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、選取您要新增的使用者類型、然後輸入所需資訊。

輸入所需的使用者資訊時、您必須指定該使用者專屬的電子郵件地址。您必須避免指定由多位使用者共用的電子郵件地址。

4. 按一下「 * 新增 * 」。

建立資料庫使用者

若要支援Workflow Automation與Unified Manager之間的連線、或是存取資料庫檢視、您必須先在Unified Manager Web UI中建立具有整合架構或報告架構角色的資料庫使用者。

您需要的是什麼

您必須具有應用程式管理員角色。

資料庫使用者可與Workflow Automation整合、並存取報告特定的資料庫檢視。資料庫使用者無法存取Unified Manager Web UI或維護主控台、因此無法執行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」對話方塊的「類型」下拉式清單中、選取「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*下拉式清單中、選取適當的角色。

如果您...	請選擇此角色
將Unified Manager與Workflow Automation連線	整合架構
存取報告和其他資料庫檢視	報告架構

6. 按一下「 * 新增 * 」。

編輯使用者設定

您可以編輯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、您可能想要變更儲存操作員使用者的角色、並將儲存管理員權限指派給使用者。

您需要的是什麼

您必須具有應用程式管理員角色。

當您修改指派給使用者的角色時、會在發生下列任一動作時套用變更：

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

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、選取您要編輯其設定的使用者、然後按一下*編輯*。
3. 在「編輯使用者」對話方塊中、編輯為使用者指定的適當設定。
4. 按一下「 * 儲存 * 」。

檢視使用者

您可以使用「使用者」頁面來檢視使用Unified Manager管理儲存物件和資料的使用者清單。您可以檢視使用者的詳細資料、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。

您需要的是什麼

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*一般*>*使用者*。

刪除使用者或群組

您可以從管理伺服器資料庫刪除一或多位使用者、以防止特定使用者存取Unified Manager。您也可以刪除群組、讓群組中的所有使用者都無法再存取管理伺服器。

您需要的是什麼

- 刪除遠端群組時、您必須重新指派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會自動取消指派。

- 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*一般*>*使用者*。
2. 在「使用者」頁面中、選取您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。

什麼是**RBAC**

RBAC（角色型存取控制）可讓您控制哪些人可以存取Active IQ Unified Manager 支援伺服器中的各種功能和資源。

以角色為基礎的存取控制功能

角色型存取控制（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所選的系統管理員、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及其可執行的作業、您必須將角色套用至您所建

立的系統管理員帳戶。

管理伺服器會使用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、則不需要登入即可檢視這些設定。

當您啟動需要特定權限的作業時、管理伺服器會提示您登入。例如、若要建立系統管理員帳戶、您必須以應用程式管理員帳戶存取權登入。

使用者類型定義

使用者類型會指定使用者擁有的帳戶類型、包括遠端使用者、遠端群組、本機使用者、資料庫使用者及維護使用者。每種類型都有自己的角色、由具有管理員角色的使用者指派。

Unified Manager使用者類型如下：

- 維護使用者

  在Unified Manager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能夠存取維護主控台的使用者。當Unified Manager安裝在Red Hat Enterprise Linux或CentOS系統上時、維護使用者會獲得「umadmin」使用者名稱。

- 本機使用者

  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所提供的角色執行功能。

- 遠端群組

  一組使用驗證伺服器上儲存的認證來存取Unified Manager UI的使用者。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會使用各自的使用者認證來存取Unified Manager UI。遠端群組可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認證資料存取Unified Manager UI。遠端使用者會根據維護使用者或具有應用程式管理員角色的使用者所提供的角色來執行功能。

- 資料庫使用者

  擁有Unified Manager資料庫中資料的唯讀存取權、無法存取Unified Manager網路介面或維護主控台、也無法執行API呼叫。

使用者角色定義

維護使用者或應用程式管理員會指派角色給每位使用者。每個角色都包含特定權限。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包含下列預先定義的使用者角色：

- 營運者

檢視由Unified Manager收集的儲存系統資訊和其他資料、包括歷史記錄和容量趨勢。此角色可讓儲存操作員檢視、指派、認可、解決及新增事件的備註。

- 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、並建立警示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,網路和AutoSupport

  > 在Linux系統上安裝Unified Manager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」。

