ONTAP 強化準則

ONTAP 9

NetApp
July 19, 2024

目錄

ONTAP 強化準則

ONTAP 安全強化概述

ONTAP 提供一系列控制功能、可強化業界領先的資料管理軟體 ONTAP 儲存作業系統。使用 ONTAP 的指引和組態設定、協助貴組織達成資訊系統機密性、完整性和可用度等規定的安全目標。

目前威脅情勢的演變、為組織帶來獨特的挑戰、以保護其最寶貴的資產：資料與資訊。我們所面臨的先進動態威脅和弱點越來越精密。系統管理員必須主動處理資料和資訊的安全性、再加上潛在入侵者混淆和偵查技術的效率提高。

自 2024 年 7 月起、先前以 PDF 格式發佈的技術報告內容已與 ONTAP 產品文件整合。ONTAP 安全性文件現在包含來自 _TR-4569 ： ONTAP 安全性強化指南的內容。

ONTAP 映像驗證

ONTAP 提供各種機制、確保 ONTAP 映像在升級和開機時有效。

升級映像驗證

程式碼簽章可協助驗證透過不中斷營運的映像更新或自動不中斷營運的映像更新、 CLI 或 ONTAP API 所安裝的 ONTAP 映像是由 NetApp 真正製作、且未遭竄改。升級映像驗證已在 ONTAP 9.3 中推出。

此功能是 ONTAP 升級或還原的無接觸安全性增強功能。除了選擇性地驗證頂層 "image.tgz" 簽章外、使用者不應採取任何不同的做法。

開機時間映像驗證

從 ONTAP 9.4 開始、統一化可延伸韌體介面（ UEFI ）安全開機已啟用 NetApp AFF A800 、 AFF A220 、 FAS2750 和 FAS2720 系統、以及採用 UEFI BIOS 的後續新一代系統。

開機期間、開機載入器會驗證安全開機金鑰的白名單資料庫、以及與載入的每個模組相關聯的簽名。每個模組都經過驗證並載入之後、開機程序會繼續 ONTAP 初始化。如果任何模組的簽章驗證失敗、系統會重新開機。

這些項目適用於 ONTAP 映像和平台 BIOS 。

本機儲存管理員帳戶

角色、應用程式和驗證

ONTAP 讓注重安全性的企業能夠透過不同的登入應用程式和方法、對不同的管理員提供精細的存取。這有助於客戶建立以資料為中心的零信任模式。

這些角色可供管理員和儲存虛擬機器管理員使用。指定登入應用程式方法和登入驗證方法。

角色

透過角色型存取控制（ RBAC ）、使用者只能存取其工作角色和功能所需的系統和選項。ONTAP 中的 RBAC 解決方案可將使用者的系統管理存取權限限制為其定義角色所授予的層級、讓系統管理員能夠依指派的角色來管理使用者。ONTAP 提供數個預先定義的角色。操作員和管理員可以建立、修改或刪除自訂存取控制角色、也可以指定特定角色的帳戶限制。

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
`admin`	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)
backup	全部	vserver services ndmp
唯讀	volume	無
所有其他命令目錄 (DEFAULT)	readonly	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	無	security
唯讀	所有其他命令目錄 (DEFAULT)	none

。 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。

儲存虛擬機器（ **SVM** ）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、但磁碟區移動除外 • 管理配額、 qtree 、 Snapshot 複本和檔案 • 管理LUN • 執行 SnapLock 作業、但特權刪除除外 • 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP • 設定服務： DNS 、 LDAP 和 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、包括磁碟區移動 • 管理配額、 qtree 、 Snapshot 複本和檔案 • 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 和 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 和 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 • 將還原的磁碟區設為讀取 / 寫入 • 管理 SnapMirror 關係和 Snapshot 複本 • 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、但磁碟區移動除外 • 管理配額、 qtree 、 Snapshot 複本和檔案 • 執行 SnapLock 作業、包括特權刪除 • 設定通訊協定： NFS 和 SMB • 設定服務： DNS 、 LDAP 和 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 • 檢視服務與通訊協定

應用程式方法

應用程式方法會指定登入方法的存取類型。可能的值包括 `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, 和 `telnet`。

設定此參數可 `service-processor` 授予使用者對服務處理器的存取權。當此參數設為 `service-processor`時、必須將參數設為、 `-authentication-method` `password` 因為服務處理器僅支援密碼驗證。SVM 使用者帳戶無法存取服務處理器。因此，當此參數設為時，操作員和管理員無法使用 `-vserver` 此參數 `service-processor`。

要進一步限制對的訪問 `service-processor` ，請使用命令 `system service-processor ssh add-allowed-addresses`。此命令 `system service-processor api-service` 可用於更新組態和憑證。

基於安全考量、依預設會停用 Telnet 和遠端 Shell （ RSH ）、因為 NetApp 建議使用安全 Shell （ SSH ）來進行安全遠端存取。如果需要 Telnet 或 RSH 、或是有獨特的需求、則必須啟用這些功能。

此 `security protocol modify` 命令會修改現有的 RSH 和 Telnet 叢集範圍組態。在叢集中啟用 RSH 和 Telnet 、方法是將啟用欄位設定為 `true`。

驗證方法

驗證方法參數指定用於登入的驗證方法。

驗證方法	說明
`cert`	SSL 憑證驗證
`community`	SNMP 社群字串
`domain`	Active Directory 驗證
`nsswitch`	LDAP 或 NIS 驗證
`password`	密碼
`publickey`	公開金鑰驗證
`usm`	SNMP 使用者安全模式

由於傳輸協定安全性弱點、不建議使用 NIS 。

從 ONTAP 9.3 開始、連結式雙因素驗證可用於使用密碼做為兩種驗證方法的本機 SSH `admin` 帳戶 `publickey` 。除了命令中的欄位之外 `-authentication-method` `security login` 、還新增了一個名為的新欄位 `-second-authentication-method` 。可以將公鑰或密碼指定爲 `-authentication-method` 或 `-second-authentication-method`。不過、在 SSH 驗證期間、訂單一律為公開金鑰、並提供部分驗證、接

著是密碼提示以進行完整驗證。

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

從 ONTAP 9.4 開始、 `nsswitch` 可以用做第二種驗證方法 `publickey`。

從 ONTAP 9.12.1 開始、 FIDO2 也可用於使用 YubiKey 硬體驗證裝置或其他 FIDO2 相容裝置進行 SSH 驗證。

從 ONTAP 9.13.1 開始：

- `domain` 帳戶可以用作第二種驗證方法 `publickey`。
- 時間型一次性密碼 (`totp`）是由演算法所產生的暫時密碼、該演算法會使用目前時間作為第二種驗證方法的驗證因素之一。
- SSH 公開金鑰和憑證均支援公開金鑰撤銷、這些憑證將在 SSH 期間檢查是否到期 / 撤銷。

如需 ONTAP System Manager 、 Active IQ Unified Manager 和 SSH 的多因素驗證（ MFA ）詳細資訊、請參閱 "TR-4647 ： ONTAP 9 中的多因素驗證"。

預設管理帳戶

應限制管理帳戶、因為系統管理員的角色可以使用所有應用程式進行存取。診斷帳戶可存取系統 Shell 、且應僅保留給技術支援人員、以執行疑難排解工作。

有兩個預設的系統管理帳戶： `admin` 和 `diag`。

孤立帳戶是一種主要的安全媒介、通常會導致弱點、包括權限升級。這些是不必要且未使用的帳戶、保留在使用者帳戶儲存庫中。這些帳戶主要是從未使用過的預設帳戶、或從未更新或變更過密碼的帳戶。為了解決此問題、 ONTAP 支援移除和重新命名帳戶。

