管理身份驗證

Active IQ Unified Manager

NetApp
October 15, 2025

目錄

管理身份驗證

您可以在 Unified Manager 伺服器上使用 LDAP 或 Active Directory 啟用身份驗證，並將其設定為與您的伺服器協同工作以對遠端使用者進行身份驗證。

若要啟用遠端身分驗證、設定身分驗證服務和新增身分驗證伺服器，請參閱上一節「設定 Unified Manager 以傳送警報通知」。

編輯身份驗證伺服器

您可以變更 Unified Manager 伺服器用於與身分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. 在左側導覽窗格中，按一下「常規」>「遠端驗證」。
2. 勾選“停用巢狀組查找”方塊。
3. 在「驗證伺服器」區域中，選擇要編輯的驗證伺服器，然後按一下「編輯」。
4. 在「編輯身份驗證伺服器」對話方塊中，編輯連接埠詳細資訊。
5. 點選“儲存”。

刪除身份驗證伺服器

如果您想要封鎖 Unified Manager 伺服器與身份驗證伺服器通信，您可以刪除該身份驗證伺服器。例如，如果您想要變更管理伺服器正在與之通訊的身份驗證伺服器，您可以刪除該驗證伺服器並新增新的身份驗證伺服器。

開始之前

您必須具有應用程式管理員角色。

當您刪除身份驗證伺服器時，該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. 在左側導覽窗格中，按一下「常規」>「遠端驗證」。
2. 選擇一個或多個要刪除的身份驗證伺服器，然後按一下「刪除」。
3. 按一下“是”確認刪除請求。

   如果啟用了「使用安全連線」選項，則與驗證伺服器關聯的憑證將與驗證伺服器一起刪除。

使用 **Active Directory** 或 **OpenLDAP** 進行驗證

您可以在管理伺服器上啟用遠端身份驗證，並將管理伺服器設定為與您的身份驗證伺服器

通信，以便身份驗證伺服器內的使用者可以存取 Unified Manager。

您可以使用下列預先定義身分驗證服務之一，也可以指定您自己的身分驗證服務：

- 微軟活動目錄

  您不能使用 Microsoft 輕量級目錄服務。

- OpenLDAP

您可以選擇所需的身份驗證服務並新增適當的身份驗證伺服器，以使身份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憑證由身份驗證伺服器維護。管理伺服器使用輕量級目錄存取協定 (LDAP) 對配置的驗證伺服器內的遠端使用者進行驗證。

對於在 Unified Manager 中建立的本機用戶，管理伺服器維護自己的用戶名稱和密碼資料庫。管理伺服器執行身份驗證，且不使用 Active Directory 或 OpenLDAP 進行身份驗證。

審計日誌

您可以使用稽核日誌偵測稽核日誌是否已外洩。使用者執行的所有活動都受到監控並記錄在稽核日誌中。審核針對Active IQ Unified Manager的所有使用者介面和公開的 API 功能進行。

您可以使用*稽核日誌：檔案檢視*來檢視和存取Active IQ Unified Manager中可用的所有稽核日誌檔案。審計日誌：文件視圖中的文件根據其建立日期列出。此視圖顯示從安裝或升級到系統中現在捕獲的所有審計日誌的資訊。每當您在 Unified Manager 中執行操作時，資訊都會更新並可在日誌中取得。使用「檔案完整性狀態」屬性擷取每個日誌檔案的狀態，該屬性受到主動監控以偵測日誌檔案的篡改或刪除。當系統中有稽核日誌時，稽核日誌可以具有下列狀態之一：

狀態	描述
積極的	目前正在記錄日誌的檔案。
普通的	系統中處於非活動狀態、壓縮並儲存的檔案。
被竄改	該文件已被手動編輯過的使用者破壞。
手動刪除	已被授權使用者刪除的檔案。
滾動刪除	根據滾動配置策略，由於滾動而被刪除的檔案。
意外刪除	由於未知原因而被刪除的檔案。

審計日誌頁麵包括以下命令按鈕：

- 配置
- 刪除

- 下載

使用 **DELETE** 按鈕可以刪除稽核日誌檢視中所列的任何稽核日誌。您可以刪除審計日誌，並可選擇提供刪除檔案的原因，這有助於將來確定有效的刪除。 REASON 欄位列出了原因以及執行刪除操作的使用者的姓名。

刪除日誌檔案將導致檔案從系統中刪除，但資料庫表中的條目不會被刪除。

您可以使用稽核日誌部分中的 **DOWNLOAD** 按鈕從Active IQ Unified Manager下載稽核日誌並匯出稽核日誌檔案。標記為“正常”或“篡改”的檔案以壓縮檔案形式下載 `.gzip`格式。

