執行組態和管理工作
OnCommand Unified Manager 9.5

NetApp
December 20, 2023

目錄

執行組態和管理工作

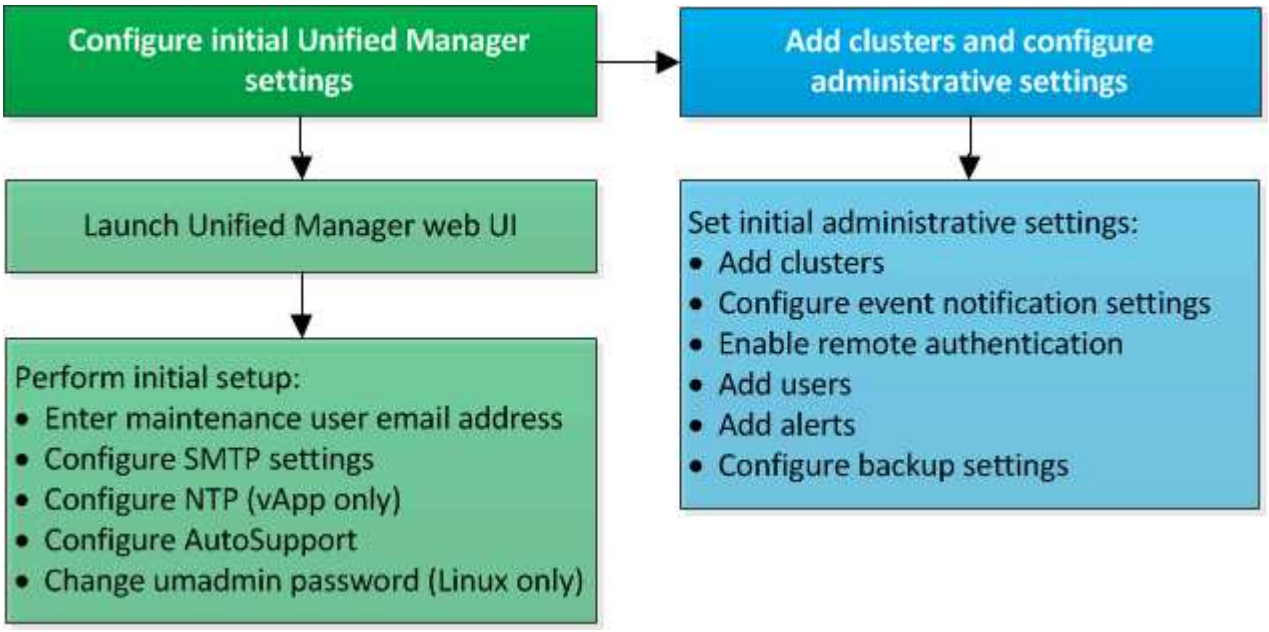
設定Unified Manager

安裝Unified Manager之後、您必須完成初始設定（也稱為第一次體驗精靈）、才能存取Web 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`。