ONTAP 無法移除或重新命名內建帳戶。不過、 NetApp 建議您使用鎖定命令鎖定任何不需要的內建帳戶。

雖然孤立帳戶是重大的安全問題、 NetApp 強烈建議您測試從本機帳戶儲存庫移除帳戶的效果。

列出本機帳戶

若要列出本機帳戶、請執行 `security login show` 命令。

```
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                             Authentication              Acct   Is-Nsswitch
User/Group Name  Application Method    Role Name         Locked Group
---------------- ----------- --------- ----------------- ------ -----------
admin            console     password  admin             no     no
admin            http        password  admin             no     no
admin            ontapi      password  admin             no     no
admin            service-processor password admin        no     no
admin            ssh         password  admin             no     no
autosupport      console     password  autosupport       no     no
6 entries were displayed.
```

移除預設的管理帳戶

該 `admin` 帳戶具有管理員角色、並允許使用所有應用程式進行存取。

步驟

1. 建立另一個管理層級帳戶。

   若要完全移除預設 `admin` 帳戶、您必須先建立另一個使用登入應用程式的管理員層級帳戶 `console` 。

   > 進行這些變更可能會造成一些不必要的影響。請務必先測試可能影響非正式作業叢集解決方案安全狀態的新設定。

   範例：

   ```
   cluster1::*> security login create -user-or-group-name NewAdmin
   -application console -authentication-method password -vserver cluster1
   ```

```
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                             Authentication              Acct   Is-
Nsswitch
User/Group Name  Application Method    Role Name         Locked Group
---------------- ----------- --------- ----------------- ------
-----------
NewAdmin         console     password  admin             no     no
admin            console     password  admin             no     no
admin            http        password  admin             no     no
admin            ontapi      password  admin             no     no
admin            service-processor password admin        no     no
admin            ssh         password  admin             no     no
autosupport      console     password  autosupport       no     no
7 entries were displayed.
```

2. 建立新的管理員帳戶後、請使用帳戶登入來測試該帳戶的存取權限 `NewAdmin` 。登入時 `NewAdmin` 、請將帳戶設定為與預設或先前的管理帳戶（例如、、、或）具有相同的登入應用程式 `http` `ontapi` `service-processor` `ssh`。此步驟可確保維持存取控制。

   範例：

```
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ssh -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application http -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ontapi -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application service-processor -authentication-method password
```

3. 在測試所有功能之後、您可以先停用所有應用程式的管理帳戶、然後再從 ONTAP 移除。此步驟是最後一項測試、可確認沒有任何仰賴先前管理帳戶的遺留功能。

```
cluster1::*> security login lock -vserver cluster1 -user-or-group-name
admin -application *
```

4. 若要移除預設的管理帳戶及其所有項目、請執行下列命令：

```
cluster1::*> security login delete -vserver cluster1 -user-or-group-name
admin -application *
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                             Authentication              Acct   Is-
Nsswitch
User/Group Name  Application Method    Role Name         Locked Group
---------------- ----------- --------- ----------------- ------
-----------
NewAdmin         console     password  admin             no     no
NewAdmin         http        password  admin             no     no
NewAdmin         ontapi      password  admin             no     no
NewAdmin         service-processor password admin        no     no
NewAdmin         ssh         password  admin             no     no
autosupport      console     password  autosupport       no     no
7 entries were displayed.
```

設定診斷（診斷）帳戶密碼

您的儲存系統會隨附一個名為的診斷帳戶 `diag` 。您可以使用 `diag` 帳戶執行中的疑難排解工作 `systemshell`。 `diag`帳戶是唯一可用於通過特權命令訪問 `systemshell` 的帳戶 `diag systemshell`。

systemshell 和相關 `diag` 帳戶是為了低層級的診斷目的而設計。他們的存取權限需要診斷權限層級、且僅保留在技術支援人員的指引下使用、以執行疑難排解工作。帳戶和都不是 `diag systemshell` 用於一般管理用途。

開始之前

在存取之前 `systemshell`、您必須使用命令設定 `diag` 帳戶密碼 `security login password`。您應該使用強式密碼原則、並定期變更 `diag` 密碼。

步驟

1. 設定 `diag` 帳戶使用者密碼：

```
cluster1::> set -privilege diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? \{y|n}: y

cluster1::*> systemshell -node node-01
    (system node systemshell)
diag@node-01's password:

Warning: The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly. Use this environment
only when directed to do so by support personnel.

node-01%
```

多管理員驗證

從 ONTAP 9.11.1 開始、您可以使用多重管理驗證（ MAV ）、只有在指定管理員核准後、才能執行某些作業、例如刪除磁碟區或 Snapshot 複本。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 MAV 包含下列項目：

- "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。"

在初始設定之後、只有 MAV 核准群組（ MAV 管理員）中的管理員可以修改這些元素。

啟用 MAV 時、完成每項受保護的作業需要三個步驟：

1. 使用者啟動作業時、請使用 "已產生要求。"
2. 在執行之前、需要的數量 "MAV 管理員必須核准。"
3. 核准後、使用者即完成作業。

MAV 不適用於需要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先獲得核准、才能完成作業。如果您想要同時使用自動化和 MAV 、 NetApp 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。

有關 MAV 的詳細信息，請參閱 "ONTAP 多管理驗證文件"。

Snapshot 複本鎖定

Snapshot 複本鎖定是一種 SnapLock 功能、可在 Volume Snapshot 原則上手動或自動以

保留期呈現 Snapshot 複本。Snapshot 複本鎖定的目的是防止惡意或不受信任的系統管理員刪除主要或次要 ONTAP 系統上的 Snapshot 。

ONTAP 9.12.1 引進 Snapshot 複本鎖定功能。Snapshot 複本鎖定也稱為防竄改 Snapshot 鎖定。雖然快照複本鎖定需要 SnapLock 授權和法規遵循時鐘的初始化、但它與 SnapLock 法規遵循或 SnapLock Enterprise 無關。沒有值得信賴的儲存管理員、就像 SnapLock Enterprise 一樣、它也無法保護基礎實體儲存基礎架構、就像 SnapLock Compliance 一樣。這是對 SnapVauling Snapshot 複本至次要系統的改善。可在主要系統上快速恢復鎖定的快照、以還原遭勒索軟體毀損的磁碟區。

如需 Snapshot 複本鎖定的詳細資訊，請參閱 "ONTAP 文件"。

設定憑證型 **API** 存取

除了用於 REST API 或 NetApp Manageability SDK API 存取 ONTAP 的使用者 ID 和密碼驗證之外、還必須使用憑證型驗證。

作為 REST API 憑證型驗證的替代方案、請使用 "OAuth 2.0 權杖型驗證"。）

您可以在 ONTAP 上產生並安裝自我簽署的憑證、如下列步驟所述。

步驟

1. 使用 Openssl 執行下列命令來產生憑證：

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
..............+++
.........................+++
writing new private key to 'test.key'
```

此命令會產生一個名為的公開憑證 `test.pem` 和一個名為的私密金鑰 `key.out`。一般名稱 CN 對應於 ONTAP 使用者 ID 。

2. 在 ONTAP 中以隱私權增強郵件（ pem ）格式安裝公開憑證內容、方法是執行下列命令、並在出現提示時貼上憑證內容：

```
security certificate install -type client-ca -vserver cluster1

Please enter Certificate: Press <Enter> when done
```

3. 啟用 ONTAP 以允許透過 SSL 存取用戶端、並定義 API 存取的使用者 ID 。

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

在下列範例中、使用者 ID `cert_user` 現在已啟用、可使用憑證驗證的 API 存取。使用簡單的 Manageability SDK Python 指令碼 `cert_user` 來顯示 ONTAP 版本、如下所示：

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

指令碼的輸出會顯示 ONTAP 版本。

