管理驗證

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/active-iq-unified-manager-918/config/task_edit_authentication_servers.html on November 13, 2026. Always check docs.netapp.com for the latest.

目錄

管理驗證 . . . 1
在 Active IQ Unified Manager 中編輯驗證伺服器 . . . 1
在 Active IQ Unified Manager 中刪除驗證伺服器 . . . 1
在 Active IQ Unified Manager 中使用 Active Directory 或 OpenLDAP 進行驗證 . . . 1
稽核記錄 . . . 2
了解 Active IQ Unified Manager 中的稽核日誌 . . . 2
設定 Active IQ Unified Manager 稽核日誌 . . . 3
在 Active IQ Unified Manager 中啟用稽核日誌的遠端記錄 . . . 3
使用 Active IQ Unified Manager 中的遠端身分驗證頁面 . . . 4
驗證伺服器區域 . . . 6

管理驗證

在 **Active IQ Unified Manager** 中編輯驗證伺服器

您可以變更 Unified Manager 伺服器與驗證伺服器通訊時使用的連接埠。

開始之前

您必須擁有應用程式管理員角色。

步驟

1. 在左側導覽窗格中，按一下 一般 > 遠端驗證。
2. 勾選 停用巢狀群組查閱 核取方塊。
3. 在 驗證伺服器 區域中，選擇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，編輯連接埠詳細資訊。
5. 按一下 **Save** 。

在 **Active IQ Unified Manager** 中刪除驗證伺服器

如果您想要阻止 Unified Manager 伺服器與某個驗證伺服器通訊，可以刪除該驗證伺服器。例如，如果您想要變更管理伺服器正在通訊的驗證伺服器，可以刪除該驗證伺服器並新增新的驗證伺服器。

開始之前

您必須擁有應用程式管理員角色。

刪除驗證伺服器後，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 一般 > 遠端驗證。
2. 選擇一個或多個要刪除的驗證伺服器，然後按一下 刪除。
3. 點擊 是 確認刪除請求。

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

在 **Active IQ Unified Manager** 中使用 **Active Directory** 或 **OpenLDAP** 進行驗證

您可以在管理伺服器上啟用遠端驗證，並將管理伺服器設定為與您的驗證伺服器通訊，以便驗證伺服器中的使用者可以存取 Unified Manager。

您可以使用以下預先定義的驗證服務之一，也可以指定您自己的驗證服務：

- Microsoft Active Directory

您無法使用 Microsoft Lightweight Directory Services。

- OpenLDAP

您可以選取所需的驗證服務並新增適當的驗證伺服器，以讓驗證伺服器中的遠端使用者存取 Unified Manager。遠端使用者或群組的認證由驗證伺服器維護。管理伺服器使用輕量型目錄存取通訊協定 （LDAP） 在已設定的驗證伺服器中驗證遠端使用者。

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，且不使用 Active Directory 或 OpenLDAP 進行驗證。

稽核記錄

了解 **Active IQ Unified Manager** 中的稽核日誌

您可以使用稽核日誌來偵測稽核日誌是否已遭到竄改。使用者執行的所有活動都會受到監控，並記錄在稽核日誌中。稽核涵蓋 Active IQ Unified Manager 的所有使用者介面及公開 API 的功能。

您可以使用 **Audit Log: File View** 檢視和存取 Active IQ Unified Manager 中所有可用的稽核日誌檔。Audit Log: File View 中的檔案會依其建立日期列出。此檢視會顯示從安裝或升級到目前系統中所擷取的所有稽核日誌資訊。每當您在 Unified Manager 中執行行動時，資訊就會更新並提供於日誌中。每個日誌檔的狀態會使用 “File Integrity Status” 屬性來擷取，該屬性會受到主動監控，以偵測日誌檔是否遭到竄改或刪除。當稽核日誌在系統中可用時，稽核日誌可能具有下列其中一種狀態：

狀態	說明
作用中	目前正在記錄日誌的檔案。
正常	系統中儲存的非作用中、已壓縮的檔案。
已竄改	已被使用者手動編輯而遭到破壞的檔案。
MANUAL_DELETE	被授權使用者刪除的檔案。
ROLLOVER_DELETE	因基於滾動組態原則進行滾動而遭刪除的檔案。
UNEXPECTED_DELETE	因不明原因被刪除的檔案。

