



執行組態和管理工作 Active IQ Unified Manager 9.9

NetApp
December 15, 2023

This PDF was generated from <https://docs.netapp.com/zh-tw/active-iq-unified-manager-99/config/concept-overview-of-the-configuration-sequence.html> on December 15, 2023. Always check docs.netapp.com for the latest.

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	24
使用維護主控台	25

執行組態和管理工作

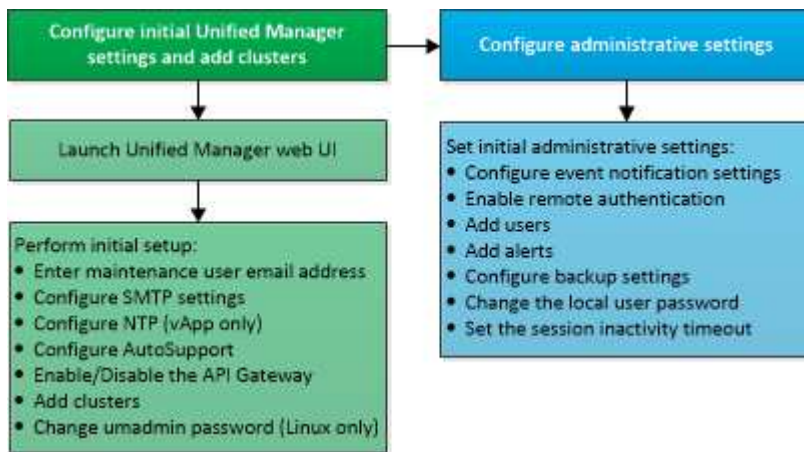
設定Active IQ Unified Manager 功能

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。

開始之前

- 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。

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

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。

開始之前

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

關於這項工作

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。

Active IQ Unified Manager

Getting Started

1 Email 2 AutoSupport 3 AFI Gateway 4 Add ONTAP Clusters 5 Finish

Notifications

Configure your email server to allow Active IQ Unified Manager to assist in the event of a forgotten password.

Maintenance User Email

Email

SMTP Server

Host Name or IP Address

Port

User Name

Password

☒ Use START / TLS ☐

☐ Use SSL ☐

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* AutoSupport 《》（） 頁面中、按一下*「Agree and Continue（同意並繼續）」*、即可從AutoSupport Unified Manager將一些不必要的訊息傳送到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、選取是否要使用API閘道功能、讓Unified Manager能夠管理ONTAP 您計畫使用ONTAP 靜態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 "[功能入門Active IQ Unified Manager](#)"。

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」。

結果

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。

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。

關於這項工作

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。

結果

在探索新叢集的所有物件（約15分鐘）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。

開始之前

您必須具有應用程式管理員角色。

關於這項工作

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。

開始之前

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。

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）。

關於這項工作

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。

1. 新增驗證伺服器、並測試驗證。
2. 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。

開始之前

- 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。

關於這項工作

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*」。

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。

開始之前

- 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。

關於這項工作

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	<ol style="list-style-type: none"> 1. 選擇*使用安全連線*選項。 2. 在「驗證伺服器」區域中、按一下「新增」。 3. 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）。 4. 在「授權主機」對話方塊中、按一下「檢視憑證」。 5. 在「檢視憑證」對話方塊中、確認憑證資訊、然後按一下「關閉」。 6. 在授權主機對話方塊中、按一下*是*。 <div>  <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>
停用它	<ol style="list-style-type: none"> 1. 清除*使用安全連線*選項。 2. 在「驗證伺服器」區域中、按一下「新增」。 3. 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。 4. 按一下「* 新增 *」。

您新增的驗證伺服器會顯示在「伺服器」區域中。

1. 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。

開始之前

- 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。

關於這項工作

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。

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。

關於這項工作

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、然後輸入必要資訊。

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 *」。

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。

開始之前

- 您必須設定通知設定、例如使用者電子郵件地址、SMTP伺服器和SNMP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。

關於這項工作

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「ample@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：

1. 按一下*名稱*、然後輸入 HealthTest 在*警示名稱*欄位中。
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. 輸入 abc 在「名稱包含」欄位中、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*、然後輸入 xyz 在「名稱包含」欄位中、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」、然後輸入 sample@domain.com 在警示這些使用者欄位中。
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 *」。