2. 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、以及SMTP伺服器主機名稱和選項。

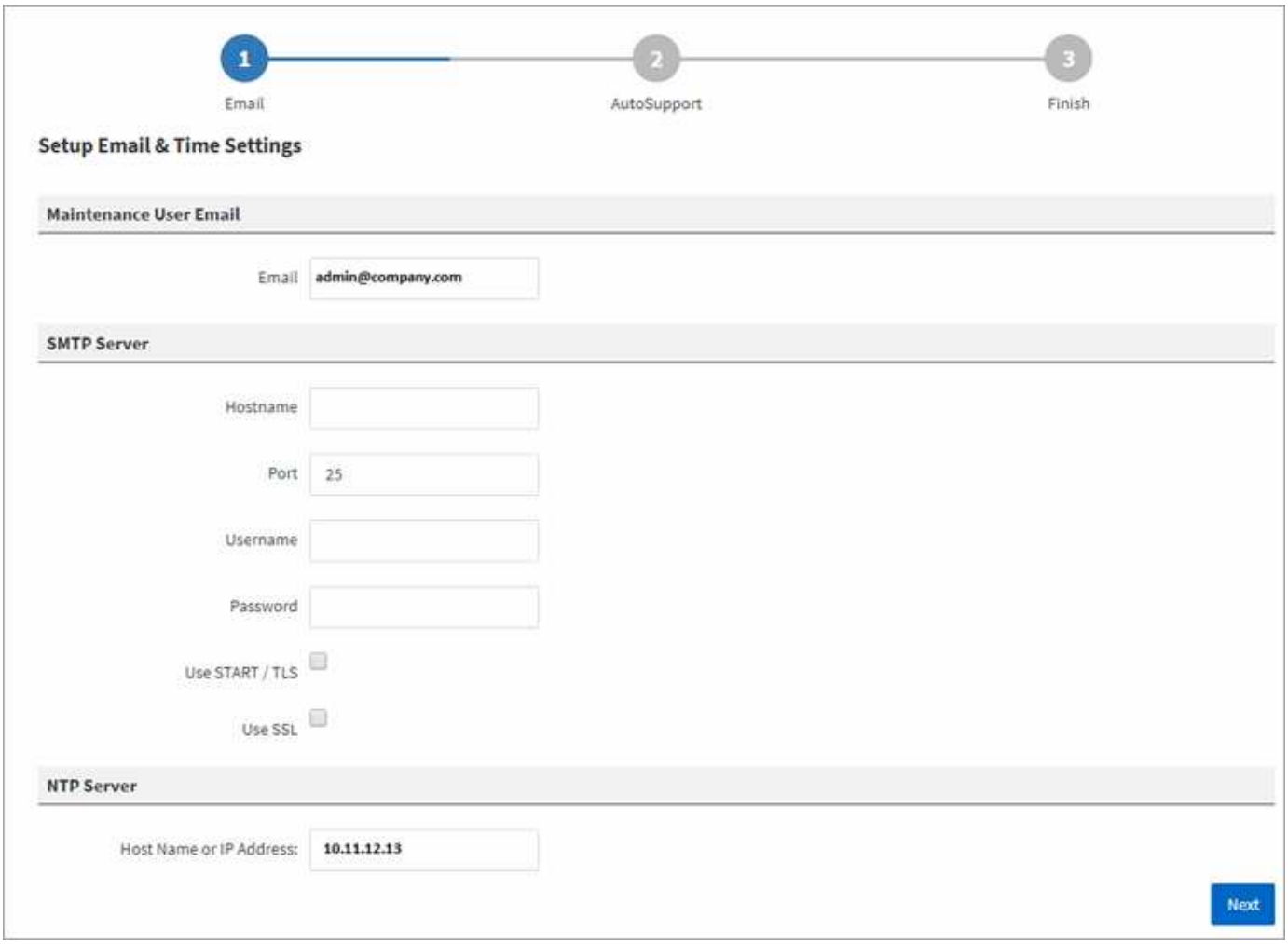
開始之前

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「The《The NetApp Unified Manager初始設定」頁面OnCommand 。以下頁面來自VMware的安裝。



如果您稍後想要變更其中任何一個選項、可以使用「管理」選項、按一下*即可存取這些選項*（在Unified Manager工具欄中）。

步驟

1. 在* OnCommand 《支援統一化管理程式初始設定》視窗中、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）。然後單擊*下一步*。
2. 在* AutoSupport 《》*頁面中、按一下「Agree and Continue （同意並繼續）」以啟用AutoSupport 「介紹」。

   如果您需要指定一個Proxy來提供網際網路存取、以便傳送AutoSupport 支援的內容、或是如果您想停用AutoSupport 「支援」、請使用「管理」選項。

3. 在Red Hat和CentOS系統上、您可以選擇將umadmin使用者密碼從預設的「admin」字串變更為個人化字串。

結果

「初始設定」視窗隨即關閉、並顯示Unified Manager Web UI。此時會出現「組態/叢集資料來源」頁面、以便您將叢集新增至系統。

新增叢集

您可以將叢集新增OnCommand 至「支援整合管理程式」、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OnCommand 具備「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。
  - 系統管理員使用者名稱和密碼Data 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。
  - 可在叢集上設定的傳輸協定類型（HTTP或HTTPS）、以及用於連線至叢集的連接埠號碼