- 整合架構

  此角色可讓您以唯讀方式存取Unified Manager資料庫檢視、以整合Unified Manager OnCommand Workflow Automation 與WFA（WFA）。

- 報告架構

  此角色可讓您直接從Unified Manager資料庫、以唯讀方式存取報告和其他資料庫檢視。可檢視的資料庫包括：

  - NetApp_mode_view
  - NetApp_Performance
  - 奧克姆
  - ocum_report
  - ocum_report_BIRT
  - OPM
  - scalemonitor

Unified Manager使用者角色與功能

根據指派的使用者角色、您可以決定可以在Unified Manager中執行哪些作業。

下表顯示每個使用者角色可以執行的功能：

功能	營運者	儲存管理員	應用程式管理員	整合架構	報告架構
檢視儲存系統資訊	•	•	•	•	•
檢視其他資料、例如歷史記錄和容量趨勢	•	•	•	•	•

功能	營運者	儲存管理員	應用程式管理員	整合架構	報告架構
檢視、指派及解決事件	•	•	•		
檢視儲存服務物件、例如SVM關聯和資源集區	•	•	•		
檢視臨界值原則	•	•	•		
管理儲存服務物件、例如SVM關聯和資源集區		•	•		
定義警示		•	•		
管理儲存管理選項		•	•		
管理儲存管理原則		•	•		
管理使用者			•		
管理管理選項			•		
定義臨界值原則			•		
管理資料庫存取			•		
管理與WFA的整合、並提供資料庫檢視的存取權限				•	
排程及儲存報告		•	•		
從管理行動執行「修復」作業		•	•		
提供資料庫檢視的唯讀存取權					•

管理SAML驗證設定

設定遠端驗證設定之後、您可以啟用安全聲明標記語言（SAML）驗證、讓遠端使用者先經過安全身分識別供應商（IDP）的驗證、才能存取Unified Manager Web UI。

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。

身分識別供應商要求

將Unified Manager設定為使用身分識別供應商（IDP）來為所有遠端使用者執行SAML驗證時、您必須知道某些必要的組態設定、才能成功連線至Unified Manager。

您必須在IDP伺服器中輸入Unified Manager URI和中繼資料。您可以從Unified ManagerSAML驗證頁面複製此資訊。Unified Manager被視為安全性聲明標記語言（SAML）標準中的服務供應商（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

已驗證的身分識別供應商

- Shibboleth
- Active Directory Federation Services（ADFS）

ADFS組態需求

- 您必須依下列順序定義三個宣告規則、Unified Manager才能剖析此信賴方信任項目的ADFS SAML回應。

請款規則	價值
Sam-account-name	名稱ID
Sam-account-name	urn:oID：0.9.2342.19200300.1001.1
權杖群組-不合格的名稱	urn:oID：1.3.6.1.4.1.5923.1.5.1.1

- 您必須將驗證方法設定為「Forms驗證」、否則使用者在登出Unified Manager時可能會收到錯誤訊息。請遵循下列步驟：
  a. 開啟ADFS管理主控台。
  b. 按一下左樹狀檢視中的「驗證原則」資料夾。
  c. 在右側的「Actions（動作）」下、按一下「Edit Global Primary驗證Policy（編輯全域主要驗
  d. 將內部網路驗證方法設為「Forms驗證」、而非預設的「Windows驗證」。
- 在某些情況下、當Unified Manager安全性憑證簽署CA時、會拒絕透過IDP登入。有兩種因應措施可解決此

問題：

- 請依照連結中所述的指示、針對連結的依賴方之鏈結CA憑證、停用在ADFS伺服器上的撤銷檢查：

  "停用每個信賴方信任的撤銷檢查"

- 讓CA伺服器位於ADFS伺服器內、以簽署Unified Manager伺服器認證要求。

其他組態需求

- Unified Manager時鐘偏移設定為5分鐘、因此IDP伺服器與Unified Manager伺服器之間的時間差異不可超過5分鐘、否則驗證將會失敗。

啟用SAML驗證

您可以啟用安全聲明標記語言（SAML）驗證、讓遠端使用者在存取Unified Manager Web UI之前、先經過安全身分識別供應商（IDP）的驗證。

您需要的是什麼

- 您必須已設定遠端驗證、並驗證是否成功。
- 您必須已建立至少一個具有應用程式管理員角色的遠端使用者或遠端群組。
- Identity Provider（IDP）必須由Unified Manager支援、且必須加以設定。
- 您必須擁有IDP URL和中繼資料。
- 您必須擁有IDP伺服器的存取權。