自動新增至Unified Manager的EMS事件

下列ONTAP 功能可自動新增至Unified Manager。在Unified Manager監控的任何叢集上觸發時、都會產生這些事件。

當監控執行ONTAP 不含更新版本的軟體的叢集時、可以使用下列EMS事件：

Unified Manager事件名稱	EMS事件名稱	受影響的資源	Unified Manager嚴重性
雲端層存取遭拒、無法進行Aggregate重新配置	arl.netra.ca.check.failed	Aggregate	錯誤
儲存容錯移轉期間、雲端層存取遭拒、無法進行集合移轉	gb.netra.ca.check.failed	Aggregate	錯誤
完成鏡射複寫重新同步FabricPool	wafl.ca.resync.complete	叢集	錯誤
幾乎已滿FabricPool	棒極了	叢集	錯誤
NVMe寬限期已開始	nvmf.graceperiod.start	叢集	警告

Unified Manager事件名稱	EMS事件名稱	受影響的資源	Unified Manager嚴重性
NVMe寬限期有效	nvmf.graceperiod.active	叢集	警告
NVMe寬限期已過期	nvmf.graceperiod.expired	叢集	警告
LUN已毀損	lun.destroy	LUN	資訊
Cloud AWS MetaDataConnFail	Cloud : aws.metadata ConnFail	節點	錯誤
Cloud AWS IAMCredsExpired	Cloud : AWs.iamCredsExpired	節點	錯誤
Cloud AWS IAMCreds無效	Cloud : AWs.iamCreds無效	節點	錯誤
Cloud AWS IAMCredsNotFound	Cloud : AWs.iamCredsNotFound	節點	錯誤
Cloud AWS IAMCredsNotinitialized	Cloud : AWs.iamNotinitialized	節點	資訊
Cloud AWS IAM勞力 無效	Cloud : AWs.iam勞力 無效	節點	錯誤
Cloud AWS IAM勞力 諾富特	Cloud 、AWs.iam勞力 士	節點	錯誤
無法解析雲端層主機	不可解析 的objstore.host.unresolvable	節點	錯誤
雲端層叢集間LIF關閉	objstore.interclusterlifDown	節點	錯誤
申請不符的雲端層簽名	ROSC認證不符	節點	錯誤
NFSv4集區之一已耗盡	Nbles.nfsV4PoolEx	節點	關鍵
QoS監控記憶體已達上限	QoS.監 控記憶體上限	節點	錯誤
QoS監控記憶體已減少	qos.監 控記憶體。已減除	節點	資訊
NVMeNS銷毀	NVMeNS.destroy	命名空間	資訊

Unified Manager事件名稱	EMS事件名稱	受影響的資源	Unified Manager嚴重性
NVMeNS線上	NVMeNs.offline	命名空間	資訊
NVMeNS離線	NVMeNs.online	命名空間	資訊
NVMeNS空間不足	NVMeNs.Out.o.space.	命名空間	警告
同步複寫不同步	SMS.STATUS.Out.o.sync	SnapMirror關係	警告
同步複寫已還原	sms.status.in.sync	SnapMirror關係	資訊
同步複寫自動重新同步失敗	SMS.resSync。嘗試失敗	SnapMirror關係	錯誤
許多CIFS連線	Nbles.scifsManyAuds	SVM	錯誤
超過CIFS連線上限	Nbles.scifsMaxOpenSameFile	SVM	錯誤
超過每位使用者的CIFS連線數量上限	Nbles.ifsMaxSessPerusrConn	SVM	錯誤
CIFS NetBios名稱衝突	Nbles.scifsNbNameConflict	SVM	錯誤
嘗試連線不存在的CIFS共用	Nbles.CifsNoPrivate共享	SVM	關鍵
CIFS陰影複製作業失敗	CIFs.ShadowCopy.f失敗	SVM	錯誤
AV伺服器發現病毒	Nblan.vscanVirusDetected	SVM	錯誤
無AV伺服器連線可進行病毒掃描	Nbles.vscannNoScannerConn	SVM	關鍵
未登錄AV伺服器	Nblan.vscannNoRegdScanner.	SVM	錯誤
無回應的AV伺服器連線	Nblan.vscannConnInactive	SVM	資訊
AV伺服器太忙、無法接受新的掃描要求	Nblan.vscannConnBack血壓	SVM	錯誤