    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。
- Unified Manager FQDN必須能夠ping通ONTAP 整個系統。

  您可以使用下列ONTAP 指令執行驗證： `ping -node node_name -destination Unified_Manager_FQDN`。
- 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*組態*>*叢集資料來源*。
2. 在「組態/叢集資料來源」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、通訊協定及連接埠號碼。

根據預設、會選取HTTPS傳輸協定和連接埠443。

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. 如果選取HTTPS、請執行下列步驟：

   a. 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。

   b. 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。

如果憑證已過期、您就無法新增叢集。您必須先更新SSL憑證、然後再新增叢集。

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、請檢查下列問題是否存在：

- 如果兩個系統上的時鐘未同步、且Unified Manager HTTPS憑證開始日期晚於叢集上的日期。您必須確保時鐘是使用NTP或類似服務來同步。
- 如果叢集已達到EMS通知目的地的最大數量、則無法新增Unified Manager位址。根據預設、叢集上只能定義20個EMS通知目的地。

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OnCommand 扮演「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
- SNMP版本、設陷目的地主機IP位址、傳出設陷連接埠和社群、以設定SNMP設陷

您必須OnCommand 具備「管理員」或「儲存管理員」角色。

步驟

1. 在工具列中、按一下*、然後按一下左設定功能表中的*通知。
2. 在*設定/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「OnCommand@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OnCommand 扮演「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. 在工具列中、按一下*、然後按一下左設定功能表中的*驗證。
2. 在*設定/驗證*頁面中、選取*啟用遠端驗證*。
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： ◦ `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）

對於驗證類型...	輸入下列資訊...
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. 新增驗證伺服器、並測試驗證。
5. 按一下*儲存並關閉*。

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OnCommand 扮演「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. 在工具列中、按一下*、然後按一下左設定功能表中的*驗證。
2. 在*設定/驗證*頁面中、勾選*停用巢狀群組查詢*方塊。
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OnCommand 扮演「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. 在工具列中、按一下*、然後按一下左設定功能表中的*驗證。
2. 在*設定/驗證*頁面中、按一下*管理伺服器*>*驗證*。
3. 啟用或停用*使用安全連線驗證*選項：

如果您想要...	然後執行此動作...
啟用它	a. 在「啟用遠端驗證」核取方塊中、選取「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。
停用它	a. 在「啟用遠端驗證」核取方塊中、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。

4. 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OnCommand 扮演「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. 在工具列中、按一下*  、然後按一下左設定功能表中的*驗證。
2. 在「設定/驗證」頁面中、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「管理/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OnCommand 扮演「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. 在工具列中、按一下*、然後按一下左管理功能表中的*使用者。
2. 在「管理/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、以便Unified Manager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「管理/指令碼」頁面將指令碼新增至Unified Manager。
- 您必須OnCommand 具備「管理員」或「儲存管理員」角色。

關於這項工作

除了從「組態/警示」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. 在左側導覽窗格中、按一下*組態*>*警示*。
2. 在「組態/警示」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「管理/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. 從<All Volumes whose name contains 'abc'> 「Available Resources（可用資源）」區域中選取「*」、然後將其移至「Selected Resources（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（選擇要執行的腳本）菜單中，選擇* Test*腳本。
8. 按一下「 * 儲存 * 」。

自動新增至**Unified Manager**的**EMS**事件

使用Unified Manager 9.4或更新版本軟體時、下列ONTAP 各項功能可自動新增至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	嚴重性ONTAP
物件存放區存取遭拒、無法進行Aggregate重新配置	arl.netra.ca.check.failed	Aggregate	錯誤
在儲存容錯移轉期間、物件存放區存取遭拒、無法進行集合移轉	gb.netra.ca.check.failed	Aggregate	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
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
可解析的對象儲存區主機	不可解析的objstore.host.unresolvable	節點	錯誤

Unified Manager事件名稱	EMS事件名稱	受影響的資源	嚴重性ONTAP
Objstore InterClusterLifDown	objstore.interclusterlifDown	節點	錯誤
要求不符的物件存放區簽名	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
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	Nbless.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