```
./version.py

V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. 若要使用 ONTAP REST API 執行憑證型驗證、請完成下列步驟：

   a. 在 ONTAP 中、定義 http 存取的使用者 ID ：

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

   b. 在您的 Linux 用戶端上、執行下列命令來產生 ONTAP 版本做為輸出：

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key
./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
    "version": {
        "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
        "generation": 9,
        "major": 7,
        "minor": 0
    },
    "_links": {
        "self": {
            "href": "/api/cluster"
        }
    }
}
```

更多資訊

- "憑證型驗證、搭配 NetApp Manageability SDK for ONTAP"。

REST API 的 ONTAP OAuth 2.0 權杖型驗證

除了憑證型驗證之外、您也可以使用 OAuth 2.0 權杖型驗證來進行 REST API 。

從 ONTAP 9.14.1 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 Token 取代使用者帳戶驗證的密碼。

如需使用 OAuth 2.0 的詳細資訊，請參閱 "使用 OAuth 2.0 驗證和授權的 ONTAP 文件"。

登入和密碼參數

有效的安全態勢遵循既定的組織原則、準則、以及適用於組織的任何治理或標準。這些需求的範例包括使用者名稱存留期、密碼長度要求、字元需求、以及這類帳戶的儲存。ONTAP 解決方案提供解決這些安全性架構的功能。

新的本機帳戶功能

為了支援組織的使用者帳戶原則、準則或標準、包括治理、 ONTAP 支援下列功能：

- 設定密碼原則以強制執行最小位數、小寫字元或大寫字元數
- 登入嘗試失敗後需要延遲
- 定義帳戶非使用中限制
- 使用者帳戶過期
- 顯示密碼過期警告訊息
- 登入無效的通知

可設定的設定是使用安全登入角色組態修改命令來管理。

支援 **SHA-512**

為了加強密碼安全性、 ONTAP 9 支援 SHA-2 密碼雜湊功能、並預設使用 SHA-512 來雜湊新建立或變更的密碼。操作員和管理員也可以視需要過期或鎖定帳戶。

在升級至 ONTAP 9.0 或更新版本之後、具有未變更密碼的現有 ONTAP 9 使用者帳戶會繼續使用 MD5 雜湊功能。不過、 NetApp 強烈建議使用者變更密碼、以移轉至更安全的 SHA-512 解決方案。

密碼雜湊功能可讓您執行下列工作：

- 顯示符合指定雜湊功能的使用者帳戶：

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver  user-or-group-name application authentication-method hash-
function
-------- ------------------ ----------- ---------------------
-------------
cluster1 NewAdmin           console     password              sha512
cluster1 NewAdmin           ontapi      password              sha512
cluster1 NewAdmin           ssh         password              sha512
```

- 使使用指定雜湊功能（例如、 MD5 ）的帳戶過期、強制使用者在下一次登入時變更其密碼：

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- 使用使用指定雜湊功能的密碼鎖定帳戶。

```
cluster1::*> security login lock -vserver * -username * -hash-function
md5
```

叢集管理 SVM 中的內部使用者無法辨識密碼雜湊功能 `autosupport` 。此問題只是表面問題。雜湊功能未知、因為此內部使用者預設沒有設定的密碼。

- 若要檢視使用者的密碼雜湊功能 `autosupport` 、請執行下列命令：

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
                Account Locked: no
                  Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: unknown
Second Authentication Method2: none
```

- 若要設定密碼雜湊功能（預設值： SHA512 ）、請執行下列命令：

```
::> security login password -username autosupport
```

無論密碼設定為何、都沒有關係。

```
security login show -user-or-group-name autosupport -instance

                      Vserver: cluster1
      User Name or Group Name: autosupport
                  Application: console
        Authentication Method: password
     Remote Switch IP Address: -
                    Role Name: autosupport
                Account Locked: no
                  Comment Text: -
      Whether Ns-switch Group: no
       Password Hash Function: sha512
Second Authentication Method2: none
```

密碼參數

ONTAP 解決方案支援密碼參數、可滿足及支援組織原則需求與準則。

屬性	說明	預設	範圍
username-minlength	需要使用者名稱長度下限	3.	3-16
username-alphanum	使用者名稱英數字元	已停用	啟用 / 停用
passwd-minlength	所需的密碼長度下限	8.	3-64
passwd-alphanum	密碼英數字元	已啟用	啟用 / 停用
passwd-min-special-chars	密碼中所需的最少特殊字元數	0%	0-64
passwd-expiry-time	密碼過期時間（以天為單位）	無限制、這表示密碼永遠不會過期	不受限制 0 = 現在到期
require-initial-passwd-update	首次登入時需要初始密碼更新	已停用	啟用 / 停用 允許透過主控台或 SSH 進行變更
max-failed-login-attempts	失敗嘗試次數上限	0 、請勿鎖定帳戶	-
lockout-duration	最長鎖定期間（以天為單位）	預設值為 0 、表示帳戶已鎖定一天	-
disallowed-reuse	不允許最後 N 個密碼	6.	最小值為 6
change-delay	密碼變更之間的延遲（以天為單位）	0%	-
delay-after-failed-login	每次登入嘗試失敗後的延遲（以秒為單位）	4.	-
passwd-min-lowercase-chars	密碼中所需的最小小寫字母字元數	0 、不需要小寫字元	0-64
passwd-min-uppercase-chars	所需的大寫字母字元數下限	0 、不需要大寫字元	0-64
passwd-min-digits	密碼中所需的最小位數	0 、不需要數字	0-64
passwd-expiry-warn-time	在密碼過期前顯示警告訊息（以天為單位）	無限制、這表示永遠不會警告密碼過期	0 、這表示每次成功登入時、都會警告使用者密碼過期
account-expiry-time	帳戶在 N 天內過期	無限、這表示帳戶永遠不會過期	帳戶過期時間必須大於帳戶非使用中限制
account-inactive-limit	帳戶過期前的最長閒置時間（以天為單位）	無限、這表示非使用中帳戶永遠不會過期	帳戶非使用中限制必須小於帳戶到期時間

範例

```
cluster1::*> security login role config show -vserver cluster1 -role admin

                                          Vserver: cluster1
                                        Role Name: admin
                  Minimum Username Length Required: 3
                            Username Alpha-Numeric: disabled
                  Minimum Password Length Required: 8
                            Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
                        Password Expires In (Days): unlimited
   Require Initial Password Update on First Login: disabled
                Maximum Number of Failed Attempts: 0
                    Maximum Lockout Period (Days): 0
                      Disallow Last 'N' Passwords: 6
            Delay Between Password Changes (Days): 0
     Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
                         Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```

從 9.14.1 開始、密碼的複雜度和鎖定規則都會增加。這僅適用於 ONTAP 的新安裝。

系統管理方法

這些是強化 ONTAP 系統管理的重要參數。

命令列存取

建立安全的系統存取權、是維護安全解決方案的重要一環。最常見的命令列存取選項是 SSH 、 Telnet 和 RSH 。其中、 SSH 是最安全、業界標準的遠端命令列存取最佳實務做法。NetApp 強烈建議使用 SSH 命令列存取 ONTAP 解決方案。

SSH 組態

此 `security ssh show` 命令會顯示叢集和 SVM 的 SSH 金鑰交換演算法、加密演算法和 MAC 演算法組態。金鑰交換方法使用這些演算法和密碼來指定一次性工作階段金鑰的產生方式、以進行加密和驗證、以及伺服器驗證的執行方式。

```
cluster1::> security ssh show

Vserver       Ciphers       Key Exchange Algorithms     MAC Algorithms
--------  ----------------  --------------------------  --------------
nsadhanacluster-2
                aes256-ctr,   diffie-helman-group-      hmac-sha2-256
                aes192-ctr,    exchange-sha256,         hmac-sha2-512
                aes128-ctr    ecdh-sha2-nistp384
vs0             aes128-gcm    curve25519-sha256         hmac-sha1
vs1             aes256-ctr,   diffie-hellman-group-     hmac-sha1-96
                aes192-ctr,   exchange-sha256           hmac-sha2-256
                aes128-ctr,   ecdh-sha2-nistp384        hmac-sha2-256-
                3des-cbc,     ecdh-sha2-nistp512        etm
                aes128-gcm                              hmac-sha2-512
3 entries were displayed.
```