從Unified Manager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IDP、才能存取圖形化使用者介面。因此您必須準備好完成連線的兩個部分、才能開始組態程序。IDP可在設定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。

> 在您完成此頁面上的SAML組態之後、Unified Manager會自動重新啟動。

步驟

1. 在左導覽窗格中、按一下*一般*>* SAML驗證*。
2. 選取「啟用**SAML**驗證」核取方塊。

   隨即顯示設定IDP連線所需的欄位。

3. 輸入IDP URI和IDP中繼資料、以將Unified Manager伺服器連線至IDP伺服器。

   如果IDP伺服器可直接從Unified Manager伺服器存取、您可以在輸入IDP URI之後按一下*擷取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至XML文字檔。

   您現在可以使用此資訊來設定IDP伺服器。

5. 按一下「 * 儲存 * 」。

   隨即顯示訊息方塊、確認您要完成組態並重新啟動Unified Manager。

6. 按一下*「Confirm and Logout*（確認並登出）」、Unified Manager即會重新啟動。

下次授權的遠端使用者嘗試存取Unified Manager圖形介面時、他們會在IDP登入頁面中輸入其認證資料、而非在Unified Manager登入頁面中輸入認證資料。

如果尚未完成、請存取IDP並輸入Unified Manager伺服器URI和中繼資料、以完成組態。

> 使用ADFS做為身分識別供應商時、Unified Manager GUI不會遵守ADFS逾時、會繼續運作、直到Unified Manager工作階段逾時為止。您可以按一下*一般*>*功能設定*>*無活動逾時*來變更GUI工作階段逾時。

變更用於**SAML**驗證的身分識別供應商

您可以變更Unified Manager用來驗證遠端使用者的身分識別供應商（IDP）。

您需要的是什麼

- 您必須擁有IDP URL和中繼資料。
- 您必須擁有IDP的存取權。

新的IDP可在設定Unified Manager之前或之後進行設定。

步驟

1. 在左導覽窗格中、按一下*一般*>* SAML驗證*。
2. 輸入將Unified Manager伺服器連線至IDP所需的新IDP URI和IDP中繼資料。

   如果IDP可直接從Unified Manager伺服器存取、您可以在輸入IDP URL後按一下*擷取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、或將中繼資料儲存至XML文字檔。
4. 按一下「儲存組態」。

   隨即顯示訊息方塊、確認您要變更組態。

5. 按一下「確定」。

存取新的IDP、然後輸入Unified Manager伺服器URI和中繼資料以完成組態。

下次授權的遠端使用者嘗試存取Unified Manager圖形介面時、他們會在新的IDP登入頁面中輸入其認證資料、而非在舊的IDP登入頁面中輸入認證資料。

在**Unified Manager**安全性憑證變更之後更新**SAML**驗證設定

若對安裝在Unified Manager伺服器上的HTTPS安全性憑證進行任何變更、都必須更新SAML驗證組態設定。如果您重新命名主機系統、指派主機系統的新IP位址、或手動變

更系統的安全性憑證、則會更新憑證。

變更安全性憑證並重新啟動Unified Manager伺服器之後、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、才能重新啟用使用者介面的存取。

步驟

1. 登入維護主控台。
2. 在*主功能表*中、輸入*停用SAML驗證*選項的編號。

   畫面會顯示訊息、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、將更新的伺服器憑證接受到瀏覽器、然後使用維護使用者認證登入。
4. 在「設定/驗證」頁面中、選取「* SAML驗證*」索引標籤、然後設定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至XML文字檔。
6. 按一下「 * 儲存 * 」。

   隨即顯示訊息方塊、確認您要完成組態並重新啟動Unified Manager。

7. 按一下*「Confirm and Logout*（確認並登出）」、Unified Manager即會重新啟動。
8. 存取您的IDP伺服器、然後輸入Unified Manager伺服器URI和中繼資料以完成組態。