Unified Manager事件名稱	EMS事件名稱	受影響的資源	嚴重性ONTAP
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
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	監控.vol.NearFull	Volume	警告
Volume邏輯空間已滿	監控.vol.full	Volume	錯誤
Volume邏輯空間正常	監控.vol.one.ok	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

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。*ONTAP 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*組態*>*管理事件*。
2. 在*組態/管理事件*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）。

   "如何在ONTAP 《不統一化管理程式》/《不統一化》中設定「不統一化事件訂閱Active IQ Unified Manager OnCommand 」"

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「表單驗證」、否則使用者在使用Internet Explorer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：

    http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/

  - 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。
- 當使用者嘗試使用Internet Explorer存取Unified Manager時、可能會看到訊息*網站無法顯示頁面*。如果發生這種情況、請務必取消勾選*工具*>*網際網路選項*>*進階*中的「HTTP錯誤訊息的友善程度」選項。

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。
- 您必須建立至少一個具備OnCommand 「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. 在工具列中、按一下*、然後按一下左設定功能表中的*驗證。
2. 在「設定/驗證」頁面中、選取「* SAML驗證*」標籤。
3. 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。

4. 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。

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。

   您現在可以使用此資訊來設定IDP伺服器。

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。

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。在Windows、Red Hat或CentOS上部署Unified Manager時、您可以使用下列Unified Manager CLI命令來變更GUI工作階段逾時： `um option set absolute.session.timeout=00:15:00`此命令會將Unified Manager GUI工作階段逾時設定為15分鐘。

設定資料庫備份設定

您可以設定Unified Manager資料庫備份設定、以設定資料庫備份路徑、保留計數和備份排程。您可以啟用每日或每週排程備份。預設會停用排程備份。

開始之前

- 您必須OnCommand 具備「操作員」、「資訊管理員」或「儲存管理員」角色。
- 在您定義為備份路徑的位置、至少必須有150 GB的可用空間。

  建議您使用Unified Manager主機系統外部的遠端位置。

- 在Linux系統上安裝Unified Manager時、請確認「jboss」使用者對備份目錄具有寫入權限。
- 在Unified Manager收集15天的歷史效能資料時、您不應安排在新增叢集之後立即執行備份作業。

關於這項工作

第一次執行備份所需的時間比後續備份多、因為第一次備份是完整備份。完整備份可能超過1 GB、可能需要三

到四小時。後續備份是遞增的、所需時間較短。

步驟

1. 在工具列中、按一下*、然後按一下*管理>*資料庫備份*。
2. 在「管理/資料庫備份」頁面中、按一下「動作」>「資料庫備份設定」。
3. 設定備份路徑和保留計數的適當值。

   保留計數的預設值為10；您可以使用0建立無限備份。

4. 在「排程頻率」區段中、選取「啟用」核取方塊、然後指定每日或每週排程。
   - * 每日 *

     如果您選取此選項、則必須以24小時格式輸入時間、才能建立備份。例如、如果您指定18：30、則會在每天下午6：30建立備份。

   - * 每週 *

     如果選取此選項、則必須指定建立備份的時間和日期。例如、如果您指定星期一和時間為16：30、則每週備份會在每週一下午4：30建立。

5. 按一下*儲存並關閉*。

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。

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OnCommand 指派「管理員」角色給您執行這些工作。

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OnCommand 會自動指派主機名稱「'還原」、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

您可能基於多種原因產生新的HTTPS安全性憑證、包括您想要使用不同的憑證授權單位簽

署、或是目前的安全性憑證已過期。新憑證會取代現有的憑證。

開始之前

您必須OnCommand 扮演「管理員角色」。

關於這項工作

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。

步驟

1. 在工具列中、按一下*、然後按一下*設定*功能表中的 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	`Click the *Update the Current Certificate Attributes* option.` 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。其他欄位不需要值、但如果您想要在憑證中填入這些值、您可以輸入城市、州和國家的值。 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。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。 +

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. 依照所示順序輸入下列命令、停止Unified Manager軟體及相關的MySQL軟體：
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、請依照所示順序輸入下列命令、重新啟動Unified Manager：