登入橫幅

登入橫幅可讓組織向任何營運者、管理員甚至是誤解者展示可接受使用的條款與條件、並指出哪些人可以存取系統。此方法有助於建立對系統存取與使用的期望。命令會 `security login banner modify` 修改登入橫幅。登入橫幅會在 SSH 和主控台裝置登入程序中的驗證步驟之前顯示。橫幅文字必須使用雙引號（「」）、如下列範例所示。

```
cluster1::> security login banner modify -vserver cluster1 -message
“Authorized users ONLY!”
```

登入橫幅參數

參數	說明
`vserver`	使用此參數以修改後的橫幅指定 SVM 。使用叢集管理 SVM 的名稱來修改叢集層級訊息。叢集層級的訊息會作為未定義訊息的資料 SVM 的預設值。
`message`	此選用參數可用於指定登入橫幅訊息。如果叢集已設定登入橫幅訊息、則所有資料 SVM 也會使用叢集登入橫幅。設定資料 SVM 的登入橫幅會覆寫叢集登入橫幅的顯示。若要重設資料 SVM 登入橫幅以使用叢集登入橫幅、請將此參數與值 "-" 一起使用。 如果您使用此參數、登入橫幅不得包含換行（也稱為行尾 [EOLS] 或換行符號）。若要以新行輸入登入橫幅訊息、請勿指定任何參數。系統會提示您以互動方式輸入訊息。以互動方式輸入的訊息可以包含新行。 非 ASCII 字元必須使用 Unicode UTF-8 。
`uri`	`(ftp

參數	說明
http):///(hostname	IPv4` 使用此參數指定登入橫幅下載來源的 URI 。 訊息長度不得超過 2048 位元組。非ASCII字元必須以UNICODE UTF-8格式提供。

當日訊息

命令會 `security login motd modify` 更新當天的訊息（ MOTD ）。

MOTD 有兩種類別：叢集層級 MOTD 和資料 SVM 層級 MOTD 。登入資料 SVM 叢集 Shell 的使用者可能會看到兩則訊息：叢集層級 MOTD 、以及該 SVM 的 SVM 層級 MOTD 。

叢集管理員可視需要個別啟用或停用每個 SVM 上的叢集層級 MOTD 。如果叢集管理員停用 SVM 的叢集層級 MOTD 、則登入 SVM 的使用者不會看到叢集層級的訊息。只有叢集管理員才能啟用或停用叢集層級的訊息。

MOTD 參數	說明
Vserver	使用此參數可指定修改 MOTD 的 SVM 。使用叢集管理 SVM 的名稱來修改叢集層級訊息。

MOTD 參數	說明
訊息	此選用參數可用於指定訊息。如果您使用此參數、則 MOTD 不能包含換行。如果您未指定參數以外的任何參數 `-vserver` 、系統會提示您以互動方式輸入訊息。以互動方式輸入的訊息可以包含新行。非ASCII字元必須以UNICODE UTF-8格式提供。訊息可以包含使用下列轉義序列動態產生的內容： • `\\` - 單一反彈字元 • `\b` - 無輸出（僅支援與 Linux 相容） • `\C` - 叢集名稱 • `\d` - 登入節點上設定的目前日期 • `\t` - 登入節點上設定的目前時間 • `\I` - 傳入 LIF IP 位址（列印主控台以供 `console` 登入） • `\l` - 登入裝置名稱（列印登入主控台 `console` ） • `\L` - 使用者在叢集中任何節點上的上次登入 • `\m` - 機器架構 • `\n` - 節點或資料 SVM 名稱 • `\N` - 登入的使用者名稱 • `\o` - 與 \O 相同提供Linux相容性。 • `\O` - 節點的 DNS 網域名稱。請注意、輸出取決於網路組態、可能是空的。 • `\r` - 軟體版本編號 • `\s` - 作業系統名稱 • `\u` - 本機節點上的作用中叢集 Shell 工作階段數目。對於叢集管理：所有叢集Shell使用者。針對資料 SVM 管理：僅適用於該資料 SVM 的作用中工作階段。 • `\U` - 與相同 `\u`、但有 `user` 或 `users` 附加 • `\v` - 有效的叢集版本字串 • `\W` - 跨叢集的作用中工作階段、供登入的使用者使用 (`who`)

如需在 ONTAP 中設定當日訊息的詳細資訊，請參閱 "當日訊息上的 ONTAP 文件"。

CLI 工作階段逾時

預設 CLI 工作階段逾時為 30 分鐘。逾時對於防止過時的工作階段和工作階段工作階段暫存是很重要的。

使用 `system timeout show` 命令檢視目前的 CLI 工作階段逾時。若要設定逾時值、請使用 `system timeout modify -timeout <minutes>` 命令。

透過 NetApp ONTAP 系統管理員存取網路

如果 ONTAP 管理員偏好使用圖形化介面而非 CLI 來存取和管理叢集、請使用 NetApp ONTAP 系統管理

員。ONTAP 隨附 Web 服務、預設為啟用、並可使用瀏覽器存取。如果使用 DNS 、 IPv4 或 IPv6 位址、請將瀏覽器指向主機名稱（透過 `https://cluster-management-LIF`）。

如果叢集使用自我簽署的數位憑證、瀏覽器可能會顯示警告、指出該憑證不受信任。您可以確認繼續存取的風險、或在叢集上安裝憑證授權單位（ CA ）簽署的數位憑證、以進行伺服器驗證。

從 ONTAP 9.3 開始、安全聲明標記語言（ SAML ）驗證是 ONTAP 系統管理員的選項。

ONTAP 系統管理員的 **SAML** 驗證

SAML 2.0 是廣泛採用的產業標準、可讓任何符合 SAML 標準的第三方身分識別供應商（ IDP ）、使用企業所選擇的 IDP 所特有的機制來執行 MFA 、並做為單一登入（ SSO ）的來源。

SAML 規格中定義了三種角色：主體、 IDP 和服務供應商。在 ONTAP 實作中、主要是叢集管理員透過 ONTAP 系統管理員或 NetApp Active IQ Unified Manager 存取 ONTAP 。IDP 是第三方 IDP 軟體。從 ONTAP 9.3 開始、支援 Microsoft Active Directory 聯合服務（ ADFS ）和開放原始碼 Shibboleth IDP 。從 ONTAP 9.12.1 開始、 Cisco 雙核心支援 IDP 。服務供應商是 ONTAP 系統管理員或 Active IQ Unified Manager 網路應用程式所使用的 ONTAP 內建 SAML 功能。

與 SSH 雙因素組態程序不同的是、啟動 SAML 驗證之後、 ONTAP 系統管理員或 ONTAP 服務處理器存取需要所有現有系統管理員透過 SAML IDP 進行驗證。叢集使用者帳戶無需變更。啟用 SAML 驗證時、會將的新驗證方法新 `saml` 增至具有與應用程式管理員角色的現有使用者 `http ontapi` 。

啟用 SAML 驗證之後、需要 SAML IDP 存取的其他新帳戶應在 ONTAP 中定義、並以系統管理員角色及和應用程式的 SAML 驗證方法定義 `http ontapi` 。如果在某個時間點停用 SAML 驗證、則這些新帳戶需要 `password` 以和應用程式的管理員角色來定義驗證方法 `http ontapi` 、並將用於本機 ONTAP 驗證的主控台應用程式新增至 ONTAP 系統管理員。

啟用 SAML IDP 之後、 IDP 會使用 IDP 可用的方法（例如輕量型目錄存取傳輸協定（ LDAP ）、 Active Directory （ AD ）、 Kerberos 、密碼等）來執行 ONTAP 系統管理員存取的驗證。可用的方法對 IDP 是唯一的。在 ONTAP 中設定的帳戶必須具有對應至 IDP 驗證方法的使用者 ID 。

已通過 NetApp 驗證的 IDP 為 Microsoft ADFS 、 Cisco Duo 和開放原始碼 Shibboleth IDP 。

從 ONTAP 9.14.1 開始、 Cisco 雙核心可作為 SSH 的第二個驗證因素。

如需更多關於 MFA for ONTAP System Manager 、 Active IQ Unified Manager 和 SSH 的資訊、請參閱 "TR-4647 ： ONTAP 9 中的多因素驗證"。

