驗證與存取控制
ONTAP 9

NetApp
February 12, 2026

目錄

驗證與存取控制

驗證與存取控制總覽

您可以管理 ONTAP 叢集驗證、以及對 ONTAP Web 服務的存取控制。

使用 System Manager 或 CLI 、您可以控制並保護用戶端和管理員對叢集和儲存設備的存取。

如果您使用的是傳統系統管理員（僅適用於 ONTAP 9.7 及更早版本）、請參閱 "System Manager Classic（ONTAP 版本9.0至9.7）"

用戶端驗證與授權

利用信任的來源驗證用戶端機器和使用者的身分、藉此驗證其身分。ONTAP利用比較使用者的認證資料與檔案或目錄上設定的權限、即可授權使用者存取檔案或目錄。ONTAP

系統管理員驗證與**RBAC**

系統管理員使用本機或遠端登入帳戶、驗證自己是否已進入叢集和儲存VM。角色型存取控制（RBAC）決定系統管理員可以存取的命令。

管理系統管理員驗證和 **RBAC**

瞭解 **ONTAP** 中的系統管理員驗證和 **RBAC**

您可以為ONTAP 叢集管理員和儲存虛擬機器（SVM）管理員啟用登入帳戶。您也可以使用角色型存取控制（RBAC）來定義系統管理員的功能。

您可以使用下列驗證類型、讓本機系統管理員帳戶存取管理儲存虛擬機器（SVM）或資料SVM：

- "密碼"
- "SSH公開金鑰"
- "SSL 憑證"
- "SSH多因素驗證（MFA）"

  從支援使用密碼和公開金鑰的驗證功能、從ONTAP 功能表9.3開始。

您可以使用下列驗證類型、讓遠端系統管理員帳戶存取管理SVM或資料SVM：

- "Active Directory"

  從 ONTAP 9.13.1 開始，您可以使用 SSH 公開金鑰做為 Active Directory 使用者的主要或次要驗證方法。

- "SAML驗證（僅適用於管理SVM）"

  從ONTAP Sf9.3開始、安全聲明標記語言（SAML）驗證可用於使用下列任一Web服務存取管理SVM：服務

處理器基礎架構、ONTAP Sf0 API或系統管理員。

- "LDAP 或 NIS"

  從ONTAP 版本9.4開始、SSH MFA可用於LDAP或NIS伺服器上的遠端使用者。支援使用nsswitch和公開金鑰進行驗證。

ONTAP 系統管理員驗證和 RBAC 工作流程

您可以啟用本機系統管理員帳戶或遠端系統管理員帳戶的驗證。本機帳戶的帳戶資訊位於儲存系統上、遠端帳戶的帳戶資訊則位於其他位置。每個帳戶都可以擁有預先定義的角色或自訂角色。

1 完成組態工作表

在建立登入帳戶及設定角色型存取控制 (RBAC) 之前，您應該先收集中每個項目的資訊"組態工作表"。

2 判斷系統管理員帳戶是本機帳戶還是遠端帳戶

- * 如果為本機： * 啟用"密碼"，，"SSH" "SSH MFA"或"SSL"存取。
- * 如果是遠端： * 判斷遠端存取的類型。取決於存取類型，"啟用 Active Directory 存取"，"啟用 LDAP 或 NIS 存取"或"設定 SAML 驗證（僅適用於管理 SVM ）"。

3 設定角色型存取

指派給系統管理員的角色會決定系統管理員可以存取的命令。角色會在您建立系統管理員帳戶時指派，稍後也可以指派"已修改"。您可以為和"SVM"管理員或"定義自訂角色"視需要使用預先定義的角色"叢集"。

4 管理系統管理員帳戶

根據您啟用帳戶存取權限的方式，您可能需要關聯"具有本機帳戶的公開金鑰" ， 管理"公開金鑰和 X.509 憑證"，配置"適用於 SSH 登入的 Cisco 雙核心 2FA" ，安裝一個"CA簽署的伺服器數位憑證"或配置"Active Directory" ， "LDAP 或 NIS"訪問。您可以在啟用帳戶存取權限之前或之後執行任何這些任務。

5 設定其他安全功能

- "管理多管理員驗證"如果您想確保某些作業需要指定的系統管理員核准。
- "管理動態授權"如果您想根據使用者的信任層級動態套用其他授權檢查，
- "設定即時 (JIT) 權限提升"如果您想要允許使用者暫時存取提升的權限來執行某些任務。

ONTAP 系統管理員驗證和 RBAC 設定工作表

在建立登入帳戶及設定角色型存取控制（RBAC）之前、您應該先收集組態工作表中每個項目的資訊。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

建立或修改登入帳戶

當您啟用登入帳戶以存取儲存 VM 時，您可以使用命令提供這些值 `security login create`。如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

修改帳戶存取儲存 VM 的方式時，您可以使用命令提供相同的值 `security login modify`。如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	帳戶存取的儲存 VM 名稱。預設值為叢集的管理儲存 VM 名稱。	
`-user-or-group-name`	帳戶的使用者名稱或群組名稱。指定群組名稱可讓您存取群組中的每個使用者。您可以將使用者名稱或群組名稱與多個應用程式建立關聯。	
`-application`	用於存取儲存 VM 的應用程式： • `http` • `ontapi` • `snmp` • `ssh`	
`-authmethod`	用於驗證帳戶的方法： • `cert` 用於 SSL 憑證驗證 • `domain` 用於 Active Directory 驗證 • `nsswitch` 用於 LDAP 或 NIS 驗證 • `password` 用於使用者密碼驗證 • `publickey` 用於公開金鑰驗證 • `community` 適用於 SNMP 社群字串 • `usm` 適用於 SNMP 使用者安全模式 • `saml` 用於安全聲明標記語言（SAML）驗證	

`-remote-switch-ipaddress`	遠端交換器的IP位址。遠端交換器可以是由叢集交換器健全狀況監控器（CSHM）監控的叢集交換器、或MetroCluster 是由不健全狀況監控器（MCC-HM）監控的光纖通道（FC）交換器。此選項僅適用於應用程式 `snmp` 驗證方法是 `usm`。	
`-role`	指派給帳戶的存取控制角色： • 對於叢集（管理儲存 VM ）、預設值為 `admin`。 • 對於資料儲存 VM 、預設值為 `vsadmin`。	
`-comment`	（選用）帳戶的說明文字。您應該以雙引號（"）括住文字。	
`-is-ns-switch-group`	帳戶是 LDAP 群組帳戶還是 NIS 群組帳戶 (`yes` 或 `no`）。	
`-second-authentication -method`	多因素驗證的第二種驗證方法： • `none` 如果不使用多因素驗證、則為預設值 • `publickey` 用於公開金鑰驗證 `authmethod` 為密碼或 nsswitch • `password` 用於使用者密碼驗證 `authmethod` 為公開金鑰 • `nsswitch` 驗證方法為 publickey 時用於使用者密碼驗證 驗證順序一律是公開金鑰、然後是密碼。	
`-is-ldap-fastbind`	從「支援支援支援」9.11.1開始ONTAP 、設定為「真」時、會啟用LDAP快速連結以進行Nsswitch驗證；預設值為「假」。要使用 LDAP 快速綁定，必須將該 `-authentication-method`值設置爲 `nsswitch`。"使用 LDAP 快速綁定對 ONTAP NFS SVM 進行 nsswitch 驗證"。	

設定 **Cisco** 雙核心安全性資訊

當您為儲存 VM 啟用 Cisco 雙核心雙因素驗證並登入 SSH 時，您可以使用命令提供這些值 `security login duo create`。如"指令參考資料ONTAP"需詳細 `security login duo create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	套用雙核心驗證設定的儲存 VM （在 ONTAP CLI 中稱為 vserver ）。	
`-integration-key`	您的整合金鑰是在向 DuoTM 註冊 SSH 應用程式時取得的。	
`-secret-key`	您的秘密金鑰是在向 DuoTM 註冊 SSH 應用程式時取得的。	
`-api-host`	API 主機名稱、是在使用 DuoTM 登錄 SSH 應用程式時取得的。例如： `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	若發生服務或組態錯誤而無法進行雙核心驗證、則會失敗 `safe` （允許存取）或 `secure` （拒絕存取）。預設值為 `safe`這表示如果由於無法存取雙核心 API 伺服器等錯誤而失敗、就會略過雙核心驗證。	
`-http-proxy`	使用指定的 HTTP Proxy 。如果 HTTP Proxy 需要驗證、請在 Proxy URL 中加入認證。例如： `http-proxy=http://username:password@proxy.example.org:8080`	

`-autopush`	也可以 `true` 或 `false`。預設為 `false`。如果 `true`，雙核會自動將推入登錄請求發送至用戶的電話，如果推入不可用，則會恢復至電話呼叫。請注意、這會有效停用密碼驗證。如果 `false`，系統會提示使用者選擇驗證方法。 當設定為時 `autopush = true`、建議您進行設定 `max-prompts = 1`。	
`-max-prompts`	如果使用者無法以第二個因素驗證、則 DUO 會提示使用者再次驗證。此選項可設定在拒絕存取之前、 DUO 顯示的提示數量上限。必須是 `1`、 `2`或 `3`。預設值為 `1`。 例如、何時 `max-prompts = 1`，使用者必須在第一個提示字元上成功驗證，如果是的話 `max-prompts = 2`如果使用者在初始提示時輸入不正確的資訊、系統會提示使用者再次驗證。 當設定為時 `autopush = true`、建議您進行設定 `max-prompts = 1`。 為了獲得最佳體驗、只有公共金鑰驗證的使用者將永遠擁有 `max-prompts` 設定為 `1`。	
`-enabled`	啟用雙核心雙因素驗證。設定為 `true` 依預設。啟用時、會根據設定的參數、在 SSH 登入期間強制執行雙核心雙因素驗證。當雙核心停用時（設為 `false`）、會忽略雙核心驗證。	
`-pushinfo`	此選項會在推播通知中提供其他資訊、例如正在存取的應用程式或服務名稱。這有助於使用者驗證登入的服務是否正確、並提供額外的安全層。	

定義自訂角色

您可以在定義自訂角色時，使用命令提供這些值 `security login role create`。如"指令參考資料ONTAP"需詳細 `security login role create`資訊，請參閱。

欄位	說明	您的價值
-vserver	（選用）與角色相關聯的儲存 VM 名稱（在 ONTAP CLI 中稱為 vserver ）。	
-role	角色名稱。	
-cmddirname	角色提供存取權的命令或命令目錄。您應該以雙引號（"）括住命令子目錄名稱。例如、 "volume snapshot"。您必須輸入 DEFAULT 指定所有命令目錄。	
-access	（選用）角色的存取層級。對於命令目錄： • none （自訂角色的預設值）會拒絕存取命令目錄中的命令 • readonly 授予存取權 show 命令目錄及其子目錄中的命令 • all 授予對命令目錄及其子目錄中所有命令的存取權 用於 _nonnonnalin 命令 _ （不以結尾的命令） create、 modify、 delete`或 `show）： • none （自訂角色的預設值）拒絕存取命令 • readonly 不適用 • all 授予對命令的存取權 若要授與或拒絕內部命令的存取權、您必須指定命令目錄。	
-query	（選用）用於篩選存取層級的查詢物件、其格式為命令的有效選項或命令目錄中的命令的有效選項。您應該以雙引號（"）括住查詢物件。例如、如果命令目錄為 volume，查詢物件 "-aggr aggr0" 將啟用的存取 aggr0 僅 Aggregate 。	

將公開金鑰與使用者帳戶建立關聯

當您將 SSH 公開金鑰與使用者帳戶建立關聯時，您可以使用命令提供這些值 security login publickey create。如"指令參考資料ONTAP"需詳細 `security login publickey create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	（選用）帳戶存取的儲存 VM 名稱。	
`-username`	帳戶的使用者名稱。預設值、`admin`，這是叢集管理員的預設名稱。	
`-index`	公開金鑰的索引編號。如果金鑰是為帳戶建立的第一個金鑰、則預設值為0；否則、預設值大於該帳戶現有的最高索引編號。	
`-publickey`	OpenSSH公開金鑰。您應該以雙引號（"）括住金鑰。	
`-role`	指派給帳戶的存取控制角色。	
`-comment`	（選用）公開金鑰的說明文字。您應該以雙引號（"）括住文字。	
`-x509-certificate`	（選用）從 ONTAP 9.13.1 開始、可讓您管理與 SSH 公開金鑰的 X.509 憑證關聯。 當您將 X.509 憑證與 SSH 公開金鑰建立關聯時、 ONTAP 會在 SSH 登入時檢查此憑證是否有效。如果已過期或遭撤銷、則不允許登入、並停用相關的 SSH 公開金鑰。可能值： • `install`：安裝指定的 PEM 編碼的 X.509 憑證、並將其與 SSH 公開金鑰建立關聯。包含您要安裝之憑證的完整文字。 • `modify`：使用指定的證書更新現有的 PEM 編碼的 X.509 證書，並將其與 SSH 公共密鑰相關聯。包含新憑證的完整文字。 • `delete`：移除現有的 X.509 憑證與 SSH 公開金鑰的關聯。	

設定動態授權全域設定

從 ONTAP 9.15.1 開始，您可以使用命令提供這些值 `security dynamic-authorization modify`。如"指令參考資料ONTAP"需詳細 `security dynamic-authorization modify`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	應修改其信任分數設定的儲存 VM 名稱。如果省略此參數、則會使用叢集層級的設定。	
`-state`	動態授權模式。可能值： • `disabled`：（預設）停用動態授權。 • `visibility`：此模式可用於測試動態授權。在此模式中、信任分數會針對每個受限活動進行檢查、但不會強制執行。但是、任何會被拒絕或受到其他驗證挑戰的活動都會記錄下來。 • `enforced`：在您完成測試之後、請使用 `visibility` 模式。在此模式中、每個受限活動都會檢查信任分數、如果符合限制條件、則會強制執行活動限制。也會強制執行抑制間隔、以防止在指定時間間隔內發生其他驗證挑戰。	
`-suppression-interval`	防止在指定時間間隔內發生其他驗證挑戰。時間間隔為 ISO-8601 格式、可接受 1 分鐘至 1 小時的值（含 1 小時）。如果設為 0 、則會停用抑制時間間隔、並在需要驗證挑戰時一律提示使用者。	
`-lower-challenge-boundary`	較低的多因素驗證（ MFA ）挑戰百分比界限。有效範圍為 0 到 99 。值 100 無效、因為這會導致拒絕所有要求。預設值為 0 。	
`-upper-challenge-boundary`	MFA 上限挑戰百分比界限。有效範圍為 0 至 100 。此值必須等於或大於下限值。值為 100 表示每個要求都會遭到拒絕或受到額外的驗證挑戰；沒有任何要求會在沒有挑戰的情況下被允許。預設值為 90 。	

安裝**CA**簽署的伺服器數位憑證

當您產生數位憑證簽署要求（ CSR ）以將儲存 VM 驗證為 SSL 伺服器時，您可以使用命令提供這些值 `security certificate generate-csr`。如"指令參考資料ONTAP"需詳細 `security certificate generate-csr`資訊，請參閱。

欄位	說明	您的價值
-common-name	憑證的名稱、可以是完整網域名稱（FQDN）或自訂通用名稱。	
-size	私密金鑰中的位元數。價值越高、金鑰就越安全。預設值為 2048。可能的值包括 512、 1024、 1536`和 `2048。	
-country	儲存 VM 的國家 / 地區、以兩個字母的代碼表示。預設值為 US。如需代碼清單，請參閱"指令參考資料ONTAP"。	
-state	儲存 VM 的州或省。	
-locality	儲存 VM 的位置。	
-organization	儲存 VM 的組織。	
-unit	儲存 VM 組織中的單位。	
-email-addr	儲存 VM 連絡管理員的電子郵件地址。	
-hash-function	用於簽署憑證的密碼編譯雜湊功能。預設值為 SHA256。可能的值包括 SHA1、 SHA256`和 `MD5。	

當您安裝 CA 簽署的數位憑證以將叢集或儲存 VM 驗證為 SSL 伺服器時，您可以使用命令提供這些值 security certificate install。下表僅顯示與帳戶組態相關的選項。如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。

欄位	說明	您的價值
-vserver	要安裝憑證的儲存 VM 名稱。	

`-type`	憑證類型： • `server` 適用於伺服器憑證和中繼憑證 • `client-ca` 用於 SSL 用戶端根 CA 的公開金鑰憑證 • `server-ca` 用於 ONTAP 為用戶端之 SSL 伺服器根 CA 的公開金鑰憑證 • `client` 適用於自我簽署或 CA 簽署的數位憑證、以及 ONTAP 做為 SSL 用戶端的私密金鑰	

設定**Active Directory**網域控制器存取

當您已為資料儲存 VM 設定 SMB 伺服器，並且想要將儲存 VM 設定為閘道或 *tunnel* ，以便 Active Directory 網域控制器存取叢集時，您可以使用命令提供這些值 `security login domain-tunnel create`。如"指令參考資料ONTAP"需詳細 `security login domain-tunnel create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	已設定 SMB 伺服器的儲存 VM 名稱。	

當您尚未設定 SMB 伺服器，且想要在 Active Directory 網域上建立儲存 VM 電腦帳戶時，您可以使用命令提供這些值 `vserver active-directory create`。如"指令參考資料ONTAP"需詳細 `vserver active-directory create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	要為其建立 Active Directory 電腦帳戶的儲存 VM 名稱。	
`-account-name`	電腦帳戶的NetBios名稱。	
`-domain`	完整網域名稱（FQDN）。	
`-ou`	網域中的組織單位。預設值為 `CN=Computers`。將此值附加到網域名稱、以產生Active Directory辨別名稱。ONTAP	

設定**LDAP**或**NIS**伺服器存取

當您為儲存 VM 建立 LDAP 用戶端組態時，可以使用命令提供這些值 `vserver services name-service ldap client create`。如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap client create`資訊，請參閱。

下表僅顯示與帳戶組態相關的選項：

欄位	說明	您的價值
`-vserver`	用戶端組態的儲存 VM 名稱。	
`-client-config`	用戶端組態的名稱。	
`-ldap-servers`	以逗號分隔的 IP 位址清單、以及用戶端所連線之 LDAP 伺服器的主機名稱。	
`-schema`	用戶端用來進行LDAP查詢的架構。	
`-use-start-tls`	用戶端是否使用 Start TLS 來加密與 LDAP 伺服器的通訊 (`true` 或 `false`) 。 支援 Start TLS 、僅能存取資料儲存 VM 。不支援存取管理儲存 VM 。	

當您將 LDAP 用戶端組態與儲存 VM 建立關聯時，可以使用命令提供這些值 `vserver services name-service ldap create`。如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	要與用戶端組態建立關聯的儲存 VM 名稱。	
`-client-config`	用戶端組態的名稱。	
`-client-enabled`	儲存 VM 是否可以使用 LDAP 用戶端組態 (`true` 或 `false`) 。	

當您在儲存 VM 上建立 NIS 網域組態時，可以使用命令提供這些值 `vserver services name-service nis-domain create`。如"指令參考資料ONTAP"需詳細 `vserver services name-service nis-domain create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	要在其中建立網域組態的儲存 VM 名稱。	

`-domain`	網域名稱。	
`-nis-servers`	網域組態所使用之 NIS 伺服器的 IP 位址和主機名稱的逗號分隔清單。	

當您指定名稱服務來源的查詢順序時，您可以使用命令來提供這些值 `vserver services name-service ns-switch create`。如"指令參考資料ONTAP"需詳細 `vserver services name-service ns-switch create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	要設定名稱服務查詢順序的儲存 VM 名稱。	
`-database`	名稱服務資料庫： • `hosts` 適用於檔案和 DNS 名稱服務 • `group` 適用於檔案、 LDAP 和 NIS 名稱服務 • `passwd` 適用於檔案、 LDAP 和 NIS 名稱服務 • `netgroup` 適用於檔案、 LDAP 和 NIS 名稱服務 • `namemap` 適用於檔案和 LDAP 名稱服務	
`-sources`	查詢名稱服務來源的順序（在以逗號分隔的清單中）： • `files` • `dns` • `ldap` • `nis`	

設定**SAML**存取

從 ONTAP 9.3 開始，您可以使用 `security saml-sp create`命令來設定 SAML 驗證。如"指令參考資料ONTAP"需詳細 `security saml-sp create`資訊，請參閱。

欄位	說明	您的價值

`-idp-uri`	身分識別供應商（IDP）主機的FTP位址或HTTP位址、可從該主機下載IDP中繼資料。	
`-sp-host`	SAML服務供應商主機ONTAP （亦即系統）的主機名稱或IP位址。根據預設、會使用叢集管理LIF的IP位址。	
`-cert-ca` 和 `-cert-serial`或 `-cert-common-name`	服務供應商主機ONTAP 的伺服器認證詳細資料（不知系統如何）。您可以輸入服務供應商的憑證發行憑證授權單位（CA）和憑證序號、或是伺服器憑證一般名稱。	
`-verify-metadata-server`	IDP 中繼資料伺服器的身分識別是否必須驗證 `true` 或 `false`）。最佳實務做法是永遠將此值設為 `true`。	

建立登入帳戶

瞭解如何建立 **ONTAP** 登入帳戶

您可以啟用本機或遠端叢集和SVM系統管理員帳戶。本機帳戶是指帳戶資訊、公開金鑰或安全性憑證位於儲存系統上的帳戶。AD帳戶資訊儲存在網域控制器上。LDAP和NIS帳戶位於LDAP和NIS伺服器上。

叢集與**SVM**管理員

_叢集管理員_存取叢集的管理SVM。管理員 SVM 和具有保留名稱的叢集管理員 `admin` 會在叢集設定時自動建立。

具有預設值的叢集管理員 `admin` 角色可以管理整個叢集及其資源。叢集管理員可視需要建立其他具有不同角色的叢集管理員。

_SVM系統管理員_存取資料SVM。叢集管理員會視需要建立資料SVM和SVM管理員。

SVM 系統管理員會被指派 `vsadmin` 依預設、角色。叢集管理員可視需要指派不同的角色給SVM管理員。

命名慣例

下列一般名稱無法用於遠端叢集和 SVM 系統管理員帳戶：

- "ADM"
- " 垃圾桶 "
- "CL1"
- " 常駐程式 "

- "FTP"
- " 遊戲 "
- " 停止 "
- "LP"
- " 郵件 "
- " 男性 "
- " 拍攝範圍 "
- 「 NetApp 」
- " 新聞 "
- " 無人 "
- " 營運者 "
- " 根目錄 "
- " 關機 "
- "sshd"
- " 同步 "
- " 系統 "
- "uucp"
- "www"

合併的角色

如果您為同一位使用者啟用多個遠端帳戶、則會將為該帳戶指定的所有角色指派給該使用者。也就是說、如果已指派 LDAP 或 NIS 帳戶 `vsadmin` 角色、以及指派給相同使用者的 AD 群組帳戶 `vsadmin-volume` 角色、 AD 使用者以更具包容性的方式登入 `vsadmin` 功能。這些角色據說是_合併_。

啟用本機帳戶存取

瞭解如何啟用本機 **ONTAP** 帳戶存取

本機帳戶是指帳戶資訊、公開金鑰或安全性憑證位於儲存系統上的帳戶。您可以使用 `security login create`命令啟用本機帳戶來存取管理或資料 SVM 。

相關資訊

- "建立安全登入"

啟用 **ONTAP** 帳戶密碼存取

您可以使用 `security login create`命令來啟用系統管理員帳戶，以密碼存取管理員或資料 SVM 。輸入命令後、系統會提示您輸入密碼。

關於這項工作

如果您不確定要指派給登入帳戶的存取控制角色，可以使用 `security login modify`命令稍後再新增該角色。

如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 讓本機系統管理員帳戶使用密碼存取SVM：

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   下列命令可啟用叢集管理員帳戶 `admin1` 使用預先定義的 `backup` 存取管理 SVM 的角色`engCluster` 使用密碼。輸入命令後、系統會提示您輸入密碼。

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

   如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

啟用 **ONTAP** 帳戶 **SSH** 公開金鑰存取

您可以使用 `security login create`命令，讓系統管理員帳戶使用 SSH 公開金鑰存取管理或資料 SVM 。

關於這項工作

- 您必須先將公開金鑰與帳戶建立關聯、帳戶才能存取SVM。

  將公開金鑰與使用者帳戶建立關聯

  您可以在啟用帳戶存取之前或之後執行此工作。

- 如果您不確定要指派給登入帳戶的存取控制角色，可以使用 `security login modify`命令稍後再新增該角色。

  如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

如果您想在叢集上啟用FIPS模式、則必須使用支援的金鑰類型來重新設定現有SSH公開金鑰帳戶、而不需要支援的金鑰演算法。 在您啟用FIPS之前、應先重新設定帳戶、否則系統管理員驗證將會失敗。

下表指出ONTAP 支援哪些主機金鑰類型演算法來進行支援以利執行支援的SSH連線。 這些金鑰類型不適用於設定SSH公用驗證。

發行版ONTAP	FIPS模式支援的金鑰類型	非FIPS模式支援的金鑰類型

9.11.1 及更新版本	ECDSA-SHA2-nistp256	ECDSA-SHA2-nistp256 RSA-SHA2-512 RSA-SHA2-256 SSH-ed25519 SSH-DSS SSH-RSA
9.10.1及更早版本	ECDSA-SHA2-nistp256 SSH-ed25519.	ECDSA-SHA2-nistp256 SSH-ed25519 SSH-DSS SSH-RSA

從 ONTAP 9.11.1 開始、移除對 ssh-ed25519 主機金鑰演算法的支援。

如需更多資訊、請參閱 "使用FIPS設定網路安全性"。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 允許本機系統管理員帳戶使用SSH公開金鑰存取SVM：

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   下列命令可啟用 SVM 管理員帳戶 `svmadmin1` 使用預先定義的 `vsadmin-volume` 存取 SVM 的角色`engData1` 使用 SSH 公開金鑰：

   ```
   cluster1::>security login create -vserver engData1 -user-or-group-name
   svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
   ```

   如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

完成後

如果您尚未將公開金鑰與系統管理員帳戶建立關聯、則必須先建立公開金鑰、帳戶才能存取SVM。

將公開金鑰與使用者帳戶建立關聯

啟用多因素驗證（ **MFA** ）帳戶

瞭解 **ONTAP** 多因素驗證

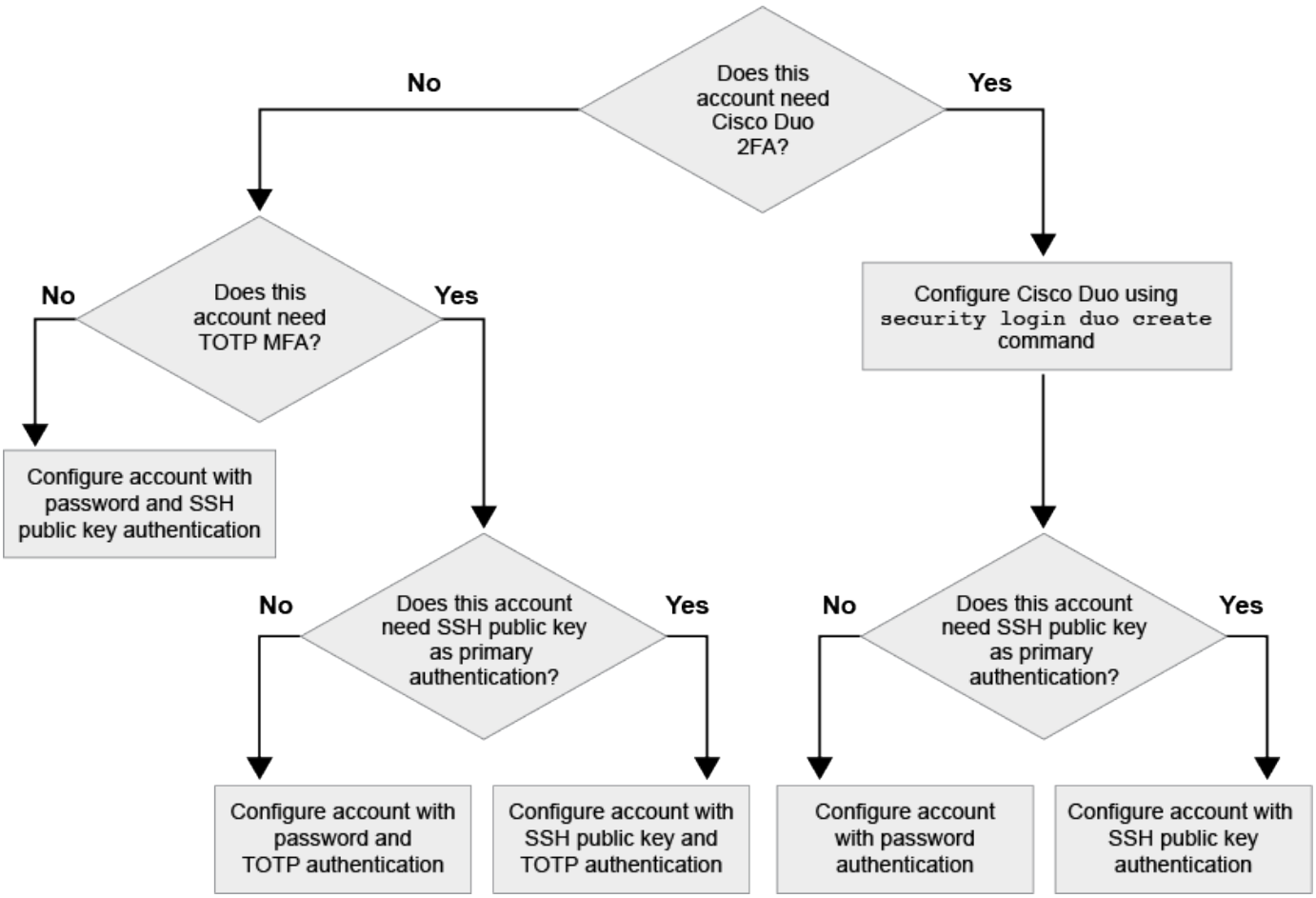
多因素驗證（ MFA ）可讓您要求使用者提供兩種驗證方法來登入管理或資料儲存 VM 、以增強安全性。

視您的 ONTAP 版本而定、您可以結合使用 SSH 公開金鑰、使用者密碼和時間型一次性密碼（ TOTP ）進行多

因素驗證。當您啟用和設定 Cisco Duo （ ONTAP 9.14.1 及更新版本）時、它會作為額外的驗證方法、以補充所有使用者的現有方法。

可從 ... 開始使用。	第一種驗證方法	第二種驗證方法
ONTAP 9.14.1.	SSH公開金鑰	TOTP
	使用者密碼	TOTP
	SSH公開金鑰	Cisco DuoTM
	使用者密碼	Cisco DuoTM
ONTAP 9.13.1.12.9.11.9.11.	SSH公開金鑰	TOTP
	使用者密碼	TOTP
ONTAP 9.3	SSH公開金鑰	使用者密碼

