



設定Active IQ Unified Manager 功能

Active IQ Unified Manager 9.14

NetApp
November 11, 2024

目錄

設定Active IQ Unified Manager 功能	1
組態順序總覽	1
存取Unified Manager Web UI	1
執行Unified Manager Web UI的初始設定	2
新增叢集	4
設定Unified Manager以傳送警示通知	6
變更本機使用者密碼	13
設定工作階段閒置逾時	14
變更Unified Manager主機名稱	14
啟用及停用原則型儲存管理	18

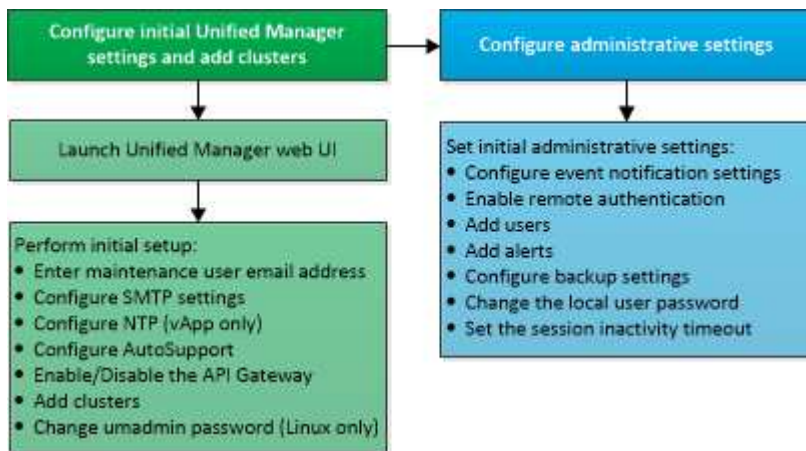
設定Active IQ Unified Manager 功能

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）。

連結的格式如下 `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。

Getting Started



Notifications

Configure your email server for assistance in case you forget your password.

Maintenance User Email

Email

SMTP Server

Host Name or IP Address

Port

User Name

Password

Use STARTTLS ⓘ Use SSL ⓘ

Continue

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 *。



如果您選取了「使用STARTTLS*或*使用SSL」選項、在您按一下「繼續」按鈕之後、就會顯示一個憑證頁面。確認憑證詳細資料、並接受憑證、以繼續進行Web UI的初始設定。

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、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：
 - Unified Manager 支援內部部署的 ONTAP 叢集、ONTAP Select、Cloud Volumes ONTAP。
 - 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_、_consol_和_http。

- 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：
 - **SSL（HTTPS）憑證***：此憑證由 Unified Manager 擁有。預設的自我簽署SSL（HTTPS）憑證會以全新安裝的Unified Manager產生。NetApp建議您將其升級至CA簽署的憑證、以獲得更好的安全性。如果伺服器憑證過期、您應該重新產生該憑證、然後重新啟動Unified Manager、讓服務整合新的憑證。如需重新產生SSL憑證的詳細資訊，請參閱"[產生HTTPS安全性憑證](#)"。
 - **EMS 憑證***：此憑證由 Unified Manager 擁有。它用於驗證從 ONTAP 接收的 EMS 通知。

相互TLS通訊的證書：在Unified Manager與ONTAP 支援中心之間進行相互TLS通訊時使用。憑證型驗證會根據ONTAP 版本啟用叢集的驗證。如果執行ONTAP 版本資訊功能的叢集低於9.5版、則不會啟用憑證型驗

證。

如果您要更新舊版 Unified Manager、則叢集不會自動啟用憑證型驗證。不過、您可以修改及儲存叢集詳細資料來啟用此功能。如果憑證過期、您應該重新產生憑證以納入新的憑證。如需檢視及重新產生憑證的詳細資訊，請參閱["編輯叢集"](#)。