ONTAP System Manager 洞見

從 ONTAP 9.11.1 開始、 ONTAP 系統管理員提供深入見解、協助叢集管理員簡化日常工作。安全性洞見是以本技術報告的建議為基礎。

Security Insight	決心
已啟用 Telnet	NetApp建議使用安全Shell（SSH）進行安全遠端存取。
已啟用遠端 Shell （ RSH ）	NetApp 建議使用 SSH 進行安全的遠端存取。
AutoSupport 使用的是不安全的傳輸協定	AutoSupport 未設定為透過連結： HTTPS 傳送。
叢集層級的叢集上未設定登入橫幅	如果未針對叢集設定登入橫幅、則會發出警告。
SSH 使用不安全的密碼	如果 SSH 使用不安全的密碼、則會發出警告。

Security Insight	決心
設定的 NTP 伺服器太少	如果設定的 NTP 伺服器數量少於三個、則會發出警告。
預設管理使用者未鎖定	如果不使用任何預設的系統管理帳戶（ admin 或 diag ）登入系統管理員、而且這些帳戶未鎖定、建議您將其鎖定。
勒索軟體防禦：磁碟區沒有 Snapshot 原則	一個或多個磁碟區未附加適當的 Snapshot 原則。
勒索軟體防禦—停用 Snapshot 自動刪除	已為一或多個磁碟區設定 Snapshot 自動刪除。
磁碟區並未受到勒索軟體攻擊的監控	多個磁碟區支援自主勒索軟體保護、但尚未設定。
SVM 未設定為自動勒索軟體保護	多個 SVM 支援自主勒索軟體保護、但尚未設定。
未設定原生 FPolicy	未針對 NAS SVM 設定 FPolicy 。
啟用自動勒索軟體保護作用中模式	數個磁碟區已完成其學習模式、您可以開啟作用中模式
停用全域 FIPS 140-2 規範	未啟用全域 FIPS 140-2 規範。
未設定叢集以接收通知	電子郵件、 Webhooks 或 SNMP traphosts 未設定為接收通知。

如需 ONTAP System Manager 深入分析的詳細資訊，請參閱 "ONTAP System Manager Insights 文件"。

ONTAP 自主勒索軟體保護

為了輔助使用者對儲存工作負載安全性的行為分析、 ONTAP 自主勒索軟體保護會分析大量工作負載和 Entropy 、以偵測勒索軟體、並取得一張快照、並在懷疑有攻擊時通知管理員。

除了使用外部 FPolicy 使用者行為分析（ UBA ）與 NetApp Cloud Insights / Cloud Secure 及 NetApp FPolicy 合作夥伴生態系統來偵測和預防勒索軟體、 ONTAP 9.10.1 還引進了自主勒索軟體保護。ONTAP 自主勒索軟體保護採用內建的機器學習（ ML ）功能、可查看大量工作負載活動及資料 Entropy 、以自動偵測勒索軟體。它會監控與 UBA 不同的活動、以便偵測 UBA 不支援的攻擊。

如需此功能的詳細資訊，請參閱 "TR-4572 ： NetApp 勒索軟體解決方案" 或 "ONTAP 自主勒索軟體保護文件"。

儲存管理系統稽核

將 ONTAP 事件卸載到遠端系統記錄伺服器、確保事件稽核的完整性。此伺服器可能是像 Splunk 這樣的安全性資訊事件管理系統。

傳送系統記錄

從支援與可用度的角度來看、記錄與稽核資訊對組織來說是非常寶貴的。此外、記錄（ Syslog ）和稽核報告和輸出中所包含的資訊和詳細資料、通常都是敏感的性質。為了維持安全控管和狀態、組織必須以安全的方式管理記錄和稽核資料。

若要將資料外洩的範圍或佔用空間限制在單一系統或解決方案、就必須卸載syslog資訊。因此、NetApp建議將系統記錄資訊安全地卸載到安全的儲存或保留位置。

建立記錄轉送目的地

使用 `cluster log-forwarding create` 命令建立記錄轉送目的地以進行遠端記錄。

參數

使用下列參數來設定 `cluster log-forwarding create` 命令：

- * 目的地主機 *此名稱是要將記錄轉送到的伺服器的主機名稱或 IPv4 或 IPv6 位址。

```
-destination <Remote InetAddress>
```

- * 目的地連接埠。 *這是目的地伺服器接聽的連接埠。

```
[-port <integer>]
```

- * 記錄轉送通訊協定。 *此傳輸協定用於傳送訊息至目的地。

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted}]
```

  記錄轉送通訊協定可以使用下列其中一個值：

  ◦ `udp-unencrypted`。沒有安全性的使用者資料包傳輸協定。

  ◦ `tcp-unencrypted`。無安全性的 TCP 。

  ◦ `tcp-encrypted`。傳輸層安全性（ TLS ）的 TCP 。

- * 驗證目的地伺服器身分識別。 *當此參數設為 true 時、會驗證其憑證、以驗證記錄轉送目的地的身分識別。只有在通訊協定欄位中選取值時、才能將值設為 true `tcpencrypted` 。

```
[-verify-server \{true|false}]
```

- * 系統記錄工具。 *此值是用於轉送記錄的 Syslog 功能。

```
[-facility <Syslog Facility>]
```

- * 跳過連線測試。 *通常、 `cluster log-forwarding create` 命令會傳送網際網路控制訊息傳輸協定（ ICMP ） ping 來檢查目的地是否可連線、如果無法連線則會失敗。將此值設定為 `true` 略過 ping 檢查、以便在無法到達目的地時設定目的地。

```
[-force [true]]
```

NetApp 建議您使用 `cluster log-forwarding` 命令強制連線至某種 `-tcp-encrypted` 類型。

事件通知

保護離開系統的資訊和資料、對於維護和管理系統的安全狀態至關重要。ONTAP 解決方案所產生的事件、提供豐富的解決方案所遇到的問題、處理的資訊等資訊。這些資料的活力、突顯了以安全的方式管理及移轉資料的必要性。

命令會 `event notification create` 將事件篩選器定義的一組事件的新通知傳送至一或多個通知目的地。下列範例說明事件通知組態和 `event notification show` 命令、該命令會顯示設定的事件通知篩選器和目的地。

```
cluster1::> event notification create -filter-name filter1 -destinations
 email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID      Filter Name        Destinations
-----   ----------------   -----------------
1 filter1 email_dest, syslog_dest, snmp-traphost
```

儲存加密

為了在磁碟遭竊、退回或重新規劃用途時保護敏感資料、請使用硬體型 NetApp 儲存加密或軟體型 NetApp Volume 加密 /NetApp Aggregate 加密。這兩種機制均已通過 FIPS 140-2 驗證、若將硬體型機制搭配軟體型機制使用、則解決方案符合商業解決方案分類（ CSfC ）方案的資格。它可在硬體和軟體層、為機密和機密資料提供強化的安全保護。

當磁碟遭竊、退回或重新使用時、靜止資料加密對於保護敏感資料非常重要。

ONTAP 9 有三種符合聯邦資訊處理標準（ FIPS ） 140-2 標準的靜態資料加密解決方案：

- NetApp 儲存加密（ NSE ）是使用自我加密磁碟機的硬體解決方案。
- NetApp Volume Encryption （ NVE ）是一種軟體解決方案、可加密任何磁碟機類型上的任何資料磁碟區、並為每個磁碟區啟用唯一的金鑰。
- NetApp Aggregate Encryption （ NAE ）是一種軟體解決方案、可加密任何磁碟機類型上的任何資料磁碟區、並為每個集合啟用唯一金鑰。

NSE 、 NVE 和 NAE 可以使用外部金鑰管理或內建金鑰管理程式（ OKM ）。使用 NSE 、 NVE 和 NAE 不會影響 ONTAP 儲存效率功能。不過、 NVE 磁碟區會排除在 Aggregate 重複資料刪除之外。Nae Volume 參與並受益於 Aggregate 重複資料刪除技術。

OKM 為 NSE 、 NVE 或 NAE 的靜態資料提供獨立加密解決方案。

NVE 、 NAE 和 OKM 使用 ONTAP CryptoMod.CryptoModis會列在CMVP FIPS 140-2驗證模組清單中。請參閱。 "FIPS 140-2 Cert# 4144"

若要開始 OKM 組態、請使用 `security key-manager onboard enable` 命令。若要設定外部金鑰管理互通性通訊協定（ KMIP ）金鑰管理員、請使用 `security key-manager external enable` 命令。從 ONTAP 9.6 開始、外部金鑰管理員可支援多處佔用。使用此 `-vserver <vserver name>` 參數為特定 SVM 啟用外部金鑰管理。在 9.6 之前、 `security key-manager setup` 命令用於設定 OKM 和外部金鑰管理員。為了進行內建金鑰管理、此組態會引導操作員或管理員完成複雜密碼設定、以及設定 OKM 的其他參數。

以下範例提供部分組態：

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the “security key-manager backup show”
command.
```

