



管理驗證

Active IQ Unified Manager 9.9

NetApp
January 31, 2025

目錄

管理驗證	1
啟用遠端驗證	1
從遠端驗證停用巢狀群組	2
設定驗證服務	3
新增驗證伺服器	4
測試驗證伺服器的組態	5
編輯驗證伺服器	6
刪除驗證伺服器	6
使用Active Directory或OpenLDAP驗證	7
啟用SAML驗證	7
身分識別供應商要求	8
變更用於SAML驗證的身分識別供應商	9
停用SAML驗證	10
稽核記錄	11
驗證視窗和對話方塊說明	13

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。

此外、您也可以啟用SAML驗證、讓遠端使用者在登入Unified Manager Web UI之前、先透過安全的身分識別供應商 (IDP) 進行驗證。

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。

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 *」。

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。

開始之前

- 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">1. 輸入管理員名稱和密碼。2. 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、則基礎辨別名稱就是cn=ou,dc=domain,dc=com。</p>
OpenLDAP	<ol style="list-style-type: none">1. 輸入綁定辨別名稱和綁定密碼。2. 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、則基礎辨別名稱就是cn=ou,dc=domain,dc=com。</p>
其他	<ol style="list-style-type: none">1. 輸入綁定辨別名稱和綁定密碼。2. 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、則基礎辨別名稱就是cn=ou,dc=domain,dc=com。</p> <ol style="list-style-type: none">3. 指定驗證伺服器支援的LDAP傳輸協定版本。4. 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。

1. 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 style="border: 1px solid #ccc; padding: 10px; 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>
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。

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。

開始之前

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。

開始之前

您必須具有應用程式管理員角色。

關於這項工作

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。

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。

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。

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) 。

開始之前

- 您必須擁有IDP URL和中繼資料。
- 您必須擁有IDP的存取權。

關於這項工作

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」。

完成後

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。

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。

關於這項工作

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。

結果

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。

完成後

存取IDP並刪除Unified Manager伺服器URI和中繼資料。

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」的檔案會以壓縮格式下載 .gzip 格式。

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。

關於這項工作

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*>*>*組態。
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。

關於這項工作

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。

憑證應上傳至 .pem 格式。此憑證應從目標Syslog伺服器取得、且不應過期。憑證應包含所選的「主機名稱」、作為的一部分 SubjectAltName (SAN) 屬性。

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：SysLog NG需要使用命令建立憑證的<雜湊> `openssl x509 -noout -hash -in cert.pem`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。

驗證視窗和對話方塊說明

您可以從「設定/驗證」頁面啟用LDAP驗證。

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](#)、則基礎辨別名稱就是 `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](#)、則基礎辨別名稱就是 `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](#)、則基礎辨別名稱就是 `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。

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格式の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)

安裝期間定義の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主機系統のURI。

- 主機中繼資料

XML格式の主機系統中繼資料。

版權資訊

Copyright © 2025 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。