身分識別供應商	組態步驟
ADFS	a. 刪除ADFS管理GUI中現有的信賴關係人信任項目。 b. 使用更新的Unified Manager伺服器中的「sAML_sp_mendors.xml」新增信賴關係人信任項目。 c. 定義Unified Manager剖析此信賴方信任項目的ADFS SAML回應所需的三種宣告規則。 d. 重新啟動ADFS Windows服務。
Shibboleth	a. 將Unified Manager伺服器的新FQDN更新為「attribute-filer.xml」和「remale-party.xml」檔案。 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、並確認SAML驗證可在您的IDP中正常運作。

停用**SAML**驗證

若要停止透過安全身分識別供應商（IDP）驗證遠端使用者、然後再登入Unified Manager Web UI、您可以停用SAML驗證。停用SAML驗證時、已設定的目錄服務供應商（例

如Active Directory或LDAP）會執行登入驗證。

停用SAML驗證後、本機使用者和維護使用者除了能存取已設定的遠端使用者之外、也能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會自動重新啟動。

步驟

1. 在左導覽窗格中、按一下*一般*>* SAML驗證*。
2. 取消核取「啟用**SAML**驗證」核取方塊。
3. 按一下「 * 儲存 * 」。

   隨即顯示訊息方塊、確認您要完成組態並重新啟動Unified Manager。

4. 按一下*「Confirm and Logout*（確認並登出）」、Unified Manager即會重新啟動。

下次遠端使用者嘗試存取Unified Manager圖形化介面時、他們會在Unified Manager登入頁面輸入其認證資料、而非IDP登入頁面。

存取IDP並刪除Unified Manager伺服器URI和中繼資料。

從維護主控台停用**SAML**驗證

當無法存取Unified Manager GUI時、您可能需要從維護主控台停用SAML驗證。這可能發生在設定錯誤或無法存取IDP的情況下。

您需要的是什麼

您必須以維護使用者的身分存取維護主控台。

停用SAML驗證時、已設定的目錄服務供應商（例如Active Directory或LDAP）會執行登入驗證。除了設定的遠端使用者之外、本機使用者和維護使用者也能存取圖形化使用者介面。

您也可以從UI的「設定/驗證」頁面停用SAML驗證。

> 停用SAML驗證後、Unified Manager會自動重新啟動。

步驟

1. 登入維護主控台。
2. 在*主功能表*中、輸入*停用SAML驗證*選項的編號。

   畫面會顯示訊息、確認您要停用SAML驗證並重新啟動Unified Manager。

3. 鍵入* y*、然後按Enter鍵、Unified Manager即會重新啟動。

下次遠端使用者嘗試存取Unified Manager圖形化介面時、他們會在Unified Manager登入頁面輸入其認證資料、而非IDP登入頁面。

如有需要、請存取IDP並刪除Unified Manager伺服器URL和中繼資料。

SAML驗證頁面

您可以使用「SAML驗證」頁面來設定Unified Manager、以便透過安全的身分識別供應商（IDP）驗證使用SAML的遠端使用者、然後才能登入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組態。
- 您必須已設定遠端驗證。
- 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之後、您可以選取「啟用SAML驗證」核取方塊、以使用安全的身分識別供應商來啟用驗證。

- * 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IDP URL可從Unified Manager伺服器存取、您可以按一下*擷取IDP中繼資料*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FQDN。如有必要、您可以變更此值。

- *主機URI *

  從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

您可以使用Unified Manager伺服器上的LDAP或Active Directory來啟用驗證、並將其設定為與伺服器搭配使用、以驗證遠端使用者。

如需啟用遠端驗證、設定驗證服務及新增驗證伺服器、請參閱上一節*設定Unified Manager以傳送警示通知*。

編輯驗證伺服器

您可以變更Unified Manager伺服器用來與驗證伺服器通訊的連接埠。

您需要的是什麼

您必須具有應用程式管理員角色。

步驟

1. 在左導覽窗格中、按一下*一般*>*遠端驗證*。
2. 選中*禁用嵌套的Group Lookup（組查找）*框。
3. 在*驗證伺服器*區域中、選取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、編輯連接埠詳細資料。
5. 按一下「 * 儲存 * 」。

刪除驗證伺服器

如果您想要防止Unified Manager伺服器與驗證伺服器通訊、可以刪除驗證伺服器。例如、如果您想要變更管理伺服器正在通訊的驗證伺服器、您可以刪除驗證伺服器並新增驗證伺服器。

您需要的是什麼

您必須具有應用程式管理員角色。

刪除驗證伺服器時、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. 在左導覽窗格中、按一下*一般*>*遠端驗證*。
2. 選取您要刪除的一或多個驗證伺服器、然後按一下*刪除*。
3. 按一下*是*以確認刪除要求。