從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode` 的「真」選項 `security key-manager setup` 、要求使用者在重新開機後輸入複雜密碼。對於 ONTAP 9.6 及更新版本、命令語法為 `security key-manager onboard enable -cc-mode-enabled yes`。

從 ONTAP 9.4 開始、您可以使用 `secure-purge` 具有進階權限的功能、在啟用 NVE 的磁碟區上不中斷地「清理」資料。清理加密磁碟區上的資料可確保無法從實體媒體恢復資料。以下命令可安全地清除 SVM VS1 上 vol1 上刪除的檔案：

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

從 ONTAP 9.7 開始、如果有 VE 授權、設定 OKM 或外部金鑰管理員、且不使用 NSE 、則預設會啟用 NAE 和 NVE 。根據預設、 NAE 集合體上會建立 Nae Volume 、而非 NAE 集合體預設會建立 NVE Volume 。您可以輸

入下列命令來覆寫：

```
cluster1::*> options -option-name
encryption.data_at_rest_encryption.disable_by_default true
```

從 ONTAP 9.6 開始、您可以使用 SVM 範圍來設定叢集中資料 SVM 的外部金鑰管理。這最適合多租戶環境、其中每個租戶使用不同的 SVM （或 SVM 組）來提供資料。只有特定租戶的SVM管理員可以存取該租戶的金鑰。如需詳細資訊、請參閱 "在 ONTAP 9.6 及更新版本中啟用外部金鑰管理" ONTAP 文件中的。

從 ONTAP 9.11.1 開始、您可以在 SVM 上指定主要和次要金鑰伺服器、以設定與叢集式外部金鑰管理伺服器的連線。如需詳細資訊、請參閱 "設定叢集式外部金鑰伺服器" ONTAP 文件中的。

從 ONTAP 9.13.1 開始、您可以在系統管理員中設定外部金鑰管理伺服器。如需詳細資訊、請參閱 "管理外部金鑰管理員" ONTAP 文件中的。

資料複寫加密

為了補充靜態加密資料、您可以使用 1.2 、將 ONTAP 資料複寫流量加密至叢集之間、並使用 SnapMirror 、 SnapVault 或 FlexCache 的預先共用金鑰。

當複寫資料以進行災難恢復、快取或備份時、您必須在從ONTAP 一個叢集傳輸到另一個叢集的過程中、透過線路來保護資料。這樣做可防止惡意攔截式攻擊、攻擊正在傳輸的敏感資料。

從 ONTAP 9.6 開始、叢集對等加密可為 ONTAP 資料複寫功能（例如 SnapMirror 、 SnapVault 和 FlexCache ）提供 TLS 1.2 AES-256 GCM 加密支援。加密是透過兩個叢集對等端點之間的預先共用金鑰（PSK）來設定。

使用 NSE 、 NVE 和 NAE 等技術來保護靜止資料的客戶、也可以升級至 ONTAP 9.6 或更新版本、使用叢集對等加密來使用端點對端資料加密。

叢集對等項會加密叢集對等項之間的所有資料。例如、使用 SnapMirror 時、來源叢集對等端點與目的地叢集對等端點之間的所有對等資料和 SnapMirror 關係都會加密。您無法在啟用叢集對等點對等點對等點對等點之間傳送純文字資料、

從 ONTAP 9.6 開始、新的叢集對等關係預設會啟用加密。若要在 ONTAP 9.6 之前建立的叢集對等關係上啟用加密、您必須將來源叢集和目的地叢集升級至 9.6 。此外、您必須使用 `cluster peer modify` 命令來變更來源和目的地叢集對等點、以使用叢集對等加密。

您可以將現有的對等關係轉換為在 ONTAP 9.6 中使用叢集對等加密、如下列範例所示：

```
On the Destination Cluster Peer

cluster2::> cluster peer modify cluster1 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter a passphrase.

On the Source Cluster Peer

cluster1::> cluster peer modify cluster2 -auth-status-admin use-
authentication -encryption-protocol-proposed tls-psk

When prompted enter the same passphrase you created in the previous step.
```

IPsec 資料傳輸中加密

使用 NetApp 儲存加密（ NSE ）或 NetApp Volume Encryption （ NVE ）和叢集對等加密（叢集對等加密）等靜態資料加密技術來進行資料複寫流量的客戶、現在可以升級至 ONTAP 9.8 或更新版本並使用、在用戶端和儲存設備之間使用端點對端加密 IPsec ：IPsec 提供 NFS 或 SMB/CIFS 加密的替代方案、也是 iSCSI 流量唯一的傳輸中加密選項。

在某些情況下、可能需要保護透過有線（或在線中）傳輸至 ONTAP SVM 的所有用戶端資料。如此可防止在敏感資料傳輸期間對其進行重播和惡意攔截式攻擊。

從 ONTAP 9.8 開始、網際網路傳輸協定安全性（ IPsec ）可為用戶端和 ONTAP SVM 之間的所有 IP 流量提供端點對端點加密支援。所有IP流量的IPsec資料加密包括NFS、iSCSI及SMB/CIFS傳輸協定。IPsec為iSCSI流量提供唯一的傳輸加密選項。

透過網路提供 NFS 加密是 IPsec 的主要使用案例之一。在 ONTAP 9.8 之前、 NFS 有線加密需要設定和組態 Kerberos 、才能使用 krb5p 來加密執行中的 NFS 資料。在每個客戶環境中、這並不總是簡單或容易達成的。

使用 NetApp 儲存加密（ NSE ）或 NetApp Volume Encryption （ NVE ）和叢集對等加密（叢集對等加密）等靜態資料加密技術來進行資料複寫流量的客戶、現在可以升級至 ONTAP 9.8 或更新版本並使用、在用戶端和儲存設備之間使用端點對端加密 IPsec ：

IPsec 是一項 IETF 標準。ONTAP 在傳輸模式中使用 IPsec 。它也運用網際網路金鑰交換（ IKE ）傳輸協定第 2 版、使用預先共用金鑰（ PSK ）在用戶端與 ONTAP 之間、以 IPv4 或 IPv6 來交涉金鑰資料。根據預設、 IPsec 使用 Suite B AES-GCM 256 位元加密。也支援採用 256 位元加密的 Suite B AES-GMAC256 和 AES-CBC256 。

雖然必須在叢集上啟用 IPsec 功能、但它會透過使用安全性原則資料庫（ SPD ）項目、套用至個別 SVM IP 位址。原則（ SPD ）項目包含用戶端 IP 位址（遠端 IP 子網路）、 SVM IP 位址（本機 IP 子網路）、要使用的加密密碼套件、以及透過 IKEv2 驗證和建立 IPsec 連線所需的預先共用密碼（ PSK ）。除了 IPsec 原則項目之外、用戶端必須使用相同的資訊（本機和遠端 IP 、 PSK 和密碼套件）進行設定、才能透過 IPsec 連線傳輸流量。從 ONTAP 9.10.1 開始、新增 IPsec 憑證驗證支援。這會移除 IPsec 原則限制、並啟用 Windows 作業系統對 IPsec 的支援。