如果已設定 MFA 、叢集管理員必須先啟用本機使用者帳戶、則該帳戶必須由本機使用者設定。



使用 **SSH** 和 **TOTP** 啟用 **ONTAP** 多因素驗證

多因素驗證（ MFA ）可讓您要求使用者提供兩種驗證方法來登入管理或資料 SVM 、以增強安全性。

關於這項工作

- 您必須是叢集管理員才能執行此工作。
- 如果您不確定要指派給登入帳戶的存取控制角色，可以使用 `security login modify`命令稍後再新增該角色。

  如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

  "修改指派給系統管理員的角色"

- 如果您使用公開金鑰進行驗證、則必須先將公開金鑰與帳戶建立關聯、帳戶才能存取 SVM 。

  "將公開金鑰與使用者帳戶建立關聯"

  您可以在啟用帳戶存取之前或之後執行此工作。

- 從S廳9.12.1開始ONTAP 、您可以使用FIDO2（Fast Identity Online）或個人身分驗證（PIV）驗證標準、將Yobikey硬體驗證裝置用於SSH用戶端MFA。

使用 **SSH** 公開金鑰和使用者密碼來啟用 **MFA**

從 ONTAP 9.3 開始、叢集管理員可以設定本機使用者帳戶、使用 SSH 公開金鑰和使用者密碼登入 MFA 。

1. 使用 SSH 公開金鑰和使用者密碼、在本機使用者帳戶上啟用 MFA ：

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_name> -application ssh -authentication-method <password|publickey>
   -role admin -second-authentication-method <password|publickey>
   ```

   下列命令需要 SVM 系統管理員帳戶 `admin2` 使用預先定義的 `admin` 登入 SVM 的角色`engData1` 使用 SSH 公開金鑰和使用者密碼：

   ```
   cluster-1::> security login create -vserver engData1 -user-or-group-name
   admin2 -application ssh -authentication-method publickey -role admin
   -second-authentication-method password

   Please enter a password for user 'admin2':
   Please enter it again:
   Warning: To use public-key authentication, you must create a public key
   for user "admin2".
   ```

   如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

使用 **TOTP** 啟用 **MFA**

從 ONTAP 9.13.1 開始、您可以要求本機使用者同時使用 SSH 公開金鑰或使用者密碼和時間型一次性密碼（ TOTP ）登入管理或資料 SVM 、以增強安全性。啟用 MFA 與 TOTP 的帳戶後、本機使用者必須登入 "完成組態設定"。

TOTP 是一種電腦演算法、使用目前時間來產生一次性密碼。 如果使用 TOTP 、它永遠是 SSH 公開金鑰或使用

者密碼之後的第二種驗證形式。

開始之前

您必須是儲存管理員才能執行這些工作。

步驟

您可以將 MFA 設為使用者密碼或 SSH 公開金鑰做為第一種驗證方法、並將 TOTP 設為第二種驗證方法。

使用使用者密碼和 **TOTP** 啟用 **MFA**

1. 使用使用者密碼和 TOTP 啟用多因素驗證的使用者帳戶。

   ◦ 適用於新使用者帳戶 *

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   ◦ 適用於現有使用者帳戶 *

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. 確認 MFA 已啟用 TOTP ：

   ```
   security login show
   ```

使用 **SSH** 公開金鑰和 **TOTP** 啟用 **MFA**

1. 使用 SSH 公開金鑰和 TOTP 啟用多因素驗證的使用者帳戶。

   ◦ 適用於新使用者帳戶 *

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role>
   -comment <comment>
   ```

   ◦ 適用於現有使用者帳戶 *

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   +
   如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

2. 確認 MFA 已啟用 TOTP ：

```
security login show
```

如"指令參考資料ONTAP"需詳細 `security login show`資訊，請參閱。

完成後

- 如果您尚未將公開金鑰與系統管理員帳戶建立關聯、則必須先建立公開金鑰、帳戶才能存取SVM。

  "將公開金鑰與使用者帳戶建立關聯"

- 本機使用者必須登入才能使用 TOTP 完成 MFA 組態。

  "使用 TOTP 設定 MFA 的本機使用者帳戶"

相關資訊

- "支援多因素驗證ONTAP 功能（TR-4647）"
- "指令參考資料ONTAP"

使用 **TOTP** 設定 **MFA** 的本機 **ONTAP** 使用者帳戶

從 ONTAP 9.13.1 開始，使用者帳戶可以使用時間型一次性密碼（ TOTP ）來設定多因素驗證（ MFA ）。

開始之前

- 儲存管理員必須 "使用 TOTP 啟用 MFA" 作為使用者帳戶的第二種驗證方法。
- 您的主要使用者帳戶驗證方法應為使用者密碼或公開 SSH 金鑰。
- 您必須將 TOTP 應用程式設定為與智慧型手機搭配使用、並建立 TOTP 秘密金鑰。

  支援 Microsoft Authenticator 、 Google Authenticator 、 Authy 及任何其他 TOTP 相容驗證器。

步驟

1. 使用目前的驗證方法登入您的使用者帳戶。

   您目前的驗證方法應該是使用者密碼或 SSH 公開金鑰。

2. 在您的帳戶上建立 TOTP 組態：

```
security login totp create -vserver "<svm_name>" -username
"<account_username >"
```

3. 確認您的帳戶已啟用 TOTP 組態：

```
security login totp show -vserver "<svm_name>" -username
"<account_username>"
```

相關資訊

- "安全登入 totp 創建"
- "安全登入 totp 顯示"

重設 **ONTAP** 使用者帳戶的 **TOTP** 秘密金鑰

為了保護您的帳戶安全、如果 TOTP 秘密金鑰遭到洩漏或遺失、您應該停用該金鑰並建立新的金鑰。

如果金鑰遭到入侵、請重設 **TOTP**

如果您的 TOTP 秘密金鑰已洩漏、但您仍有權存取、您可以移除洩漏的金鑰並建立新的金鑰。

1. 使用您的使用者密碼或 SSH 公開金鑰、以及您遭入侵的 TOTP 秘密金鑰、登入您的使用者帳戶。
2. 移除遭入侵的 TOTP 秘密金鑰：

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. 建立新的 TOTP 秘密金鑰：

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. 確認您的帳戶已啟用 TOTP 組態：

```
security login totp show -vserver <svm_name> -username
<account_username>
```

如果金鑰遺失、請重設 **TOTP**

如果 TOTP 秘密金鑰遺失、請聯絡您的儲存管理員 "停用金鑰"。停用金鑰後、您可以使用第一種驗證方法登入並設定新的 TOTP 。

開始之前

TOTP 秘密金鑰必須由儲存管理員停用。
如果您沒有儲存管理員帳戶、請聯絡您的儲存管理員以停用金鑰。

步驟

1. 儲存管理員停用 TOTP 密碼後、請使用主要驗證方法登入您的本機帳戶。
2. 建立新的 TOTP 秘密金鑰：

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. 確認您的帳戶已啟用 TOTP 組態：

```
security login totp show -vserver <svm_name> -username
<account_username>
```

相關資訊

- "安全登入 totp 創建"
- "安全登入 totp 刪除"
- "安全登入 totp 顯示"

停用 **ONTAP** 使用者帳戶的 **TOTP** 秘密金鑰

如果本機使用者的時間型一次性密碼（ TOTP ）秘密金鑰遺失、則儲存管理員必須先停用遺失的金鑰、使用者才能建立新的 TOTP 秘密金鑰。

關於這項工作

此工作只能從叢集管理員帳戶執行。

步驟

1. 停用 TOTP 秘密金鑰：

```
security login totp modify -vserver <svm_name> -username
<account_username> -enabled false
```

如"指令參考資料ONTAP"需詳細 `security login totp modify`資訊，請參閱。

啟用 **SSL** 憑證 **ONTAP** 帳戶存取

您可以使用 `security login create`命令來啟用系統管理員帳戶，以 SSL 憑證存取管理或資料 SVM 。

關於這項工作

- 您必須先安裝CA簽署的伺服器數位憑證、帳戶才能存取SVM。

  產生及安裝CA簽署的伺服器憑證

您可以在啟用帳戶存取之前或之後執行此工作。

- 如果您不確定要指派給登入帳戶的存取控制角色、可以稍後再使用新增該角色 `security login modify` 命令。

  修改指派給系統管理員的角色

> 對於叢集管理員帳戶、支援憑證驗證 `http`、 `ontapi`和 `rest` 應用程式：對於 SVM 系統管理員帳戶、僅支援憑證驗證 `ontapi` 和 `rest` 應用程式：

步驟

1. 啟用本機系統管理員帳戶、以使用SSL憑證存取SVM：

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   下列命令可啟用 SVM 管理員帳戶 `svmadmin2` 使用預設值 `vsadmin` 存取 SVM 的角色`engData2` 使用 SSL 數位憑證。

   ```
   cluster1::>security login create -vserver engData2 -user-or-group-name
   svmadmin2 -application ontapi -authmethod cert
   ```

   如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

完成後

如果您尚未安裝CA簽署的伺服器數位憑證、則必須先安裝該憑證、帳戶才能存取SVM。

產生及安裝CA簽署的伺服器憑證

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

啟用 **Active Directory ONTAP** 帳戶存取

您可以使用 `security login create`命令來啟用 Active Directory （ AD ）使用者或群組帳戶，以存取管理員或資料 SVM 。AD群組中的任何使用者都可以使用指派給群組的角色來存取SVM。

關於這項工作

- 您必須先設定AD網域控制器存取叢集或SVM、帳戶才能存取SVM。

  設定Active Directory網域控制器存取

  您可以在啟用帳戶存取之前或之後執行此工作。

- 從 ONTAP 9.13.1 開始、您可以使用 SSH 公開金鑰做為主要或次要驗證方法、並提供 AD 使用者密碼。

  如果您選擇使用 SSH 公開金鑰做為主要驗證、則不會進行 AD 驗證。

- 從 ONTAP 9.11.1 開始，如果 AD LDAP 伺服器支援，您可以使用"使用 LDAP 快速綁定對 ONTAP NFS SVM 進行 nsswitch 驗證"。
- 如果您不確定要指派給登入帳戶的存取控制角色，可以使用 `security login modify`命令稍後再新增該角色。

  如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

  修改指派給系統管理員的角色

僅支援 AD 群組帳戶存取 `SSH`、 `ontapi`和 `rest` 應用程式：SSH 公開金鑰驗證通常用於多因素驗證、因此不支援 AD 群組。

開始之前

- 叢集時間必須在AD網域控制器上的時間後五分鐘內同步處理。
- 您必須是叢集管理員才能執行此工作。

步驟

1. 啟用AD使用者或群組管理員帳戶以存取SVM：

   ◦ 針對 AD 使用者： *

版本**ONTAP**	主要驗證	次要驗證	命令
9.13.1 及更新版本	公開金鑰	無	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

版本**ONTAP**	主要驗證	次要驗證	命令

9.13.1 及更新版本	網域	公開金鑰	• 適用於新使用者 *
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			• 適用於現有使用者 *
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

9.0 及更新版本	網域	無	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

◦ 對於 AD 群組： *

版本**ONTAP**	主要驗證	次要驗證	命令
9.0 及更新版本	網域	無	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

完成後

如果您尚未設定AD網域控制器對叢集或SVM的存取、則必須先設定、帳戶才能存取SVM。

設定Active Directory網域控制器存取

相關資訊

- "建立安全登入"

啟用 **LDAP** 或 **NIS ONTAP** 帳戶存取

您可以使用 `security login create`命令來啟用 LDAP 或 NIS 使用者帳戶，以存取管理或資料 SVM 。如果您尚未設定LDAP或NIS伺服器存取SVM、則必須先設定、帳戶才能存取SVM。

關於這項工作

- 不支援群組帳戶。
- 您必須先設定LDAP或NIS伺服器存取SVM、帳戶才能存取SVM。

  設定LDAP或NIS伺服器存取

  您可以在啟用帳戶存取之前或之後執行此工作。

- 如果您不確定要指派給登入帳戶的存取控制角色，可以使用 `security login modify`命令稍後再新增該角色。

  如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

  修改指派給系統管理員的角色

- 從ONTAP 功能支援的版本為2、9.4開始、透過LDAP或NIS伺服器、遠端使用者可支援多因素驗證（MFA）。
- 從 ONTAP 9.11.1 開始，如果 LDAP 伺服器支援，您可以使用"使用 LDAP 快速綁定對 ONTAP NFS SVM 進行 nsswitch 驗證"。
- 由於已知的 LDAP 問題、您不應使用 `':'` （結腸） LDAP 使用者帳戶資訊任何欄位中的字元（例如、 `gecos`、 `userPassword`等）。否則、該使用者的查詢作業將會失敗。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 啟用LDAP或NIS使用者或群組帳戶以存取SVM：

   ```
   security login create -vserver SVM_name -user-or-group-name user_name
   -application application -authmethod nsswitch -role role -comment comment -is
   -ns-switch-group yes|no [-is-ldap-fastbind true]
   ```

   "建立或修改登入帳戶"

   下列命令可啟用 LDAP 或 NIS 叢集管理員帳戶 `guest2` 使用預先定義的 `backup` 存取管理 SVM 的角色`engCluster`。

```
cluster1::>security login create -vserver engCluster -user-or-group-name
guest2 -application ssh -authmethod nsswitch -role backup
```

如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

2. 為LDAP或NIS使用者啟用MFA登入：

```
security login modify -user-or-group-name rem_usr1 -application ssh
-authentication-method nsswitch -role admin -is-ns-switch-group no -second
-authentication-method publickey
```

驗證方法可以指定為 `publickey` 和第二種驗證方法 `nsswitch`。

下列範例顯示正在啟用MFA驗證：

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

完成後

如果您尚未設定LDAP或NIS伺服器存取SVM、則必須先設定、帳戶才能存取SVM。

設定LDAP或NIS伺服器存取

相關資訊

- "安全登入"

管理存取控制角色

瞭解如何管理 **ONTAP** 存取控制角色

指派給系統管理員的角色會決定系統管理員可以存取的命令。當您為系統管理員建立帳戶時、可以指派角色。您可以指派不同的角色、或視需要定義自訂角色。

修改指派給 **ONTAP** 管理員的角色

您可以使用 `security login modify`命令來變更叢集或 SVM 管理員帳戶的角色。您可以指派預先定義或自訂的角色。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 變更叢集或SVM管理員的角色：

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

"建立或修改登入帳戶"

下列命令會變更 AD 叢集管理員帳戶的角色 `DOMAIN1\guest1` 至預先定義的 `readonly` 角色：

```
cluster1::>security login modify -vserver engCluster -user-or-group-name
DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
```

下列命令會變更 AD 群組帳戶中 SVM 管理員帳戶的角色 `DOMAIN1\adgroup` 自訂 `vol_role` 角色：

```
cluster1::>security login modify -vserver engData -user-or-group-name
DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
```

如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

為 ONTAP 管理員定義自訂角色

您可以使用 `security login role create`命令來定義自訂角色。您可以視需要多次執行命令、以取得想要與角色建立關聯的確切功能組合。

關於這項工作

- 無論是預先定義或自訂的角色、都會授予或拒絕ONTAP 存取各種指令或命令目錄。

  命令目錄 (`volume`（例如）是一組相關命令和命令子目錄。除非如本程序所述、否則授與或拒絕存取命令目錄會授與或拒絕存取目錄及其子目錄中的每個命令。

- 特定命令存取或子目錄存取會覆寫父目錄存取。

  如果某個角色是以命令目錄定義、然後以不同的存取層級再次定義、以用於特定命令或父目錄的子目錄、則為該命令或子目錄指定的存取層級會覆寫父目錄的存取層級。

> ⓘ 您無法為 SVM 管理員指派一個角色、讓其存取僅供使用的命令或命令目錄 `admin` 叢集管理員、例如 `security` 命令目錄。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 定義自訂角色：

   ```
   security login role create -vserver SVM_name -role role -cmddirname
   command_or_directory_name -access access_level -query query
   ```

下列命令會授與 `vol_role` 角色完整存取中的命令 `volume` 命令目錄及中命令的唯讀存取權 `volume snapshot` 子目錄。

```
cluster1::>security login role create -role vol_role -cmddirname
"volume" -access all

cluster1::>security login role create -role vol_role -cmddirname "volume
snapshot" -access readonly
```

下列命令會授與 `SVM_storage` 角色對中命令的唯讀存取權 `storage` 命令目錄、無法存取中的命令 `storage encryption` 子目錄、以及對的完整存取權 `storage aggregate plex offline` 非固有命令。

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

如"指令參考資料ONTAP"需詳細 `security login role create`資訊，請參閱。

相關資訊

- "建立安全登入角色"
- "離線儲存Aggregate叢"
- "儲存加密"

預先定義的 **ONTAP** 叢集管理員角色

叢集管理員的預先定義角色應能滿足您大部分的需求。您可以視需要建立自訂角色。依預設、會指派預先定義的叢集管理員 `admin` 角色：

下表列出叢集管理員的預先定義角色：

此角色...	具有此存取層級...	至下列命令或命令目錄
管理	全部	所有命令目錄 (`DEFAULT`)

Admin-NO FSA （從 ONTAP 9.12.1 開始提供）	讀取/寫入	• 所有命令目錄 (DEFAULT) • security login rest-role • security login role
唯讀	• security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics	無
volume file show-disk-usage	AutoSupport	全部
• set • system node autosupport	無	所有其他命令目錄 (DEFAULT)
備份	全部	vserver services ndmp
唯讀	volume	無
所有其他命令目錄 (DEFAULT)	唯讀	全部

• `security login password` 僅用於管理自己的使用者帳戶本機密碼和金鑰資訊 • `set`	• 從 ONTAP 9.8 開始，只讀 • ONTAP 9.8 之前，無	`security`
唯讀	所有其他命令目錄 (`DEFAULT`)	SnapLock
全部	• `set` • `volume create` • `volume modify` • `volume move` • `volume show`	無
• `volume move governor` • `volume move recommend`	無	所有其他命令目錄 (`DEFAULT`)
無	無	所有命令目錄 (`DEFAULT`)

。 `autosupport` 角色會指派給預先定義的 `autosupport` 帳戶、由 AutoSupport OnDemand 使用。ONTAP 可防止您修改或刪除 `autosupport` 帳戶。ONTAP 也會防止您指派 `autosupport` 其他使用者帳戶的角色。

相關資訊

- "安全登入"
- "設定"
- "Volume"
- "Vserver 服務 NDMP"

預先定義的 **ONTAP SVM** 管理員角色

SVM系統管理員的預先定義角色應能滿足您大部分的需求。您可以視需要建立自訂角色。根據預設、系統會指派預先定義的 SVM 管理員 `vsadmin` 角色：

下表列出SVM系統管理員的預先定義角色：

角色名稱	功能

vsadmin	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 管理磁碟區、磁碟區移動除外 • 管理配額， qtree ，快照和檔案 • 管理LUN • 執行SnapLock 不含權限刪除的功能 • 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP • 設定服務：DNS、LDAP及NIS • 監控工作 • 監控網路連線和網路介面 • 監控SVM的健全狀況
vsadmin-volume	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 管理磁碟區、磁碟區移動除外 • 管理配額， qtree ，快照和檔案 • 管理LUN • 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP • 設定服務：DNS、LDAP及NIS • 監控網路介面 • 監控SVM的健全狀況
vsadmin-Protocol	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP • 設定服務：DNS、LDAP及NIS • 管理LUN • 監控網路介面 • 監控SVM的健全狀況
vsadmin-Backup	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 管理NDMP作業 • 使還原的Volume能夠讀取/寫入 • 管理 SnapMirror 關係和快照 • 檢視磁碟區和網路資訊

vsadmin-SnapLock	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 管理磁碟區、磁碟區移動除外 • 管理配額， qtree ，快照和檔案 • 執行SnapLock 包含特權刪除在內的功能 • 設定傳輸協定：NFS和SMB • 設定服務：DNS、LDAP及NIS • 監控工作 • 監控網路連線和網路介面
vsadmin-readonly	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 監控SVM的健全狀況 • 監控網路介面 • 檢視磁碟區和LUN • 檢視服務與傳輸協定

使用系統管理員管理 **ONTAP** 管理員存取

指派給系統管理員的角色會決定系統管理員可以使用System Manager執行哪些功能。叢集管理員和儲存VM管理員的預先定義角色由System Manager提供。 您可以在建立系統管理員帳戶時指派角色、也可以稍後指派不同的角色。

視啟用帳戶存取的方式而定、您可能需要執行下列任一項：

- 將公開金鑰與本機帳戶建立關聯。
- 安裝CA簽署的伺服器數位憑證。
- 設定AD、LDAP或NIS存取。

您可以在啟用帳戶存取之前或之後執行這些工作。

指派角色給系統管理員

指派角色給系統管理員、如下所示：

步驟

1. 選擇*叢集>設定*。
2. 選取 → * 使用者與角色 * 旁的。
3. 在 * 使用者 * 下選取 + Add 。
4. 指定使用者名稱、然後在下拉式功能表中選取*角色*的角色。
5. 指定使用者的登入方法和密碼。

變更系統管理員的角色

變更系統管理員的角色、如下所示：

步驟

1. 按一下*叢集>設定*。
2. 選取您要變更其角色的使用者名稱、然後按一下 ⋮ 出現在使用者名稱旁的。
3. 按一下 * 編輯 * 。
4. 在下拉式功能表中選取*角色*的角色。

在**ONTAP**中存取 **JIT** 權限提升

從ONTAP 9.17.1 開始，叢集管理員可以"配置即時（JIT）權限提升"允許ONTAP使用者暫時提升其權限以執行某些任務。為使用者設定 JIT 後，使用者可以將其權限暫時提升到具有執行任務所需權限的角色。會話到期後，使用者將恢復其原始存取等級。

叢集管理員可以設定使用者存取 JIT 提升的時長。例如，叢集管理員可以將使用者存取 JIT 提升的權限配置為每次會話 30 分鐘（會話有效期），為期 30 天（JIT 有效期）。在 30 天的期限內，使用者可以根據需要多次提升權限，但每次會話的時長限制為 30 分鐘。

關於這項工作

- JIT 權限提升僅適用於使用 SSH 存取ONTAP的使用者。提升的權限僅在目前 SSH 會話中可用，但您可以根據需要在任意數量的並發 SSH 會話中提升權限。
- JIT 權限提升僅支援使用密碼、nsswitch 或網域驗證登入的使用者。 JIT 權限提升不支援多重身分驗證 (MFA)。
- 如果設定的會話或 JIT 有效期到期，或叢集管理員撤銷使用者的 JIT 存取權限，則使用者的 JIT 會話將會終止。

開始之前

- 若要存取 JIT 權限提升，叢集管理員必須為您的帳戶設定 JIT 存取權限。叢集管理員將確定您可以提升權限的角色，以及您可以存取提升權限的時間長度。

步驟

1. 暫時將您的權限提升至配置的角色：

   ```
   security jit-privilege elevate
   ```

   輸入此指令後，系統會提示您輸入登入密碼。如果您的帳戶配置了 JIT 存取權限，您將在配置的會話時間長度內獲得提升的存取權限。會話時長到期後，您將恢復到原始存取等級。您可以在設定的 JIT 有效期內根據需要多次提升權限。

2. 查看 JIT 會話中的剩餘時間：

   ```
   security jit-privilege show-remaining-time
   ```

如果您目前處於 JIT 會話中，此命令將顯示剩餘時間。

3. 如果需要，請提前結束 JIT 會話：

```
security jit-privilege reset
```

如果您目前處於 JIT 會話中，此命令將結束 JIT 會話並恢復您的原始存取等級。

在**ONTAP**中設定 **JIT** 權限提升

從ONTAP 9.17.1 開始，叢集管理員可以設定即時 (JIT) 權限提升，以允許ONTAP使用者暫時提升其權限以執行某些任務。為使用者配置 JIT 後，他們可以臨時"提升他們的特權"賦予具有執行任務所需權限的角色。會話持續時間到期後，使用者將恢復其原始存取等級。

叢集管理員可以設定使用者存取 JIT 提升的時長。例如，您可以設定使用者存取 JIT 提升的時長，在 30 天的時間內（即「JIT 有效期」），每次會話的時長限制為 30 分鐘（即「會話有效期限」）。在這 30 天的時間段內，使用者可以根據需要多次提升權限，但每次會話的時間限制為 30 分鐘。

JIT 權限提升支援最小權限原則，讓使用者執行需要提升權限的任務，而無需永久授予這些權限。這有助於降低未經授權的存取或意外更改系統的風險。以下範例描述了 JIT 權限提升的一些常見用例：

- 允許臨時訪問 `security login create`和 `security login delete`命令來啟用使用者的入職和離職。
- 允許臨時訪問 `system node image update`和 `system node upgrade-revert`在更新視窗期間。更新完成後，命令存取權限將被撤銷。
- 允許臨時訪問 `cluster add-node`， `cluster remove-node`， 和 `cluster modify`以啟用叢集擴充或重新配置。叢集變更完成後，命令存取權限將被撤銷。
- 允許臨時訪問 `volume snapshot restore`啟用還原作業和備份目標管理。還原或設定完成後，命令存取權限將被撤銷。
- 允許臨時訪問 `security audit log show`在合規性檢查期間啟用稽核日誌審查和匯出。

如需查看更詳細的常見 JIT 用例列表，請參閱常見的 JIT 用例 。

叢集管理員可以為ONTAP使用者設定 JIT 存取權限，並在整個叢集範圍內或為特定 SVM 配置預設 JIT 有效期。

關於這項工作

- JIT 權限提升僅適用於使用 SSH 存取ONTAP的使用者。提升的權限僅在使用者目前的 SSH 會話中可用，但使用者可以根據需要在任意數量的並發 SSH 會話中提升權限。
- JIT 權限提升僅支援使用密碼、nsswitch 或網域驗證登入的使用者。 JIT 權限提升不支援多重身分驗證 (MFA)。

開始之前

- 您必須是ONTAP叢集管理員 `admin`權限等級來執行下列任務。

修改全域 **JIT** 設定

您可以修改ONTAP叢集全域或特定 SVM 的預設 JIT 設定。這些設定決定了已配置 JIT 存取的使用者的預設會話有效期和最大 JIT 有效期。

關於這項工作

- 預設 `default-session-validity-period`值為一小時。此設定決定使用者在 JIT 會話中可以存取提升權限的時間，之後需要重新提升權限。
- 預設 `max-jit-validity-period`值為 90 天。此設定決定了使用者在配置的開始日期之後可以存取 JIT 提升權限的最長期限。您可以為單一使用者設定 JIT 有效期，但不能超過最長 JIT 有效期。

步驟

1. 檢查目前 JIT 設定：

```
security jit-privilege show -vserver <svm_name>
```

`-vserver`是可選的。如果您未指定 SVM，則命令將顯示全域 JIT 設定。

2. 全域或針對 SVM 修改 JIT 設定：

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

如果您未指定 SVM，則命令將修改全域 JIT 設定。以下範例將 SVM 的預設 JIT 會話時長設定為 45 分鐘，最大 JIT 長度設定為 30 天 `svm1` ：+
`security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

在此範例中，使用者將能夠一次存取 45 分鐘的 JIT 提升，並且可以在配置的開始日期之後最多 30 天內啟動 JIT 工作階段。

為使用者配置 **JIT** 權限提升存取權限

您可以為ONTAP使用者指派 JIT 權限提升存取權限。

步驟

1. 檢查使用者目前的 JIT 存取權限：

```
security jit-privilege user show -username <username>
```

`-username`是可選的。如果您未指定使用者名，該命令將顯示所有使用者的 JIT 存取權限。

2. 為使用者指派新的 JIT 存取權限：

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

- 如果 `-vserver`未指定，則在叢集層級分配 JIT 存取。
- `-role`是使用者將被提升到的 RBAC 角色。如果未指定， `-role`預設為 `admin`。
- `-session-validity-period`是使用者在需要啟動新的 JIT 會話之前可以存取提升角色的時間長度。如果未指定，則全域或 SVM `default-session-validity-period`被使用。
- `-jit-validity-period`是使用者在配置的開始日期之後可以發起 JIT 會話的最長持續時間。如果未指定，則 `session-validity-period`被使用。此參數不能超過全域或 SVM `max-jit-validity-period`。
- `-start-time`是使用者可以啟動 JIT 會話的日期和時間。如果未指定，則使用目前日期和時間。

  下面的例子將允許 `ontap_user`訪問 `admin`角色運行 1 小時後才需要開始新的 JIT 會話。 `ontap_user`將能夠從 2025 年 7 月 1 日下午 1 點開始啟動為期 60 天的 JIT 會話：+
  `security jit-privilege user create -username ontap_user -role admin -session-validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"`

3. 如果需要，撤銷使用者的 JIT 存取權限：

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

此命令將撤銷使用者的 JIT 存取權限，即使其存取權限尚未過期。如果 `-vserver`如果未指定，則 JIT 存取權限將在叢集層級撤銷。如果使用者處於活動的 JIT 會話中，則該會話將被終止。

常見的 **JIT** 用例

下表包含 JIT 權限提升的常見用例。對於每個用例，都需要配置一個 RBAC 角色來提供對相關命令的存取權限。每個命令都連結到ONTAP命令參考，其中包含有關該命令及其參數的更多資訊。

使用案例	命令	細節
使用者和角色管理	• `security login create` • `security login delete`	在入職或離職期間暫時提升新增/刪除使用者或變更角色的權限。
證書管理	• `security certificate create` • `security certificate install`	授予證書安裝或更新的短期存取權限。
SSH/CLI 存取控制	• `security login create -application ssh`	暫時授予 SSH 存取權限以進行故障排除或供應商支援。
授權管理	• `system license add` • `system license delete`	授予在功能啟動或停用期間新增或刪除許可證的權限。

使用案例	命令	細節
系統升級和修補	• `system node image update` • `system node upgrade-revert`	提升升級窗口，然後撤銷。
網路安全設定	• `security login role create` • `security login role modify`	允許對網路相關的安全角色進行臨時更改。
叢集管理	• `cluster add-node` • `cluster remove-node` • `cluster modify`	提升叢集擴充或重新配置。
SVM 管理	• `vserver create` • `vserver delete` • `vserver modify`	暫時授予 SVM 管理員權限以進行設定或停用。
磁碟區管理	• `volume create` • `volume delete` • `volume modify`	提升磁碟區配置、調整大小或刪除的權限。
快照管理	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	提升快照刪除或在復原期間復原的權限。
網路組態	• `network interface create` • `network port vlan create`	授予在維護時段內進行網路變更的權利。
磁碟/聚合管理	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	提升新增或刪除磁碟或管理聚合的能力。

使用案例	命令	細節
資料保護	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	暫時提升以配置或恢復SnapMirror關係。
效能調優	• `qos policy-group create` • `qos policy-group modify`	提升性能故障排除或調整。
審計日誌訪問	• `security audit log show`	在合規性檢查期間暫時提升稽核日誌審查或匯出權限。
事件和警報管理	• `event notification create` • `event notification modify`	提升設定或測試事件通知或 SNMP 陷阱的權限。
合規性驅動的數據訪問	• `volume show` • `security audit log show`	授予審計員臨時唯讀存取權限以審查敏感資料或日誌。
特權訪問審查	• `security login show` • `security login role show`	暫時提升權限以審查和報告特權存取權限。在限定時間內授予唯讀權限。