   如果啟用*使用安全連線*選項、則與驗證伺服器相關的憑證會連同驗證伺服器一起刪除。

使用**Active Directory**或**OpenLDAP**驗證

您可以在管理伺服器上啟用遠端驗證、並設定管理伺服器與驗證伺服器通訊、讓驗證伺服器內的使用者能夠存取Unified Manager。

您可以使用下列其中一項預先定義的驗證服務、或是指定您自己的驗證服務：

- Microsoft Active Directory

  您無法使用Microsoft輕量型目錄服務。

- OpenLDAP

您可以選取所需的驗證服務、並新增適當的驗證伺服器、讓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認證資料由驗證伺服器維護。管理伺服器使用輕量型目錄存取傳輸協定（LDAP）來驗證已設定驗證伺服器內的遠端使用者。

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、不會使用Active Directory或OpenLDAP進行驗證。

稽核記錄

您可以使用稽核日誌來偵測稽核日誌是否已洩漏。使用者執行的所有活動都會受到監控、並記錄在稽核記錄中。稽核是針對Active IQ Unified Manager 所有使用者介面及公開API功能執行的、

您可以使用「稽核記錄：檔案檢視」來檢視Active IQ Unified Manager 及存取您的無法使用的所有稽核記錄檔。稽核記錄：檔案檢視中的檔案會根據建立日期列出。此檢視會顯示從安裝或升級到系統中現有的所有稽核記錄的資訊。每當您在Unified Manager中執行動作時、資訊都會更新、並可在記錄中使用。每個記錄檔的狀態都是使用「檔案完整性狀態」屬性擷取、該屬性會主動受到監控、以偵測記錄檔的竄改或刪除。稽核日誌可在系統中使用時、具有下列其中一種狀態：

州/省	說明
使用中	記錄目前所在的檔案。
正常	非作用中、已壓縮並儲存在系統中的檔案。
遭竄改	已遭手動編輯檔案之使用者破壞的檔案。
手冊刪除	已由授權使用者刪除的檔案。
指標移轉刪除	因為根據循環組態原則進行復原而刪除的檔案。
Unexpected刪除	因為不明原因而刪除的檔案。

「稽核記錄」頁面包含下列命令按鈕：

- 設定
- 刪除
- 下載

「刪除」按鈕可讓您刪除「稽核記錄」檢視中所列的任何稽核記錄。您可以刪除稽核記錄、並選擇性地提供刪除檔案的理由、以便日後判斷有效刪除。原因欄會列出原因、以及執行刪除作業的使用者名稱。

> 刪除記錄檔會導致從系統刪除檔案、但不會刪除資料庫表格中的項目。

您可以Active IQ Unified Manager 使用「稽核記錄」區段中的「下載」按鈕、從更新下載稽核記錄檔、然後匯出稽核記錄檔。標示為「正常」或「竄改」的檔案會以壓縮的「.gzip」格式下載。

當產生完整AutoSupport 的支援套件組合時、支援套件會同時包含已歸檔和作用中的稽核記錄檔。但是當產生輕度支援套件時、它只會包含作用中的稽核記錄。不包含歸檔的稽核記錄。

設定稽核記錄

您可以使用「稽核記錄」區段中的「設定」按鈕來設定稽核記錄檔的循環原則、以及啟用稽核記錄的遠端記錄。

您可以根據想要儲存在系統中的資料數量和頻率、設定* MAX檔案大小*和*稽核記錄保留天數*中的值。字段*總稽核日誌大小*中的值是系統中目前稽核日誌資料總數的大小。復原原則取決於*稽核記錄保留天數*、* MAX檔案大小*及*稽核記錄總大小*欄位中的值。當稽核日誌備份的大小達到*總稽核日誌大小*所設定的值時、會刪除先歸檔的檔案。這表示會刪除最舊的檔案。但檔案項目仍可在資料庫中使用、並標示為「滾存刪除」。「稽核記錄保留天數」值是保留稽核記錄檔的天數。超過此欄位中設定值的任何檔案都會被復原。