Unified Manager事件名稱	EMS事件名稱	受影響的資源	Unified Manager嚴重性
未獲授權的使用者嘗試使用AV伺服器	Nblad.vscandUserPrivate存取	SVM	錯誤
包含空間問題的要素FlexGroup	flexgroup.soites.se.me.space.Issues	Volume	錯誤
所有資訊均正常FlexGroup	flexgroup.soites.space.STATUS.all.ok	Volume	資訊
包含inode問題FlexGroup	flexgroup.constituents.have.inodes.issues	Volume	錯誤
不確定的成分inode狀態FlexGroup	flexgroup.constituents.inodes.status.all.ok	Volume	資訊
Volume邏輯空間幾乎已滿	monitor.vol.nearFull.inc.sav	Volume	警告
Volume邏輯空間已滿	monitor.vol.full.inc.sav	Volume	錯誤
Volume邏輯空間正常	monitor.vol.one.ok.inc.sav	Volume	資訊
無法自動調整規模WAFL	wafl.vol.autoSize.fail	Volume	錯誤
完成了自動調整規模WAFL	wafl.vol.autoSize.done	Volume	資訊
程式庫讀取檔案操作逾時WAFL	WAFL.readdir.Expired	Volume	錯誤

訂閱ONTAP E不到EMS活動

您可以訂閱以接收由安裝ONTAP 了此軟體的系統所產生的事件管理系統（EMS）事件。系統會自動將一部分EMS事件報告給Unified Manager、但只有在您訂閱了這些事件之後、才會報告其他EMS事件。

開始之前

請勿訂閱已自動新增至Unified Manager的EMS事件、因為這可能會在收到兩個事件以處理同一個問題時造成混淆。

關於這項工作

您可以訂閱任何數量的EMS事件。您訂閱的所有事件都會經過驗證、而且只有已驗證的事件會套用至您在Unified Manager中監控的叢集。*SUR9 EMS Event Catalog* 提供指定版本之32個軟體的所有EMS訊息詳細資訊。

訊。ONTAP 請從ONTAP「VMware產品文件」頁面找到適當版本的_EMS事件目錄、以取得適用事件的清單。

"產品庫ONTAP"

您可以針對ONTAP 訂閱的各項E不到EMS事件設定警示、也可以建立自訂指令碼、以便針對這些事件執行。



如果您未收到ONTAP 您訂閱的EseEms事件、則叢集的DNS組態可能會發生問題、導致叢集無法到達Unified Manager伺服器。若要解決此問題、叢集管理員必須修正叢集的DNS組態、然後重新啟動Unified Manager。如此將會將擱置的EMS事件排清到Unified Manager伺服器。

步驟

1. 在左導覽窗格中、按一下*儲存管理*>*事件設定*。
2. 在*事件設定*頁面中、按一下*訂閱EMS事件*按鈕。
3. 在*訂閱EMS events（緊急醫療服務事件）對話方塊中、輸入ONTAP 您要訂閱的「還原緊急醫療服務」事件名稱。

若要檢視您可以訂閱的EMS事件名稱、ONTAP 您可以從叢集Shell使用 `event route show` 命令（ONTAP 在版本號不低於版本9之前）或 `event catalog show` 命令（ONTAP 更新版本、僅限功能更新版本）。

"如何設定ONTAP 及接收Active IQ Unified Manager 來自於《關於在本》中訂閱的《關於EEMS事件的警示》"

4. 按一下「* 新增 *」。

EMS事件會新增至訂閱的EMS事件清單、但「適用於叢集」欄會針對您新增的EMS事件、將狀態顯示為「Unknown」（未知）。

5. 按一下*「Save and Close」（儲存並關閉）*、將EMS事件訂閱登錄至叢集。
6. 再按一下*訂閱EMS事件*。

您所新增之EMS事件的「適用的叢集」欄會顯示「是」狀態。

如果狀態不是「Yes（是）」、請檢查ONTAP 是否拼寫了Eqing事件名稱。如果輸入的名稱不正確、您必須移除不正確的事件、然後重新新增事件。

完成後

當發生「事件」事件時、事件會顯示在「事件」頁面上。ONTAP您可以選取事件、在「事件詳細資料」頁面中檢視有關EMS事件的詳細資料。您也可以管理事件的配置碼、或為事件建立警示。

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（編輯全域主要驗證）」。
 - 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。

開始之前

- 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。

關於這項工作

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。

結果

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。

完成後

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。

開始之前

您必須以本機使用者的身分登入。

關於這項工作

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*」。

完成後

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）。

開始之前

您必須具有應用程式管理員角色。

關於這項工作

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。

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給您、才能執行這些工作。

關於這項工作

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。

開始之前

您必須具有應用程式管理員角色。

關於這項工作

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 選項、然後建立新的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> <div>  <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。 </div>