相關資訊

- "叢集"
- "事件通知"
- "網路"
- "QoS策略組"
- "安全性"
- "SnapMirror"
- "貯存"
- "系統"
- "Volume"
- "Vserver"

管理系統管理員帳戶

瞭解如何管理 **ONTAP** 系統管理員帳戶

視啟用帳戶存取的方式而定、您可能需要將公開金鑰與本機帳戶建立關聯、安裝CA簽署的

伺服器數位憑證、或設定AD、LDAP或NIS存取。您可以在啟用帳戶存取之前或之後執行所有這些工作。

將公開金鑰與 ONTAP 系統管理員帳戶建立關聯

若要進行SSH公開金鑰驗證、您必須先將公開金鑰與系統管理員帳戶建立關聯、帳戶才能存取SVM。您可以使用 `security login publickey create`命令將金鑰與系統管理員帳戶建立關聯。

關於這項工作

如果您同時使用密碼和SSH公開金鑰透過SSH驗證帳戶、則會先使用公開金鑰驗證帳戶。

開始之前

- 您必須已產生SSH金鑰。
- 您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 將公開金鑰與系統管理員帳戶建立關聯：

   ```
   security login publickey create -vserver SVM_name -username user_name -index
   index -publickey certificate -comment comment
   ```

   如"指令參考資料ONTAP"需詳細 `security login publickey create`資訊，請參閱。

2. 檢視公開金鑰以驗證變更：

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

   如"指令參考資料ONTAP"需詳細 `security login publickey show`資訊，請參閱。

範例

下列命令會將公開金鑰與 SVM 管理員帳戶建立關聯 `svmadmin1` 適用於 SVM `engData1`。公開金鑰已指派索引編號5。

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

管理 ONTAP 系統管理員的 SSH 公開金鑰和 X.509 憑證

為了提高使用系統管理員帳戶的 SSH 驗證安全性，您可以使用 `security login publickey` 一組命令來管理 SSH 公開金鑰及其與 X.509 憑證的關聯性。

將公開金鑰和 X.509 憑證與系統管理員帳戶建立關聯

從 ONTAP 9.13.1 開始、您可以將 X.509 憑證與您與系統管理員帳戶相關聯的公開金鑰建立關聯。這可讓您在登入該帳戶的 SSH 時、更安全地進行憑證過期或撤銷檢查。

關於這項工作

如果您透過 SSH 同時使用 SSH 公開金鑰和 X.509 憑證來驗證帳戶、 ONTAP 會在使用 SSH 公開金鑰進行驗證之前、先檢查 X.509 憑證的有效性。如果該憑證過期或撤銷、 SSH 登入將會被拒絕、而且會自動停用公開金鑰。

開始之前

- 您必須是叢集或SVM管理員、才能執行此工作。
- 您必須已產生SSH金鑰。
- 如果您只需要檢查 X.509 憑證是否過期、您可以使用自我簽署的憑證。
- 如果您需要檢查 X.509 憑證是否過期及撤銷：
  - 您必須已從憑證授權單位（ CA ）收到憑證。
  - 您必須使用命令來安裝憑證鏈結（中繼和根 CA 憑證） `security certificate install`。如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。
  - 您需要啟用 SSH 的 OCSP 。請參閱 "使用OCSP驗證數位憑證是否有效" 以取得相關指示。

步驟

1. 將公開金鑰和 X.509 憑證與系統管理員帳戶建立關聯：

   ```
   security login publickey create -vserver SVM_name -username user_name -index
   index -publickey certificate -x509-certificate install
   ```

   如"指令參考資料ONTAP"需詳細 `security login publickey create`資訊，請參閱。

2. 檢視公開金鑰以驗證變更：

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

   如"指令參考資料ONTAP"需詳細 `security login publickey show`資訊，請參閱。

範例

下列命令會將公開金鑰和 X.509 憑證與 SVM 系統管理員帳戶建立關聯 `svmadmin2` 適用於 SVM `engData2`。公開金鑰會被指派索引編號 6 。

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

從系統管理員帳戶的 SSH 公開金鑰中移除憑證關聯

您可以從帳戶的 SSH 公開金鑰中移除目前的憑證關聯、同時保留公開金鑰。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 從系統管理員帳戶移除 X.509 憑證關聯、並保留現有的 SSH 公開金鑰：

   ```
   security login publickey modify -vserver SVM_name -username user_name -index
   index -x509-certificate delete
   ```

   如"指令參考資料ONTAP"需詳細 `security login publickey modify`資訊，請參閱。

2. 檢視公開金鑰以驗證變更：

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

範例

下列命令會從 SVM 系統管理員帳戶移除 X.509 憑證關聯 `svmadmin2` 適用於 SVM `engData2` 索引編號 6 。

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

從系統管理員帳戶移除公開金鑰和憑證關聯

您可以從帳戶移除目前的公開金鑰和憑證組態。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 從系統管理員帳戶移除公開金鑰和 X.509 憑證關聯：

   ```
   security login publickey delete -vserver SVM_name -username user_name -index
   index
   ```

   如"指令參考資料ONTAP"需詳細 `security login publickey delete`資訊，請參閱。

2. 檢視公開金鑰以驗證變更：

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

範例

下列命令會從 SVM 系統管理員帳戶移除公開金鑰和 X.509 憑證 `svmadmin3` 適用於 SVM `engData3` 索引編號

7 。

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

相關資訊

- "安全登入公鑰"

為 ONTAP SSH 登入設定 Cisco 雙核心 2FA

從 ONTAP 9.14.1 開始、您可以將 ONTAP 設定為在登入 SSH 期間使用 Cisco 雙核心進行雙重驗證（ 2FA ）。您可以在叢集層級設定雙核心、而且預設會套用至所有使用者帳戶。或者、您也可以在儲存 VM 層級（之前稱為 vserver ）設定雙核心、在這種情況下、它只適用於該儲存 VM 的使用者。如果您啟用和設定雙核心、它會作為額外的驗證方法、以補充所有使用者的現有方法。

如果您為 SSH 登入啟用雙核心驗證、使用者下次使用 SSH 登入時、將需要註冊裝置。如需報名資訊、請參閱 Cisco Duo "註冊文件"。

您可以使用 ONTAP 命令列介面來執行 Cisco 雙核心的下列工作：

- 設定 Cisco Duo
- 變更 Cisco Duo 組態
- 移除 Cisco Duo 組態
- 查看 Cisco Duo 組態
- 移除 " 雙核心 " 群組
- [檢視雙核心群組]
- [略過使用者的雙核心驗證]

設定 Cisco Duo

您可以使用命令為整個叢集或特定儲存 VM （在 ONTAP CLI 中稱為 Vserver ）建立 Cisco 雙核心組態 `security login duo create`。當您這麼做時、 Cisco Duo 會啟用此叢集或儲存 VM 的 SSH 登入。如"指令參考資料ONTAP"需詳細 `security login duo create`資訊，請參閱。

步驟

1. 登入 Cisco Duo 管理面板。
2. 前往 * 應用程式 > UNIX 應用程式 * 。
3. 記錄您的整合金鑰、秘密金鑰和 API 主機名稱。
4. 使用 SSH 登入您的 ONTAP 帳戶。
5. 啟用此儲存 VM 的 Cisco Duo 驗證、以環境中的資訊取代方括號中的值：

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

變更 **Cisco Duo** 組態

您可以變更 Cisco Duo 驗證使用者的方式（例如、提供多少驗證提示、或使用什麼 HTTP Proxy ）。如果您需要變更儲存 VM 的 Cisco 雙核心組態（在 ONTAP CLI 中稱為 vserver ），您可以使用 `security login duo modify`命令。如"指令參考資料ONTAP"需詳細 `security login duo modify`資訊，請參閱。

步驟

1. 登入 Cisco Duo 管理面板。
2. 前往 * 應用程式 > UNIX 應用程式 * 。
3. 記錄您的整合金鑰、秘密金鑰和 API 主機名稱。
4. 使用 SSH 登入您的 ONTAP 帳戶。
5. 變更此儲存 VM 的 Cisco Duo 組態、以您環境中的更新資訊取代方括號中的值：

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-max-prompts 1|2|3 \
-is-enabled true|false \
-fail-mode safe|secure
```

移除 **Cisco Duo** 組態

您可以移除 Cisco Duo 組態、這樣就不需要 SSH 使用者在登入時使用 DuoTM 進行驗證。若要移除儲存 VM 的 Cisco 雙核心組態（在 ONTAP CLI 中稱為 vserver ），您可以使用 `security login duo delete`命令。如"指令參考資料ONTAP"需詳細 `security login duo delete`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 移除此儲存 VM 的 Cisco Duo 組態、以您的儲存 VM 名稱取代 `<STORAGE_VM_NAME>`：

```
security login duo delete  -vserver <STORAGE_VM_NAME>
```

這會永久刪除此儲存 VM 的 Cisco Duo 組態。

查看 Cisco Duo 組態

您可以使用命令檢視儲存 VM （在 ONTAP CLI 中稱為 vserver ）的現有 Cisco 雙核心組態 `security login duo show`。如"指令參考資料ONTAP"需詳細 `security login duo show`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 顯示此儲存 VM 的 Cisco Duo 組態。您也可以選擇使用 `vserver` 用於指定儲存 VM 的參數、請將儲存 VM 名稱取代為 `<STORAGE_VM_NAME>`：

```
security login duo show -vserver <STORAGE_VM_NAME>
```

您應該會看到類似下列的輸出：

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

建立雙核心群組

您可以指示 Cisco DuoTM 僅在特定 Active Directory 、 LDAP 或本機使用者群組中加入使用者、以進行 DuoTM 驗證程序。如果您建立雙核心群組、系統只會提示該群組中的使用者進行雙核心驗證。您可以使用命令建立雙核心群組 `security login duo group create`。建立群組時、您可以選擇性地將該群組中的特定使用者排除在雙核心驗證程序之外。如"指令參考資料ONTAP"需詳細 `security login duo group create`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 建立 DuoTM 群組、以環境中的資訊取代方括號中的值。如果您省略 `-vserver` 參數、群組會在叢集層級建

立：

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

雙核心群組的名稱必須符合 Active Directory 、 LDAP 或本機群組。您使用選用參數指定的使用者 `-excluded-users`將不會納入雙核心驗證程序。

檢視雙核心群組

您可以使用命令來檢視現有的 Cisco 雙核心群組項目 `security login duo group show`。如"指令參考資料ONTAP"需詳細 `security login duo group show`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 顯示 DUO 群組項目、以環境中的資訊取代方括號中的值。如果您省略 `-vserver` 參數、群組會顯示在叢集層級：

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

雙核心群組的名稱必須符合 Active Directory 、 LDAP 或本機群組。您使用選用參數指定的使用者 `-excluded-users`將不會顯示。

移除 " 雙核心 " 群組

您可以使用命令移除雙核心群組項目 `security login duo group delete`。如果您移除群組、該群組中的使用者將不再包含在雙核心驗證程序中。如"指令參考資料ONTAP"需詳細 `security login duo group delete`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 移除 DuoTM 群組項目、以環境中的資訊取代方括號中的值。如果您省略 `-vserver` 參數、群組會在叢集層級移除：

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME>
```

雙核心群組的名稱必須符合 Active Directory 、 LDAP 或本機群組。

略過使用者的雙核心驗證

您可以將所有使用者或特定使用者排除在雙核心 SSH 驗證程序之外。

排除所有雙核心使用者

您可以為所有使用者停用 Cisco 雙核心 SSH 驗證。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 停用 SSH 使用者的 Cisco Duo 驗證、以 vserver 名稱取代 `<STORAGE_VM_NAME>`：

```
security login duo modify -vserver <STORAGE_VM_NAME> -is-enabled false
```

不包括雙核心群組使用者

您可以從雙核心 SSH 驗證程序中排除屬於雙核心群組的特定使用者。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 針對群組中的特定使用者停用 Cisco Duo 驗證。以群組名稱和使用者清單取代方括號中的值：

```
security login duo group modify -group-name <GROUP_NAME> -excluded-users
<USER1, USER2>
```

雙核心群組的名稱必須符合 Active Directory 、 LDAP 或本機群組。您使用參數指定的使用者 `-excluded-users`將不會包含在雙核心驗證程序中。

如"指令參考資料ONTAP"需詳細 `security login duo group modify`資訊，請參閱。

排除本機雙核心使用者

您可以使用 Cisco 雙核心管理面板、排除特定的本機使用者使用雙核心驗證。如需相關指示、請參閱 "Cisco Duo 文件"。

在 **ONTAP** 中產生並安裝 **CA** 簽署的伺服器憑證

在正式作業系統上、最佳做法是安裝CA簽署的數位憑證、以用於將叢集或SVM驗證為SSL伺服器。您可以使用命令來產生憑證簽署要求（ CSR ），並 `security certificate install`使用 `security certificate generate-csr`命令來安裝從憑證授權單位收到的憑證。深入瞭解 `security certificate generate-csr`及 `security certificate install` "指令參考資料ONTAP"。

產生憑證簽署要求

您可以使用 `security certificate generate-csr` 產生憑證簽署要求（ CSR ）的命令。在處理您的要求之後、憑證授權單位（CA）會傳送簽署的數位憑證給您。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 產生CSR：

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

下列命令會建立 CSR ，其中包含由雜湊函數產生的 2048 位元私密金鑰 `SHA256`，供自訂一般名稱為的公司部門 `server1.companyname.com`中的群組 `IT`使用 `Software`，位於美國加州森尼維爾。SVM 連絡人管理員的電子郵件地址為 `web@example.com`。系統會在輸出中顯示CSR和私密金鑰。

建立 **CSR** 的範例

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

NOTE: Keep a copy of your certificate request and private key for
future reference.
```

2. 從CSR輸出複製憑證要求、然後以電子形式（例如電子郵件）將其傳送至信任的協力廠商CA進行簽署。

   在處理您的要求之後、CA會將簽署的數位憑證傳送給您。您應該保留一份私密金鑰和CA簽署的數位憑證複本。

安裝**CA**簽署的伺服器憑證

您可以使用 `security certificate install`命令在 SVM 上安裝 CA 簽署的伺服器憑證。系統會提示您輸入憑證授權單位（CA）根憑證和中繼憑證、以構成伺服器憑證的憑證鏈結。ONTAP如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 安裝 CA 簽署的伺服器憑證：

```
security certificate install -vserver SVM_name -type certificate_type
```

> 系統會提示您輸入CA根憑證和中繼憑證、這些憑證構成伺服器憑證的憑證鏈結。ONTAP鏈結從發行伺服器憑證的CA憑證開始、範圍最多可達CA的根憑證。任何遺失的中繼憑證都會導致伺服器憑證安裝失敗。

以下命令可在 SVM 上安裝 CA 簽署的伺服器憑證和中繼憑證 `engData2`。

安裝 **CA** 簽署的伺服器憑證中繼憑證的範例

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

相關資訊

- "產生安全性憑證-CSR"

從ONTAP 版本號《21：10.1》開始、您可以使用System Manager來管理信任的憑證授權單位、用戶端/伺服器憑證、以及本機（內建）憑證授權單位。

有了System Manager、您可以管理從其他應用程式接收到的憑證、以便驗證這些應用程式的通訊。 您也可以管理自己的憑證、以便將系統識別給其他應用程式。

檢視憑證資訊

使用System Manager、您可以檢視儲存在叢集上的信任憑證授權單位、用戶端/伺服器憑證和本機憑證授權單位。

步驟

1. 在System Manager中、選取*叢集>設定*。
2. 捲動至* Security（安全性）區域。
   在「*憑證」區段中、會顯示下列詳細資料：
   - 儲存的信任憑證授權單位數目。
   - 儲存的用戶端/伺服器憑證數目。
   - 儲存的本機憑證授權單位數目。
3. 選取任何數字以檢視有關某一類別憑證的詳細資料、或選取 → 以開啟包含所有類別資訊的 * 憑證 * 頁面。
   清單會顯示整個叢集的資訊。如果您只想顯示特定儲存VM的資訊、請執行下列步驟：
   a. 選取 * 儲存 > 儲存 VM* 。
   b. 選取儲存VM。
   c. 切換至 * 設定 * 索引標籤。
   d. 選取 * 憑證 * 區段中顯示的數字。

接下來該怎麼做

- 您可以從*憑證*頁面 [產生憑證簽署要求]。
- 憑證資訊分成三個索引標籤、每個類別各一個。 您可以從每個索引標籤執行下列工作：

在此索引標籤上…	您可以執行下列程序…
受信任的憑證授權單位	• [install-trusted-cert] • [刪除信任的憑證授權單位] • [續約信任的憑證授權單位]
用戶端/伺服器憑證	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]

當地證書管理機構	• [建立新的本機憑證授權單位] • [使用本機憑證授權單位簽署憑證] • [刪除本機憑證授權單位] • [更新本機憑證授權單位]

產生憑證簽署要求

您可以從「憑證」頁面的任何索引標籤、使用System Manager產生憑證簽署要求（CSR）。系統會產生私密金鑰和對應的CSR、您可以使用憑證授權單位來簽署以產生公開憑證。

步驟

1. 查看*憑證*頁面。 請參閱 [檢視憑證資訊]。
2. 選取 **+** 產生 **CSR** 。
3. 填寫主旨名稱的資訊：
   a. 輸入*通用名稱*。
   b. 選擇*國家/地區*。
   c. 輸入*組織*。
   d. 輸入*組織單位*。
4. 如果您要置換預設值、請選取*更多選項*並提供其他資訊。

安裝（新增）信任的憑證授權單位

您可以在System Manager中安裝其他信任的憑證授權單位。

步驟

1. 檢視*信任的憑證授權單位*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選擇。 + Add
3. 在「新增信任的憑證授權單位」面板上、執行下列步驟：
   - 輸入*名稱*。
   - 對於*範圍*、請選取儲存VM。
   - 輸入*通用名稱*。
   - 選擇*類型*。
   - 輸入或匯入*憑證詳細資料*。

刪除信任的憑證授權單位

使用System Manager、您可以刪除信任的憑證授權單位。

ⓘ 您無法刪除預先安裝 ONTAP 的信任憑證授權單位。

步驟

1. 檢視*信任的憑證授權單位*索引標籤。請參閱 [檢視憑證資訊]。
2. 選取信任的憑證授權單位名稱。
3. 選取 ⋮ 名稱旁邊的，然後選取 * 刪除 * 。

續約信任的憑證授權單位

有了System Manager、您可以續約已過期或即將過期的信任憑證授權單位。

步驟

1. 檢視*信任的憑證授權單位*索引標籤。請參閱 [檢視憑證資訊]。
2. 選取信任的憑證授權單位名稱。
3. 選取 ⋮ 憑證名稱旁邊的 * 更新 * 。

安裝（新增）用戶端/伺服器憑證

有了System Manager、您可以安裝其他用戶端/伺服器憑證。

步驟

1. 檢視*用戶端/伺服器憑證*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選擇。 + Add
3. 在「新增用戶端/伺服器憑證」面板上、執行下列步驟：
   - 輸入*憑證名稱*。
   - 對於*範圍*、請選取儲存VM。
   - 輸入*通用名稱*。
   - 選擇*類型*。
   - 輸入或匯入*憑證詳細資料*。
     您可以從文字檔寫入或複製及貼上憑證詳細資料、也可以按一下*匯入*從憑證檔案匯入文字。
   - 輸入 * 私密金鑰 * 。
     您可以從文字檔中寫入或複製及貼上私密金鑰、也可以按一下*匯入*從私密金鑰檔匯入文字。

產生（新增）自我簽署的用戶端/伺服器憑證

有了System Manager、您可以產生額外的自我簽署用戶端/伺服器憑證。

步驟

1. 檢視*用戶端/伺服器憑證*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選取 *+ 產生自我簽署的憑證 * 。
3. 在「產生自我簽署的憑證」面板上、執行下列步驟：
   - 輸入*憑證名稱*。
   - 對於*範圍*、請選取儲存VM。
   - 輸入*通用名稱*。

- 選擇*類型*。
- 選取*雜湊函數*。
- 選取*金鑰大小*。
- 選擇*儲存VM*。

刪除用戶端/伺服器憑證

使用System Manager、您可以刪除用戶端/伺服器憑證。

步驟

1. 檢視*用戶端/伺服器憑證*索引標籤。請參閱 [檢視憑證資訊]。
2. 選取用戶端 / 伺服器憑證的名稱。
3. 選取 ⋮ 名稱旁邊的，然後按一下 * 刪除 * 。

續約用戶端/伺服器憑證

有了System Manager、您可以續約已過期或即將過期的用戶端/伺服器憑證。

步驟

1. 檢視*用戶端/伺服器憑證*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選取用戶端 / 伺服器憑證的名稱。
3. 選取 ⋮ 名稱旁邊的、然後按一下 * 更新 * 。

建立新的本機憑證授權單位

有了System Manager、您就能建立新的本機憑證授權單位。

步驟

1. 查看*本地證書頒發機構*選項卡。 請參閱 [檢視憑證資訊]。
2. 選擇。 + Add
3. 在「新增本機憑證授權單位」面板上、執行下列步驟：
   - 輸入*名稱*。
   - 對於*範圍*、請選取儲存VM。
   - 輸入*通用名稱*。
4. 如果您要置換預設值、請選取*更多選項*並提供其他資訊。

使用本機憑證授權單位簽署憑證

在System Manager中、您可以使用本機憑證授權單位來簽署憑證。

步驟

1. 查看*本地證書頒發機構*選項卡。 請參閱 [檢視憑證資訊]。
2. 選取本機憑證授權單位的名稱。

3. 選擇 ⋮ 名稱旁邊的，然後 * 簽署證書 * 。
4. 填寫*簽署憑證簽署要求*表單。
   - 您可以貼上憑證簽署內容、或按一下*匯入*以匯入憑證簽署要求檔案。
   - 指定憑證有效的天數。

刪除本機憑證授權單位

使用System Manager、您可以刪除本機憑證授權單位。

步驟

1. 檢視*本機憑證授權單位*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選取本機憑證授權單位的名稱。
3. 選擇 ⋮ 名稱旁邊的 * 刪除 * 。

更新本機憑證授權單位

有了System Manager、您可以續約已過期或即將過期的本機憑證授權單位。

步驟

1. 檢視*本機憑證授權單位*索引標籤。請參閱 [檢視憑證資訊]。
2. 選取本機憑證授權單位的名稱。
3. 選取 ⋮ 名稱旁邊的、然後按一下 * 更新 * 。

在 **ONTAP** 中設定 **Active Directory** 網域控制站存取

您必須先設定AD網域控制器存取叢集或SVM、AD帳戶才能存取SVM。如果您已為資料SVM設定SMB伺服器、則可將SVM設定為閘道、或將_tunnel_設定為用於AD存取叢集的閘道。如果您尚未設定SMB伺服器、可以在AD網域上建立SVM的電腦帳戶。

支援下列網域控制器驗證服務：ONTAP

- Kerberos
- LDAP
- Netlogon
- 本機安全性授權（LSA）

支援下列工作階段金鑰演算法以確保Netlogon連線安全：ONTAP

工作階段金鑰演算法	可從 … 開始使用。

HMA-SHA256、以進階加密標準（AES）為基礎 如果您的叢集執行的是 ONTAP 9.9.1 或更早版本、而且您的網域控制器會強制執行 AES 來提供安全的 Netlogon 服務、則連線會失敗。在這種情況下、您需要重新設定網域控制器、改為接受與 ONTAP 的強大金鑰連線。	零點9.10.1 ONTAP
DE和HMC-MD5（設定強式金鑰時）	所有ONTAP 的版本

如果您想要在 Netlogon 安全通道建立期間使用 AES 工作階段金鑰、則需要驗證 SVM 上是否已啟用 AES 。

- 從 ONTAP 9.14.1 開始、在建立 SVM 時、預設會啟用 AES 、而且您不需要修改 SVM 的安全設定、即可在 Netlogon 安全通道建立期間使用 AES 工作階段金鑰。
- 在 ONTAP 9.10.1 至 9.13.1 中、建立 SVM 時、預設會停用 AES 。您需要使用下列命令來啟用 AES ：

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

當您升級至 ONTAP 9.14.1 或更新版本時、以舊版 ONTAP 建立的現有 SVM 的 AES 設定將不會自動變更。您仍需要更新此設定的值、才能在這些 SVM 上啟用 AES 。

設定驗證通道

如果您已為資料 SVM 設定 SMB 伺服器、則可以使用 `security login domain-tunnel create` 命令將 SVM 設定為閘道或 *tunnel* 、以便 AD 存取叢集。

在 ONTAP 9.16.1 之前，您必須使用驗證通道來管理具有 AD 的叢集管理員帳戶。

開始之前

- 您必須為資料SVM設定SMB伺服器。
- 您必須啟用AD網域使用者帳戶、才能存取叢集的管理SVM。
- 您必須是叢集管理員才能執行此工作。

從ONTAP 《S209.10.1》開始、如果您有SVM閘道（網域通道）可供AD存取、則如果您在AD網域中停用了NTLM、就可以使用Kerberos進行系統管理驗證。在舊版中、不支援Kerberos搭配SVM閘道的管理驗證。此功能預設為可用、不需設定。

一律會先嘗試Kerberos驗證。一旦失敗、就會嘗試執行NTLM驗證。

步驟

1. 將啟用SMB的資料SVM設定為驗證通道、以便AD網域控制器存取叢集：

```
security login domain-tunnel create -vserver <svm_name>
```

如"指令參考資料ONTAP"需詳細 `security login domain-tunnel create`資訊，請參閱。

SVM必須執行、使用者才能通過驗證。

下列命令會將啟用 SMB 的資料 SVM 設定 `engData`為驗證通道。

```
cluster1::>security login domain-tunnel create -vserver engData
```

在網域上建立**SVM**電腦帳戶

如果您尚未設定資料 SVM 的 SMB 伺服器、則可以使用 `vserver active-directory create` 命令、為網域上的 SVM 建立電腦帳戶。

關於這項工作

輸入之後 `vserver active-directory create` 命令時、系統會提示您提供 AD 使用者帳戶的認證、並提供足夠的權限、以便將電腦新增至網域中指定的組織單位。帳戶密碼不可空白。

從 ONTAP 9.16.1 開始，您可以使用此程序來管理具有 AD 的叢集管理員帳戶。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 在AD網域上建立SVM的電腦帳戶：

```
vserver active-directory create -vserver <SVM_name> -account-name
<NetBIOS_account_name> -domain <domain> -ou <organizational_unit>
```

從 ONTAP 9.16.1 開始，此 `-vserver`參數會接受管理 SVM 。如"指令參考資料ONTAP"需詳細 `vserver active-directory create`資訊，請參閱。

以下命令將在 SVM 的域上 `example.com`創建一個名爲的 `engData`計算機帳戶 `ADSERVER1`。輸入命令後、系統會提示您輸入AD使用者帳戶認證。

```
cluster1::>vserver active-directory create -vserver engData -account
-name ADSERVER1 -domain example.com

In order to create an Active Directory machine account, you must supply
the name and password of a Windows account with sufficient privileges to
add computers to the "CN=Computers" container within the "example.com"
domain.