步驟

1. 按一下「稽核記錄>*設定*」。
2. 在* MAX檔案大小*、*稽核記錄總大小*和*稽核記錄保留天數*中輸入值。

   如果您要啟用遠端記錄、則應選取*啟用遠端記錄*。

啟用遠端記錄稽核記錄

您可以選取「設定稽核記錄」對話方塊上的「*啟用遠端記錄」核取方塊、以啟用遠端稽核記錄。您可以使用此功能將稽核記錄傳輸到遠端Syslog伺服器。如此一來、您就能在空間有限時管理稽核記錄。

遠端記錄稽核日誌可在Active IQ Unified Manager 監查伺服器上的稽核日誌檔遭到竄改時、提供防竄改備份。

步驟

1. 在「設定稽核記錄」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. 輸入您要連線的遠端伺服器*主機名稱*和*連接埠*。
3. 在*伺服器CA憑證*欄位中、按一下*瀏覽*以選取目標伺服器的公開憑證。

   證書應以「.pem」格式上傳。此憑證應從目標Syslog伺服器取得、且不應過期。憑證應包含選定的「主機名稱」、作為「SubjectAltName」（SAN）屬性的一部分。

4. 輸入下列欄位的值：字元集、連線逾時、重新連線延遲。

   這些欄位的值應以毫秒為單位。

5. 在*格式*和*傳輸協定*欄位中選取所需的Syslog格式和TLS傳輸協定版本。
6. 如果目標Syslog伺服器需要憑證型驗證、請選取「啟用用戶端驗證」核取方塊。

   您必須先下載用戶端驗證憑證、然後將其上傳至Syslog伺服器、再儲存稽核記錄組態、否則連線將會失敗。視Syslog伺服器類型而定、您可能需要建立用戶端驗證憑證的雜湊。

範例：SysL-NG需要使用命令「openssl x509 -noout -hash -in cert.pem」建立憑證的<雜湊>、然後您應該以符號方式將用戶端驗證憑證連結至以<hash>.0命名的檔案。

7. 按一下「儲存」以設定與伺服器的連線、並啟用遠端記錄。

   您將被重新導向至「稽核記錄」頁面。

遠端驗證頁面

您可以使用「遠端驗證」頁面設定Unified Manager與驗證伺服器通訊、以驗證嘗試登入Unified Manager Web UI的遠端使用者。

您必須具有應用程式管理員或儲存管理員角色。

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

  可讓您設定管理伺服器、以驗證目錄服務供應商（例如Active Directory、OpenLDAP）中的使用者、或是指定您自己的驗證機制。只有在啟用遠端驗證時、才能指定驗證服務。

  - * Active Directory *
    - 系統管理員名稱

      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。

    - 基礎辨別名稱

      指定驗證伺服器中遠端使用者的位置。例如、如果驗證伺服器的網域名稱是+ou@domain.com、則基礎辨別名稱是* 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詢選項。此選項預設為停用。如果您使用Active Directory、可以停用對巢狀群組的支援、以加速驗證。

    - 使用安全連線

      指定用於與驗證伺服器通訊的驗證服務。

  - * OpenLDAP*
    - 連結辨別名稱

      指定用於在驗證伺服器中尋找遠端使用者的繫結辨別名稱、以及基礎辨別名稱。

    - 連結密碼

指定存取驗證伺服器的密碼。

- 基礎辨別名稱

  指定驗證伺服器中遠端使用者的位置。例如、如果驗證伺服器的網域名稱是+ou@domain.com、則基礎辨別名稱是* CN=ou,DC=domain,DC=com*。

- 使用安全連線

  指定安全LDAP用於與LDAPS驗證伺服器通訊。

◦ 其他

- 連結辨別名稱

  指定連結辨別名稱、搭配基礎辨別名稱使用、以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。

- 基礎辨別名稱

  指定驗證伺服器中遠端使用者的位置。例如、如果驗證伺服器的網域名稱是+ou@domain.com、則基礎辨別名稱是* CN=ou,DC=domain,DC=com*。