審計日誌檔案定期歸檔並保存到資料庫以供參考。在存檔之前，審計日誌經過數位簽章以維護安全性和完整性。

產生完整的AutoSupport套件時，支援包將包括存檔和活動審計日誌檔案。但是，當產生輕量級支援包時，它僅包含活動審計日誌。不包括存檔的稽核日誌。

配置審計日誌

您可以使用稽核日誌部分中的「設定」按鈕來設定稽核日誌檔案的捲動策略，並為稽核日誌啟用遠端日誌記錄。

您可以根據要在系統中儲存的資料量和頻率設定*MAX FILE SIZE*和*AUDIT LOG RETENTION DAYS*中的值。欄位 **TOTAL AUDIT LOG SIZE** 中的值是系統中存在的稽核日誌資料的總大小。捲動原則由欄位 **AUDIT LOG RETENTION DAYS**、**MAX FILE SIZE** 和 **TOTAL AUDIT LOG SIZE** 中的值決定。當稽核日誌備份的大小達到*TOTAL AUDIT LOG SIZE*中配置的值時，將刪除第一個已存檔的檔案。這意味著最舊的檔案被刪除。但文件條目仍然在資料庫中可用，並被標記為“`Rollover Delete`”。 **AUDIT LOG RETENTION DAYS** 值表示稽核日誌檔案保留的天數。任何比此欄位中設定的值更舊的檔案都會被翻轉。

步驟

1. 點選*審計日誌*>>*配置*。
2. 在 **MAX FILE SIZE**、**TOTAL AUDIT LOG SIZE** 和 **AUDIT LOG RETENTION DAYS** 中輸入數值。

   如果您想啟用遠端日誌記錄，那麼您應該選擇*啟用遠端日誌記錄*。 /// 2025-6-11，OTHERDOC-133

啟用稽核日誌的遠端記錄

您可以在「設定稽核日誌」對話方塊中選取「啟用遠端日誌記錄」核取方塊來啟用遠端稽核日誌記錄。您可以使用此功能將稽核日誌傳輸到遠端 Syslog 伺服器。這將使您能夠在空間受限的情況下管理稽核日誌。

稽核日誌的遠端記錄提供了防篡改備份，以防Active IQ Unified Manager伺服器上的稽核日誌檔案被篡改。

步驟

1. 在*設定稽核日誌*對話方塊中，選取*啟用遠端日誌記錄*複選框。

   顯示用於配置遠端日誌記錄的附加欄位。

2. 輸入您想要連接的遠端伺服器的 **HOSTNAME** 和 **PORT**。
3. 在*伺服器 CA 憑證*欄位中，按一下*瀏覽*以選擇目標伺服器的公共憑證。

證書應上傳至 `.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 `SubjectAltName`（SAN）屬性。

4. 輸入以下欄位的值：**CHARSET**、**CONNECTION TIMEOUT**、**RECONNECTION DELAY**。

   這些欄位的值應以毫秒為單位。

5. 在 **FORMAT** 和 **PROTOCOL** 欄位中選擇所需的 Syslog 格式和 TLS 協定版本。
6. 如果目標 Syslog 伺服器需要基於憑證的驗證，請勾選「啟用用戶端驗證」複選框。

   在儲存審計日誌配置之前，您需要下載用戶端身份驗證憑證並將其上傳到 Syslog 伺服器，否則連線將失敗。根據 Syslog 伺服器的類型，您可能需要建立用戶端身份驗證憑證的雜湊值。

   範例：syslog-ng 需要使用下列命令建立憑證的 <hash> `openssl x509 -noout -hash -in cert.pem`，然後您應該將客戶端身份驗證憑證符號連結到以 <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日誌記錄。

   您將被重新導向到稽核日誌頁面。

*連線逾時*值會影響配置。如果配置回應的時間比定義值長，則可能會因連線錯誤而導致配置失敗。若要建立成功的連接，請增加*連接逾時*值，然後再次嘗試配置。

遠端身份驗證頁面

您可以使用遠端身份驗證頁面設定 Unified Manager 與您的身份驗證伺服器通信，以對嘗試登入 Unified Manager Web UI 的遠端使用者進行身份驗證。

您必須具有應用程式管理員或儲存管理員角色。

選取啟用遠端身份驗證複選框後，您可以使用身份驗證伺服器啟用遠端身份驗證。

- 認證服務

  使您能夠設定管理伺服器以在目錄服務提供者（例如 Active Directory、OpenLDAP）中對使用者進行驗證，或指定您自己的驗證機制。只有當您啟用了遠端身份驗證時，您才可以指定身份驗證服務。