Enter the user name: Administrator

Enter the password:
```

您必須先設定LDAP或NIS伺服器存取SVM、LDAP或NIS帳戶才能存取SVM。交換器功能可讓您使用LDAP或NIS做為替代名稱服務來源。

設定**LDAP**伺服器存取

您必須先設定LDAP伺服器存取SVM、LDAP帳戶才能存取SVM。您可以使用 `vserver services name-service ldap client create` 在 SVM 上建立 LDAP 用戶端組態的命令。然後您就可以使用 `vserver services name-service ldap create` 用於將 LDAP 用戶端組態與 SVM 建立關聯的命令。

關於這項工作

大多數LDAP伺服器都可以使用ONTAP 由下列功能提供的預設架構：

- ms-AD-BIS（大多數Windows 2012及更新版本AD伺服器的偏好架構）
- AD-IDMU （ Windows 2008 、 Windows 2016 及更新版本的 AD 伺服器）
- AD-SFU（Windows 2003和舊版AD伺服器）
- RFC-2307（UNIX LDAP伺服器）

除非有其他需求、否則最好使用預設架構。如果是、您可以複製預設架構並修改複本、以建立自己的架構。如需詳細資訊、請參閱：

- "NFS 組態"
- "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"

開始之前

- 您必須已在 SVM 上安裝"CA簽署的伺服器數位憑證"。
- 您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 在 SVM 上建立 LDAP 用戶端組態：

   ```
   vserver services name-service ldap client create -vserver <SVM_name> -client
   -config <client_configuration> -servers <LDAP_server_IPs> -schema <schema>
   -use-start-tls <true|false>
   ```

   只有資料SVM存取才支援Start TLS。不支援存取管理SVM。

   如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap client create`資訊，請參閱。

   以下命令用於創建名爲 SVM `engData` 的 LDAP 客戶端配置 `corp`。用戶端會匿名連結至 IP 位址為 172.0.0.100 和 172.16.0.101 的 LDAP 伺服器。用戶端使用 RFC-2307 架構進行 LDAP 查詢。用戶端與伺服器之間的通訊會使用Start TLS加密。

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```

這 `-ldap-servers`字段替換 `-servers`字段。您可以使用 `-ldap-servers`欄位指定 LDAP 伺服器的主機名稱或 IP 位址。

2. 將 LDAP 用戶端組態與 SVM 建立關聯： `vserver services name-service ldap create -vserver <SVM_name> -client-config <client_configuration> -client-enabled <true|false>`

   如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap create`資訊，請參閱。

   下列命令會關聯 LDAP 用戶端組態 `corp` 使用 SVM `engData`，並在 SVM 上啟用 LDAP 用戶端。

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```

這 `vserver services name-service ldap create`如果ONTAP無法聯繫名稱伺服器，則該命令將執行自動設定驗證並報告錯誤訊息。

3. 使用vserver services name-service LDAP檢查命令來驗證名稱伺服器的狀態。

   下列命令會驗證SVM vs0上的LDAP伺服器。

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                  |
| Client Configuration Name: c1                                 |
| LDAP Status: up                                               |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                |
```

   您可以使用 `name service check``命令來驗證名稱伺服器的狀態。

設定 **NIS** 伺服器存取

您必須先設定NIS伺服器對SVM的存取權、NIS帳戶才能存取SVM。您可以使用 `vserver services name-service nis-domain create` 在 SVM 上建立 NIS 網域組態的命令。

開始之前

- 在SVM上設定NIS網域之前、所有已設定的伺服器都必須可供使用和存取。
- 您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 在 SVM 上建立 NIS 網域組態：

   ```
   vserver services name-service nis-domain create -vserver <SVM_name> -domain
   <client_configuration> -nis-servers <NIS_server_IPs>
   ```

   如"指令參考資料ONTAP"需詳細 `vserver services name-service nis-domain create`資訊，請參閱。

   這 `-nis-servers`字段替換 `-servers`字段。您可以使用 `-nis-servers`欄位指定 NIS 伺服器的主機名稱或 IP 位址。

   以下命令在 SVM 上創建 NIS 域配置 `engData`。NIS 網域 `nisdomain`會與 `IP` 位址為的 `NIS` 伺服器進行通訊 `192.0.2.180`。

   ```
   cluster1::>vserver services name-service nis-domain create
   -vserver engData -domain nisdomain -nis-servers 192.0.2.180
   ```

建立名稱服務交換器

名稱服務交換器功能可讓您使用LDAP或NIS做為替代名稱服務來源。您可以使用 `vserver services name-service ns-switch modify` 命令以指定名稱服務來源的查詢順序。

開始之前

- 您必須已設定LDAP和NIS伺服器存取。
- 您必須是叢集管理員或SVM管理員、才能執行此工作。

步驟

1. 指定名稱服務來源的查詢順序：

   ```
   vserver services name-service ns-switch modify -vserver <SVM_name> -database
   <name_service_switch_database> -sources <name_service_source_order>
   ```

   如"指令參考資料ONTAP"需詳細 `vserver services name-service ns-switch modify`資訊，請參閱。

   以下命令指定 SVM 上資料庫 `engData`的 `LDAP` 和 `NIS` 名稱服務來源的查詢順序 `passwd`。

   ```
   cluster1::>vserver services name-service ns-switch
   modify -vserver engData -database passwd -source files ldap,nis
   ```

變更 **ONTAP** 管理員密碼

首次登入系統後、您應該立即變更初始密碼。如果您是 SVM 管理員、可以使用 `security login password` 命令以變更您自己的密碼。如果您是叢集管理員、可以使用 `security login password` 命令以變更任何系統管理員的密碼。

關於這項工作

新密碼必須遵守下列規則：

- 它不能包含使用者名稱
- 長度必須至少八個字元
- 它必須包含至少一個字母和一個數字
- 不能與最後六個密碼相同

您可以使用 `security login role config modify`命令來修改與指定角色相關聯之帳戶的密碼規則。

開始之前

- 您必須是叢集或SVM管理員、才能變更自己的密碼。
- 您必須是叢集管理員、才能變更其他管理員的密碼。

步驟

1. 變更管理員密碼： `security login password -vserver svm_name -username user_name`

   下列命令會變更系統管理員的密碼 `admin1` 適用於 SVM`vs1.example.com`。系統會提示您輸入目前密碼、然後輸入並重新輸入新密碼。

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

相關資訊

- "安全登入角色組態修改"
- "安全登入密碼"

鎖定及解除鎖定 **ONTAP** 系統管理員帳戶

您可以使用 `security login lock` 用於鎖定系統管理員帳戶的命令、以及 `security login unlock` 解除鎖定帳戶的命令。

開始之前

您必須是叢集管理員才能執行這些工作。

步驟

1. 鎖定系統管理員帳戶：

   ```
   security login lock -vserver SVM_name -username user_name
   ```

   下列命令會鎖定系統管理員帳戶 `admin1` 適用於 SVM `vs1.example.com`：

```
cluster1::>security login lock -vserver engData -username admin1
```

如"指令參考資料ONTAP"需詳細 `security login lock`資訊，請參閱。

2. 解除鎖定系統管理員帳戶：

   `security login unlock -vserver SVM_name -username user_name`

   下列命令會解除鎖定系統管理員帳戶 `admin1` 適用於 SVM `vs1.example.com`：

```
cluster1::>security login unlock -vserver engData -username admin1
```

如"指令參考資料ONTAP"需詳細 `security login unlock`資訊，請參閱。

相關資訊

- "安全登入"

在 **ONTAP** 中管理失敗的登入嘗試

重複失敗的登入嘗試有時表示入侵者正在嘗試存取儲存系統。您可以採取許多步驟來確保不會發生入侵。

如何得知登入嘗試失敗

事件管理系統（EMS）每小時都會通知您登入失敗的嘗試。您可以在中找到登入嘗試失敗的記錄 `audit.log` 檔案：

重複登入嘗試失敗時該怎麼辦

從短期來看、您可以採取許多步驟來預防入侵：

- 密碼必須由最少的大寫字元、小寫字元、特殊字元和/或數字組成
- 在登入嘗試失敗後強制延遲
- 限制允許的失敗登入嘗試次數、並在指定的失敗嘗試次數後鎖定使用者
- 過期並封鎖在指定天數內處於非使用中狀態的帳戶

您可以使用 `security login role config modify`命令來執行這些工作。如"指令參考資料ONTAP"需詳細 `security login role config modify`資訊，請參閱。

長期而言、您可以採取下列額外步驟：

- 使用 `security ssh modify`命令可限制所有新建立的 SVM 失敗登入嘗試次數。如"指令參考資料ONTAP"需詳細 `security ssh modify`資訊，請參閱。
- 要求使用者變更密碼、將現有的MD5-演算 法帳戶移轉至更安全的SHA-512演算法。

對 ONTAP 系統管理員帳戶密碼強制執行 SHA-2

在升級之後、ONTAP 在更新之前建立的管理員帳戶會繼續使用md5密碼、直到手動變更密碼為止。與SHA-2相比、MD5的安全性較低。因此、在升級之後、您應該提示使用者將密碼變更為使用預設的SHA-512雜湊功能。

關於這項工作

密碼雜湊功能可讓您執行下列動作：

- 顯示符合指定雜湊功能的使用者帳戶。
- 使使用指定雜湊功能的帳戶過期（例如、md5）、強制使用者在下次登入時變更密碼。
- 鎖定密碼使用指定雜湊功能的帳戶。
- 還原至ONTAP 版本早於發揮作用9的版本時、請重設叢集管理員自己的密碼、使其與舊版支援的雜湊功能（md5）相容。

ONTAP 只接受預先散列的 SHA-2 密碼、只能使用 NetApp Manageability SDK (`security-login-create` 和 `security-login-modify-password`) 。

步驟

1. 將md5系統管理員帳戶移轉至SHA-512密碼雜湊功能：
   a. 使所有 MD5 系統管理員帳戶過期： `security login expire-password -vserver * -username * -hash-function md5`

      如此一來、會強制md5帳戶使用者在下次登入時變更密碼。

   b. 要求具有MD5帳戶的使用者透過主控台或SSH工作階段登入。

      系統偵測到帳戶已過期、並提示使用者變更密碼。SHA-512預設用於變更的密碼。

2. 若使用者未在一段時間內登入以變更密碼的MD5帳戶、請強制進行帳戶移轉：
   a. 鎖定仍使用 MD5 雜湊功能的帳戶（進階權限層級）： `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

      在指定的天數之後 `-lock-after`、使用者無法存取其 MD5 帳戶。

   b. 當使用者準備好變更密碼時、請解除鎖定帳戶： `security login unlock -vserver svm_name -username user_name`
   c. 請使用者透過主控台或SSH工作階段登入帳戶、並在系統提示使用者時變更密碼。

相關資訊

- "安全登入過期密碼"
- "安全登入解除鎖定"

使用系統管理員診斷並修正 ONTAP 檔案存取問題

從功能不全的9.8開始ONTAP 、您可以追蹤及檢視檔案存取問題。

步驟

1. 在System Manager中、選取* Storage > Storage VM*。
2. 選取您要在其中執行追蹤的儲存VM。
3. 按一下 * 更多 * 。
4. 按一下*追蹤檔案存取*。
5. 提供使用者名稱和用戶端IP位址、然後按一下*開始追蹤*。

   追蹤結果會顯示在表格中。 「理由」欄提供無法存取檔案的原因。

6. 按一下 結果表左欄、即可檢視檔案存取權限。

管理多管理員驗證

瞭解 **ONTAP** 多管理驗證

從 ONTAP 9.11.1 開始，您可以使用多管理驗證（ MAV ）來確保某些作業（例如刪除磁碟區或快照）只能在指定管理員核准後執行。如此可防止遭到入侵、惡意或缺乏經驗的系統管理員進行不必要的變更或刪除資料。

設定多管理員驗證包括：

- "建立一個或多個系統管理員核准群組。"
- "啟用多管理員驗證功能。"
- "新增或修改規則。"

初始設定之後、這些元素只能由MAV核准群組（MAV系統管理員）中的系統管理員修改。

啟用多重管理驗證時、完成每項受保護的作業都需要下列步驟：

1. 當使用者啟動作業時 "已產生要求。"
2. 在執行作業之前，請至少先執行一個"MAV管理員必須核准。"
3. 核准後，系統會提示使用者並完成作業。

如果您需要在未經 MAV 管理員批准的情況下停用多管理員驗證功能，請聯絡NetApp支援並提及以下內容"NetApp知識庫：如果 MAV 管理員不可用，如何停用多管理員驗證"。

多管理員驗證不適用於涉及大量自動化的磁碟區或工作流程、因為每項自動化工作都需要核准才能完成作業。如果您想要同時使用自動化和 MAV ，建議您針對特定的 MAV 作業使用查詢。例如，您只能將 MAV 規則套用 `volume delete`至不涉及自動化的磁碟區，而且可以使用特定的命名方案來指定這些磁碟區。

Cloud Volumes ONTAP 無法使用多重管理驗證。

多管理員驗證的運作方式

多管理員驗證包括：

- 一或多位系統管理員的群組、擁有核准和否決的權限。
- _規則表_中的一組受保護作業或命令。
- _規則engine _以識別及控制受保護作業的執行。

根據角色型存取控制（RBAC）規則、評估MAV規則。因此、執行或核准受保護作業的系統管理員必須已擁有這些作業的最低RBAC權限。 "深入瞭解RBAC"。

系統定義的規則

啟用多管理員驗證時、系統定義的規則（也稱為_guard rail _規則）會建立一組MAV作業、以控制規避MAV程序本身的風險。這些作業無法從規則表格中移除。啟用MAV之後、以星號（）指定的作業在執行之前、必須先經過一或多位管理員的核准、 show*命令除外。

- `security multi-admin-verify modify` 營運 *

  控制多管理員驗證功能的組態。

- `security multi-admin-verify approval-group` 營運 *

  以多管理員驗證認證身分證明來控制系統管理員群組的成員資格。

- `security multi-admin-verify rule` 營運 *

  控制需要多管理員驗證的命令集。

- `security multi-admin-verify request` 營運

  控制核准程序。

受規則保護的命令

除了系統定義的操作外，啟用多管理員驗證時，以下命令預設受到保護，但您可以修改規則以刪除對這些命令的保護：

- "安全登入密碼"
- "安全登入解除鎖定"
- "設定"

每個 ONTAP 版本都提供更多命令、讓您可以選擇使用多重管理驗證規則來保護這些命令。請選擇您的 ONTAP 版本、以取得可保護的命令完整清單。

9.17.1

- `cluster date modify` [3]
- `cluster log-forwarding create` [3]
- `cluster log-forwarding delete` [3]
- `cluster log-forwarding modify` [3]
- `cluster peer delete`
- `cluster time-service ntp server create` [3]
- `cluster time-service ntp server delete` [3]
- `cluster time-service ntp key create`[3]
- `cluster time-service ntp key delete`[3]
- `cluster time-service ntp key modify`[3]
- `cluster time-service ntp server modify` [3]
- `event config modify`
- `event config set-mail-server-password` [3]
- `lun delete` [3]
- `security anti-ransomware volume attack clear-suspect` [1]
- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume event-log modify`[2]
- `security anti-ransomware volume pause` [1]
- `security anti-ransomware vserver event-log modify`[2]
- `security audit modify` [3]
- `security ipsec config modify` [3]
- `security ipsec policy create` [3]
- `security ipsec policy delete` [3]
- `security ipsec policy modify` [3]
- `security login create`
- `security login delete`
- `security login modify`
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase`[3]
- `security saml-sp create` [3]

- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete[4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline[4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start[4]
- volume encryption rekey start[4]

- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume rename [5]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create[2]
- vserver consistency-group create[4]
- vserver consistency-group delete[4]
- vserver consistency-group modify[4]
- vserver consistency-group snapshot create[4]
- vserver consistency-group snapshot delete[4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]

- `vserver object-store-server audit delete` [3]
- `vserver object-store-server audit disable` [3]
- `vserver object-store-server audit modify` [3]
- `vserver object-store-server audit rotate-log` [3]
- `vserver object-store-server bucket cors-rule create` [4]
- `vserver object-store-server bucket cors-rule delete` [4]
- `vserver options` [3]
- `vserver peer delete`
- `vserver security file-directory apply` [3]
- `vserver security file-directory remove-slag` [3]
- `vserver stop` [4]
- `vserver vscan disable` [3]
- `vserver vscan on-access-policy create` [3]
- `vserver vscan on-access-policy delete` [3]
- `vserver vscan on-access-policy disable` [3]
- `vserver vscan on-access-policy modify` [3]
- `vserver vscan scanner-pool create` [3]
- `vserver vscan scanner-pool delete` [3]
- `vserver vscan scanner-pool modify` [3]

9.16.1.

- `cluster date modify` [3]
- `cluster log-forwarding create` [3]
- `cluster log-forwarding delete` [3]
- `cluster log-forwarding modify` [3]
- `cluster peer delete`
- `cluster time-service ntp server create` [3]
- `cluster time-service ntp server delete` [3]
- `cluster time-service ntp key create` [3]
- `cluster time-service ntp key delete` [3]
- `cluster time-service ntp key modify` [3]
- `cluster time-service ntp server modify` [3]
- `event config modify`
- `event config set-mail-server-password` [3]

- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify[2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify[2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- security key-manager onboard update-passphrase[3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete[4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline[4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]

- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]
- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create[2]
- vserver consistency-group create[4]
- vserver consistency-group delete[4]
- vserver consistency-group modify[4]
- vserver consistency-group snapshot create[4]
- vserver consistency-group snapshot delete[4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create[4]
- vserver object-store-server bucket cors-rule delete[4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop[4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]

- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.15.1..

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create[3]
- cluster time-service ntp key delete[3]
- cluster time-service ntp key modify[3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]
- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify[2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify[2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete

- security login publickey modify
- security key-manager onboard update-passphrase[3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume file privileged-delete [3]

- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create[2]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]

- vserver security file-directory remove-slag [3]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.14.1.

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify[2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify[2]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot delete

- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver create[2]
- vserver modify[2]
- vserver peer delete

9.13.1.12.9.12.9.

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect[1]
- security anti-ransomware volume disable[1]
- security anti-ransomware volume pause[1]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snaplock modify[1]
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

9.12.1/9.11.1

- cluster peer delete
- event config modify
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

1. 9.13.1 全新的規則保護命令
2. 適用於 9.14.1 的全新規則保護命令
3. 9.15.1 的新規則保護命令
4. 9.16.1 的新規則保護命令
5. 9.17.1 的新規則保護命令
    - 此命令僅適用於 CLI ，在某些版本中不適用於 System Manager 。

只要在受MAV保護的叢集上輸入受保護的作業、就會將作業執行要求傳送至指定的MAV系統管理員群組。

您可以設定：

- MAV群組中的系統管理員名稱、聯絡資訊和數量。

  MAV管理員應具備具備叢集管理員權限的RBAC角色。

- MAV系統管理員群組的數目。
  - 每個受保護的作業規則都會指派一個MAV群組。
  - 對於多個MAV群組、您可以設定哪個MAV群組核准特定規則。
- 執行受保護作業所需的MAV核准數。
- MAV管理員必須在_核准到期_期間內回應核准要求。
- 執行過期_期間、要求的系統管理員必須在此期間內完成作業。

設定這些參數後、必須取得MAV核准才能加以修改。

MAV系統管理員無法核准自己執行受保護作業的要求。因此：

- 不應在只有一位系統管理員的叢集上啟用MAV。
- 如果 MAV 群組中只有一個人、則 MAV 管理員無法啟動受保護的作業；一般管理員必須啟動受保護的作業、且 MAV 管理員只能核准。
- 如果您想讓MAV管理員能夠執行受保護的作業、則MAV管理員人數必須大於所需的核准人數。
  例如、如果受保護的作業需要兩次核准、而您希望MAV系統管理員執行這些核准、則MAV系統管理員群組中必須有三位人員。

MAV系統管理員可以接收電子郵件警示中的核准要求（使用EMS）、也可以查詢要求佇列。 當他們收到要求時、可以採取下列三種行動之一：

- 核准
- 拒絕（否決）
- 忽略（無行動）

在下列情況下、電子郵件通知會傳送給與MAV規則相關的所有核准者：

- 隨即建立要求。
- 申請已核准或遭否決。
- 系統會執行核准的申請。

如果申請者在該作業的同一個核准群組中、他們會在申請獲得核准時收到一封電子郵件。

申請者即使在核准群組中，也無法核准自己的申請（雖然他們可以針對自己的申請取得電子郵件通知）。不在核准群組中的申請者（即非MAV系統管理員）不會收到電子郵件通知。

受保護的作業執行方式

如果已核准執行受保護的作業、則要求的使用者會在收到提示時繼續執行該作業。如果作業遭否決、申請使用者必須先刪除申請、然後再繼續。

MAV規則會在RBAC權限之後評估。因此、沒有足夠RBAC權限執行作業的使用者無法啟動MAV要求程序。

在執行受保護的操作之前，MAV 規則會被評估。這意味著規則會根據系統的目前狀態執行。例如，如果為以下物件建立了 MAV 規則： `volume modify`查詢 `-size 5GB` ，使用 `volume modify`將 5GB 磁碟區大小調整為 2GB 需要 MAV 批准，但將 2GB 磁碟區大小調整為 5GB 則不需要。

相關資訊

- "叢集"
- "LUN"
- "安全性"
- "終止合法持有SnapLock"
- "儲存聚合"
- "儲存加密"
- "系統"

管理 **MAV** 的 **ONTAP** 管理員核准群組

在啟用多管理員驗證（MAV）之前、您必須先建立管理員核准群組、其中包含一或多位系統管理員、以便獲得核准或否決權限。啟用多管理員驗證之後、任何對核准群組成員資格的修改都必須取得現有合格管理員的核准。

關於這項工作

您可以將現有的系統管理員新增至MAV群組、或建立新的系統管理員。

MAV功能可執行現有的角色型存取控制（RBAC）設定。潛在的MAV系統管理員必須擁有足夠的權限、才能執行受保護的作業、才能將其新增至MAV系統管理員群組。 "深入瞭解RBAC。"

您可以設定MAV來警示MAV系統管理員核准要求已擱置。若要這麼做、您必須設定電子郵件通知、尤其是 `Mail From` 和 `Mail Server` 參數 — 或者您可以清除這些參數以停用通知。沒有電子郵件警示、MAV管理員必須手動檢查核准佇列。

從ONTAP 9.15.1 開始，您可以將 Active Directory (AD) 使用者設定為 MAV 管理員。 AD 使用者必須是"配置為ONTAP管理員"。

System Manager程序

如果您想第一次建立MAV核准群組、請參閱的系統管理員程序 "啟用多管理員驗證。"

若要修改現有的核准群組或建立其他核准群組：

1. 識別要接收多管理員驗證的系統管理員。
    a. 按一下*叢集>設定。*

b. 按一下 → * 使用者和角色旁邊的。 *

c. 按一下 + Add * 使用者 * 。 *

d. 視需要修改名單。

如需詳細資訊、請參閱 "控制系統管理員存取權。"

2. 建立或修改MAV核准群組：

a. 按一下*叢集>設定。*

b. 按一下 → * 安全性 * 區段中 * 多重管理核准 * 旁的。（如果尚未設定 MAV 、您會看到 ⚙ 圖示。）

- 名稱：輸入群組名稱。
- 核准者：從使用者清單中選取核准者。
- 電子郵件地址：輸入電子郵件地址。
- 預設群組：選取群組。

啟用MAV後、必須取得MAV核准才能編輯現有的組態。

CLI程序

1. 確認已為設定值 `Mail From` 和 `Mail Server` 參數。輸入：

```
event config show
```

顯示器應類似於下列內容：

```
cluster01::> event config show
                            Mail From:  admin@localhost
                          Mail Server:  localhost
                            Proxy URL:  -
                           Proxy User:  -
 Publish/Subscribe Messaging Enabled:  true
```

若要設定這些參數、請輸入：

```
event config modify -mail-from email_address -mail-server server_name
```

深入瞭解 `event config show`及 `event config modify` "指令參考資料ONTAP"。

2. 識別要接收多管理員驗證的系統管理員

如果您想...	輸入此命令
顯示目前的系統管理員	`security login show`
修改目前系統管理員的認證資料	`security login modify <parameters>`

如果您想...	輸入此命令
建立新的系統管理員帳戶	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

深入瞭解 `security login show`，`security login modify`和 `security login create` "指令參考資料ONTAP"。

3. 建立MAV核准群組：

   `security multi-admin-verify approval-group create [ -vserver svm_name] -name group_name -approvers approver1[,approver2…] [[-email address1], address1…]`

   - `-vserver` - 此版本僅支援管理 SVM 。
   - `-name` - MAV 群組名稱、最多 64 個字元。
   - `-approvers`- 一個或多個審核者的清單。對於 AD 用戶，使用格式 `domain\user`。例如，`mydomain\pavan` 。
   - `-email` ：一或多個電子郵件地址、在建立、核准、遭否決或執行要求時收到通知。

     *範例：*下列命令會建立一個MAV群組、其中包含兩個成員及相關的電子郵件地址。

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. 驗證群組建立與成員資格：

   `security multi-admin-verify approval-group show`

   範例：

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name        Approvers        Email
-------  ----------------- ------------------
------------------------------------------------------------
svm-1    mav-grp1   pavan,julia      email
pavan@myfirm.com,julia@myfirm.com
```

使用這些命令來修改初始MAV群組組態。

*附註：*所有項目都需要MAV系統管理員核准才能執行。

如果您想...	輸入此命令
修改群組特性或修改現有的成員資訊	`security multi-admin-verify approval-group modify [parameters]`
新增或移除成員	`security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2…]][-approvers-to-remove approver1[,approver2…]]`
刪除群組	`security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name`

相關資訊

- "安全多管理員驗證"

在 **ONTAP** 中啟用或停用多管理驗證

必須明確啟用多管理員驗證（MAV）。啟用多管理員驗證後、必須取得MAV核准群組（MAV系統管理員）的系統管理員核准、才能將其刪除。

關於這項工作

啟用MAV之後、修改或停用MAV需要MAV管理員核准。

如果您需要在未經 MAV 管理員批准的情況下停用多管理員驗證功能，請聯絡NetApp支援並提及以下內容"NetApp知識庫：如果 MAV 管理員不可用，如何停用多管理員驗證"。

啟用MAV時、您可以全域指定下列參數。

核准群組

全域核准群組清單。至少需要一個群組才能啟用MAV功能。

如果您使用 MAV 搭配自主勒索軟體保護（ ARP ）、請定義一個新的或現有的核准群組、負責核准 ARP 暫停、停用及清除可疑的要求。

必要的核准者

執行受保護作業所需的核准者數量。預設和最小數字為1。

必要的核准者數量必須小於預設核准群組中唯一核准者的總數。

核准過期（小時、分鐘、秒）

MAV管理員必須回應核准要求的期間。預設值為1小時（1小時）、支援的最小值為1秒、支援的最大值為14天（14d）。

執行過期（小時、分鐘、秒）

要求系統管理員必須完成以下作業的期間：預設值為1小時（1小時）、支援的最小值為1秒、支援的最大值為14天（14d）。

您也可以針對特定項目覆寫任何這些參數 "營運規則。"

System Manager程序

1. 識別要接收多管理員驗證的系統管理員。
   a. 按一下*叢集>設定。*
   b. 按一下 → * 使用者和角色旁邊的。 *
   c. 按一下 + Add * 使用者 * 。 *
   d. 視需要修改名單。

      如需詳細資訊、請參閱 "控制系統管理員存取權。"

2. 建立至少一個核准群組並新增至少一個規則、以啟用多管理員驗證。
   a. 按一下*叢集>設定。*
   b. 按一下 ⚙ * 安全性 * 區段中 * 多重管理核准 * 旁的。
   c. 按一下 + Add 以新增至少一個核准群組。
      - 名稱–輸入群組名稱。
      - 核准者：從使用者清單中選取核准者。
      - 電子郵件地址–輸入電子郵件地址。
      - 預設群組–選取群組。
   d. 至少新增一個規則。
      - 作業–從清單中選取支援的命令。
      - 查詢–輸入任何所需的命令選項和值。
      - 選用參數；保留空白以套用全域設定、或為特定規則指派不同的值以覆寫全域設定。
        - 必要的核准人數
        - 核准群組
   e. 按一下*進階設定*以檢視或修改預設值。
      - 必要的核准人數（預設：1）
      - 執行要求過期（預設：1小時）
      - 核准要求過期（預設：1小時）
      - 郵件伺服器*
      - 寄件者電子郵件地址*

        *這些更新在「通知管理」下管理的電子郵件設定。如果尚未設定、系統會提示您進行設定。
   f. 按一下「啟用」以完成MAV初始組態。

初始組態之後、目前的MAV狀態會顯示在*多管理員核准*方塊中。

- 狀態（已啟用或未啟用）
- 需要核准的作用中作業
- 處於擱置狀態的未處理要求數

您可以按一下以顯示現有的組態 → 。需要MAV核准才能編輯現有的組態。

若要停用多管理員驗證：

1. 按一下*叢集>設定。*
2. 按一下 ⚙ * 安全性 * 區段中 * 多重管理核准 * 旁的。
3. 按一下「已啟用」切換按鈕。

   必須取得MAV核准才能完成此作業。

CLI程序

在CLI中啟用MAV功能之前、請先至少啟用一項 "MAV系統管理員群組" 必須已建立。

如果您想...	輸入此命令

啟用MAV功能	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`
	
	範例：下列命令可啟用具有1個核准群組、2個必要核准者及預設到期期間的MAV。
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	至少新增一組、以完成初始組態 "營運規則："

修改MAV組態（需要MAV核准）	`security multi-admin-verify approval-group modify [-approval-groups group1[,group2…]] [-required-approvers nn ] [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`

如果您想...	輸入此命令

驗證MAV功能	`security multi-admin-verify show`
	
	範例：
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution`
	`Approval Approval`
	`Enabled Approvers Expiry Expiry`
	`Groups`
	`------- --------- ---------`
	`-------- ----------`
	`true 2 1h 1h`
	`mav-grp1`

停用MAV功能（需要MAV核准）	`security multi-admin-verify modify -enabled false`

相關資訊

- "安全多管理員驗證"

管理 **ONTAP** 中受保護作業的多重管理驗證規則

您可以建立多管理員驗證（MAV）規則、以指定需要核准的作業。只要啟動作業、就會攔截受保護的作業、並產生核准要求。

任何具備適當RBAC功能的系統管理員都可以在啟用MAV之前建立規則、但一旦啟用MAV、對規則集的任何修改都需要MAV核准。

每個作業只能建立一個 MAV 規則、例如、您無法建立多個 `volume-snapshot-delete` 規則。任何所需的規則限制都必須包含在單一規則中。

您可以建立規則來保護 "這些命令"。您可以從 ONTAP 版本開始保護每個命令、在此版本中、命令的保護功能會先開始提供。

MAV 系統預設命令的規則 `security multi-admin-verify` "命令"、不可變更。

除了系統定義的操作外，啟用多管理員驗證時，以下命令預設受到保護，但您可以修改規則以刪除對這些命令的保護：

- "安全登入密碼"
- "安全登入解除鎖定"
- "設定"

規則限制

建立規則時，您可以選擇性地指定 `-query`選項，將要求限制為命令功能的子集。此 `-query`選項也可用於限制組態元素，例如 SVM ， Volume 和 Snapshot 名稱。

例如，在命令 `-query`中 `volume snapshot delete`，可以設定為 `-snapshot !hourly*,!daily*,!weekly*`，表示以每小時，每天或每週屬性為前置的 Volume 快照不受 MAV 保護。

```
smci-vsim20::> security multi-admin-verify rule show
                                                Required  Approval
Vserver Operation                               Approvers Groups
------- --------------------------------------- --------- -------------
vs01    volume snapshot delete                  -         -
          Query: -snapshot !hourly*,!daily*,!weekly*
```

任何排除的組態元素都不會受到 MAV 保護、任何管理員都可以刪除或重新命名。

根據預設，規則會指定在輸入受保護的作業時自動產生對應的 `security multi-admin-verify request create *"protected_operation"*`命令。您可以修改此預設值，要求 `request create`分別輸入命令。

根據預設、規則會繼承下列全域MAV設定、不過您可以指定規則特定的例外狀況：

- 所需核准者人數
- 核准群組
- 核准到期日
- 執行到期期間

System Manager程序

如果您想要第一次新增受保護的作業規則、請參閱的系統管理員程序 "啟用多管理員驗證。"

若要修改現有的規則集：

1. 選擇*叢集>設定*。
2. 在 * 安全性 * 區段中、選取 * 多重管理核准 * 旁的。
3. 選取 + Add 以新增至少一個規則；您也可以修改或刪除現有規則。
   - 作業–從清單中選取支援的命令。
   - 查詢–輸入任何所需的命令選項和值。
   - 選用參數–保留空白以套用全域設定、或為特定規則指派不同的值以覆寫全域設定。
     - 必要的核准人數
     - 核准群組

CLI程序

全部 `security multi-admin-verify rule` 命令必須先獲得 MAV 管理員核准、才能執行 `security multi-admin-verify rule show`。

如果您想...	輸入此命令
建立規則	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

修改目前系統管理員的認證資料	`security login modify <parameters>`
	
	範例：下列規則需要核准才能刪除根Volume。
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

修改規則	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
刪除規則	`security multi-admin-verify rule delete -operation "protected_operation"`
顯示規則	`security multi-admin-verify rule show`

相關資訊

- "安全多管理員驗證規則"
- "修改安全登入"

要求在 **ONTAP** 中執行受 **MAV** 保護的作業

當您在啟用多管理員驗證（MAV）的叢集上啟動受保護的作業或命令時ONTAP 、多方面的操作或命令都會自動攔截、並要求產生要求、而該要求必須獲得一或多位MAV核准群組（MAV系統管理員）中的系統管理員核准。或者、您也可以建立不含對話方塊的MAV要求。

如果核准、您必須回應查詢、才能在申請到期期間內完成作業。如果被否決、或是超過申請或過期期間、您必須刪除申請並重新提交。

MAV功能會遵守現有的RBAC設定。也就是您的系統管理員角色必須擁有足夠的權限、才能在不考慮MAV設定的情況下執行受保護的作業。"深入瞭解RBAC"。

如果您是MAV管理員、則執行受保護作業的要求也必須獲得MAV管理員核准。

System Manager程序

當使用者按一下功能表項目以啟動作業且作業受到保護時、系統會產生核准要求、且使用者會收到類似下列內容的通知：

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

啟用MAV時、可使用*多管理員要求*視窗、顯示根據使用者登入ID和MAV角色（核准者或非核准者）而擱置的要求。針對每個擱置的要求、會顯示下列欄位：

- 營運
- 索引（數字）
- 狀態（「Pending（擱置）」、「Approved（已核准）」、「Rejected（已拒絕）

  如果某個申請被一位核准者拒絕、則不可能採取進一步行動。

- 查詢（所要求作業的任何參數或值）
- 正在申請使用者
- 申請截止日期
- （數量）待核准者
- （數量）潛在核准者

申請核准後、申請使用者可在到期期間內重試該作業。

如果使用者在未經核准的情況下重試作業、則會顯示類似下列的通知：

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

CLI程序

1. 直接輸入受保護的作業、或使用MAV REQUEST命令輸入。

   範例：若要刪除磁碟區、請輸入下列其中一個命令：

   ◦ `volume delete`

```
cluster-1::*> volume delete -volume vol1 -vserver vs0

Warning: This operation requires multi-admin verification. To create
a
         verification request use "security multi-admin-verify
request
         create".