稽核日誌頁面包含下列命令按鈕：

- 設定
- 刪除
- 下載

DELETE 按鈕可讓您刪除「稽核日誌」檢視中所列的任何稽核日誌。您可以刪除稽核日誌，並可選擇提供刪除檔案的原因，以便未來判斷刪除是否有效。REASON 欄會列出原因以及執行刪除作業的使用者名稱。

刪除日誌檔會將檔案從系統中刪除，但不會刪除資料庫表格中的項目。

您可以使用 Active IQ Unified Manager 中「稽核日誌」區段的 **DOWNLOAD** 按鈕下載稽核日誌，並匯出稽核日

誌檔案。標記為 “NORMAL” 或 “TAMPERED” 的檔案將以壓縮 `.gzip`格式下載。

稽核日誌檔會定期歸檔並儲存到資料庫中以供參考。歸檔前，稽核日誌會進行數位簽章，以維護安全性和完整性。

產生完整的 AutoSupport 套裝組合時，支援套裝組合包含已歸檔和作用中的稽核日誌檔案。但產生精簡支援套裝組合時，僅包含作用中的稽核日誌。不包含已歸檔的稽核日誌。

設定 **Active IQ Unified Manager** 稽核日誌

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輪替原則，並啟用稽核日誌的遠端記錄。

您可以根據您希望在系統中儲存的資料量和頻率，設定 **MAX FILE SIZE** 和 **AUDIT LOG RETENTION DAYS** 的值。**TOTAL AUDIT LOG SIZE** 欄位的值表示系統中存在的稽核日誌資料總量。滾動原則由 **AUDIT LOG RETENTION DAYS** 、 **MAX FILE SIZE** 和 **TOTAL AUDIT LOG SIZE** 欄位的值決定。當稽核日誌備份的大小達到 **TOTAL AUDIT LOG SIZE** 中設定的值時，系統會刪除最先歸檔的檔案。這意味著最舊的檔案將被刪除。但該檔案條目仍保留在資料庫中，並標記為 “Rollover Delete”。**AUDIT LOG RETENTION DAYS** 的值表示稽核日誌檔案的保留天數。任何早於此欄位中設定值的檔案將被滾動刪除。

步驟

1. 按一下 稽核日誌 > > 設定。
2. 在 最大檔案大小、稽核日誌總大小 和 稽核日誌保留天數 中輸入數值。

   若要啟用遠端記錄，請選擇 啟用遠端記錄。

在 **Active IQ Unified Manager** 中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 啟用遠端記錄 核取方塊來啟用遠端稽核記錄。您可以使用此功能將稽核日誌傳輸到遠端 Syslog 伺服器。這可讓您在有空間限制時管理稽核日誌。

遠端記錄稽核日誌可在 Active IQ Unified Manager 伺服器上的稽核日誌檔案被篡改時提供防篡改備份。

步驟

1. 在 設定稽核日誌 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. 輸入要連線的遠端伺服器的*主機名稱*和*連接埠*。
3. 在 伺服器 **CA** 憑證 欄位中，按一下 瀏覽 以選擇目標伺服器的公開憑證。

   憑證應以 `.pem`格式上傳。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 “`hostname`” 作為 `SubjectAltName`（SAN）屬性的一部分。

4. 請輸入下列欄位的值：**CHARSET**、**CONNECTION TIMEOUT**、**RECONNECTION DELAY**。

   這些欄位的值應以毫秒為單位。

5. 請在 **FORMAT** 和 **PROTOCOL** 欄位中選擇所需的 Syslog 格式和 TLS 傳輸協定版本。
6. 如果目標 Syslog 伺服器需要以憑證為基礎的驗證，請選取 啟用用戶端身分驗證 核取方塊。

   您需要在儲存稽核記錄組態之前下載用戶端身分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分驗證憑證的雜湊值。

   範例：syslog-ng 需要使用命令 `openssl x509 -noout -hash -in cert.pem`建立憑證的<hash>，然後您應將用戶端身分驗證憑證以符號連結的方式連結至以<hash> .0 命名的檔案。