如果用戶端和 SVM IP 位址之間有防火牆、則必須允許 ESP 和 UDP （連接埠 500 和 4500 ）傳輸協定（輸入）和輸出（輸出））、讓 IKEv2 交涉成功、從而允許 IPsec 傳輸。

對於 NetApp SnapMirror 和叢集對等流量加密、仍建議透過 IPsec 使用叢集對等加密（ CPe ）、以確保有線傳輸的安全。對於這些工作負載而言、 CPE 的效能比 IPsec 更好。您不需要 IPsec 的授權、也不需要任何匯入或匯出限制。

您可以在叢集上啟用 IPsec 、並為單一用戶端和單一 SVM IP 位址建立 SPD 項目、如下列範例所示：

```
On the Destination Cluster Peer

cluster1::> security ipsec config modify -is-enabled true

cluster1::> security ipsec policy create -vserver vs1 -name test34 -local
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32

When prompted enter and confirm the pre shared secret (PSK).
```

TLS 和 SSL 管理

您可以使用 ONTAP 命令將參數設為 true 、為控制平面介面啟用 FIPS 140-2/3 規範模式 `is-fips-enabled` `security config modify` 。

從ONTAP 功能支援範圍9開始、您可以針對整個叢集的控制面板介面啟用FIPS 140-2相容模式。預設會停用FIPS 140-2模式。您可以將命令的參數設為、以啟用 FIPS 140-2 規範模式 `is-fips-enabled` `true` `security config modify` 。然後您可以使用 `security config show command` 確認線上狀態。

啟用FIPS 140-2規範時、會停用TLSv1和SSLv3、而且只有TLSv1.1和TLSv1.2會維持啟用狀態。啟用FIPS 140-2規範時、無法啟用TLSv1和SSLv3。ONTAP如果您啟用 FIPS 140-2 、然後再停用、 TLSv1 和 SSLv3 仍會保持停用狀態、但 TLSv1.2 或 TLSv1.1 和 TLSv1.2 仍會保持啟用狀態、視先前的組態而定。

此命令會 `security config modify` 修改現有的叢集範圍安全性組態。如果您啟用 FIPS 相容模式、叢集會自動僅選取 TLS 通訊協定。使用此 `-supported-protocols` 參數可在 FIPS 模式之外、自行納入或排除 TLS 通訊協定。根據預設、 FIPS 模式會停用、 ONTAP 支援 TLSv1.2 、 TLSv1.1 和 TLSv1 傳輸協定。

為了回溯相容性、 ONTAP 支援在停用 FIPS 模式時、將 SSLv3 新增至 `supported-protocols` 清單。使用此 `-supported-cipher-suites` 參數僅設定進階加密標準（ AES ）或 AES 和 3DES 。您也可以透過指定 !RC4 來停用弱式加密方式、例如 RC4 。依預設，支援的密碼設定為 `ALL:!LOW:!aNULL:!EXP:!eNULL` 。此設定表示所有支援的通訊協定加密套件都已啟用、但不含驗證、無加密、未匯出及低加密密碼套件的加密套件除外。這些套件使用 64 位元或 56 位元加密演算法。

選取對應選取的傳輸協定所提供的加密套件。無效的組態可能會導致某些功能無法正常運作。

如需正確的加密字串語法、請參閱 "密碼" 「 Openssl 」（由 OpenSSL 軟體基礎所發佈）頁面。從 ONTAP 9.9.1 及更新版本開始、您不再需要在修改安全性組態之後手動重新啟動所有節點。

啟用 FIPS 140-2 規範會影響其他系統、以及 ONTAP 9 內部和外部的通訊。NetApp 強烈建議在具有主控台存取權的非正式作業系統上測試這些設定。

如果使用 SSH 管理 ONTAP 9 、則必須使用 OpenSSH 5.7 或更新版本的用戶端。SSH 用戶端必須與省略曲線數位簽章演算法（ ECDSA ）公開金鑰演算法交涉、才能成功連線。

只啟用 TLS 1.2 和使用支援完全轉送機密（ PFS ）的加密套件、就能進一步強化 TLS 安全性。PFS 是一種金鑰交換方法、搭配 TLS 1.2 等加密通訊協定使用時、可協助防止攻擊者解密用戶端和伺服器之間的所有網路工作階段。若要僅啟用 TLS 1.2 和 PFS 功能的加密套件、請使用進階權限層級的命令、 `security config modify` 如下列範例所示。