         Would you like to create a request for this operation?
          {y|n}: y

Error: command failed: The security multi-admin-verify request (index
3) is
       auto-generated and requires approval.
```

- `security multi-admin-verify request create "volume delete"`

```
Error: command failed: The security multi-admin-verify request (index
3)
       requires approval.
```

2. 檢查申請狀態、並回應MAV通知。
   a. 如果申請獲得核准、請回應CLI訊息以完成作業。

      範例：

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: approved
Required Approvers: 1
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Info: Volume "vol1" in Vserver "vs0" will be marked as deleted and
placed in the volume recovery queue. The space used by the volume
will be recovered only after the retention period of 12 hours has
completed. To recover the space immediately, get the volume name
using (privilege:advanced) "volume recovery-queue show vol1_*" and
then "volume recovery-queue purge -vserver vs0 -volume <volume_name>"
command. To recover the volume use the (privilege:advanced) "volume
recovery-queue recover -vserver vs0       -volume <volume_name>"
command.

Warning: Are you sure you want to delete volume "vol1" in Vserver
"vs0" ?
{y|n}: y
```

b. 如果申請遭否決或過期、請刪除申請、然後重新提交或聯絡MAV管理員。

   範例：

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: vetoed
Required Approvers: 1
 Pending Approvers: 1
   Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
         Approvals: -
       User Vetoed: admin2
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:38:47
     Time Approved: -
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

相關資訊

- "安全多管理員驗證"

在 ONTAP 中管理受 MAV 保護的作業要求

當 MAV 審批組中的管理員（MAV 管理員）收到待處理的操作執行請求通知時，他們必須在固定時間內（審批到期）回覆批准或否決訊息。如果沒有收到足夠數量的批准，請求者必須刪除該請求並提出另一個請求。

關於這項工作

核准要求會以索引編號來識別、這些索引編號會包含在電子郵件訊息中、並顯示要求佇列。

> `multi-admin-verify`處於終端狀態的請求可能會自動覆寫或刪除。使用"審計日誌"審查先前的請求。

可顯示來自要求佇列的下列資訊：

營運

建立要求的受保護作業。

查詢

使用者想要套用作業的物件（或物件）。

州/省

申請的目前狀態；擱置、核准、拒絕、過期、 已執行。如果某個申請被一位核准者拒絕、則不可能採取進一步行動。

必要的核准者

核准申請所需的MAV系統管理員人數。使用者可以為作業規則設定必要的核准者參數。如果使用者未將必要的核准者設定為規則、則會套用全域設定的必要核准者。

待核准者

仍需核准申請並將申請標記為「已核准」的MAV系統管理員人數。

核准過期

MAV管理員必須回應核准要求的期間。任何獲授權的使用者都可以設定作業規則的核准過期時間。如果未針對規則設定核准到期、則會套用全域設定的核准到期日。

執行過期

要求系統管理員必須完成作業的期間。任何授權使用者都可以設定作業規則的執行到期時間。如果未針對規則設定執行過期、則會套用全域設定的執行過期。

使用者已核准

已核准申請的MAV系統管理員。

使用者遭否決

已否決要求的MAV系統管理員。

儲存**VM**（**Vserver**）

與要求相關聯的SVM。此版本僅支援管理SVM。

使用者要求

建立要求之使用者的使用者名稱。

建立時間

建立要求的時間。

核准時間

申請狀態變更為「已核准」的時間。

留言

與申請相關的任何意見。

允許的使用者

允許執行已核准要求之受保護作業的使用者清單。如果 `users-permitted` 為空白、則任何具有適當權限的

使用者都可以執行此作業。

系統管理員

MAV 管理員會收到一封電子郵件，其中包含批准請求的詳細資訊、請求到期期限以及批准或拒絕請求的連結。他們可以透過點擊電子郵件中的連結存取批准對話框，或導航至系統管理員中的*事件和作業>請求*。

啟用多管理員驗證時，*請求*視窗可用，根據使用者的登入 ID 和 MAV 角色（是否為批准者）顯示待處理的請求。

- 營運
- 索引（數字）
- 狀態（「Pending（擱置）」、「Approved（已核准）」、「Rejected（已拒絕）

  如果某個申請被一位核准者拒絕、則不可能採取進一步行動。
- 查詢（所要求作業的任何參數或值）
- 正在申請使用者
- 申請截止日期
- （數量）待核准者
- （數量）潛在核准者

MAV系統管理員在此視窗中有其他控制項、他們可以核准、拒絕或刪除個別作業、或是選取的作業群組。但是、如果MAV管理員是申請使用者、則他們無法核准、拒絕或刪除自己的申請。

CLI

1. 當透過電子郵件收到待處理請求的通知時，請記下請求的索引號和核准有效期限。索引號碼也可以使用下面提到的 **show** 或 **show-pending** 選項顯示。
2. 核准或否決要求。

如果您想...	輸入此命令
核准申請	`security multi-admin-verify request approve` *nn*
否決要求	`security multi-admin-verify request veto` *nn*
顯示所有要求、擱置中的要求或單一要求	`security multi-admin-verify request { show
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  您可以顯示佇列中的所有要求、或只顯示擱置中的要求。如果您輸入索引編號、則只會顯示該索引編號的資訊。您可以顯示特定欄位的相關資訊（使用 `-fields` 參數）或關於所有欄位（使用 `-instance` 參數）。

如果您想...	輸入此命令
刪除要求	`security multi-admin-verify request delete nn`

範例：

下列順序會在MAV管理員收到索引編號為3的要求電子郵件後核准申請、該電子郵件已獲得一次核准。

```
          cluster1::> security multi-admin-verify request show-pending
                                      Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         julia


cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: approved
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: julia
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

範例：

下列順序會在MAV管理員收到索引編號為3的要求電子郵件後、將要求覆寫、該電子郵件已獲得一次核准。

```
      cluster1::> security multi-admin-verify request show-pending
                                     Pending
Index Operation      Query State    Approvers Requestor
----- -------------- ----- -------- --------- ---------
    3 volume delete  -     pending 1         pavan


cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: vetoed
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin1
       User Vetoed: mav-admin2
           Vserver: cluster-1
    User Requested: pavan
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

相關資訊

- "安全多管理員驗證"

管理動態授權

瞭解 ONTAP 動態授權

從 ONTAP 9.15.1 開始、系統管理員可以設定並啟用動態授權、以提高遠端存取 ONTAP 的安全性、同時降低惡意攻擊者可能造成的潛在損害。有了 ONTAP 9.15.1 、動態授權提供了一個初始架構、可將安全分數指派給使用者、如果他們的活動看起來可疑、則可透過額外的授權檢查來挑戰他們、或是完全拒絕作業。系統管理員可以建立規則、指派信任分數、以及限制命令、以決定何時允許或拒絕使用者的特定活動。系統管理員可以在整個叢集範圍內啟用動態授權、或是為個別的儲存 VM 啟用授權。

動態授權的運作方式

動態授權使用信任評分系統、根據授權原則、將不同的信任等級指派給使用者。根據使用者的信任層級、可以允許或拒絕他們執行的活動、也可以提示使用者進行進一步驗證。

請參閱"自訂動態授權"以深入瞭解如何設定準則分數權重和其他動態授權屬性。

信任的裝置

使用動態授權時、受信任裝置的定義是使用者使用公開金鑰驗證作為驗證方法之一來登入 ONTAP 的裝置。裝置受信任、因為只有該使用者擁有對應的私密金鑰。

動態授權範例

以嘗試刪除磁碟區的三個不同使用者為例。當他們嘗試執行作業時、會檢查每位使用者的風險等級：

- 第一位使用者從信任的裝置登入時、先前的驗證失敗次數極少、這使得她的風險等級偏低；無需額外驗證即可執行此作業。
- 第二位使用者從信任的裝置登入時、其先前的驗證失敗百分比適中、因此風險等級較為溫和；在允許操作之前、系統會提示她進行額外驗證。
- 第三位使用者從不受信任的裝置登入時、其先前的驗證失敗率很高、因此風險等級很高；不允許此作業。

下一步

- "啟用或停用動態授權"
- "自訂動態授權"

在 **ONTAP** 中啟用或停用動態授權

從 ONTAP 9.15.1 開始、系統管理員可以在中設定及啟用動態授權 `visibility` 測試組態的模式、或在中 `enforced` 模式、可啟動透過 SSH 連線的 CLI 使用者組態。如果您不再需要動態授權、可以停用它。當您停用動態授權時、組態設定會保持可用狀態、如果您決定重新啟用、您可以稍後再使用。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization modify`資訊，請參閱。

啟用動態授權以進行測試

您可以在可見度模式中啟用動態授權、藉此測試功能、並確保使用者不會被意外鎖定。在此模式中、信任分數會針對每個受限活動進行檢查、但不會強制執行。但是、任何會被拒絕或受到其他驗證挑戰的活動都會記錄下來。最佳實務做法是先在此模式中測試您想要的設定、然後再執行設定。

即使您尚未設定任何其他動態授權設定、也可以依照此步驟第一次啟用動態授權。"自訂動態授權"如需設定其他動態授權設定的步驟、請參閱以根據您的環境進行自訂。

步驟

1. 設定全域設定並將功能狀態變更為、即可在可見度模式中啟用動態授權 `visibility`。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。更新括弧 <> 中的值以符合您的環境。必須使用粗體參數：

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. 使用檢查結果 `show` 顯示全域組態的命令：

```
security dynamic-authorization show
```

在強制模式中啟用動態授權

您可以在強制模式中啟用動態授權。一般而言、在使用可見度模式完成測試之後、您會使用此模式。在此模式中、每個受限活動都會檢查信任分數、如果符合限制條件、則會強制執行活動限制。也會強制執行抑制間隔、以防止在指定時間間隔內發生其他驗證挑戰。

此步驟假設您先前已在中設定並啟用動態授權 `visibility` 強烈建議使用模式。

步驟

1. 在中啟用動態授權 `enforced` 模式、將其狀態變更為 `enforced`。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。更新括弧 <> 中的值以符合您的環境。必須使用粗體參數：

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage_VM_name>
```

2. 使用檢查結果 `show` 顯示全域組態的命令：

```
security dynamic-authorization show
```

停用動態授權

如果不再需要新增的驗證安全性、您可以停用動態授權。

步驟

1. 將動態授權狀態變更為、以停用動態授權 `disabled`。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。更新括弧 <> 中的值以符合您的環境。必須使用粗體參數：

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. 使用檢查結果 `show` 顯示全域組態的命令：

```
security dynamic-authorization show
```

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization show`資訊，請參閱。

下一步

（選用）視您的環境而定"自訂動態授權"、請參閱以設定其他動態授權設定。

在 **ONTAP** 中自訂動態授權

身為管理員、您可以自訂動態授權組態的不同層面、以提高遠端系統管理員 SSH 連線至 ONTAP 叢集的安全性。

您可以根據安全需求自訂下列動態授權設定：

- [設定動態授權全域設定]
- [設定動態授權信任分數元件]
- [設定自訂信任分數提供者]
- [設定受限命令]
- [設定動態授權群組]

設定動態授權全域設定

您可以設定動態授權的全域設定、包括要保護的儲存 VM 、驗證挑戰的抑制時間間隔、以及信任分數設定。

如"指令參考資料ONTAP"需詳細 `security login domain-tunnel create`資訊，請參閱。

步驟

1. 設定動態授權的全域設定。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。更新括弧 <> 中的值以符合您的環境：

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. 檢視產生的組態：

```
security dynamic-authorization show
```

設定受限命令

啟用動態授權時、此功能會包含一組預設的限制命令。您可以修改此清單以符合您的需求。請參閱 "多重管理驗證（ MAV ）文件" 以取得受限命令的預設清單資訊。

新增受限制的命令

您可以將命令新增至受限於動態授權的命令清單。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization rule create`資訊，請參閱。

步驟

1. 新增命令。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage_VM_name>
```

2. 檢視所產生的限制命令清單：

```
security dynamic-authorization rule show
```

移除受限制的命令

您可以從受限於動態授權的命令清單中移除命令。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization rule delete`資訊，請參閱。

步驟

1. 移除命令。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage_VM_name>
```

2. 檢視所產生的限制命令清單：

```
security dynamic-authorization rule show
```

設定動態授權群組

根據預設、動態授權會在您啟用後立即套用至所有使用者和群組。不過、您可以使用建立群組 `security dynamic-authorization group create` 因此動態授權僅適用於這些特定使用者。

新增動態授權群組

您可以新增動態授權群組。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization group create`資訊，請參閱。

步驟

1. 建立群組。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization group create \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name> \
-excluded-usernames <user1,user2,user3...>
```

2. 檢視產生的動態授權群組：

```
security dynamic-authorization group show
```

移除動態授權群組

您可以移除動態授權群組。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization group delete`資訊，請參閱。

步驟

1. 刪除群組。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization group delete \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. 檢視產生的動態授權群組：

```
security dynamic-authorization group show
```

設定動態授權信任分數元件

您可以設定最大分數權重、以變更評分準則的優先順序、或移除風險評分的特定準則。

最佳做法是保留預設分數權重值、並在需要時才進行調整。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization trust-score-component modify`資訊，請參閱。

以下是您可以修改的元件、以及其預設分數和百分比權重：

準則	元件名稱	預設原始分數權重	預設百分比權重
信任的裝置	`trusted-device`	20.	50
使用者登入驗證記錄	`authentication-history`	20.	50

步驟

1. 修改信任分數元件。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. 檢視產生的信任分數元件設定：

```
security dynamic-authorization trust-score-component show
```

重設使用者的信任分數

如果使用者因系統原則而遭拒存取、且能夠證明其身分識別、則系統管理員可以重設使用者的信任分數。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization user-trust-score reset`資訊，請參閱。

步驟

1. 新增命令。請參閱 [設定動態授權信任分數元件] 取得您可以重設的信任分數元件清單。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

顯示您的信任分數

使用者可以顯示自己的登入工作階段信任分數。

步驟

1. 顯示您的信任分數：

   ```
   security login whoami
   ```

   您應該會看到類似下列的輸出：

   ```
   User: admin
   Role: admin
   Trust Score: 50
   ```

   如"指令參考資料ONTAP"需詳細 `security login whoami`資訊，請參閱。

設定自訂信任分數提供者

如果您已經收到外部信任分數提供者的評分方法、可以將自訂提供者新增至動態授權組態。

開始之前

- 自訂信任分數提供者必須傳回 JSON 回應。必須符合下列語法需求：
  - 傳回信任分數的欄位必須是純量欄位、而非陣列的元素。
  - 傳回信任分數的欄位可以是巢狀欄位、例如 `trust_score.value`。
  - JSON 回應中必須有一個欄位可傳回數值信任分數。如果無法原生使用、您可以撰寫包裝函式指令碼來傳回此值。
- 提供的值可以是信任分數或風險分數。差異在於信任分數以遞增順序排列、分數較高則代表較高的信任層級、而風險分數則以遞減順序排列。例如、分數範圍為 0 至 100 的信任分數為 90 、表示分數非常值得信賴、可能會導致「允許」而不需要其他挑戰、 雖然分數範圍為 0 到 100 的風險分數為 90 、表示風險高、可能導致「拒絕」、而不會有額外的挑戰。
- 自訂信任分數提供者必須透過 ONTAP REST API 存取。
- 自訂信任分數提供者必須使用其中一個支援的參數進行設定。不支援需要不在支援參數清單中的組態的自訂信任分數提供者。

  如"指令參考資料ONTAP"需詳細 `security dynamic-authorization trust-score-component create`資訊，請參閱。

步驟

1. 新增自訂信任分數提供者。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. 檢視產生的信任分數提供者設定：

```
security dynamic-authorization trust-score-component show
```

設定自訂信任分數提供者標記

您可以使用標記與外部信任分數提供者通訊。這可讓您將 URL 中的資訊傳送給信任分數提供者、而不會洩漏敏感資訊。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization trust-score-component create`資訊，請參閱。

步驟

1. 啟用信任分數提供者標記。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

例如：

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

使用 OAuth 2.0 進行驗證與授權

ONTAP OAuth 2.0 實作總覽

從 ONTAP 9.14 開始、您可以選擇使用開放授權（ OAuth 2.0 ）架構來控制對 ONTAP 叢集的存取。您可以使用任何 ONTAP 管理介面（包括 ONTAP CLI 、系統管理員和 REST API ）來設定此功能。不過、 OAuth 2.0 授權和存取控制決策只能在用戶端使用 REST API 存取 ONTAP 時套用。

OAuth 2.0 支援是 ONTAP 9.14.0 首次推出、因此可用度取決於您使用的 ONTAP 版本。請參閱 "發行說明ONTAP" 以取得更多資訊。

功能與優勢

以下說明搭配 ONTAP 使用 OAuth 2.0 的主要功能與優點。

支援 OAuth 2.0 標準

OAuth 2.0 是業界標準授權架構。它可用來限制及控制使用簽署存取權杖來存取受保護資源的權限。使用 OAuth 2.0 有幾個好處：

- 授權組態有許多選項
- 切勿洩漏用戶端認證、包括密碼
- 您可以根據組態將權杖設定為過期
- 非常適合與 REST API 搭配使用

使用熱門授權伺服器進行測試

ONTAP OAuth 2.0 實作已針對數個熱門伺服器或服務進行測試，其依據為 ONTAP 版本，如下所示：

- ONTAP 9 。 16.1 （支援群組 UUID 至名稱對應和外部角色）：
  - Microsoft Entra ID
- ONTAP 9 。 14.1 （支援標準 OAuth 2.0 功能）
  - 驗證0
  - Active Directory Federation Service （ ADFS ）
  - Keycloak

如需每個 ONTAP 版本可用功能的詳細資訊，請參閱"授權伺服器和存取權杖"。

支援多個並行授權伺服器

您最多可以為單一 ONTAP 叢集定義八個授權伺服器。如此一來、您就能靈活地滿足各種安全環境的需求。

與 **REST** 角色整合

ONTAP 授權決策最終取決於指派給使用者或群組的其餘角色。這些角色可在存取權杖中作為獨立範圍、或是根據本機 ONTAP 定義以及 Active Directory 或 LDAP 群組來執行。

使用寄件者限制存取權杖的選項

您可以將 ONTAP 和授權伺服器設定為使用相互傳輸層安全性（ MTLS ）、以強化用戶端驗證。它保證 OAuth 2.0 存取權杖只能由最初核發的用戶端使用。此功能支援並符合數項常用的安全性建議、包括由 FAPI 和斜接建立的建議。

實作與組態

在較高層級、 OAuth 2.0 實作和組態有幾個層面、您應該在開始使用時考慮。

ONTAP 內的 **OAuth 2.0** 實體

OAuth 2.0 授權架構定義了數個實體、可對應至資料中心或網路中的實際或虛擬元素。下表列出 OAuth 2.0 實體及其對 ONTAP 的調適。

OAuth 2.0 實體	說明
資源	REST API 端點、可透過內部 ONTAP 命令存取 ONTAP 資源。
資源擁有者	建立受保護資源或依預設擁有資源的 ONTAP 叢集使用者。
資源伺服器	受保護資源的主機、即 ONTAP 叢集。
用戶端	代表或取得資源擁有者權限、要求存取 REST API 端點的應用程式。
授權伺服器	通常是負責發行存取權杖和強制執行管理原則的專用伺服器。

核心 **ONTAP** 組態

您需要設定 ONTAP 叢集以啟用和使用 OAuth 2.0 。這包括建立與授權伺服器的連線、以及定義所需的 ONTAP 授權組態。您可以使用任何管理介面來執行此組態、包括：

- 指令行介面ONTAP
- 系統管理員
- 靜態API ONTAP

環境與支援服務

除了 ONTAP 定義之外、您也需要設定授權伺服器。如果您使用群組對角色對應、也需要設定 Active Directory 群組或 LDAP 等量。

支援的 **ONTAP** 用戶端

從 ONTAP 9.14 開始、 REST API 用戶端可以使用 OAuth 2.0 存取 ONTAP 。在發出 REST API 呼叫之前、您需要從授權伺服器取得存取權杖。然後、用戶端使用 HTTP 授權要求標頭、將此權杖以 _bon承載 權杖的形式傳送至 ONTAP 叢集。視所需的安全性層級而定、您也可以在用戶端建立及安裝憑證、以使用以 MTLS 為基礎的寄件者限制權杖。

選定的術語

當您開始使用 ONTAP 探索 OAuth 2.0 部署時、熟悉其中一些詞彙是很有幫助的。請參閱 "其他資源" 取得有關 OAuth 2.0 的詳細資訊連結。

存取權杖

由授權伺服器發出的權杖、由 OAuth 2.0 用戶端應用程式用來發出存取受保護資源的要求。

JSON Web Token

用於格式化存取權杖的標準。JSON 用於以精簡格式呈現 OAuth 2.0 宣告、並將宣告分為三個主要區段。

寄件者限制的存取權杖

以相互傳輸層安全性（ MTLS ）傳輸協定為基礎的選用功能。藉由在權杖中使用額外的確認宣告、這可確保存取權杖僅供最初核發的用戶端使用。

JSON Web 金鑰集

JWKS 是 ONTAP 用來驗證用戶端所呈現 JWT Token 的公開金鑰集合。金鑰集通常可透過專用 URI 在授權伺服器上使用。

範圍

範圍提供一種方法來限制或控制應用程式對受保護資源（例如 ONTAP REST API ）的存取。它們在存取權杖中以字串表示。

ONTAP REST 角色

REST 角色是 ONTAP 9.6 引進的、是 ONTAP RBAC 架構的核心部分。這些角色與 ONTAP 仍支援的舊版傳統角色不同。ONTAP 中的 OAuth 2.0 實作僅支援 REST 角色。

HTTP 授權標頭

HTTP 要求中包含的標頭、用於在進行 REST API 呼叫時識別用戶端及相關權限。視驗證和授權的執行方式而定、有多種類型或實作可供選擇。將 OAuth 2.0 存取權杖呈現給 ONTAP 時、該權杖會識別為 _stoning 權杖 _ 。

HTTP 基本驗證

ONTAP 仍支援早期的 HTTP 驗證技術。純文字認證（使用者名稱和密碼）會與冒號串連、並以 base64 編碼。字串會放在授權要求標頭中、並傳送至伺服器。

FAPI

OpenID Foundation 的工作群組、為金融產業提供通訊協定、資料架構及安全建議。API 原本稱為財務等級 API 。

斜接

一家私人非營利公司、為美國空軍和美國政府提供技術與安全指引。

其他資源

以下提供幾項額外資源。您應該檢閱這些網站、以取得有關 OAuth 2.0 及相關標準的更多資訊。

通訊協定與標準

- "RFC 6749 ： OAuth 2.0 授權架構"

- "RFC 7519 ： JSON Web Token （ JWT ）"
- "RFC 7523 ：適用於 OAuth 2.0 用戶端驗證和授權授與的 JSON Web Token （ JWT ）設定檔"
- "RFC 7662 ： OAUTH 2.0 Token 反思"
- "RFC 7800 ： JWTs 的持有證明金鑰"
- "RFC 8705 ： OAuth 2.0 雙向 TLS 用戶端驗證和憑證繫結存取權杖"

組織

- "OpenID Foundation"
- "FAPI 工作組"
- "斜接"
- "IANA - JWT"

產品與服務

- "驗證0"
- "entra ID"
- "ADFS 總覽"
- "Keycloak"

其他工具與公用程式

- "JWT by Auth0"
- "Openssl"

NetApp 文件與資源

- "ONTAP 自動化文件"

概念

ONTAP中的 **OAuth 2.0** 授權伺服器和存取令牌

授權伺服器會在 OAuth 2.0 授權架構中執行多項重要功能、做為中央元件。

OAuth 2.0 授權伺服器

授權伺服器主要負責建立和簽署存取權杖。這些權杖包含身分識別與授權資訊、可讓用戶端應用程式選擇性地存取受保護的資源。這些伺服器通常彼此隔離、可透過多種不同方式實作、包括獨立的專用伺服器、或是作為較大型的身分識別與存取管理產品的一部分。

> 授權伺服器有時會使用不同的術語、尤其是 OAuth 2.0 功能會封裝在較大的身分識別與存取管理產品或解決方案中。例如，術語 * 身分識別提供者（ IDP ） * 經常與 * 授權伺服器 * 互換使用。

系統管理

除了發行存取權杖之外、授權伺服器也會提供相關的管理服務、通常是透過 Web 使用者介面。例如、您可以定義和管理：

- 使用者和使用者驗證
- 範圍
- 透過租戶和領域進行管理隔離
- 原則強制執行
- 連線至各種外部服務
- 支援其他身分識別傳輸協定（例如 SAML ）

ONTAP 與符合 OAuth 2.0 標準的授權伺服器相容。

定義至 **ONTAP**

您需要定義一或多個 ONTAP 授權伺服器。ONTAP 會安全地與每部伺服器通訊、以驗證權杖、並執行其他相關工作來支援用戶端應用程式。

ONTAP 組態的主要層面如下所示。另請參閱 "OAuth 2.0 部署案例" 以取得更多資訊。

存取權杖的驗證方式與位置

驗證存取權杖有兩個選項。

- 本機驗證

  ONTAP 可以根據發行權杖的授權伺服器所提供的資訊、在本機驗證存取權杖。從授權伺服器擷取的資訊會由 ONTAP 快取、並定期重新整理。

- 遠端自我反思

  您也可以使用遠端自我反思來驗證授權伺服器上的權杖。introspection 是一種允許授權方查詢授權伺服器有關存取權杖的通訊協定。它提供 ONTAP 從存取權杖擷取特定中繼資料並驗證權杖的方法。由於效能原因、ONTAP 會快取部分資料。

網路位置

ONTAP 可能位於防火牆後方。在這種情況下、您需要將 Proxy 識別為組態的一部分。

授權伺服器的定義方式

您可以使用任何管理介面（包括 CLI 、系統管理員或 REST API ）來定義 ONTAP 的授權伺服器。例如、您可以使用 CLI 使用命令 `security oauth2 client create`。

如"指令參考資料ONTAP"需詳細 `security oauth2 client create`資訊，請參閱。

授權伺服器數量

您最多可以定義八個授權伺服器到單一 ONTAP 叢集。只要發卡行或發卡行 / 受眾聲明是唯一的、同一授權伺服器就可以多次定義到同一個 ONTAP 叢集。例如、使用 Keycloak 時、使用不同領域時、這種情況永遠都會發生。

ONTAP 支援的 **OAuth 2.0** 功能

OAUTH 2.0 的支援最初隨 ONTAP 9 提供。 14.1 之後的版本將持續增強。ONTAP 支援的 OAuth 2.0 功能如下所述。

隨特定 ONTAP 版本推出的功能將會持續到未來的版本。

ONTAP 9.16.1.

ONTAP 9 。 16.1 擴充標準 OAuth 2.0 功能，以納入原生 Entra ID 群組的 Entra ID 專屬副檔名。這涉及在存取權杖中使用 GUID ，而非名稱。此外，此版本還新增外部角色對應支援，可利用存取權杖中的「角色」欄位，將原生身分識別提供者角色對應至 ONTAP 角色。

ONTAP 9.14.1.