7. 點擊 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日誌頁面。

   連線逾時 值會影響組態。如果組態回應時間超過定義的值，則可能會因連線錯誤而導致組態故障。若要成功建立連線，請增加 連線逾時 值，然後重試組態。

使用 **Active IQ Unified Manager** 中的遠端身分驗證頁面

您可以使用遠端驗證頁面設定 Unified Manager 與您的驗證伺服器通訊，以驗證嘗試登入 Unified Manager Web UI 的遠端使用者。

您必須擁有應用程式系統管理員或儲存系統管理員角色。

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

  允許您設定管理伺服器，使其能夠透過目錄服務供應商（例如 Active Directory 、 OpenLDAP ）驗證使用者，或指定您自己的驗證機制。只有在啟用遠端驗證後，才能指定驗證服務。

  - **Active Directory**
    - 系統管理員姓名

      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。

    - 基本辨識名稱

      指定遠端使用者在驗證伺服器中的位置。例如，如果驗證伺服器的網域名稱為 ou@domain.com，則基本可分辨名稱為 **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閱選項。預設情況下，此選項處於停用狀態。如果您使用 Active Directory，則可以透過停用對巢狀群組的支援來加快驗證速度。

    - 使用安全的連線

指定用於與驗證伺服器通訊的驗證服務。

- **OpenLDAP**
  - 連結辨別名稱

    指定與基本可分辨名稱一起使用的連結可分辨名稱，以便在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。

  - 基本辨識名稱

    指定遠端使用者在驗證伺服器中的位置。例如，如果驗證伺服器的網域名稱為 ou@domain.com，則基本可分辨名稱為 **cn=ou,dc=domain,dc=com**。

  - 使用安全的連線

    指定使用安全 LDAP 與 LDAP 驗證伺服器通訊。

- 其他
  - 連結辨別名稱

    指定與基本可分辨名稱一起使用的連結可分辨名稱，以便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。

  - 基本辨識名稱

    指定遠端使用者在驗證伺服器中的位置。例如，如果驗證伺服器的網域名稱為 ou@domain.com，則基本可分辨名稱為 **cn=ou,dc=domain,dc=com**。

  - 傳輸協定版本

    指定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傳輸協定版本，也可以將版本設定為 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進行驗證的使用者登入名稱的屬性名稱。

  - 群組成員屬性

    指定一個值，該值根據使用者驗證伺服器中指定的屬性和值，將管理伺服器群組成員身分指派給遠端使用者。

  - UGID

    如果遠端使用者在驗證伺服器中被包含為 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。

- 停用巢狀群組查詢

  指定是否啟用或停用巢狀群組查閱選項。預設情況下，此選項處於停用狀態。如果您使用 Active Directory，則可以透過停用對巢狀群組的支援來加快驗證速度。

- 成員

  指定驗證伺服器用於儲存有關群組內各個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* 屬性輸入的值應與您的 Active Directory、OpenLDAP 和 LDAP 組態中新增的值相同。否則，驗證可能會失敗。

- 使用安全的連線

  指定用於與驗證伺服器通訊的驗證服務。

如果您要修改驗證服務，請務必刪除任何現有的驗證伺服器，並新增新的驗證伺服器。

驗證伺服器區域

「驗證伺服器」區域顯示管理伺服器用於尋找和驗證遠端使用者的驗證伺服器。遠端使用者或群組的憑證由驗證伺服器維護。

- 命令按鈕

  允許您新增、編輯或刪除驗證伺服器。

  - 新增

    允許您新增驗證伺服器。

  如果您新增的驗證伺服器是高可用性配對（使用相同資料庫）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，與合作夥伴進行通訊。

  - 編輯

    允許您編輯所選驗證伺服器的設定。

  - 刪除

    刪除選定的驗證伺服器。

- 名稱或 **IP** 位址

顯示用於在管理伺服器上驗證使用者身分的驗證伺服器的主機名稱或 IP 位址。

- 連接埠

  顯示驗證伺服器的連接埠號碼。

- 測試驗證

  此按鈕透過驗證遠端使用者或群組來驗證您的驗證伺服器組態。

  測試時，如果僅指定使用者名稱，管理伺服器會在驗證伺服器中搜尋遠端使用者，但不會驗證該使用者。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

Copyright © 2026 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。