- 您可以從 Web UI 新增叢集、並自動啟用憑證型驗證。
- 您可以透過 Unified Manager CLI 新增叢集、預設不會啟用憑證型驗證。如果您使用 Unified Manager CLI 新增叢集、則必須使用 Unified Manager UI 來編輯叢集。您可以參閱["支援的Unified Manager CLI命令"](#)使用 Unified Manager CLI 新增叢集。
- 如果叢集已啟用憑證型驗證、且您從伺服器備份Unified Manager、並還原至另一個變更主機名稱或IP位址的Unified Manager伺服器、則叢集監控可能會失敗。若要避免故障、請編輯並儲存叢集詳細資料。如需編輯叢集詳細資料的詳細["編輯叢集"](#)資訊，請參閱。

- 叢集憑證 *：此憑證為 ONTAP 所有。您無法使用過期的憑證將叢集新增至 Unified Manager、如果憑證已過期、則應在新增叢集之前重新產生叢集。有關證書生成的信息，請參閱知識庫 (KB) 文章 ["如何在ONTAP System Manager使用者介面中更新自我簽署的認證"](#)。
- 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

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」。

儲存叢集詳細資料之後、您可以看到叢集的相互 TLS 通訊憑證。

如果未啟用憑證型驗證、Unified Manager只會在一開始新增叢集時才檢查憑證。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。

相關資訊

["安裝CA簽署並傳回HTTPS憑證"](#)

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。
 - 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。
3. 按一下「* 儲存 *」。
4. 如果您選取了「使用**ARTTLS***或*使用**SSL**」選項、在您按一下「儲存」按鈕之後、就會顯示憑證頁面。驗證憑證詳細資料、並接受憑證以儲存通知設定。

您可以按一下「檢視憑證詳細資料」按鈕來檢視憑證詳細資料。如果現有的憑證已過期、請取消勾選「使用**ARTTLS***或*使用**SSL**」方塊、儲存通知設定、然後再次勾選「使用**ARTTLS***或*使用**SSL**」方塊以檢視新的憑證。

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	<ul style="list-style-type: none">• 驗證伺服器管理員名稱的格式如下：<ul style="list-style-type: none">◦ domainname\username◦ username@domainname◦ Bind Distinguished Name（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	<ul style="list-style-type: none">• 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	<ol style="list-style-type: none"> 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。 <p>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*。</p>
OpenLDAP	<ol style="list-style-type: none"> 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。 <p>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*。</p>

如果您選取...	然後執行此動作...
其他	<p>a. 輸入綁定辨別名稱和綁定密碼。</p> <p>b. 指定驗證伺服器的基礎辨別名稱。</p> <p>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*。</p> <p>c. 指定驗證伺服器支援的LDAP傳輸協定版本。</p> <p>d. 輸入使用者名稱、群組成員資格、使用者群組和成員屬性。</p>



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...
<p>啟用它</p>	<p>a. 選擇*使用安全連線*選項。</p> <p>b. 在「驗證伺服器」區域中、按一下「新增」。</p> <p>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）。</p> <p>d. 在「授權主機」對話方塊中、按一下「檢視憑證」。</p> <p>e. 在「檢視憑證」對話方塊中、確認憑證資訊、然後按一下「關閉」。</p> <p>f. 在授權主機對話方塊中、按一下*是*。</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>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。</p> </div>
<p>停用它</p>	<p>a. 清除*使用安全連線*選項。</p> <p>b. 在「驗證伺服器」區域中、按一下「新增」。</p> <p>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。</p> <p>d. 按一下「*新增*」。</p>

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 and 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. 從「可用資源」區域中選取 *+ [All Volumes whose name contains 'abc'] *，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。如果您使用`Reset Server Certificate`維護主控台的選項、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。
使用不同的值產生憑證	<p>按一下*更新目前的憑證屬性*選項。</p> <p>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。</p> <ul style="list-style-type: none">• 金鑰大小的允許值為 2048、3072 和 4096。• 有效期間最短為1天、最長為36500天。 <p>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。</p> <ul style="list-style-type: none">• 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。

6. 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：

```
systemctl stop ocieau ocie mysqld
```

3. 使用Linux命令變更主機名稱 hostnamectl：

```
hostnamectl set-hostname new_FQDN
```

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

4. 重新產生伺服器的HTTPS憑證：

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

5. 重新啟動網路服務：

```
systemctl restart NetworkManager.service
```

6. 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：

```
systemctl 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。

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。