從 ONTAP 9 。 14.1 開始，授權伺服器可透過下列標準 OAuth 2.0 功能來支援使用的應用程式：

- OAuth 2.0 標準欄位包括「 iss 」，「 aud 」和「 exp 」，如和 "RFC 7519 ： JSON Web Token （ JWT ）"中所述 "RFC6749 ： OAuth 2.0 授權架構"。這也支援透過存取權杖中的欄位來唯一識別使用者，例如「 UPN 」，「 AppID 」，「 Sub" ，「使用者名稱」或「 Preferred _UserName 」。
- 針對具有「群組」欄位的群組名稱，針對特定於供應商的 ADFS 副檔名。
- Azure 廠商專屬的群組 UUID 延伸功能，並具有「群組」欄位。
- 使用 OAuth 2.0 存取權杖範圍內的獨立角色和具名角色來提供授權支援的 ONTAP 延伸功能。其中包括「範圍」和「 scp 」欄位，以及範圍內的群組名稱。

使用 **OAuth 2.0** 存取權杖

由授權伺服器發出的 OAuth 2.0 存取權杖是由 ONTAP 驗證、用於為 REST API 用戶端要求做出角色型存取決策。

取得存取權杖

您需要從定義至 ONTAP 叢集的授權伺服器取得存取權杖、以便在其中使用 REST API 。若要取得權杖、您必須直接聯絡授權伺服器。

ONTAP 不會核發存取權杖、也不會將用戶端的要求重新導向至授權伺服器。

您要求權杖的方式取決於多項因素、包括：

- 授權伺服器及其組態選項
- OAuth 2.0 授與類型
- 用於發出要求的用戶端或軟體工具

授與類型

_Grant 是定義完善的程序、包括一組網路流量、用於要求及接收 OAuth 2.0 存取權杖。視用戶端、環境和安全性需求而定、可使用多種不同的授與類型。下表列出熱門的補助類型清單。

授與類型	說明
用戶端認證	一種僅使用認證（例如 ID 和共用密碼）的常用授與類型。假設用戶端與資源擁有者有密切的信任關係。

授與類型	說明
密碼	資源擁有者密碼認證授與類型可用於資源擁有者與用戶端建立信任關係的情況。將舊版 HTTP 用戶端移轉至 OAuth 2.0 時、這項功能也很實用。
授權代碼	這是機密用戶端的理想授與類型、是以重新導向為基礎的流程為基礎。它可用於取得存取權杖和重新整理權杖。

JWT 內容

OAuth 2.0 存取權杖格式化為 JWT 。內容是由授權伺服器根據您的組態建立。不過、這些 Token 對用戶端應用程式來說是不透明的。用戶端沒有理由檢查權杖或是知道其內容。

每個 JWT 存取權杖都包含一組宣告。聲明說明發卡行的特性、以及根據授權伺服器的管理定義進行的授權。下表說明部分已登錄於標準的索賠。所有字串都區分大小寫。

請款	關鍵字	說明
發卡行	ISS	識別發出權杖的主體。請款處理是針對特定應用程式。
主旨	子	權杖的主旨或使用者。名稱的範圍是全域或本機唯一的。
目標對象	AUD	權杖的目標收件者。以字串陣列形式實作。
過期	到期	權杖過期且必須拒絕的時間。

請參閱 "RFC 7519 ： JSON Web Token" 以取得更多資訊。

用戶端授權

ONTAP 用戶端授權的總覽與選項

ONTAP OAUTH 2.0 實作的設計既靈活又穩健，提供您保護 ONTAP 環境所需的功能。有多種互斥的組態選項可供選擇。授權決策最終取決於 OAuth 2.0 存取權杖中包含或衍生的 ONTAP REST 角色。

> 您只能使用 "ONTAP REST 角色" 設定 OAuth 2.0 授權時。不支援舊版 ONTAP 傳統角色。

ONTAP 會根據您的組態，套用最適當的單一授權選項。如需 ONTAP 如何做出用戶端存取決策的詳細資訊，請參閱"ONTAP 如何決定存取"。

OAuth 2.0 獨立範圍

這些範圍包含一或多個自訂 REST 角色，每個角色都封裝在存取權杖中的單一字串內。它們不受 ONTAP 角色定義的影響。您需要在授權伺服器上設定範圍字串。如需詳細資訊、請參閱 "獨立 OAuth 2.0 範圍" 。

本機 ONTAP REST 角色

可以使用單一命名 REST 角色，無論是內建或自訂。命名角色的範圍語法是 *ONTAP 角色 <URL-encoded-ONTAP-role-name> 。例如，如果 ONTAP 角色是範圍字串，則 `admin`為 `ontap-role-admin`。

使用者

您可以使用存取權杖中定義的使用者名稱，以存取應用程式「 http 」。根據定義的驗證方法，以下列順序測試使用者：密碼，網域（ Active Directory ）， nsswitch （ LDAP ）。

群組

授權伺服器可設定為使用 ONTAP 群組進行授權。如果檢查本機 ONTAP 定義、但無法做出存取決定、則會使用 Active Directory （「網域」）或 LDAP （「 nsswitch 」）群組。群組資訊可透過下列兩種方式之一來指定：

- OAuth 2.0 範圍字串

  支援使用用戶端認證流程的機密應用程式、而該流程沒有使用者擁有群組成員資格。範圍應命名為 *ONTAP 群組 <URL-encoded-ONTAP-group-name> 。例如、如果群組為「開發」、範圍字串將為「 ontap 群組開發」。

- 在「群組」請款中

  這是針對使用資源擁有者（密碼授予）流程的 ADFS 所發行的存取權杖。

看"在ONTAP中使用 OAuth 2.0 或 SAML IdP 群組"了解更多。

ONTAP中的獨立 OAuth 2.0 範圍

自我包含的範圍是存取權杖中攜帶的字串。每個角色都是完整的自訂角色定義、包括 ONTAP 做出存取決策所需的一切。範圍與 ONTAP 本身定義的任何其他角色是分開的。

範圍字串的格式

在基礎層級、範圍會以連續字串表示、並由六個以冒號分隔的值組成。範圍字串中使用的參數如下所述。

ONTAP 文字

範圍必須以文字值開頭 `ontap` 以小寫形式顯示。這會將範圍識別為 ONTAP 特有的範圍。

叢集

這會定義範圍所適用的 ONTAP 叢集。這些值可以包括：

- 叢集 UUID

  識別單一叢集。

- 星號（ * ）

  表示範圍適用於所有叢集。

您可以使用 ONTAP CLI 命令 `cluster identity show`來顯示叢集的 UUID 。如果未指定、範圍會套用至所有叢集。如"指令參考資料ONTAP"需詳細 `cluster identity show`資訊，請參閱。

角色

包含在獨立範圍中的 REST 角色名稱。ONTAP 不會檢查此值、也不會與任何定義給 ONTAP 的現有 REST 角色相符。名稱用於記錄。

存取層級

此值表示在範圍內使用 API 端點時、套用至用戶端應用程式的存取層級。下表說明了六個可能的值。

存取層級	說明
無	拒絕對指定端點的所有存取。
唯讀	僅允許使用 GET 進行讀取存取。
read_create	允許讀取存取、以及使用 POST 建立新的資源執行個體。
Read_modify	允許讀取存取權、以及使用修補程式更新現有資源的能力。
read_create_modify	允許刪除以外的所有存取。允許的作業包括 GET （讀取）、 POST （建立）和修補程式（更新）。
全部	允許完整存取。

SVM

適用範圍之叢集內的 SVM 名稱。使用 * 值（星號）表示所有 SVM 。

ONTAP 9.14.1 不完全支援此功能。您可以忽略 SVM 參數、並使用星號做為預留位置。檢閱 "發行說明ONTAP" 檢查將來的 SVM 支援。

REST API URI

資源或一組相關資源的完整或部分路徑。字串必須以開頭 `/api`。如果您未指定值、範圍會套用至 ONTAP 叢集上的所有 API 端點。

範圍範例

以下是一些自我包含範圍的範例。

ONTAP ： * ： jjoes-role ： read_create_modify ： * ： /API/cluster

提供指派此角色的使用者讀取、建立及修改對的存取權 `/cluster` 端點：

CLI 管理工具

為了讓自我包含範圍的管理更容易且更容易出錯、 ONTAP 提供了 CLI 命令 `security oauth2 scope` 根據輸入參數產生範圍字串。

命令 `security oauth2 scope` 根據您的意見、有兩種使用案例：

- 範圍字串的 CLI 參數

  您可以使用此版本的命令來根據輸入參數產生範圍字串。

- 範圍字串至 CLI 參數

  您可以使用此版本的命令、根據輸入範圍字串產生命令參數。

範例

下列範例會產生範圍字串、並在下列命令範例之後包含輸出。此定義適用於所有叢集。

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

如"指令參考資料ONTAP"需詳細 `security oauth2 scope`資訊，請參閱。

ONTAP中的 OAuth 2.0 外部角色映射

外部角色是在設定供 ONTAP 使用的識別供應商處定義。您可以使用 ONTAP CLI 建立及管理這些外部角色與 ONTAP 角色之間的對應關係。

您也可以使用 ONTAP REST API 來設定外部角色對應功能。如需詳細資訊，請參閱 "ONTAP 自動化文件"。

存取權杖中的外部角色

以下是包含兩個外部角色的 JSON 存取權杖片段。

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

組態

您可以使用 ONTAP 命令列介面來管理外部角色對應功能。

建立

您可以使用命令定義角色對應組態 `security login external-role-mapping create`。您必須處於 ONTAP * 管理 * 權限層級，才能發出此命令及相關選項。

參數

用於建立群組對應的參數如下所述。

參數	說明
external-role	在外部身分識別提供者定義的角色名稱。
provider	身分識別提供者的名稱。這應該是系統的識別碼。
ontap-role	表示外部角色對應的現有 ONTAP 角色。

範例

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

如"指令參考資料ONTAP"需詳細 `security login external-role-mapping create`資訊，請參閱。

其他 **CLI** 作業

此命令支援多項額外作業，包括：

- 顯示
- 修改
- 刪除

相關資訊

- "指令參考資料ONTAP"

ONTAP 如何決定用戶端存取

若要正確設計及實作 OAuth 2.0 、您必須瞭解 ONTAP 如何使用您的授權組態來為用戶端做出存取決策。根據 ONTAP 版本，決定存取權限的主要步驟如下所示。

ONTAP 9 · 15.1 沒有重大的 OAuth 2.0 更新。如果您使用的是 9.15.1 版，請參閱 ONTAP 9 。14.1 的說明。

相關資訊

- "ONTAP 支援的 OAuth 2.0 功能"

ONTAP 9.16.1.

ONTAP 9 。 16.1 擴充標準 OAuth 2.0 支援，以納入適用於原生 Entra ID 群組的 Microsoft Entra ID 特定副檔名，以及外部角色對應。

判斷 **ONTAP 9** 的用戶端存取權。 **16.1**

步驟 **1** ：自我包含的範圍

如果存取權杖包含任何獨立的範圍， ONTAP 會先檢查這些範圍。如果沒有獨立的範圍、請前往步驟 2 。

如果存在一個或多個獨立的範圍、 ONTAP 會套用每個範圍、直到可以做出明確的 * 允許 * 或 * 拒絕 * 決策為止。如果做出明確的決定、處理程序就會結束。

如果 ONTAP 無法做出明確的存取決策、請繼續執行步驟 2 。

步驟 **2** ：檢查本機角色旗標

ONTAP 檢查布爾參數 `use-local-roles-if-present`。此旗標的值會針對定義為 ONTAP 的每個授權伺服器分別設定。

- 如果值為 `true` 繼續進行步驟 3 。
- 如果值為 `false` 處理結束、存取遭拒。

步驟 **3** ：具名的 **ONTAP REST** 角色

如果存取權杖在 OR `scp` 欄位中包含具名的 REST 角色 `scope`，或是宣告， ONTAP 會使用該角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果沒有指定的 REST 角色或找不到角色、請繼續執行步驟 4 。

步驟 **4** ：使用者

從存取權杖擷取使用者名稱，並嘗試將其與有權存取應用程式「 http 」的使用者配對。根據驗證方法，依下列順序檢查使用者：

- 密碼
- 網域（ Active Directory ）
- NSWITCH （ LDAP ）

如果找到相符的使用者， ONTAP 會使用為使用者定義的角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果使用者不相符，或存取權杖中沒有使用者名稱，請繼續執行步驟 5 。

步驟 **5** ：群組

如果包含一個或多個群組，則檢查其格式。如果群組以 UUID 表示，則搜尋內部群組對應表。如果存在符合的群組和關聯的角色，ONTAP將使用為該群組定義的角色做出存取決策。這始終會導致“允許”或“拒絕”決策，處理結束。有關更多信息，請參閱"在ONTAP中使用 OAuth 2.0 或 SAML IdP 群組" 。

如果群組是以名稱表示，並已設定網域或 nsswitch 授權，則 ONTAP 會分別嘗試將其與 Active Directory 或 LDAP 群組進行比對。如果有群組相符項目、 ONTAP 會使用為群組定義的角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果沒有符合的群組、或存取權杖中沒有群組、則會拒絕存取並結束處理。

ONTAP 9.14.1.

支援的初始 OAUTH 2.0 是根據標準 OAUTH 2.0 功能而在 ONTAP 9 中推出的。

決定 **ONTAP 9** 的用戶端存取權。 **14.1**

步驟 **1** ：自我包含的範圍

如果存取權杖包含任何獨立的範圍， ONTAP 會先檢查這些範圍。如果沒有獨立的範圍、請前往步驟 2 。

如果存在一個或多個獨立的範圍、 ONTAP 會套用每個範圍、直到可以做出明確的 * 允許 * 或 * 拒絕 * 決策為止。如果做出明確的決定、處理程序就會結束。

如果 ONTAP 無法做出明確的存取決策、請繼續執行步驟 2 。

步驟 **2** ：檢查本機角色旗標

ONTAP 檢查布爾參數 `use-local-roles-if-present`。此旗標的值會針對定義為 ONTAP 的每個授權伺服器分別設定。

- 如果值為 `true` 繼續進行步驟 3 。
- 如果值為 `false` 處理結束、存取遭拒。

步驟 **3** ：具名的 **ONTAP REST** 角色

如果存取權杖在 OR `scp` 欄位中包含具名的 REST 角色 `scope`， ONTAP 會使用該角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果沒有指定的 REST 角色或找不到角色、請繼續執行步驟 4 。

步驟 **4** ：使用者

從存取權杖擷取使用者名稱，並嘗試將其與有權存取應用程式「 http 」的使用者配對。根據驗證方法，依下列順序檢查使用者：

- 密碼
- 網域（ Active Directory ）
- NSWITCH （ LDAP ）

如果找到相符的使用者， ONTAP 會使用為使用者定義的角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果使用者不相符，或存取權杖中沒有使用者名稱，請繼續執行步驟 5 。

步驟 **5** ：群組

如果包含一個或多個群組，並設定了網域或 nsswitch 授權， ONTAP 會分別嘗試將它們與 Active Directory 或 LDAP 群組配對。

如果有群組相符項目、 ONTAP 會使用為群組定義的角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果沒有符合的群組、或存取權杖中沒有群組、則會拒絕存取並結束處理。

使用**ONTAP** 的**OAuth 2.0** 部署場景

將授權伺服器定義為 ONTAP 時、有幾個組態選項可供使用。根據這些選項，您可以使用多種部署案例之一，定義適合您環境的授權伺服器。

組態參數摘要

將授權伺服器定義為 ONTAP 時、有幾個組態參數可供使用。這些參數通常在所有管理介面中都受到支援。

個別參數或欄位使用的名稱可能會因 ONTAP 管理介面而異。為了因應管理介面的差異，表格中的每個參數都會使用單一通用名稱。根據上下文，與特定介面搭配使用的確切名稱應該是顯而易見的。

參數	說明
名稱	ONTAP 已知的授權伺服器名稱。
應用程式	定義所適用的 ONTAP 內部應用程式。這必須是 * http * 。
發卡行 URI	具有路徑的 FQDN 、可識別發出權杖的站台或組織。
提供者 JWKS URI	ONTAP 取得用於驗證存取權杖之 JSON 網頁金鑰集的路徑和檔案名稱 FQDN 。
JWKS 重新整理時間間隔	決定 ONTAP 從提供者 JWKS URI 重新整理憑證資訊的頻率的時間間隔。此值以 ISO-8601 格式指定。
introspection 端點	ONTAP 透過自我介紹來執行遠端權杖驗證所使用的路徑 FQDN 。
用戶端ID	授權伺服器上定義的用戶端名稱。包含此值時、您也需要根據介面提供相關的用戶端機密。
傳出 Proxy	這是為了在 ONTAP 位於防火牆後方時提供對授權伺服器的存取。URI 必須為 cURL 格式。
如果存在、請使用本機角色	判斷是否使用本機 ONTAP 定義的布林旗標、包括具名 REST 角色和本機使用者。
遠端使用者請款	ONTAP 用來比對本機使用者的替代名稱。使用 `sub` 存取權杖中的欄位、以符合本機使用者名稱。
目標對象	此欄位定義可使用存取權杖的端點。

部署案例

以下提供幾種常見的部署案例。它們是根據權杖驗證是由 ONTAP 在本機執行、還是由授權伺服器遠端執行來組織。每個案例都包含所需組態選項的清單。請參閱 "在 ONTAP 中部署 OAuth 2.0" 以取得組態命令的範例。

定義授權伺服器之後、您可以透過 ONTAP 管理介面顯示其組態。例如、使用命令 `security oauth2 client show` 使用 ONTAP CLI 。

本機驗證

下列部署案例是以 ONTAP 在本機執行權杖驗證為基礎。

使用不含 **Proxy** 的自我控制範圍

這是僅使用 OAuth 2.0 獨立範圍的最簡單部署。不會使用任何本機 ONTAP 身分識別定義。您需要包含下列參數

：

- 名稱
- 應用程式（ http ）
- 提供者 JWKS URI
- 發卡行 URI

您也需要在授權伺服器上新增範圍。

在 **Proxy** 中使用自我包含的範圍

此部署案例使用 OAuth 2.0 獨立範圍。不會使用任何本機 ONTAP 身分識別定義。但是授權伺服器位於防火牆後方、因此您需要設定 Proxy 。您需要包含下列參數：

- 名稱
- 應用程式（ http ）
- 提供者 JWKS URI
- 傳出 Proxy
- 發卡行 URI
- 目標對象

您也需要在授權伺服器上新增範圍。

使用本機使用者角色和預設使用者名稱對應搭配 **Proxy**

此部署案例使用具有預設名稱對應的本機使用者角色。遠端使用者宣告使用的預設值 `sub` 因此、存取權杖中的這個欄位是用來比對本機使用者名稱。使用者名稱必須少於 40 個字元。授權伺服器位於防火牆後方、因此您也需要設定 Proxy 。您需要包含下列參數：

- 名稱
- 應用程式（ http ）
- 提供者 JWKS URI
- 如果存在、請使用本機角色 (`true`)
- 傳出 Proxy
- 發卡行

您必須確定本機使用者已定義為 ONTAP 。

使用本機使用者角色和替代使用者名稱對應搭配 **Proxy**

此部署案例使用具有替代使用者名稱的本機使用者角色、用於與本機 ONTAP 使用者配對。授權伺服器位於防火牆後方、因此您需要設定 Proxy 。您需要包含下列參數：

- 名稱
- 應用程式（ http ）
- 提供者 JWKS URI

- 如果存在、請使用本機角色 (`true`)
- 遠端使用者請款
- 傳出 Proxy
- 發卡行 URI
- 目標對象

您必須確定本機使用者已定義為 ONTAP 。

遠端自我反思

下列部署組態是以 ONTAP 透過自我反思遠端執行權杖驗證為基礎。

使用不含 **Proxy** 的自我控制範圍

這是以 OAuth 2.0 獨立範圍為基礎的簡單部署。不會使用任何 ONTAP 身分識別定義。您必須包含下列參數：

- 名稱
- 應用程式（ http ）
- introspection 端點
- 用戶端ID
- 發卡行 URI

您需要在授權伺服器上定義範圍以及用戶端和用戶端機密。

相關資訊

- "安全 oauth2 用戶端展示"

使用 **OAuth 2.0 Mutual TLS** 進行**ONTAP**客戶端身份驗證

視您的安全需求而定、您可以選擇性地設定相互 TLS （ MTLS ）來實作強式用戶端驗證。搭配 ONTAP 搭配 OAuth 2.0 部署使用時、 MTLS 保證存取權杖只能由最初核發的用戶端使用。

與 **OAuth 2.0** 共同使用 **TLS**

傳輸層安全性（ TLS ）用於在兩個應用程式（通常是用戶端瀏覽器和 Web 伺服器）之間建立安全的通訊通道。相互 TLS 可透過用戶端憑證提供用戶端的強大識別功能、藉此延伸此功能。在具有 OAuth 2.0 的 ONTAP 叢集中使用時、可透過建立和使用寄件者限制的存取權杖來擴充基礎 MTLS 功能。

傳送者限制的存取權杖只能由最初核發的用戶端使用。若要支援此功能、請提出新的確認聲明 (`cnf`）插入令牌中。欄位包含內容 `x5t#S256` 其中包含要求存取權杖時所使用的用戶端憑證摘要。此值由 ONTAP 驗證、作為驗證權杖的一部分。未受寄件者限制的授權伺服器所核發的存取權杖、不包含額外的確認宣告。

您需要將 ONTAP 設定為針對每個授權伺服器分別使用 MTLS 。例如、 CLI 命令 `security oauth2 client` 包含參數 `use-mutual-tls` 根據下表所示的三個值來控制 MTLS 處理。

在每個組態中、 ONTAP 所採取的結果和行動、都要視組態參數值、以及存取權杖和用戶端憑證的內容而定。表格中的參數是從最少組織到最嚴格的組織。

參數	說明
無	授權伺服器的 OAuth 2.0 相互 TLS 驗證已完全停用。ONTAP 不會執行 MTLS 用戶端憑證驗證、即使憑證中有確認宣告、或是用戶端憑證隨附 TLS 連線。
要求	如果用戶端提供寄件者限制的存取權杖、則會強制執行 OAuth 2.0 相互 TLS 驗證。也就是說、只有在確認宣告（含屬性）時、才會強制執行 MTLS `x5t#S256`）存在於存取權杖中。這是預設設定。
必要	對於由授權伺服器發出的所有存取權杖、都會強制執行 OAuth 2.0 相互 TLS 驗證。因此、所有存取權杖都必須受寄件者限制。如果存取權杖中沒有確認宣告、或是用戶端憑證無效、驗證和 REST API 要求就會失敗。

高階實作流程

在 ONTAP 環境中搭配 OAuth 2.0 使用 MTLS 時所涉及的一般步驟如下所示。請參閱 "RFC 8705 ： OAuth 2.0 雙向 TLS 用戶端驗證和憑證繫結存取權杖" 以取得更多詳細資料。

步驟 **1** ：建立及安裝用戶端憑證

建立用戶端身分識別的基礎、是證明客戶端私密金鑰的知識。對應的公開金鑰會放置在用戶端提供的簽署 X.509 憑證中。在較高層級、建立用戶端憑證所涉及的步驟包括：

1. 產生公開金鑰與私密金鑰配對
2. 建立憑證簽署要求
3. 將 CSR 檔案傳送至知名的 CA
4. CA 會驗證要求並核發簽署的憑證

您通常可以在本機作業系統中安裝用戶端憑證、或直接搭配一般公用程式（例如 Curl ）使用。

步驟 **2** ：將 **ONTAP** 設定為使用 **MTLS**

您需要設定 ONTAP 以使用 MTLS 。每個授權伺服器都會分別完成此組態設定。例如、使用 CLI 命令 `security oauth2 client` 與選用參數搭配使用 `use-mutual-tls`。請參閱 "在 ONTAP 中部署 OAuth 2.0" 以取得更多資訊。

步驟 **3** ：用戶端要求存取權杖

用戶端需要從設定為 ONTAP 的授權伺服器要求存取權杖。用戶端應用程式必須在步驟 1 中建立並安裝憑證時使用 MTLS 。

步驟 **4** ：授權伺服器會產生存取權杖

授權伺服器會驗證用戶端要求並產生存取權杖。在此過程中、它會建立用戶端憑證的訊息摘要、並將其作為確認宣告（欄位 `cnf`）。

步驟 **5** ：用戶端應用程式會將存取權杖呈現給 **ONTAP**

用戶端應用程式會對 ONTAP 叢集進行 REST API 呼叫、並在授權要求標頭中以 * 承載權杖 * 的形式包含存取權杖。用戶端必須使用 MTLS 搭配用於要求存取權杖的相同憑證。

步驟 **6** ： **ONTAP** 會驗證用戶端和權杖。

ONTAP 會在 HTTP 要求中接收存取權杖、以及作為 MTLS 處理一部分的用戶端憑證。ONTAP 會先驗證存取權杖中的簽章。根據組態、 ONTAP 會產生用戶端憑證的訊息摘要、並將其與權杖中的確認宣告 **cnf** 進行比較。如果這兩個值相符、 ONTAP 已確認發出 API 要求的用戶端與最初發出存取權杖的用戶端相同。

相關資訊

- "安全oauth2客戶端"

設定與部署

準備使用 **ONTAP** 部署 **OAuth 2.0**

在 ONTAP 環境中設定 OAuth 2.0 之前、您應該先準備部署。主要任務和決定摘要如下。各節的排列方式通常與您應遵循的順序一致。不過、雖然它適用於大多數的部署、但您應該視需要調整以符合您的環境。您也應該考慮建立正式的部署計畫。

根據您的環境、您可以為定義為 ONTAP 的授權伺服器選取組態。這包括您需要針對每種部署類型指定的參數值。請參閱 "OAuth 2.0 部署案例" 以取得更多資訊。

受保護的資源和用戶端應用程式

OAuth 2.0 是一個授權架構、用於控制受保護資源的存取。有鑑於此、任何部署的重要第一步、就是判斷可用資源為何、以及哪些用戶端需要存取這些資源。

識別用戶端應用程式

您需要決定在發出 REST API 呼叫時、哪些用戶端會使用 OAuth 2.0 、以及哪些 API 端點需要存取。

檢閱現有的 **ONTAP REST** 角色和本機使用者

您應該檢閱現有的 ONTAP 身分識別定義、包括其餘角色和本機使用者。視您設定 OAuth 2.0 的方式而定、這些定義可用於做出存取決策。

全域移轉至 **OAuth 2.0**

雖然您可以逐步實作 OAuth 2.0 授權、但也可以為每個授權伺服器設定全域旗標、立即將所有其餘 API 用戶端移至 OAuth 2.0 。如此一來、就能根據現有的 ONTAP 組態來做出存取決策、而無需建立獨立的範圍。

授權伺服器

授權伺服器在 OAuth 2.0 部署中扮演重要角色、方法是核發存取權杖並強制執行管理原則。

選取並安裝授權伺服器

您需要選取並安裝一或多個授權伺服器。請務必熟悉身分識別供應商的組態選項和程序、包括如何定義範圍。請注意，某些授權伺服器（包括 Microsoft Entra ID ）代表使用 UUID 而非名稱的群組。

判斷是否需要安裝授權根 **CA** 憑證

ONTAP 使用授權伺服器的憑證來驗證用戶端所提供的已簽署存取權杖。為達此目的、 ONTAP 需要根 CA 憑證和任何中繼憑證。這些可能已預先安裝在 ONTAP 中。如果沒有、您需要安裝它們。

評估網路位置和組態

如果授權伺服器位於防火牆之後、則需要將 ONTAP 設定為使用 Proxy 伺服器。

用戶端驗證與授權

您需要考量用戶端驗證和授權的幾個層面。

獨立範圍或本機 **ONTAP** 身分識別定義

在高層級、您可以定義在授權伺服器上定義的自我包含範圍、或是仰賴現有的本機 ONTAP 身分識別定義、包括角色和使用者。

具有本機 **ONTAP** 處理功能的選項

如果您使用 ONTAP 身分識別定義、則必須決定要套用的項目、包括：

- 具名 REST 角色
- 符合本機使用者
- Active Directory 或 LDAP 群組

本機驗證或遠端自我反省

您需要決定存取權杖是由 ONTAP 在本機驗證、還是透過自我反省在授權伺服器驗證。也有幾個相關的值需要考量、例如重新整理時間間隔。

寄件者限制的存取權杖

對於需要高安全性的環境、您可以使用以 MTLS 為基礎的傳送限制存取權杖。這需要每個用戶端的憑證。

群組為 **UUID** 和身分識別對應

如果您使用的授權伺服器代表使用 UUID 的群組，則需要規劃如何將這些群組對應至群組名稱，並可能對應至相關角色。

管理介面

您可以透過任何 ONTAP 介面執行 OAuth 2.0 管理、包括：

- 命令列介面
- 系統管理員
- REST API

用戶端如何要求存取權杖

用戶端應用程式必須直接從授權伺服器要求存取權杖。您需要決定如何執行、包括授與類型。

設定**ONTAP** 功能

您需要執行幾項 ONTAP 組態工作。

定義 **REST** 角色和本機使用者

根據您的授權組態、可使用本機 ONTAP 識別處理。在這種情況下、您需要檢閱並定義其餘角色和使用者定義。此外，視您的授權伺服器而定，這也可能包括根據 UUID 值管理群組。

核心組態

執行核心 ONTAP 組態需要三個主要步驟、包括：

- 您也可以為簽署授權伺服器憑證的 CA 安裝根憑證（及任何中繼憑證）。

- 定義授權伺服器。
- 啟用叢集的 OAuth 2.0 處理。

在 **ONTAP** 中部署 **OAuth 2.0**

部署核心 OAuth 2.0 功能需要三個主要步驟。

開始之前

您必須準備 OAuth 2.0 部署、才能設定 ONTAP 。例如、您需要評估授權伺服器、包括其憑證的簽署方式、以及它是否位於防火牆的後方。請參閱 "準備使用 ONTAP 部署 OAuth 2.0" 以取得更多資訊。

步驟 **1** ：安裝授權伺服器根 **CA** 憑證

ONTAP 包含大量預先安裝的根 CA 憑證。因此、在許多情況下、 ONTAP 會立即辨識您的授權伺服器憑證、而無需額外設定。但視授權伺服器憑證的簽署方式而定、您可能需要安裝根 CA 憑證和任何中繼憑證。

如有需要、請依照下列指示安裝憑證。您應該在叢集層級安裝所有必要的憑證。

根據您存取 ONTAP 的方式、選擇正確的程序。

範例 **1.** 步驟

系統管理員

1. 在 System Manager 中，選擇 **Cluster** >* Settings* 。
2. 向下捲動至 * 安全性 * 區段。
3. 單擊 * 證書 * 旁邊的 → 。
4. 在 * 信任的憑證授權單位 * 索引標籤下、按一下 * 新增 * 。
5. 按一下 * 匯入 * 並選取憑證檔案。
6. 完成環境的組態參數。
7. 按一下「 * 新增 * 」 。

CLI

1. 開始安裝：

   ```
   security certificate install -type server-ca
   ```

2. 查看下列主控台訊息：

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. 使用文字編輯器開啟憑證檔案。
4. 複製整個憑證、包括下列幾行：

   ```
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

5. 在命令提示字元之後、將憑證貼到終端機。
6. 按 **Enter** 鍵完成安裝。
7. 使用下列其中一項來確認已安裝憑證：

   ```
   security certificate show-user-installed
   ```

   ```
   security certificate show
   ```

步驟 **2** ：設定授權伺服器

您需要定義至少一個 ONTAP 授權伺服器。您應該根據組態和部署計畫來選擇參數值。檢閱 "OAuth2 部署案例" 以判斷您的組態所需的確切參數。

若要修改授權伺服器定義、您可以刪除現有定義並建立新定義。

以下提供的範例是根據第一個簡單部署案例、網址為： "本機驗證"。不使用 Proxy 就能使用獨立的範圍。

根據您存取 ONTAP 的方式、選擇正確的程序。CLI 程序會使用您在發出命令之前需要置換的符號變數。

範例 **2.** 步驟

系統管理員

1. 在 System Manager 中，選擇 **Cluster** >* Settings* 。
2. 向下捲動至 * 安全性 * 區段。
3. 按一下 * oAuth 2.0 授權 * 旁的 * + * 。
4. 選擇 * 更多選項 * 。
5. 提供部署所需的值、例如：
   - 名稱
   - 應用程式（ http ）
   - 提供者 JWKS URI
   - 發卡行 URI
6. 按一下「 * 新增 * 」。

CLI

1. 再次建立定義：

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

例如：

```
security oauth2 client create \
-config-name auth0 \
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
realm/protocol/openid-connect/certs \
-application http \
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

如"指令參考資料ONTAP"需詳細 `security oauth2 client create`資訊，請參閱。

步驟 **3** ：啟用 **OAuth 2.0**

最後一步是啟用 OAuth 2.0 。這是 ONTAP 叢集的全域設定。

在您確認 ONTAP 、授權伺服器及任何支援服務均已正確設定之前、請勿啟用 OAuth 2.0 處理。

根據您存取 ONTAP 的方式、選擇正確的程序。

範例 **3.** 步驟

系統管理員

1. 在 System Manager 中，選擇 **Cluster** >* Settings* 。
2. 向下捲動至 * 安全性區段 * 。
3. 按一下 **OAuth 2.0** 授權 * 旁邊的 *→ 。
4. 啟用 * oAuth 2.0 授權 * 。

CLI

1. 啟用 OAuth 2.0 ：

```
security oauth2 modify -enabled true
```

2. 確認 OAuth 2.0 已啟用：

```
security oauth2 show
Is OAuth 2.0 Enabled: true
```

相關資訊

- "安全性憑證安裝"
- "安全證書展示"
- "安全oauth2修改"
- "安全 oauth2 顯示"

使用 **OAuth 2.0** 發出**ONTAP REST API** 呼叫

ONTAP 中的 OAuth 2.0 實作支援 REST API 用戶端應用程式。您可以使用 Curl 發出簡單的 REST API 呼叫、開始使用 OAuth 2.0 。以下範例擷取 ONTAP 叢集版本。

開始之前

您必須為 ONTAP 叢集設定並啟用 OAuth 2.0 功能。這包括定義授權伺服器。

步驟 **1** ：取得存取權杖

您必須取得存取權杖、才能與 REST API 呼叫搭配使用。權杖要求是在 ONTAP 之外執行、具體程序取決於授權伺服器及其組態。您可以透過網頁瀏覽器、使用 cURL 命令或使用程式設計語言來要求權杖。

以下是使用捲曲向 Keycloak 申請存取權杖的範例。

Keycloak 範例

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

您應該複製並儲存傳回的權杖。

步驟 **2** ：發出 **REST API** 呼叫

擁有有效的存取權杖之後、您可以使用具有存取權杖的 cURL 命令來發出 REST API 呼叫。

參數與變數

下表說明了捲髮範例中的兩個變數。

變動	說明
$FQDN_IP	ONTAP 管理 LIF 的完整網域名稱或 IP 位址。
$access_token	由授權伺服器發出的 OAuth 2.0 存取權杖。

您應該先在 Bash Shell 環境中設定這些變數、然後再發佈 Curl 範例。例如、在 Linux CLI 中、輸入下列命令以設定及顯示 FQDN 變數：

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

在本機 Bash Shell 中定義兩個變數之後、您可以複製 curl 命令並將其貼到 CLI 中。按 **Enter** 以替換變數並發出命令。

Curl範例

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

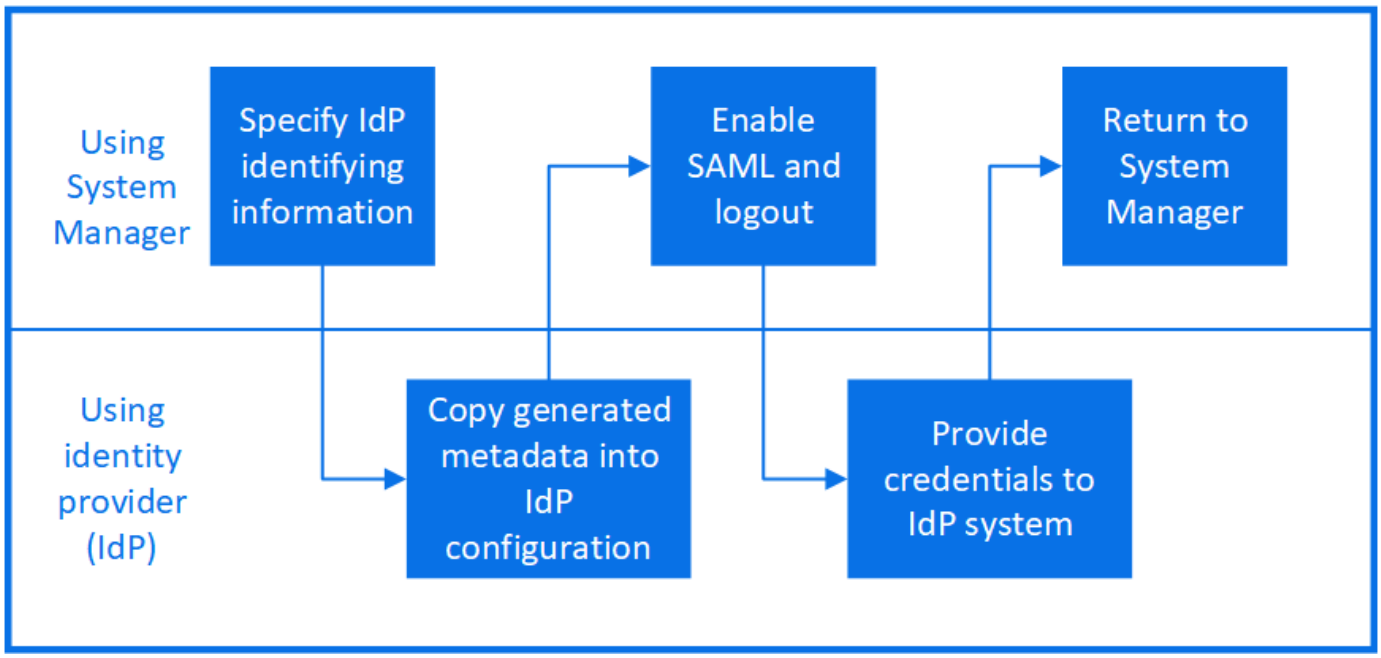
為遠端ONTAP用戶設定 SAML 身份驗證

從ONTAP 9.3 開始，您可以為 Web 服務設定安全性斷言標記語言 (SAML) 驗證。設定並啟用 SAML 驗證後，使用者將透過外部身分提供者 (IdP) 進行身份驗證，而不是透過 Active Directory 和 LDAP 等目錄服務提供者進行驗證。停用 SAML 驗證後，將使用已設定的目錄服務提供者（例如 Active Directory 和 LDAP）進行驗證。

啟用SAML驗證

若要使用 System Manager 或 CLI 啟用 SAML 驗證、請執行下列步驟。如果您的叢集執行的是 ONTAP 9.7 或更早版本、則您需要遵循的系統管理員步驟會有所不同。請參閱系統上的 System Manager 線上說明。

啟用 SAML 身份驗證後，只有已配置了 SAML 身份驗證的遠端使用者才能存取系統管理員 GUI。啟用 SAML 身份驗證後，本機使用者將無法存取系統管理員 GUI。



關於這項工作

- SAML 驗證僅適用於ONTAP `http`和 `ontapi`應用程式.