- 傳輸協定版本

  指定驗證伺服器所支援的輕量型目錄存取傳輸協定（LDAP）版本。您可以指定是否必須自動偵測通訊協定版本、或將版本設定為2或3。

- 使用者名稱屬性

  指定驗證伺服器中包含要由管理伺服器驗證之使用者登入名稱的屬性名稱。

- 群組成員資格屬性

  根據在使用者驗證伺服器中指定的屬性和值、指定一個值來指派管理伺服器群組成員資格給遠端使用者。

- UGid

  如果遠端使用者是驗證伺服器中的一群組功能名稱物件成員、則此選項可讓您根據該群組功能名稱物件中的指定屬性、將管理伺服器群組成員資格指派給遠端使用者。

- 停用巢狀群組查詢

  指定是否啟用或停用巢狀群組查詢選項。此選項預設為停用。如果您使用Active Directory、可以停用對巢狀群組的支援、以加速驗證。

- 成員

  指定驗證伺服器用來儲存群組個別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。

- 使用安全連線

  指定用於與驗證伺服器通訊的驗證服務。

> 如果您想要修改驗證服務、請務必刪除任何現有的驗證伺服器、然後新增驗證伺服器。

驗證伺服器區域

驗證伺服器區域會顯示管理伺服器用來尋找及驗證遠端使用者的驗證伺服器。遠端使用者或群組的認證資料由驗證伺服器維護。

- 命令按鈕

  可讓您新增、編輯或刪除驗證伺服器。

  - 新增

    可讓您新增驗證伺服器。

  如果您要新增的驗證伺服器是高可用度配對的一部分（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個驗證伺服器無法連線時、與合作夥伴通訊。

  - 編輯

    可讓您編輯所選驗證伺服器的設定。

  - 刪除

    刪除選取的驗證伺服器。

- 名稱或**IP**位址

  顯示驗證伺服器的主機名稱或IP位址、用於驗證管理伺服器上的使用者。

- 連接埠

  顯示驗證伺服器的連接埠號碼。

- 測試驗證

  此按鈕會驗證遠端使用者或群組、以驗證驗證驗證伺服器的組態。

  測試時、如果您只指定使用者名稱、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。

管理安全性憑證

您可以在Unified Manager伺服器中設定HTTPS、以便透過安全連線監控及管理叢集。

檢視**HTTPS**安全性憑證

您可以將HTTPS憑證詳細資料與瀏覽器中擷取的憑證進行比較、以確保瀏覽器與Unified Manager的加密連線不會被攔截。

您需要的是什麼

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內容、或檢視可從中存取Unified Manager的主體替代名稱（SAN）。

步驟

1. 在左導覽窗格中、按一下*一般*>* HTTPS憑證*。

   HTTPS憑證會顯示在頁面頂端

如果您需要檢視安全性憑證的詳細資訊、而非HTTPS憑證頁面所顯示的詳細資訊、您可以在瀏覽器中檢視連線憑證。

正在下載**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、以便將檔案提供給憑證授權單位進行簽署。CA簽署的憑證有助於預防攔截式攻擊、並提供比自我簽署憑證更好的安全保護。

您需要的是什麼

您必須具有應用程式管理員角色。

步驟

1. 在左導覽窗格中、按一下*一般*>* HTTPS憑證*。
2. 按一下*下載HTTPS憑證簽署要求*。
3. 儲存「.csr」檔案。

您可以將檔案提供給「憑證授權單位」進行簽署、然後安裝簽署的憑證。

安裝**CA**簽署並傳回**HTTPS**憑證

您可以在「憑證授權單位」簽署並傳回安全性憑證之後、再上傳及安裝安全性憑證。您上傳和安裝的檔案必須是現有自我簽署憑證的簽署版本。CA簽署的憑證有助於預防攔截式攻擊、並提供比自我簽署憑證更好的安全保護。

您需要的是什麼

您必須完成下列動作：

- 已下載「憑證簽署要求」檔案、並由「憑證授權單位」簽署
- 已將憑證鏈結儲存為PEE格式
- 包括鏈中的所有憑證、從Unified Manager伺服器憑證到根簽署憑證、包括任何存在的中繼憑證

您必須具有應用程式管理員角色。

> 如果建立CSR的憑證有效時間超過3997天、則CA在簽署並傳回憑證之前、將會將有效時間減至3997天

步驟

1. 在左導覽窗格中、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...*以找出要上傳的檔案。
4. 選取檔案、然後按一下「安裝」以安裝檔案。

   "安裝使用外部工具產生的HTTPS憑證"