  - 活動目錄
    - 管理員姓名

      指定認證伺服器的管理員名稱。

    - 密碼

      指定存取認證伺服器的密碼。

    - 基本可分辨名稱

      指定遠端使用者在認證伺服器中的位置。例如，如果認證伺服器的網域是+ou@domain.com+，那麼

基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。

- 禁用嵌套組查找

  指定是否啟用或停用嵌套組查找選項。預設此選項是禁用的。如果您使用 Active Directory，則可以透過停用對嵌套群組的支援來加快身份驗證速度。

- 使用安全連接

  指定用於與身份驗證伺服器通訊的身份驗證服務。

- **OpenLDAP**
  - 綁定可分辨名稱

    指定與基本可分辨名稱一起使用的綁定可分辨名稱，以在身份驗證伺服器中尋找遠端使用者。

  - 綁定密碼

    指定存取認證伺服器的密碼。

  - 基本可分辨名稱

    指定遠端使用者在認證伺服器中的位置。例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。

  - 使用安全連接

    指定使用安全 LDAP 與 LDAP 驗證伺服器進行通訊。

- 其他的
  - 綁定可分辨名稱

    指定綁定可分辨名稱，該名稱與基本可分辨名稱一起使用，以在您配置的身份驗證伺服器中尋找遠端使用者。

  - 綁定密碼

    指定存取認證伺服器的密碼。

  - 基本可分辨名稱

    指定遠端使用者在認證伺服器中的位置。例如，如果認證伺服器的網域是+ou@domain.com+，那麼基本可分辨名稱就是*cn=ou,dc=domain,dc=com*。

  - 協議版本

    指定您的驗證伺服器支援的輕量級目錄存取協定 (LDAP) 版本。您可以指定是否必須自動偵測協定版本或將版本設定為 2 或 3。

  - 使用者名稱屬性

    指定驗證伺服器中的屬性名稱，該屬性包含要由管理伺服器進行驗證的使用者登入名稱。

- 群組成員身分屬性

  指定一個值，該值根據使用者的身份驗證伺服器中指定的屬性和值為遠端使用者指派管理伺服器群組成員身分。

- UGID

  如果遠端使用者作為身分驗證伺服器中 GroupOfUniqueNames 物件的成員，則此選項可讓您根據該 GroupOfUniqueNames 物件中的指定屬性將管理伺服器群組成員身分指派給遠端使用者。

- 禁用嵌套組查找

  指定是否啟用或停用嵌套組查找選項。預設此選項是禁用的。如果您使用 Active Directory，則可以透過停用對嵌套群組的支援來加快身份驗證速度。

- 成員

  指定身份驗證伺服器用於儲存有關群組的各個成員的資訊的屬性名稱。

- 使用者物件類別

  指定遠端認證伺服器中使用者的物件類別。

- 群組物件類別

  指定遠端認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 配置中新增的值相同。否則，身份驗證可能會失敗。

- 使用安全連接

  指定用於與身份驗證伺服器通訊的身份驗證服務。

如果要修改身份驗證服務，請確保刪除所有現有的身份驗證伺服器並新增新的身份驗證伺服器。

身份驗證伺服器區域

身份驗證伺服器區域顯示管理伺服器與之通訊以尋找和驗證遠端使用者的身份驗證伺服器。遠端使用者或群組的憑證由身份驗證伺服器維護。

- 命令按鈕

  使您能夠新增、編輯或刪除身份驗證伺服器。

  - 添加

    使您能夠新增身份驗證伺服器。

  如果您要新增的身份驗證伺服器是高可用性對的一部分（使用相同的資料庫），那麼您也可以新增合作夥伴

驗證伺服器。當其中一個身份驗證伺服器無法存取時，這使得管理伺服器能夠與合作夥伴進行通訊。

- 編輯

  使您能夠編輯選定身份驗證伺服器的設定。

- 刪除

  刪除選定的認證伺服器。

- 姓名或 **IP** 位址

  顯示用於在管理伺服器上驗證使用者的驗證伺服器的主機名稱或 IP 位址。

- 港口

  顯示認證伺服器的連接埠號碼。

- 測試認證

  此按鈕透過驗證遠端使用者或群組來驗證您的身份驗證伺服器的配置。

  測試時，如果僅指定用戶名，管理伺服器會在認證伺服器中搜尋遠端用戶，但不會對用戶進行認證。如果您同時指定使用者名稱和密碼，管理伺服器將搜尋並驗證遠端使用者。

  如果遠端身份驗證已停用，則您無法測試身份驗證。