  這 `http`和 `ontapi`應用程式由下列 Web 服務使用：服務處理器基礎架構、 ONTAP API 和系統管理員。

- SAML驗證僅適用於存取管理SVM。
- 從ONTAP 9.17.1 開始，IdP 提供的群組資訊可以對應到ONTAP角色。這樣，您就可以根據 IdP 中定義的群組為使用者指派角色。有關更多信息，請參閱"在ONTAP中使用 OAuth 2.0 或 SAML IdP 群組" 。

下列 IDP 已通過 System Manager 驗證：

- Microsoft Entra ID（已通過ONTAP 9.17.1 及更高版本驗證）
- Active Directory Federation Services
- Cisco Duo（已通過以下ONTAP版本驗證：）

- 9.7P21 及更新版本 9.7 版本（請參閱 "System Manager Classic 文件"）
- 9.8P17 及更高版本的 9.8 補丁版本
- 9.9.1P13 及更高版本的 9.9.1 補丁版本
- 9.10.1P9 及更高版本的 9.10.1 補丁版本
- 9.11.1P4 及更高版本的 9.11.1 補丁版本
- 9.12.1 及更新版本

- Shibboleth

開始之前

- 您計劃用於遠端驗證的 IdP 必須是 配置.您必須擁有 IdP 的 URI。 IdPURI 是ONTAP向其發送身份驗證請求並接收回應的 Web 位址
- ONTAP叢集和 IdP 之間必須開啟連接埠 443。
- ONTAP叢集和 IdP 必須能夠 ping 通對方的完全限定域名。確保 DNS 配置正確，且叢集憑證未過期。
- 如果需要，請將 IdP 的受信任憑證授權單位 (CA) 新增至ONTAP。您可以"使用系統管理員管理ONTAP證書"。您可能需要在 IdP 中設定ONTAP叢集憑證。
- 您必須能夠存取ONTAP叢集的"服務處理器（SP）"控制台。如果 SAML 設定錯誤，則需要從SP控制台將其停用。
- 如果您使用的是 Entra ID（從ONTAP 9.17.1 開始已驗證），則必須在建立ONTAP SAML 設定之前使用ONTAP元資料配置 Entra ID。 EntraID 只有在配置了ONTAP元資料後才會提供 IdP URI。建立ONTAP SAML 配置需要 IdP URI。

  - 如果您使用 System Manager 設定 SAML，請將 IdP URI 欄位留空，直到 System Manager 提供ONTAP元資料。使用ONTAP元資料配置 Entra ID，然後將 IdP URI 複製到 System Manager 中，然後再啟用 SAML 設定。
  - 如果您使用ONTAP CLI 設定 SAML，則必須先生成ONTAP元數據，然後才能啟用ONTAP SAML 設定。您可以使用以下命令產生ONTAP元資料檔：

    ```
    security saml-sp default-metadata create -sp-host <ontap_host_name>
    ```

    `ontap_host_name`是 SAML 服務提供者主機（在本例中為ONTAP系統）的主機名稱或 IP 位址。預設情況下，使用叢集管理 IP 位址。您可以選擇提供ONTAP伺服器憑證資訊。預設情況下，使用ONTAP Web 伺服器憑證資訊。

  使用提供的元資料配置 Entra ID。您必須在建立ONTAP SAML 設定之前設定 Entra ID。配置 Entra 後，繼續執行下列 CLI 程序。

  - 在叢集中的所有節點都達到版本 9.17.1 之前，您無法產生 Entra ID 的ONTAP元資料。

步驟

視您的環境而定、請執行下列步驟：

系統管理員

1. 按一下*叢集>設定*。
2. 在 * SAML 驗證 * 旁邊、按一下 ⚙ 。
3. 請確認「啟用**SAML**驗證」核取方塊已勾選。
4. 輸入 IdP URI 的 URL（包括"https://" ）。如果您使用Entra ID，請跳過此步驟。
5. 如果需要，請修改主機系統位址。這是 IdP 在身份驗證後將定向到的地址。預設值為群集管理 IP 位址。
6. 確保使用正確的憑證：
   - 如果您的系統只對應一個類型為「server」的憑證、則該憑證會被視為預設憑證、不會顯示出來。
   - 如果您的系統已對應多個憑證做為「server」類型、則會顯示其中一個憑證。 若要選取不同的憑證、請按一下*變更*。
7. 按一下「 * 儲存 * 」。確認視窗會顯示已自動複製到剪貼簿的中繼資料資訊。
8. 前往您指定的 IdP 系統，並從剪貼簿複製元資料以更新系統元資料。如果您使用的是 Entra ID，請在使用系統元資料配置 Entra ID 後，將 IdP URI 複製到ONTAP中。
9. 返回確認視窗（在System Manager中）、然後勾選「I have configured the IDP with the host URI or medetid*（我已使用主機URI或中繼資料*設定IDP）」核取方塊。
10. 按一下*登出*以啟用SAML型驗證。 IDP系統會顯示驗證畫面。
11. 在 IdP 登入頁面，輸入您的基於 SAML 的憑證。憑證驗證完成後，您將被導向到系統管理器主頁。

CLI

1. 建立SAML組態、ONTAP 以便讓整個程序能夠存取IDP中繼資料：

   ```
   security saml-sp create -idp-uri <idp_uri> -sp-host <ontap_host_name>
   ```

   `idp_uri` 是 IDP 主機的 FTP 或 HTTP 位址、可從其中下載 IDP 中繼資料。

   > ⓘ 某些 URL 包含問號 (?)。問號用於啟動ONTAP命令列活動幫助。要輸入帶有問號的URL，您需要先使用以下命令停用活動協助 `set -active-help false` 。稍後可以使用以下命令重新啟用主動協助 `set -active-help true`了解更多信息"指令參考資料ONTAP" 。

   `ontap_host_name` 是 SAML 服務供應商主機的主機名稱或 IP 位址、在此情況下為 ONTAP 系統。根據預設、會使用叢集管理LIF的IP位址。

   您可以選擇性地提供ONTAP 伺服器的驗證資訊。根據預設ONTAP 、會使用「驗證」Web伺服器憑證資訊。

```
cluster_12::> security saml-sp create -idp-uri
https://example.url.net/idp/shibboleth

Warning: This restarts the web server. Any HTTP/S connections that
are active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and ONTAP users for the same directory server
domain to ensure that users are the same for different
authentication methods. See the "security login show" command for
the ONTAP user configuration.
```

畫面ONTAP 會顯示存取主機中繼資料的URL。

2. 從 IdP 主機， 配置 IdP使用ONTAP主機元資料。如果您使用的是 Entra ID，則已完成此步驟。
3. 配置 IdP 後，啟用 SAML 設定：

   ```
   security saml-sp modify -is-enabled true
   ```

   存取的任何現有使用者 `http` 或 `ontapi` 應用程式會自動設定以進行 SAML 驗證。

4. 如果你想為 `http`或者 `ontapi`設定 `SAML` 後，請將 `SAML` 指定為新使用者的驗證方法。在`ONTAP 9.17.1` 之前的版本中，系統會自動為現有使用者建立 `SAML` 登入名 `http`或者 `ontapi`啟用 `SAML` 時，使用者必須設定新使用者。從`ONTAP 9.17.1` 開始，所有使用 `password ， domain ， 或者 `nsswitch`當啟用 SAML 時，身份驗證方法會自動針對 IdP 進行身份驗證。

   a. 為新使用者建立使用 SAML 驗證的登入方法。 `user_name`必須與 IdP 中配置的使用者名稱相符：

      該 `user_name`值區分大小寫。除非您使用 Entra ID ，否則請僅包含使用者名稱，不要包含網域的任何部分。如果您使用 Entra ID ，則可以建立包含網域的使用者名稱，例如 *user_name@domain.com* 。

      ```
      security login create -user-or-group-name <user_name> -application [http
      | ontapi] -authentication-method saml -vserver <svm_name>
      ```

      範例：

      ```
      cluster_12::> security login create -user-or-group-name admin1
      -application http -authentication-method saml -vserver cluster_12
      ```

   b. 確認已建立使用者項目：

```
security login show
```

範例：

```
cluster_12::> security login show

Vserver: cluster_12

Second
User/Group                  Authentication                 Acct
Authentication
Name            Application Method        Role Name        Locked
Method
--------------- ----------- ------------- ---------------- ------
--------------
admin           console     password      admin            no
none
admin           http        password      admin            no
none
admin           http        saml          admin            -
none
admin           ontapi      password      admin            no
none
admin           ontapi      saml          admin            -
none
admin           service-processor
                            password      admin            no
none
admin           ssh         password      admin            no
none
admin1          http        password      backup           no
none
admin1          http        saml          backup           -
none
```

+
如"指令參考資料ONTAP"需詳細 `security login show`資訊，請參閱。

停用SAML驗證

當您想要停止使用外部身分提供者 (IdP) 對遠端系統管理員使用者進行驗證時，可以停用 SAML 驗證。停用 SAML 驗證後，系統將使用本機使用者驗證或已設定的目錄服務提供者（例如 Active Directory 和 LDAP）對使用者進行驗證。

視您的環境而定、請執行下列步驟：

範例 **4.** 步驟

系統管理員

1. 按一下*叢集>設定*。
2. 在「* SAML驗證*」下、按一下「已啟用」切換按鈕。
3. *Optional* ：您也可以按一下 * SAML 驗證 * 旁的、然後取消勾選 * 啟用 SAML 驗證 * 核取方塊。

CLI

1. 停用SAML驗證：

```
security saml-sp modify -is-enabled false
```

2. 如果您不想再使用SAML驗證、或想要修改IDP、請刪除SAML組態：

```
security saml-sp delete
```

配置第三方 IdP

關於這項工作

為了使用ONTAP進行身份驗證，您可能需要變更 IdP 的設定。以下部分提供了受支援的 IdP 的配置資訊。

entra ID

配置 Entra ID 時，建立一個新的應用程序，並使用ONTAP提供的元資料配置 SAML 登入。建立應用程式後，編輯應用程式 SAML 設定的「屬性和聲明」部分，以符合以下內容：

設定	價值
名稱	urn：oid：0.9.2342.19200300.100.1.1
命名空間	留空
名稱格式	URI
來源	屬性
來源屬性	使用者.使用者主體名稱

如果您想使用具有 Entra ID 的群組，請使用下列設定新增群組聲明：

設定	價值
名稱	urn：oid：1.3.6.1.4.1.5923.1.5.1.1
命名空間	留空
來源屬性	群組ID

Entra ID 以 UUID 格式提供群組資訊。有關使用 Entra ID 群組的更多信息，請參閱"使用 UUID 管理群組"。

應用程式 SAML 設定的「SAML 憑證」部分中提供的「應用程式聯合元資料 URL」是您將在ONTAP中輸入的 IdP URI。

有關配置 Entra ID 多因素身份驗證的信息，請參閱"規劃 Microsoft Entra 多重驗證部署"。

欲了解更多信息，請參閱"Entra ID 文件"。

Active Directory Federation Services

設定 Active Directory 聯合驗證服務 (AD FS) 時，必須使用ONTAP提供的服務提供者元資料新增的可感知聲明的依賴方信任。建立依賴方信任後，使用「將 LDAP 屬性作為聲明傳送」範本將下列聲明規則新增至依賴方信任的聲明頒發策略：

屬性儲存	**LDAP** 屬性	傳出索賠類型
Active Directory	SAM 帳戶名稱	姓名 ID
Active Directory	SAM 帳戶名稱	urn：oid：0.9.2342.19200300.100.1.1
Active Directory	名稱格式	urn:oasis:names:tc:SAML:2.0:attrname-format:uri
Active Directory	令牌組 - 按網域限定	urn：oid：1.3.6.1.4.1.5923.1.5.1.1
Active Directory	sAM帳戶名稱	urn:oid:1.2.840.113556.1.4.221

AD FS 以名稱格式提供群組資訊。有關在 AD FS 中使用群組的更多信息，請參閱"使用名稱管理群組"。

欲了解更多信息，請參閱"AD FS 文檔" 。

Cisco DuoTM

請參閱"Cisco Duo 文件"取得配置資訊。

Shibboleth

在設定 Shibboleth IdP 之前，您必須已經設定了 LDAP 伺服器。

在ONTAP上啟用 SAML 時，請儲存提供的主機元資料 XML。在安裝了 Shibboleth 的主機上，將以下內容替換為 `metadata/sp-metadata.xml`使用 Shibboleth IdP 主目錄中的主機元資料 XML。

有關詳細信息，請參閱"Shibboleth" 。

疑難排解SAML組態問題

如果設定安全性聲明標記語言（SAML）驗證失敗、您可以手動修復SAML組態失敗的每個節點、並從故障中恢復。在修復程序期間、會重新啟動Web伺服器、並中斷任何作用中的HTTP連線或HTTPS連線。

關於這項工作

設定SAML驗證時ONTAP 、將會以每個節點為基礎來套用SAML組態。啟用SAML驗證時ONTAP 、如果發生組態問題、則會自動嘗試修復每個節點。如果任何節點上的SAML組態發生問題、您可以停用SAML驗證、然後重新啟用SAML驗證。在重新啟用SAML驗證後、SAML組態仍無法套用至一或多個節點的情況下、可能會發生。您可以識別SAML組態失敗的節點、然後手動修復該節點。

步驟

1. 登入進階權限層級：

   ```
   set -privilege advanced
   ```

2. 識別SAML組態失敗的節點：

   ```
   security saml-sp status show -instance
   ```

   範例：

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                 Update Status: config-success
                Database Epoch: 9
    Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
         ID of SAML Config Job: 179

                          Node: node2
                 Update Status: config-failed
                Database Epoch: 9
    Database Transaction Count: 997
                    Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
         ID of SAML Config Job: 180
2 entries were displayed.
```

如"指令參考資料ONTAP"需詳細 `security saml-sp status show`資訊，請參閱。

3. 修復故障節點上的SAML組態：

   `security saml-sp repair -node <node_name>`

   範例：

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
          will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

   Web伺服器會重新啟動、且任何作用中的HTTP連線或HTTPS連線都會中斷。

   如"指令參考資料ONTAP"需詳細 `security saml-sp repair`資訊，請參閱。

4. 確認已在所有節點上成功設定SAML：

   `security saml-sp status show -instance`

   範例：

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

如"指令參考資料ONTAP"需詳細 `security saml-sp status show`資訊，請參閱。

相關資訊

- "指令參考資料ONTAP"
- "安全性 SAML SP"
- "建立安全登入"

在ONTAP中使用 OAuth 2.0 或 SAML IdP 群組

ONTAP提供了多種基於 OAuth 2.0 授權伺服器或 SAML 身分提供者 (IdP) 設定群組的選項。然後，可以將這些群組對應到ONTAP用於確定存取權限的角色。

從ONTAP 9.17.1 開始，SAML IdP 提供的群組資訊可以對應到ONTAP角色。這樣，您就可以根據 IdP 中定義的群組為使用者指派角色。如需詳細資訊，請參閱"設定SAML驗證"。從ONTAP 9.14.1 開始， ONTAP支援 OAuth 2.0 的群組名稱驗證。從ONTAP 9.16.1 開始， ONTAP支援 OAuth 2.0 群組 UUID 驗證和角色對應。"ONTAP OAuth 2.0 實作總覽" 。

如何識別群組

在授權伺服器或 SAML IdP 上設定群組時，系統會使用名稱或 UUID 在 OAuth 2.0 存取權杖或 SAML 斷言中識別並攜帶該群組。在設定ONTAP之前，您需要了解授權伺服器或 SAML IdP 如何處理群組。

如果存取權杖中包含多個群組， ONTAP 會嘗試使用每個群組，直到有相符項目為止。

群組名稱

許多授權伺服器和 SAML IdP（例如 Active Directory Federation Service (ADFS)）都使用名稱來識別和表示群組。以下是 ADFS 產生的包含多個群組的 JSON OAuth 2.0 存取權杖片段。請參閱[使用名稱管理群組]了解更多。

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

群組 **UUID**

一些授權伺服器和 SAML IdP（例如 Microsoft Entra ID）使用 UUID 來識別和表示群組。以下是 Entra ID 產生的包含多個群組的 OAuth 2.0 存取權杖片段。請參閱使用 UUID 管理群組了解更多。

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

使用名稱管理群組

如果您的授權伺服器或 SAML IdP 使用名稱來識別群組，則需要確保已為ONTAP叢集定義了每個群組。根據您的安全環境，您可能已經定義了相應的群組。

以下是定義ONTAP組的 CLI 指令範例。請注意，它使用範例存取令牌中的命名組。您需要具有ONTAP 管理員權限等級才能發出該指令。

範例

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

使用 `-authentication-method` `domain`或者 `nsswitch`用於 SAML IdP 和 OAuth 2.0 授權伺服器群組。

您也可以使用ONTAP REST API 來設定此功能。了解更多信息，請參閱 "ONTAP 自動化文件" 。

使用 UUID 管理群組

如果您的授權伺服器或 SAML IdP 使用 UUID 值來表示群組，則在使用群組之前需要執行兩步驟設定。從ONTAP 9.16.1 開始，提供了兩種映射功能，並且已使用 Entra ID 進行測試。從ONTAP 9.16.1 開始支援 OAuth 2.0 的 Entra ID，從ONTAP 9.17.1 開始支援 SAML 的 Entra ID。您需要具有ONTAP 管理員 權限等級才能發出 CLI 命令。

您也可以使用 ONTAP REST API 來設定這些功能。如需詳細資訊，請參閱 "ONTAP 自動化文件"。

將群組 UUID 對應至群組名稱

如果您使用的授權伺服器或 SAML IdP 使用 UUID 值來表示群組，則需要將群組 UUID 對應到群組名稱。主要的ONTAP CLI 操作如下所述。

建立

您可以使用以下方式定義新的群組映射配置 `security login group create`命令。群組 UUID 和名稱應與授權伺服器或 SAML IdP 上的設定相符。詳細了解 `security login group create`在"指令參考資料ONTAP" 。

參數

用於建立群組對應的參數如下所述。

參數	說明
`vserver`	選擇性地指定群組所關聯的 SVM （ Vserver ）名稱。如果省略，群組就會與 ONTAP 叢集相關聯。
`name`	ONTAP 將使用的群組唯一名稱。
`type`	此值表示群組來源的身分識別提供者。
`uuid`	指定授權伺服器或 SAML IdP 提供的群組的通用唯一識別碼。

以下是為ONTAP定義群組的範例 CLI 指令。請注意，它使用範例存取令牌中的 UUID 群組。

範例

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

建立群組之後，會為群組產生唯一的唯讀整數識別碼。

其他 CLI 作業

此命令支援多項額外作業，包括：

- 顯示

- 修改
- 刪除

您可以使用 `show`選項來擷取為群組所產生的唯一群組 ID 。如"指令參考資料ONTAP"需詳細 `show`資訊，請參閱。

將群組 **UUID** 對應至角色

如果您使用的授權伺服器或 SAML IdP 使用 UUID 值來表示群組，則可以將群組對應到角色。如需 ONTAP 中基於角色的存取控制的詳細資訊，請參閱 "瞭解如何管理 ONTAP 存取控制角色"。主要的ONTAP CLI 操作如下所述。需要具有ONTAP **admin** 權限等級才能發出這些命令。

> 你需要先將群組 UUID 對應到群組名並檢索為該組產生的唯一整數 ID。您需要該 ID 來將群組對應到角色。

建立

您可以使用 `security login group role-mapping create`命令。詳細了解 `security login group role-mapping create`在"指令參考資料ONTAP" 。

參數

用於將群組對應至角色的參數如下所述。

參數	說明
`group-id`	指定使用命令為群組產生的唯一 ID `security login group create` 。
`role`	群組對應的 ONTAP 角色名稱。

範例

```
security login group role-mapping create -group-id 1 -role admin
```

其他 **CLI** 作業

此命令支援多項額外作業，包括：

- 顯示
- 修改
- 刪除

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

相關資訊

- "外部角色對應"

使用 **WebAuthn MFA** 進行驗證與授權

了解 **ONTAP System Manager** 使用者的 **WebAuthn** 多因素驗證

從 ONTAP 9 。 16.1 開始，系統管理員可以為登入系統管理員的使用者啟用 WebAuthn 多因素驗證（ MFA ）。這可讓系統管理員以 FIDO2 金鑰（例如 YibiKey ）作為第二種驗證形式登入。根據預設，新的和現有的 ONTAP 使用者會停用 WebAuthn MFA 。

第一種驗證方法使用下列驗證類型的使用者和群組可支援 WebAuthn MFA ：

- 使用者：密碼，網域或 nsswitch
- 群組：網域或 nsswitch

當您將 WebAuthn MFA 啟用為使用者的第二種驗證方法之後，系統會要求使用者在登入 System Manager 時登錄硬體驗證者。註冊後，私密金鑰會儲存在驗證者中，而公開金鑰則儲存在 ONTAP 中。

ONTAP 支援每位使用者一個 WebAuthn 認證。如果使用者遺失驗證者，需要更換驗證者，則 ONTAP 管理員需要刪除使用者的 WebAuthn 認證，以便使用者在下次登入時註冊新的驗證者。

> 啟用 WebAuthn MFA 做為第二種驗證方法的使用者"https://192.168.100.200"，必須使用 FQDN （例如"https://myontap.example.com"）而非 IP 位址（例如）來存取 System Manager 。對於啟用 WebAuthn MFA 的使用者，會拒絕使用 IP 位址登入 System Manager 的嘗試。

為 **ONTAP** 系統管理員使用者或群組啟用 **WebAuthn MFA**

身為 ONTAP 管理員，您可以新增已啟用 WebAuthn MFA 選項的新使用者或群組，或是啟用現有使用者或群組的選項，為系統管理員使用者或群組啟用 WebAuthn MFA 。

> 將 WebAuthn MFA 啟用為使用者或群組的第二種驗證方法之後，下次登入 System Manager 時，系統會要求使用者（或該群組中的所有使用者）登錄硬體 FIDO2 裝置。此登錄由使用者的本機作業系統處理，通常包括插入安全金鑰，建立金鑰，以及輕觸安全金鑰（如果支援）。

建立新使用者或群組時，請啟用 **WebAuthn MFA**

您可以使用系統管理員或 ONTAP CLI ，建立啟用 WebAuthn MFA 的新使用者或群組。

系統管理員

1. 選擇*叢集>設定*。
2. 選取 * 使用者和角色 * 旁邊的箭頭圖示。
3. 在 * 使用者 * 下選取 * 新增 * 。
4. 指定使用者或群組名稱，然後在 * 角色 * 的下拉式功能表中選取角色。
5. 指定使用者或群組的登入方法和密碼。

   WebAuthn MFA 支援使用者的「密碼」，「網域」或「 nsswitch 」登入方法，以及群組的「網域」或「 nsswitch 」登入方法。

6. 在 **MFA for HTTP** 欄中，選取 * Enabled* 。
7. 選擇*保存*。

CLI

1. 啟用 WebAuthn MFA ，建立新的使用者或群組。

   在下列範例中，選擇第二種驗證方法的「 publickey 」即可啟用 WebAuthn MFA ：

   ```
   security login create -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

   如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

為現有的使用者或群組啟用 **WebAuthn MFA**

您可以為現有的使用者或群組啟用 WebAuthn MFA 。

系統管理員

1. 選擇*叢集>設定*。
2. 選取 * 使用者和角色 * 旁邊的箭頭圖示。
3. 在使用者和群組清單中，選取您要編輯之使用者或群組的選項功能表。

   WebAuthn MFA 支援使用者的「密碼」，「網域」或「 nsswitch 」登入方法，以及群組的「網域」或「 nsswitch 」登入方法。

4. 在該使用者的 * MFA for HTTP* 欄中，選取 * Enabled* 。
5. 選擇*保存*。

CLI

1. 修改現有的使用者或群組，為該使用者或群組啟用 WebAuthn MFA 。

   在下列範例中，選擇第二種驗證方法的「 publickey 」即可啟用 WebAuthn MFA ：

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

   如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

停用 **ONTAP System Manager** 使用者的 **WebAuthn MFA**

身為 ONTAP 管理員，您可以使用系統管理員或 ONTAP CLI 編輯使用者或群組，為使用者或群組停用 WebAuthn MFA 。

停用現有使用者或群組的 **WebAuthn MFA**

您可以隨時停用現有使用者或群組的 WebAuthn MFA 。

> 如果停用已登錄的認證，則會保留認證。如果您在未來再次啟用認證，則會使用相同的認證，因此使用者在登入時不需要重新登錄。

系統管理員

1. 選擇*叢集>設定*。
2. 選取 * 使用者和角色 * 旁邊的箭頭圖示。
3. 在使用者和群組清單中，選取您要編輯的使用者或群組。
4. 在該使用者的 * MFA for HTTP* 欄中，選取 * 停用 * 。
5. 選擇*保存*。

CLI

1. 修改現有的使用者或群組，以停用該使用者或群組的 WebAuthn MFA 。

   在下列範例中，選擇「無」作為第二種驗證方法，即可停用 WebAuthn MFA 。

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method none \
                         -application http \
                         -role admin
   ```

   如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

檢視 **ONTAP WebAuthn MFA** 設定並管理認證

身為 ONTAP 管理員，您可以檢視整個叢集的 WebAuthn MFA 設定，並管理 WebAuthn MFA 的使用者和群組認證。

檢視 **WebAuthn MFA** 的叢集設定

您可以使用 ONTAP CLI 檢視 WebAuthn MFA 的叢集設定。

步驟

1. 檢視 WebAuthn MFA 的叢集設定。您可以選擇使用下列引數指定儲存 VM `vserver` ：

   ```
   security webauthn show -vserver <storage_vm_name>
   ```

   如"指令參考資料ONTAP"需詳細 `security webauthn show`資訊，請參閱。

檢視支援的公開金鑰 **WebAuthn MFA** 演算法

您可以檢視儲存 VM 或叢集所支援的 WebAuthn MFA 公開金鑰演算法。

步驟

1. 列出支援的公開金鑰 WebAuthn MFA 演算法。您可以選擇使用下列引數指定儲存 VM `vserver` ：

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

如"指令參考資料ONTAP"需詳細 `security webauthn supported-algorithms show`資訊，請參閱。

檢視已註冊的 **WebAuthn MFA** 認證

身為 ONTAP 管理員，您可以檢視所有使用者的註冊 WebAuthn 認證。使用此程序的非系統管理員使用者只能檢視自己已註冊的 WebAuthn 認證。

步驟

1. 檢視已註冊的 WebAuthn MFA 認證：