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。

完成後

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。

開始之前

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。

關於這項工作

您也可以使用「*重新啟動來賓」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。

開始之前

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

關於這項工作

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變更主機名稱 `hostnamectl` 命令：`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：`service network restart`
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。

開始之前

您必須具有應用程式管理員角色。

關於這項工作

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Active IQ 叢集健全狀況_的_32@Unified Manager Workflow Guide》（英文）中的「老舊備份與還原作業」。

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。

開始之前

您必須已安裝並設定Unified Manager。

關於這項工作

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	<ol style="list-style-type: none">1. 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。2. 使用您的維護使用者名稱和密碼登入維護主控台。
Linux	<ol style="list-style-type: none">1. 使用Secure Shell連線至Unified Manager系統的IP位址或完整網域名稱。2. 使用維護使用者（umadmin）名稱和密碼登入系統。3. 輸入命令 <code>maintenance_console</code> 然後按 Enter。
Windows	<ol style="list-style-type: none">1. 以系統管理員認證登入Unified Manager系統。2. 以Windows系統管理員身分啟動PowerShell。3. 輸入命令 <code>maintenance_console</code> 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。

開始之前

- 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）。

- 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。

開始之前

- 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：`passwd 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。

開始之前

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。

關於這項工作

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。

步驟

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。

結果

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。

開始之前

您必須使用vSphere將網路介面新增至虛擬應用裝置。

虛擬應用裝置必須開啟電源。

關於這項工作



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主控台*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。

1. 存取維護主控台。

2. 選擇*網路組態*>*啟用網路介面*。

3. 選擇新的網路介面、然後按* Enter *。

選擇* eth1*並按* Enter *。

1. 鍵入 * y*以啟用網路介面。

2. 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。

1. 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

如果您為分配的磁碟空間不足 /opt/netapp/data 目錄若要支援Unified Manager、當您最初設定Linux主機、然後安裝Unified Manager時、您可以在安裝後增加磁碟空間、方法是增加上的磁碟空間 /opt/netapp/data 目錄。

開始之前

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。

關於這項工作

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：`systemctl stop ocieau ocie mysqld`
3. 建立暫用備份資料夾（例如 /backup-data）、並有足夠的磁碟空間來容納目前的資料 /opt/netapp/data 目錄。
4. 複製現有的內容和權限組態 /opt/netapp/data 目錄至備份資料目錄：`cp -arp /opt/netapp/data/* /backup-data`
5. 如果已啟用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
```

系統會傳回類似下列的確認訊息：

```
echo $se_type  
mysqld_db_t
```

- a. 執行 `chcon` 設定備份目錄的SE Linux類型命令：`chcon -R --type=mysqld_db_t /backup-data`

6. 移除的內容 `/opt/netapp/data` 目錄：

- a. `cd /opt/netapp/data`
- b. `rm -rf *`

7. 擴充的大小 `/opt/netapp/data` 透過LVM命令或新增額外的磁碟、目錄最少可達150 GB。



如果您已建立 `/opt/netapp/data` 從磁碟、您不應該嘗試掛載 `/opt/netapp/data` 做為NFS或CIFS共用區。因為在這種情況下、如果您嘗試擴充磁碟空間、某些LVM命令（例如）`resize`和`extend`可能無法如預期運作。

1. 確認 `/opt/netapp/data` 目錄擁有者（MySQL）和群組（root）沒有改變：`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
```

1. 如果已啟用SE Linux、請確認的內容 `/opt/netapp/data` 目錄仍設定為`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
```

1. 刪除檔案 `abc` 如此一來、此無關檔案在未來不會造成資料庫錯誤。
2. 從複製內容 `backup-data` 回到擴充的 `/opt/netapp/data` 目錄：`cp -arp /backup-data/* /opt/netapp/data/`
3. 如果已啟用SE Linux、請執行下列命令：`chcon -R --type=mysqld_db_t /opt/netapp/data`
4. 啟動MySQL服務：`systemctl start mysqld`
5. MySQL服務啟動後、請依下列順序啟動`ocie`和`ocieau`服務：`systemctl start ocie ocieau`
6. 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。

開始之前

- 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。

關於這項工作

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、然後新增更多磁碟容量至資料 disk 3。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*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。

開始之前

您必須擁有Windows系統管理員權限。

關於這項工作

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"

版權資訊

Copyright © 2023 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。