



G

SANtricity commands

NetApp
June 16, 2025

目錄

- G 1
 - 身份驗證入門 - SANtricity CLI 1
 - 外部金鑰管理入門 - SANtricity CLI 1
 - 工作流程步驟 1
 - 內部金鑰管理入門 - SANtricity CLI 2
 - 工作流程步驟 2

G

身份驗證入門 - SANtricity CLI

驗證需要使用者以指派的登入認證來存取系統。每個使用者登入都會與包含特定角色和存取權限的使用者設定檔建立關聯。

系統管理員可實作系統驗證、如下所示：

- 使用儲存陣列中強制執行的RBAC（角色型存取控制）功能、包括預先定義的使用者和角色。
- 連線至LDAP（輕量型目錄存取傳輸協定）伺服器 and 目錄服務（例如Microsoft的Active Directory）、然後將LDAP使用者對應至儲存陣列的內嵌角色。
- 使用安全聲明標記語言（SAML）2.0與身分識別供應商（IDP）連線、然後將使用者對應至儲存陣列的內嵌角色。



SAML是儲存陣列的內嵌功能（韌體層級8.42及更新版本）、只能從SANtricity「支援系統管理程式」使用者介面進行設定。

外部金鑰管理入門 - SANtricity CLI

安全金鑰是一串字元、可在已啟用安全功能的磁碟機和儲存陣列中的控制器之間共用。使用外部金鑰管理時、您可以在金鑰管理伺服器上建立及維護安全金鑰

如SANtricity 需使用外部金鑰管理伺服器和安全金鑰的概念資訊、請參閱《支援系統管理員》線上說明。

以下是實作外部安全金鑰的基本工作流程：

1. 產生憑證簽署要求
2. 從KMIP伺服器取得用戶端和伺服器憑證
3. 安裝用戶端憑證
4. 設定KMIP伺服器的IP位址和連接埠號碼
5. 測試與KMIP伺服器的通訊
6. 建立儲存陣列安全金鑰
7. 驗證安全金鑰

工作流程步驟

SANtricity 11.40版本的新安全功能包括憑證管理和外部金鑰管理。若要開始使用、請使用下列基本步驟：

1. 使用「儲存陣列keyManagementClientCSR」命令產生憑證簽署要求。請參閱 [產生金鑰管理憑證簽署要求](#)。
2. 從KMIP伺服器要求用戶端和伺服器憑證。
3. 使用「download storageArray keyManagementCertificate」命令安裝用戶端憑證、並將「certificateType」參數設為「client」。請參閱 [安裝儲存陣列外部金鑰管理憑證](#)。

4. 使用「download storageArray keyManagementCertificate」命令安裝伺服器憑證、並將「certificateType」參數設為「伺服器」。請參閱 [安裝儲存陣列外部金鑰管理憑證](#)。
5. 使用「set storageArray externalKeyManagement」命令、設定金鑰管理伺服器的IP位址和連接埠號碼。請參閱 [設定外部金鑰管理設定](#)。
6. 使用「Start storageArray externalKeyManagement test」命令測試與外部金鑰管理伺服器的通訊。請參閱 [測試外部金鑰管理通訊](#)。
7. 使用「create storageArray SECURITY Key」命令建立安全金鑰。請參閱 [建立安全金鑰](#)。
8. 使用「validate storageArray securityKey」命令驗證安全金鑰。請參閱 [驗證內部或外部安全金鑰](#)。

內部金鑰管理入門 - SANtricity CLI

安全金鑰是一串字元、可在已啟用安全功能的磁碟機和儲存陣列中的控制器之間共用。使用內部金鑰管理時、您可以在控制器的持續記憶體上建立及維護安全金鑰。

如SANtricity 需使用內部安全金鑰的概念性資訊、請參閱《支援系統管理員》線上說明。

以下是使用內部安全金鑰的基本工作流程：

1. 建立安全金鑰
2. 設定安全金鑰
3. 驗證安全金鑰

工作流程步驟

下列命令可讓您開始使用內部安全金鑰：

1. 使用「create storageArray SECURITY Key」命令建立儲存陣列安全金鑰。請參閱 [建立儲存陣列安全金鑰](#)。
2. 使用「set storageArray SECURITY Key」命令設定儲存陣列安全金鑰。請參閱 [設定儲存陣列安全金鑰](#)。
3. 使用「validate storageArray securityKey」命令驗證安全金鑰。請參閱 [驗證儲存陣列安全金鑰](#)。

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。