```
security webauthn credentials show
```

如"指令參考資料ONTAP"需詳細 `security webauthn credentials show`資訊，請參閱。

移除已註冊的 **WebAuthn MFA** 認證

您可以移除已註冊的 WebAuthn MFA 認證。當使用者的硬體金鑰遺失，遭竊或不再使用時，此功能非常實用。當使用者仍擁有原始硬體驗證者，但想要以新的驗證者來取代時，您也可以移除已登錄的認證。移除認證之後，系統會提示使用者註冊替換驗證者。

> ⓘ 移除使用者的登錄認證並不會停用使用者的 WebAuthn MFA 。如果使用者遺失硬體驗證者，需要先登入再進行更換，您需要使用這些步驟移除認證，也需要針對使用者移除認證"停用 WebAuthn MFA"。

系統管理員

1. 選擇*叢集>設定*。
2. 選取 * 使用者和角色 * 旁邊的箭頭圖示。
3. 在使用者和群組清單中，針對您要移除其認證的使用者或群組，選取選項功能表。
4. 選取 * 移除 MFA 以取得 HTTP 認證 * 。
5. 選擇*移除*。

CLI

1. 刪除已註冊的認證。請注意下列事項：
   - 您可以選擇性地指定使用者的儲存 VM 。如果省略，則會在叢集層級移除認證。
   - 您可以選擇性地指定要刪除認證的使用者名稱。如果省略，則會移除目前使用者的認證。

   ```
   security webauthn credentials delete -vserver <storage_vm_name>
   -username <username>
   ```

   如"指令參考資料ONTAP"需詳細 `security webauthn credentials delete`資訊，請參閱。

管理Web服務

管理網路服務總覽

您可以啟用或停用叢集或儲存虛擬機器（SVM）的Web服務、顯示Web服務的設定、以及控制角色使用者是否可以存取Web服務。

您可以使用下列方式來管理叢集或SVM的Web服務：

- 啟用或停用特定的Web服務
- 指定是否僅限加密的HTTP（SSL）存取Web服務
- 顯示Web服務的可用度
- 允許或禁止角色使用者存取Web服務
- 顯示允許存取Web服務的角色

若要讓使用者存取Web服務、必須符合下列所有條件：

- 使用者必須通過驗證。

  例如、Web服務可能會提示輸入使用者名稱和密碼。使用者的回應必須符合有效的帳戶。

- 使用者必須使用正確的存取方法來設定。

  驗證只會針對使用者成功、並針對指定的Web服務提供正確的存取方法。適用於 ONTAP API Web 服務

ontapi）、使用者必須擁有 ontapi 存取方法。對於所有其他 Web 服務、使用者必須擁有 http 存取方法。

> 您可以使用 security login 管理使用者存取方法和驗證方法的命令。

- Web服務必須設定為允許使用者的存取控制角色。

> 您可以使用 vserver services web access 控制角色存取 Web 服務的命令。

如果啟用防火牆、則必須設定用於Web服務的LIF防火牆原則、以允許HTTP或HTTPS。

如果您使用HTTPS進行Web服務存取、也必須啟用提供Web服務之叢集或SVM的SSL、而且必須提供叢集或SVM的數位憑證。

管理對ONTAP Web 服務的訪問

Web服務是使用者可以使用HTTP或HTTPS存取的應用程式。叢集管理員可以設定Web傳輸協定引擎、設定SSL、啟用Web服務、以及讓角色的使用者存取Web服務。

從支援下列Web服務的支援範圍ONTAP 起、從功能支援的9.6開始：

- 服務處理器基礎架構 (spi)

  此服務可透過叢集管理LIF或節點管理LIF、讓節點的記錄檔、核心傾印檔和MIBA檔案可供HTTP或HTTPS存取。預設設定為 enabled。

  當請求存取節點的日誌檔案或核心轉儲檔案時， spi Web 服務會自動建立一個從一個節點到另一個節點的根磁碟區（檔案所在的根磁碟區）的掛載點。您無需手動建立掛載點。

- ONTAP API (ontapi)

  這項服務可讓您執行ONTAP IsyAPI、以遠端程式執行管理功能。預設設定為 enabled。

  某些外部管理工具可能需要此服務。例如、如果您使用System Manager、則應保持啟用此服務。

- Data ONTAP 探索 (disco)

  此服務可讓隨裝即用的管理應用程式在網路中探索叢集。預設設定為 enabled。

- 支援診斷 (supdiag)

  此服務可控制系統上的權限環境存取、以協助進行問題分析和解決問題。預設設定為 disabled。您只能在技術支援人員的指示下啟用此服務。

- 系統管理員 (sysmgr)

  此服務可控制系統管理員的可用度、ONTAP 而此功能隨附於本服務。預設設定為 enabled。此服務僅在叢集上受支援。

- 韌體基礎板管理控制器（ BMC ）更新 (FW_BMC)

此服務可讓您下載BMC韌體檔案。預設設定為 `enabled`。

- 資訊文件ONTAP (`docs`)

  此服務可讓您存取ONTAP 有關的資料。預設設定為 `enabled`。

- ONTAP RESTful API (`docs_api`)

  此服務可讓您存取ONTAP 「REST風格的API」文件。預設設定為 `enabled`。

- 檔案上傳與下載 (`fud`)

  此服務提供檔案上傳與下載。預設設定為 `enabled`。

- ONTAP 訊息 (`ontapmsg`)

  此服務支援發佈及訂閱介面、可讓您訂閱活動。預設設定為 `enabled`。

- ONTAP 入口網站 (`portal`)

  此服務會將閘道實作至虛擬伺服器。預設設定為 `enabled`。

- ONTAP REST 風格的介面 (`rest`)

  此服務支援RESTful介面、可用於遠端管理叢集基礎架構的所有元素。預設設定為 `enabled`。

- 安全聲明標記語言（ SAML ）服務供應商支援 (`saml`)

  此服務提供資源來支援SAML服務供應商。預設設定為 `enabled`。

- SAML 服務供應商 (`saml-sp`)

  此服務可為服務供應商提供SP中繼資料和聲明使用者服務等服務。預設設定為 `enabled`。

從支援下列附加服務的支援範圍ONTAP 起、從支援使用者支援的範圍開始：

- 組態備份檔案 (`backups`)

  此服務可讓您下載組態備份檔案。預設設定為 `enabled`。

- ONTAP 安全性 (`security`)

  此服務支援CSRF權杖管理、以加強驗證。預設設定為 `enabled`。

在 **ONTAP** 中管理網路傳輸協定引擎

您可以在叢集上設定Web傳輸協定引擎、以控制是否允許Web存取、以及可以使用哪些SSL版本。您也可以顯示Web傳輸協定引擎的組態設定。

您可以透過下列方式、在叢集層級管理Web傳輸協定引擎：

- 您可以使用指定遠端用戶端是否可以使用 HTTP 或 HTTPS 來存取 Web 服務內容 `system services web modify` 命令 `-external` 參數。
- 您可以使用來指定是否應使用 SSLv3 來進行安全的 Web 存取 `security config modify` 命令 `-supported-protocol` 參數。
  根據預設、SSLv3會停用。傳輸層安全性1.0（TLSv1.0）已啟用、可視需要停用。

  如"指令參考資料ONTAP"需詳細 `security config modify`資訊，請參閱。

- 您可以針對整個叢集的控制面板Web服務介面、啟用聯邦資訊處理標準（FIPS）140-2法規遵循模式。

  預設會停用FIPS 140-2相容模式。

  - 當**FIPS 140-2**相容模式停用時
    您可以透過設定來啟用 FIPS 140-2 規範模式 `is-fips-enabled` 參數至 `true` 適用於 `security config modify` 命令、然後使用 `security config show` 確認線上狀態的命令。
  - 啟用**FIPS 140-2**規範模式時
    - 從 ONTAP 9.11.1 開始， TLSv1 ， TLSv1.1 和 SSLv3 都會停用，只有 TSLv1.2 和 TSLv1.3 會保持啟用狀態。它會影響ONTAP 到其他內部和外部的系統和通訊、而這些系統和通訊則是來自於19。如果您啟用FIPS 140-2規範模式、然後停用、則TLSv1、TLSv1.1及SSLv3會維持停用狀態。視先前的組態而定、TLSv1.2或TLSSv1.3仍會保持啟用狀態。
    - 對於9.11.1之前的ONTAP 版本、TLSv1和SSLv3都會停用、只有TLSv1.1和TLSv1.2會維持啟用狀態。啟用FIPS 140-2相容模式時、無法同時啟用TLSv1和SSLv3。ONTAP如果您啟用FIPS 140-2規範模式、然後停用該模式、則TLSv1和SSLv3仍會維持停用狀態、但根據先前的組態、TLSv1.2或同時啟用TLSv1.1和TLSv1.2。
- 您可以使用顯示叢集整體安全性的組態 `system security config show` 命令。

  如"指令參考資料ONTAP"需詳細 `security config show`資訊，請參閱。

如果啟用防火牆、則必須設定用於Web服務的邏輯介面（LIF）防火牆原則、以允許HTTP或HTTPS存取。

如果您使用HTTPS進行Web服務存取、則提供Web服務的叢集或儲存虛擬機器（SVM）的SSL也必須啟用、而且您必須提供叢集或SVM的數位憑證。

在「樣」組態中、您對叢集上的Web傳輸協定引擎所做的設定變更不會複寫到合作夥伴叢集上。MetroCluster

用於管理 **Web** 協定引擎的**ONTAP**指令

您可以使用 `system services web` 用於管理網路傳輸協定引擎的命令。您可以使用 `system services firewall policy create` 和 `network interface modify` 允許 Web 存取要求通過防火牆的命令。

如果您想要...	使用此命令...
在叢集層級設定Web傳輸協定引擎： • 啟用或停用叢集的Web傳輸協定引擎 • 啟用或停用叢集的SSLv3 • 啟用或停用安全網路服務（HTTPS）的FIPS 140-2法規遵循	`system services web modify`
在叢集層級顯示Web傳輸協定引擎的組態、判斷Web傳輸協定是否在整個叢集內正常運作、並顯示FIPS 140-2相容性是否已啟用且處於線上狀態	`system services web show`
顯示節點層級的Web傳輸協定引擎組態、以及叢集中節點的Web服務處理活動	`system services web node show`
建立防火牆原則、或將HTTP或HTTPS傳輸協定服務新增至現有的防火牆原則、以允許Web存取要求通過防火牆	`system services firewall policy create` 設定 `-service` 參數至 `http` 或 `https` 允許 Web 存取要求通過防火牆。
將防火牆原則與LIF建立關聯	`network interface modify` 您可以使用 `-firewall-policy` 修改 LIF 防火牆原則的參數。

相關資訊

- "修改網路介面"

配置對ONTAP Web 服務的存取

設定Web服務存取權可讓授權使用者使用HTTP或HTTPS存取叢集或儲存虛擬機器（SVM）上的服務內容。

步驟

1. 如果已啟用防火牆、請確定將用於Web服務的LIF防火牆原則中已設定HTTP或HTTPS存取：

   您可以使用檢查是否啟用防火牆 `system services firewall show` 命令。

   a. 若要確認已在防火牆原則中設定 HTTP 或 HTTPS 、請使用 `system services firewall policy show` 命令。

      您可以設定 `-service` 的參數 `system services firewall policy create` 命令至 `http` 或 `https` 啟用原則以支援網路存取。

   b. 若要驗證支援 HTTP 或 HTTPS 的防火牆原則是否與提供 Web 服務的 LIF 相關聯、請使用 `network interface show` 命令 `-firewall-policy` 參數。

如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

您可以使用 `network interface modify` 命令 `-firewall-policy` 將防火牆原則對 LIF 生效的參數。

如"指令參考資料ONTAP"需詳細 `network interface modify`資訊，請參閱。

2. 若要設定叢集層級的 Web 傳輸協定引擎、並讓 Web 服務內容可供存取、請使用 `system services web modify` 命令。
3. 如果您打算使用安全 Web 服務（ HTTPS ）、請啟用 SSL 、並使用為叢集或 SVM 提供數位憑證資訊 `security ssl modify` 命令。

   如"指令參考資料ONTAP"需詳細 `security ssl modify`資訊，請參閱。

4. 若要啟用叢集或 SVM 的 Web 服務、請使用 `vserver services web modify` 命令。

   您必須針對要為叢集或SVM啟用的每個服務重複此步驟。

5. 若要授權角色存取叢集或 SVM 上的 Web 服務、請使用 `vserver services web access create` 命令。

   您授予存取權的角色必須已經存在。您可以使用顯示現有角色 `security login role show` 使用命令或建立新角色 `security login role create` 命令。

   深入瞭解 `security login role show`及 `security login role create` "指令參考資料ONTAP"。

6. 對於已獲授權存取 Web 服務的角色、請檢查的輸出、以確保其使用者也使用正確的存取方法進行設定 `security login show` 命令。

   存取 ONTAP API Web 服務 `ontapi`）、使用者必須使用設定 `ontapi` 存取方法。若要存取所有其他 Web 服務、必須使用設定使用者 `http` 存取方法。

   如"指令參考資料ONTAP"需詳細 `security login show`資訊，請參閱。

   > ⓘ 您可以使用 `security login create`命令來新增使用者的存取方法。如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

用於管理 **Web** 服務的**ONTAP**命令

您可以使用 `vserver services web` 用於管理叢集或儲存虛擬機器（ SVM ） Web 服務可用度的命令。您可以使用 `vserver services web access` 控制角色存取 Web 服務的命令。

如果您想要...	使用此命令...
設定叢集或AnSVM的Web服務： • 啟用或停用Web服務 • 指定是否只能使用HTTPS存取Web服務	`vserver services web modify`
顯示叢集或anSVM的Web服務組態和可用度	`vserver services web show`
授權角色存取叢集或anSVM上的Web服務	`vserver services web access create`
顯示授權存取叢集或anSVM上Web服務的角色	`vserver services web access show`
防止角色存取叢集或anSVM上的Web服務	`vserver services web access delete`

相關資訊

"指令參考資料ONTAP"

用於管理ONTAP節點上的掛載點的命令

。 `spi` Web 服務會在要求存取節點的記錄檔或核心檔案時、自動從一個節點建立掛載點到另一個節點的根磁碟區。雖然您不需要手動管理掛載點、但可以使用來進行 `system node root-mount` 命令。

如果您想要...	使用此命令...
手動從一個節點建立掛載點到另一個節點的根磁碟區	`system node root-mount create` 只有一個掛載點可以從一個節點存在到另一個節點。
在叢集中的節點上顯示現有的掛載點、包括建立掛載點的時間及其目前狀態	`system node root-mount show`
從一個節點刪除掛載點到另一個節點的根磁碟區、並強制關閉與掛載點的連線	`system node root-mount delete`

相關資訊

"指令參考資料ONTAP"

在ONTAP中管理 SSL

使用 `security ssl` 用於管理叢集或儲存虛擬機器（ SVM ） SSL 傳輸協定的命令。SSL 通訊協定可利用數位憑證在 Web 伺服器與瀏覽器之間建立加密連線、進而改善網路存取的安全性。

您可以透過下列方式管理叢集或儲存虛擬機器（SVM）的SSL：

- 啟用SSL
- 產生及安裝數位憑證、並將其與叢集或SVM建立關聯
- 顯示SSL組態以查看是否已啟用SSL、以及SSL憑證名稱（如果有）
- 設定叢集或SVM的防火牆原則、以便Web存取要求能夠通過
- 定義可以使用的SSL版本
- 限制僅存取Web服務的HTTPS要求

管理 **SSL** 的命令

您可以使用 `security ssl` 用於管理叢集或儲存虛擬機器（ SVM ） SSL 傳輸協定的命令。

如果您想要...	使用此命令...
為叢集或 SVM 啟用 SSL 、並將數位憑證與其建立關聯	`security ssl modify`
顯示叢集或 SVM 的 SSL 組態和憑證名稱	`security ssl show`

深入瞭解 `security ssl modify`及 `security ssl show` "指令參考資料ONTAP"。

將 **HSTS** 用於**ONTAP Web** 服務

HTTP 嚴格傳輸安全性 (HSTS) 是一種 Web 安全性原則機制，可協助保護網站免受中間人攻擊，例如協定降級攻擊和 Cookie 劫持。透過強制使用 HTTPS，HSTS 可確保使用者瀏覽器與伺服器之間的所有通訊都經過加密。從ONTAP 9.17.1 開始， ONTAP可以為ONTAP Web 服務強制使用 HTTPS 連線。

只有在與ONTAP建立初始安全 HTTPS 連線後，Web 瀏覽器才會強制執行 HSTS。如果瀏覽器未建立初始安全連接，則不會強制執行 HSTS。有關 HSTS 管理的信息，請參閱您的瀏覽器文件。

關於這項工作

- 對於 9.17.1 及更高版本，新安裝的ONTAP叢集預設為啟用 HSTS。升級到 9.17.1 後，HSTS 預設不啟用。您必須在升級後啟用 HSTS。
- 所有產品均支援 HSTS "ONTAP Web 服務" 。

開始之前

- 以下任務需要進階權限。

顯示 **HSTS** 配置

您可以顯示目前的 HSTS 配置以檢查它是否已啟用並查看最大年齡設定。

步驟

1. 使用 `system services web show`指令顯示目前的 Web 服務配置，包括 HSTS 設定：

```
cluster-1::system services web*> show

                    External Web Services: true
                                HTTP Port: 80
                               HTTPS Port: 443
                          Protocol Status: online
                       Per Address Limit: 80
                     Wait Queue Capacity: 192
                            HTTP Enabled: true
                  CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                            HSTS Enabled: true
                  HSTS max age (Seconds): 63072000
```

啟用 **HSTS** 並設定最大使用期限

從ONTAP 9.17.1 開始，新的ONTAP叢集預設啟用 HSTS。如果您將現有叢集升級至 9.17.1 或更高版本，則需要在叢集上手動啟用 HSTS 以強制使用 HTTPS。您可以啟用 HSTS 並設定最長使用期限。如果已啟用 HSTS，您可以隨時變更最長使用期限。啟用 HSTS 後，瀏覽器僅在建立初始安全連線後才會開始強制執行安全連線。

步驟

1. 使用 `system services web modify`啟用 HSTS 或修改最大年齡的命令：

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age`指定瀏覽器記住強制執行 HTTPS 的時長（以秒為單位）。預設值為 63072000 秒（兩年）。

禁用 **HSTS**

瀏覽器會在每次連接時保存 HSTS 最長使用期限設置，即使在ONTAP上停用 HSTS，它們也會在整個連接期間繼續強制執行 HSTS。停用 HSTS 後，瀏覽器需要等待配置的最長使用期限才能停止強制執行 HSTS。如果在此期間無法建立安全連接，則強制執行 HSTS 的瀏覽器將不允許存取ONTAP Web 服務，直到問題解決或瀏覽器的最長使用期限到期。

步驟

1. 使用 `system services web modify`命令：

```
system services web modify -hsts-enabled false
```

相關資訊

"RFC 6797 - HTTP 嚴格傳輸安全性 (HSTS)"

解決ONTAP Web 服務存取問題

組態錯誤會導致網路服務存取問題。您可以確保LIF、防火牆原則、Web傳輸協定引擎、Web服務、數位憑證、 而且使用者存取授權均設定正確。

下表可協助您識別及解決Web服務組態錯誤：

此存取問題...	發生原因是此組態錯誤...	若要解決錯誤...
您的 Web 瀏覽器會傳回 `unable to connect` 或 `failure to establish a connection` 嘗試存取 Web 服務時發生錯誤。	您的LIF設定可能不正確。	請確定您可以ping提供Web服務的LIF。 您可以使用 `network ping`命令 ping LIF 。
您的防火牆可能設定不正確。	請確定防火牆原則已設定為支援HTTP或HTTPS、而且原則已指派給提供Web服務的LIF。 您可以使用 `system services firewall policy` 管理防火牆原則的命令。您可以使用 `network interface modify` 命令 `-firewall -policy` 將原則與 LIF 建立關聯的參數。	您的網路傳輸協定引擎可能已停用。
確保已啟用Web傳輸協定引擎、以便存取Web服務。 您可以使用 `system services web` 用於管理叢集 Web 傳輸協定引擎的命令。	您的網路瀏覽器會傳回 A `not found` 嘗試存取 Web 服務時發生錯誤。	Web服務可能已停用。

此存取問題...	發生原因是此組態錯誤...	若要解決錯誤...
確保您要允許存取的每個Web服務都已個別啟用。 您可以使用 `vserver services web modify` 命令以啟用 Web 服務進行存取。	Web瀏覽器無法以使用者的帳戶名稱和密碼登入Web服務。	無法驗證使用者、存取方法不正確、或使用者無權存取Web服務。
請確定使用者帳戶存在、並使用正確的存取方法和驗證方法進行設定。此外、請確認使用者的角色已獲授權可存取Web服務。 您可以使用 `security login` 管理使用者帳戶及其存取方法和驗證方法的命令。存取 ONTAP API Web 服務需要 `ontapi` 存取方法。存取所有其他 Web 服務需要 `http` 存取方法。您可以使用 `vserver services web access` 用於管理角色存取 Web 服務的命令。	您使用HTTPS連線至Web服務、而您的Web瀏覽器則表示連線中斷。	您可能未在提供Web服務的叢集或儲存虛擬機器（SVM）上啟用SSL。
確認叢集或SVM已啟用SSL、且數位憑證有效。 您可以使用 `security ssl` 用於管理 HTTP 伺服器和的 SSL 組態的命令 `security certificate show` 顯示數位憑證資訊的命令。	您使用HTTPS連線至Web服務、Web瀏覽器則表示該連線不受信任。	您可能使用自我簽署的數位憑證。

相關資訊

- "ONTAP網路配置的最佳實務是什麼？"
- "網路ping"
- "修改網路介面"

- "產生安全性憑證-CSR"
- "安全性憑證安裝"
- "安全證書展示"
- "安全 SSL"

使用憑證驗證遠端伺服器的身分

了解如何在**ONTAP**中使用憑證驗證遠端伺服器的身份

支援安全認證功能、可驗證遠端伺服器的身分。ONTAP

利用下列數位憑證功能與傳輸協定、支援安全連線：ONTAP

- 線上憑證狀態傳輸協定（OCSP）會使用ONTAP SSL和傳輸層安全（TLS）連線、驗證來自支援服務的數位憑證要求狀態。此功能預設為停用。
- 預設的一組信任根憑證會隨ONTAP 附於整套的軟體中。
- 金鑰管理互通性傳輸協定（KMIP）憑證可讓叢集和KMIP伺服器相互驗證。

使用**ONTAP**中的 **OCSP** 驗證數位憑證是否有效

線上憑證狀態協定 (OCSP) 可讓使用傳輸層安全性 (TLS) 通訊的ONTAP應用程式能夠在啟用 OCSP 時接收數位憑證狀態。您可以隨時啟用或停用特定應用程式的OCSP憑證狀態檢查。根據預設、OCSP憑證狀態檢查會停用。

開始之前

您需要進階權限層級存取權限才能執行此工作。

關於這項工作

OCSP支援下列應用程式：

- AutoSupport
- 事件管理系統（EMS）
- LDAP over TLS
- 金鑰管理互通性傳輸協定（KMIP）
- 稽核記錄
- FabricPool
- SSH （從 ONTAP 9.13.1 開始）

步驟

1. 將權限層級設為進階： `set -privilege advanced`。
2. 若要啟用或停用OCSP憑證狀態檢查以檢查特定ONTAP 的功能、請使用適當的命令。

如果您希望**OCSP**憑證狀態檢查某些應用程式...	使用命令...
已啟用	`security config ocsp enable -app app name`
已停用	`security config ocsp disable -app app name`

下列命令可支援AutoSupport OCSP for the flexf及EMS。

```
cluster::*> security config ocsp enable -app asup,ems
```

啟用OCSP時、應用程式會收到下列其中一個回應：

- 好-憑證有效且通訊繼續進行。
- 已撤銷：憑證由其核發的憑證授權單位永久視為不信任、且無法繼續通訊。
- 不明：伺服器沒有任何關於憑證的狀態資訊、而且無法繼續通訊。
- 憑證中缺少OCSP伺服器資訊-伺服器的運作方式如同OCSP已停用、並繼續進行TLS通訊、但不會進行狀態檢查。
- OCSP伺服器無回應-應用程式無法繼續。

3. 若要啟用或停用使用TLS通訊之所有應用程式的OCSP憑證狀態檢查、請使用適當的命令。

如果您希望**OCSP**憑證狀態檢查所有應用程式...	使用命令...
已啟用	`security config ocsp enable -app all`
已停用	`security config ocsp disable -app all`

啟用時、所有應用程式都會收到已簽署的回應、表示指定的憑證良好、已撤銷或不明。若憑證遭撤銷、應用程式將無法繼續進行。如果應用程式無法從OCSP伺服器接收回應、或伺服器無法連線、則應用程式將無法繼續進行。

4. 使用 `security config ocsp show` 顯示所有支援 OCSP 的應用程式及其支援狀態的命令。

```
cluster::*> security config ocsp show
         Application                          OCSP Enabled?
         -------------------                  ---------------------
         autosupport                          false
         audit_log                            false
         fabricpool                           false
         ems                                  false
         kmip                                 false
         ldap_ad                              true
         ldap_nis_namemap                     true
         ssh                                  true

         8 entries were displayed.
```

相關資訊

- "啟用安全性組態OCSP"
- "安全性組態OCSP停用"
- "安全組態OCSP顯示"

查看ONTAP中基於 TLS 的應用程式的預設證書

ONTAP使用傳輸層安全性 (TLS) 為ONTAP應用程式提供了一組預設的受信任根憑證。

開始之前

預設憑證僅在管理 SVM 建立期間或升級期間安裝在管理 SVM 上。

關於這項工作

目前做為用戶端且需要驗證憑證的應用程式包括AutoSupport ：FabricPool 和KMIP。

當憑證過期時、系統會呼叫一則EMS訊息、要求使用者刪除憑證。預設憑證只能在進階權限層級刪除。

> 刪除預設憑證可能會導致部分ONTAP 功能不正常的應用程式（例如AutoSupport 、「可靠性記錄」和「稽核記錄」）。

步驟

1. 您可以使用安全性憑證show命令來檢視安裝在管理SVM上的預設憑證：

   `security certificate show -vserver -type server-ca`

```
cluster1::> security certificate show

Vserver    Serial Number   Certificate Name
Type
---------- -------------- ----------------------------------------
---------
vs0        4F4E4D7B         www.example.com
server
    Certificate Authority:  www.example.com
          Expiration Date: Thu Feb 28 16:08:28 2013
```

如"指令參考資料ONTAP"需詳細 `security certificate show`資訊，請參閱。

相互驗證叢集和 KMIP 伺服器

相互驗證ONTAP叢集和 KMIP 伺服器概述

相互驗證叢集和外部金鑰管理程式（例如金鑰管理互通性傳輸協定（KMIP）伺服器）、可讓金鑰管理程式使用KMIP over SSL與叢集進行通訊。當應用程式或特定功能（例如儲存加密功能）需要安全金鑰來提供安全的資料存取時、您就會這麼做。

在 ONTAP 中為叢集產生憑證簽署要求

您可以使用安全性憑證 `generate-csr` 產生憑證簽署要求（ CSR ）的命令。在處理您的要求之後、憑證授權單位（CA）會傳送簽署的數位憑證給您。

開始之前

您必須是叢集管理員或SVM管理員、才能執行此工作。

步驟

1. 產生CSR：

```
security certificate generate-csr -common-name <FQDN_or_common_name>
-size 512|1024|1536|2048 -country <country> -state <state> -locality
<locality> -organization <organization> -unit <unit> -email-addr
<email_of_contact> -hash-function SHA1|SHA256|MD5
```

如"指令參考資料ONTAP"需詳細 `security certificate generate-csr`資訊，請參閱。

下列命令會建立CSR、其中包含由SHA256雜湊功能所產生的2、048位元私密金鑰、供公司IT部門的軟體群組使用、其自訂通用名稱為server1.companyname.com、位於美國加州桑尼維爾。SVM聯絡人管理員的電子郵件地址為web@example.com。系統會在輸出中顯示CSR和私密金鑰。

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. 從CSR輸出複製憑證要求、然後以電子形式（例如電子郵件）將其傳送至信任的協力廠商CA進行簽署。

   在處理您的要求之後、CA會將簽署的數位憑證傳送給您。您應該保留一份私密金鑰和CA簽署的數位憑證複本。

為ONTAP叢集安裝 CA 簽署的伺服器憑證

若要讓SSL伺服器將叢集或儲存虛擬機器（SVM）驗證為SSL用戶端、請在叢集或SVM上安裝具有用戶端類型的數位憑證。然後將用戶端CA憑證提供給SSL伺服器管理員、以便在伺服器上安裝。

開始之前

您必須已在叢集上安裝 SSL 伺服器的根憑證、或是在上安裝 SVM `server-ca` 憑證類型。

步驟

1. 若要使用自我簽署的數位憑證進行用戶端驗證、請使用 `security certificate create` 命令 `type client` 參數。

   如"指令參考資料ONTAP"需詳細 `security certificate create`資訊，請參閱。

2. 若要使用CA簽署的數位憑證進行用戶端驗證、請完成下列步驟：

   a. 使用安全性憑證產生數位憑證簽署要求（ CSR ） `generate-csr` 命令。

      包含憑證要求和私密金鑰的CSR輸出會顯示出來、並提醒您將輸出複製到檔案、以供日後參考。ONTAP

   b. 將CSR輸出的憑證要求以電子形式（例如電子郵件）傳送至信任的CA進行簽署。

      您應該保留一份私密金鑰和CA簽署憑證的複本、以供日後參考。

   在處理您的要求之後、CA會將簽署的數位憑證傳送給您。

a. 使用安裝 CA 簽署的憑證 `security certificate install` 命令 `-type client` 參數。

b. 在系統提示時輸入憑證和私密金鑰、然後按* Enter *。

c. 在出現提示時輸入任何其他根或中繼憑證、然後按* Enter *。

如果從信任的根CA開始且以核發給您的SSL憑證結束的憑證鏈結遺失中繼憑證、您可以在叢集或SVM上安裝中繼憑證。中繼憑證是由信任的根所核發的次要憑證、專門用於發行終端實體伺服器憑證。結果是憑證鏈結從信任的根CA開始、經過中繼憑證、最後以核發給您的SSL憑證結束。

3. 提供 `client-ca` 將叢集或 SVM 的憑證交給 SSL 伺服器的管理員、以便在伺服器上安裝。

的安全性憑證 show 命令 `-instance` 和 `-type client-ca` 參數會顯示 `client-ca` 憑證資訊。

相關資訊

- "安全性憑證安裝"
- "安全證書展示"

在ONTAP中為 KMIP 伺服器安裝 CA 簽署的客戶端憑證

金鑰管理互通性傳輸協定（KMIP）的憑證子類型（-subtype kmip-cert參數）、以及用戶端和伺服器-ca類型、都會指定該憑證用於互動驗證叢集和外部金鑰管理程式、例如KMIP伺服器。

關於這項工作

安裝KMIP憑證、將KMIP伺服器驗證為叢集的SSL伺服器。

步驟

1. 使用 `security certificate install` 命令 `-type server-ca` 和 `-subtype kmip-cert` 用於為 KMIP 伺服器安裝 KMIP 憑證的參數。
2. 出現提示時、請輸入憑證、然後按Enter。

提醒您保留一份憑證複本、以供日後參考。ONTAP

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```

相關資訊

- "安全性憑證安裝"