管理驗證

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

目錄

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 及存取您的整個過程中的所有稽核記錄檔。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。

稽核記錄檔會定期歸檔、並儲存至資料庫以供參考。在歸檔之前、稽核記錄會經過數位簽署、以維持安全性和完整性。

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。

   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。

> ◦ 連線逾時 * 值可能會影響組態。如果組態回應所需的時間比定義的值長、可能會因為連線錯誤而導致組態失敗。若要建立成功的連線、請增加 * 連線逾時 * 值、然後再試一次組態。

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 Secure LDAP 用於與 LDAP 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。

  您為_Member _、_User Object Class _和_Group Object Class _屬性輸入的值、應與在Active Directory、OpenLDAP和LDAP組態中新增的值相同。否則、驗證可能會失敗。

- 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。

版權資訊

商標資訊