範例憑證鏈結

下列範例顯示憑證鏈結檔案的顯示方式：

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

安裝使用外部工具產生的**HTTPS**憑證

您可以安裝自我簽署或CA簽署的憑證、並使用OpenSSL、BoringSSL、LetsEncrypt等外部工具產生。

您應該將私密金鑰與憑證鏈結一起載入、因為這些憑證是由外部產生的公開私密金鑰配對。允許的金鑰配對演算

法為「'rSA'」和「'EC'」。「一般」區段下方的「HTTPS憑證」頁面提供「安裝**HTTPS**憑證」選項。您上傳的檔案應採用下列輸入格式。

1. 屬於Active IQ 該伺服器的私有金鑰
2. 與私密金鑰相符的伺服器憑證
3. CA的憑證會反轉至根憑證、用於簽署上述憑證

以**EC**金鑰配對載入憑證的格式

允許的曲線為「prime256v1」和「cep384r1」。外部產生EC配對的憑證範例：

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

以**RSA**金鑰配對載入憑證的格式

屬於主機憑證的RSA金鑰配對允許金鑰大小為2048、3072和4096。具有外部產生* RSA金鑰組*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 更新以使變更生效。

上傳外部產生的憑證時進行檢查

系統會在上傳使用外部工具產生的憑證時執行檢查。如果有任何檢查失敗、則會拒絕該憑證。產品內的CSR產生的憑證以及使用外部工具產生的憑證也包含驗證功能。

- 輸入中的私密金鑰會根據輸入中的主機憑證進行驗證。
- 主機憑證中的「Common Name（CN）（一般名稱（CN））」會對照主機的FQDN進行檢查。
- 主機憑證的一般名稱（CN）不應為空白或空白、且不應設定為localhost。
- 有效開始日期不應為未來日期、而且憑證的有效到期日不應為過去日期。
- 如果存在中介CA或CA、則憑證的有效開始日期不應為未來日期、而且有效到期日不應為過去日期。

> 輸入中的私密金鑰不應加密。如果有任何私密金鑰已加密、則系統會拒絕這些金鑰。

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-----
```

憑證管理的頁面說明

您可以使用「HTTPS憑證」頁面來檢視目前的安全性憑證、並產生新的HTTPS憑證。

HTTPS憑證頁面

「HTTPS憑證」頁面可讓您檢視目前的安全性憑證、下載憑證簽署要求、產生新的HTTPS憑證、或安裝新的HTTPS憑證。

如果您尚未產生新的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

命令按鈕可讓您執行下列作業：

- 下載**HTTPS**憑證簽署要求

  下載目前安裝之HTTPS憑證的認證要求。您的瀏覽器會提示您儲存.csr檔案、以便將檔案提供給憑證授權單位進行簽署。

- 安裝**HTTPS**憑證

  可讓您在「憑證授權單位」簽署並傳回安全性憑證之後、再上傳及安裝安全性憑證。重新啟動管理伺服器後、新的憑證即會生效。

- 重新產生**HTTPS**憑證

  可讓您產生HTTPS憑證、取代目前的安全性憑證。重新啟動Unified Manager之後、新的憑證即會生效。

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。

目前的憑證資訊會顯示在此頁面上。

「使用目前的憑證屬性重新產生」和「更新目前的憑證屬性」選項可讓您以目前的資訊重新產生憑證、或是以新資訊產生憑證。

- 通用名稱

  必要。您要保護的完整網域名稱（FQDN）。

  在Unified Manager高可用度組態中、使用虛擬IP位址。

- 電子郵件

  選用。聯絡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

  選用。通常是貴公司的註冊名稱。

- 部門

  選用。貴公司部門的名稱。

- 城市

  選用。貴公司的城市位置。

- 州

  選用。貴公司的州或省位置（非縮寫）。

- 國家

  選用。貴公司的國家/地區位置。這通常是國家/地區的兩個字母ISO代碼。

- 替代名稱

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

  如果您要從憑證的替代名稱欄位中移除本機識別資訊、請選取「排除本機識別資訊（例如localhost）」核取方塊。如果選中此複選框，則只有您在字段中輸入的內容才用於替代名稱字段。如果保留空白、則產生的憑證將完全沒有替代名稱欄位。

- 金鑰大小（金鑰演算法：**RSA**）

  金鑰演算法設定為RSA。您可以從其中一個金鑰大小中選取：2048、3072或4096位元。預設金鑰大小設為2048位元。

- 有效期間

  預設的有效期間為397-97天。如果您已從舊版升級、則先前的憑證有效性可能會維持不變。