在變更 SSL 介面組態之前、請務必記住、當用戶端連線至 ONTAP 時、必須支援所述的加密器（ DHE 、 ECDHE ）。否則、不允許連線。

```
cluster1::*> security config modify -interface SSL -supported-protocols
TLSv1.2 -supported-cipher-suites
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

請針對每個提示進行確認 `y` 。如需 PFS 的詳細資訊，請參閱 "此 NetApp 部落格"。

從 ONTAP 9.11.1 和 TLS 1.3 支援開始、您可以驗證 FIPS 140-3 。

FIPS 組態適用於 ONTAP 和平台 BMC 。

建立 CA 簽署的數位憑證

對於許多組織而言、用於 ONTAP 網路存取的自我簽署數位憑證不符合其資訊安全原則。在正式作業系統上、安裝 CA 簽署的數位憑證以用於驗證叢集或 SVM 作為 SSL 伺服器、是 NetApp 的最佳做法。

您可以使用命令來產生憑證簽署要求（ CSR ）、並使用 `security certificate generate-csr` `security certificate install` 命令來安裝您從 CA 收到的憑證。

步驟

1. 若要建立由組織 CA 簽署的數位憑證、請執行下列步驟：
   a. 產生 CSR 。
   b. 請遵循貴組織的程序、使用組織 CA 的 CSR 申請數位憑證。例如、使用 Microsoft Active Directory 憑證服務 Web 介面、前往 `<CA_server_name>/certsrv` 並要求憑證。
   c. 在 ONTAP 中安裝數位憑證。

線上憑證狀態傳輸協定

線上憑證狀態傳輸協定（ OCSP ）可讓使用 TLS 通訊的 ONTAP 應用程式（例如 LDAP 或 TLS ）在啟用 OCSP 時接收數位憑證狀態。應用程式會收到簽署的回應、表示要求的憑證為「良好」、「已撤銷」或「未知」。

OCSP 可在不需要憑證撤銷清單（ CRL ）的情況下、判斷數位憑證的目前狀態。

根據預設、OCSP憑證狀態檢查會停用。您可以使用命令開啟 `security config ocsp enable -app name`應用程式名稱、 `autosupport audit_log、 fabricpool、 ems、、、 kmip ldap_ad `ldap_nis_namemap`或全部。此命令需要進階權限層級。

SSHv2 管理

此命令會 `security ssh modify` 以您指定的組態設定取代叢集或 SVM 的 SSH 金鑰交換演算法、加密演算法或 MAC 演算法的現有組態。

NetApp 建議：

- 使用密碼進行使用者工作階段。
- 使用公開金鑰存取機器。

支援的密碼與金鑰交換

密碼	金鑰交換
AES256-ctr	Diffie-Hellman-group-exchange — sha 256 （SHA-2）
aes192-ctr	Diffie-Hellman-group-exchange — sha 1 （SHA-1）
AES128/ctr	Diffie-Hellman-group14-sha 1 （SHA-1）
AES256-CBC	Diffie-Hellman-group1-sha （SHA-1）
aes192-CBC	-
AES128/CBC	-
AES128/GCM	-
AES256-GCM	-
3DES-CBC	-

支援的 AES 和 3DES 對稱加密

ONTAP 也支援下列類型的 AES 和 3DES 對稱加密（也稱為加密）：

- HMAC-sha1
- HMAC-sha1-96
- HMAC-MD5
- HMAC-MD5-96
- HMAC-ripemd160
- umac-64
- umac-64
- umac-128
- HMAC-SHA2-256

- HMAC-SHA2-512
- HMAC-sha1-ETM
- HMAC-sha1-96-ETM
- HMAC-SHA2-256-ETM
- HMAC-SHA2-512-ETM
- HMAC-MD5-ETM
- HMAC-MD5-96-ETM
- HMAC-ripemd160-ETM
- umac-64-ETM
- umac-128/ETM

SSH 管理組態適用於 ONTAP 和平台 BMC 。

NetApp AutoSupport

ONTAP 的 AutoSupport 功能可讓您主動監控系統健全狀況、並自動傳送訊息和詳細資料給 NetApp 技術支援、貴組織的內部支援團隊或支援合作夥伴。根據預設、第一次設定儲存系統時、會啟用傳送給 NetApp 技術支援的 AutoSupport 訊息。此外、 AutoSupport 會在啟用後 24 小時、開始傳送訊息給 NetApp 技術支援。此 24 小時期間是可設定的。若要利用與組織內部支援團隊的通訊、必須完成郵件主機組態。

只有叢集管理員可以執行 AutoSupport 管理（組態）。SVM 管理員無法存取 AutoSupport 。可停用此功能。AutoSupport不過、 NetApp 建議您啟用此功能、因為如果儲存系統發生問題、 AutoSupport 有助於加速問題識別與解決。根據預設、即使您停用 AutoSupport 、系統仍會收集 AutoSupport 資訊並將其儲存在本機。

如需 AutoSupport 訊息的詳細資訊、包括各種訊息所包含的內容、以及傳送不同類型訊息的位置、請參閱 "NetApp Active IQ Digital Advisor" 文件。

AutoSupport 訊息包含敏感資料、包括但不限於下列項目：

- 記錄檔
- 與特定子系統相關的內容相關資料
- 組態與狀態資料
- 效能資料

支援HTTPS、HTTP和SMTP傳輸傳輸傳輸傳輸傳輸傳輸協定。AutoSupport由於資訊內容敏感、NetApp強烈建議使用HTTPS作為預設傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸傳輸協定、以將資訊傳送給NetApp支援部門。AutoSupport AutoSupport

此外、您應該運用 `system node autosupport modify` 命令來指定 AutoSupport 資料的目標（例如 NetApp 技術支援、組織內部營運或合作夥伴）。此命令也可讓您指定要傳送的特定 AutoSupport 詳細資料（例如效能資料、記錄檔等）。

若要完全停用 AutoSupport 、請使用 `system node autosupport modify -state disable` 命令。

網路時間傳輸協定

雖然 ONTAP 可讓您手動設定叢集上的時區、日期和時間、但您必須設定網路時間傳輸協定（ NTP ）伺服器、使叢集時間至少與三個外部 NTP 伺服器同步。

當叢集時間不準確時、可能會發生問題。雖然 ONTAP 可讓您手動設定叢集上的時區、日期和時間、但您必須設定網路時間傳輸協定（ NTP ）伺服器、使叢集時間與外部 NTP 伺服器同步。

從使用S25 9.5開始ONTAP 、您可以使用對稱驗證來設定NTP伺服器。

您最多可以使用命令建立 10 個外部 NTP 伺服器的關聯 `cluster time-service ntp server create` 。為了提供備援和時間服務品質、您應將至少三部外部NTP伺服器與叢集建立關聯。

如需 ONTAP 中 NTP 組態的詳細資訊、請參閱 "管理叢集時間（僅限叢集管理員）"。

NAS 檔案系統本機帳戶（ CIFS 工作群組）

工作群組用戶端驗證可為 ONTAP 解決方案提供額外的安全層級、且與傳統的網域驗證狀態一致。使用 `vserver cifs session show` 命令可顯示許多與狀態相關的詳細資料、包括 IP 資訊、驗證機制、傳輸協定版本和驗證類型。

從 ONTAP 9 開始、您可以在具有 CIFS 用戶端的工作群組中、使用本機定義的使用者和群組來驗證伺服器的 CIFS 伺服器。工作群組用戶端驗證可為 ONTAP 解決方案提供額外的安全層級、且與傳統的網域驗證狀態一致。若要設定 CIFS 伺服器、請使用 `vserver cifs create` 命令。建立 CIFS 伺服器之後、您可以將其加入 CIFS 網域、或加入工作群組。若要加入工作群組、請使用 `-workgroup` 參數。以下是組態範例：

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

工作群組模式中的 CIFS 伺服器僅支援 Windows NT LAN Manager （ NTLM ）驗證、不支援 Kerberos 驗證。

NetApp 建議將 NTLM 驗證功能搭配 CIFS 工作群組使用、以維持組織的安全狀態。為了驗證 CIFS 安全狀態、NetApp 建議使用 `vserver cifs session show` 命令來顯示許多與狀態相關的詳細資料、包括 IP 資訊、驗證機制、傳輸協定版本和驗證類型。

NAS 檔案系統稽核

NAS 檔案系統在現今的威脅環境中佔用更多資源、因此稽核功能對於支援可見度至關重要。

安全性需要驗證。ONTAP 9 可在整個解決方案中提供更多的稽核事件和詳細資料。由於 NAS 檔案系統在現今的威脅環境中佔用更多資源、因此稽核功能對於支援可見度至關重要。由於 ONTAP 9 的稽核功能有所改善、CIFS 稽核詳細資料比以往更豐富。關鍵詳細資料、包括下列資訊、會記錄建立的事件：

- 檔案、資料夾及共用存取

- 建立、修改或刪除的檔案
- 成功的檔案讀取存取
- 嘗試讀取或寫入檔案失敗
- 資料夾權限變更

建立稽核組態

您必須啟用 CIFS 稽核、才能產生稽核事件。使用 `vserver audit create` 命令建立稽核組態。根據預設、稽核記錄會根據大小使用旋轉方法。如果在「旋轉參數」欄位中指定、您可以使用時間型旋轉選項。其他記錄稽核輪調組態詳細資料包括輪調排程、輪調限制、一週的輪調天數、以及輪調大小。下列文字提供範例組態、描述稽核組態、使用每月的時間輪換、排定在每週的所有日期 12 ： 30 進行。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

CIFS 稽核事件

CIFS 稽核事件如下：

- * 檔案共用 * ：使用相關命令新增、修改或刪除 CIFS 網路共用時、會產生稽核事件 `vserver cifs share` 。
- * 稽核原則變更 * ：使用相關命令停用、啟用或修改稽核原則時，會產生稽核事件 `vserver audit` 。
- * 使用者帳戶 * ：建立或刪除本機 CIFS 或 UNIX 使用者時、會產生稽核事件；啟用、停用或修改本機使用者帳戶；或重設或變更密碼。此事件使用 `vserver cifs users-and-groups local-group` 命令或相關 `vserver services name-service unix-user` 命令。
- * 安全性群組 * ：使用命令或相關命令建立或刪除本機 CIFS 或 UNIX 安全性群組時、會產生稽核事件 `vserver cifs users-and-groups local-group` `vserver services name-service unix-group` 。
- * 授權原則變更 * ：使用命令授與或撤銷 CIFS 使用者或 CIFS 群組的權限時、會產生稽核事件 `vserver cifs users-and-groups privilege` 。

這項功能是以系統稽核功能為基礎、可讓系統管理員從資料使用者的角度來檢閱系統允許和執行的項目。

REST API 對 NAS 稽核的影響

ONTAP 包括管理員帳戶使用 REST API 存取及操作 SMB/CIFS 或 NFS 檔案的能力。雖然 REST API 只能由 ONTAP 管理員執行、 REST API 命令卻會略過系統 NAS 稽核記錄。此外、 ONTAP 系統管理員也可以在使用 REST API 時略過檔案權限。不過、系統命令記錄檔會擷取系統管理員對檔案執行 REST API 的動作。

建立無存取權限 **REST API** 角色

您可以建立無法透過 REST 存取 ONTAP 磁碟區的 REST API 角色、以防止 ONTAP 管理員使用 REST API 進行檔案存取。若要配置此角色、請完成下列步驟。

步驟

1. 建立新的 REST 角色、此角色無法存取儲存磁碟區、但具有所有其他 REST API 存取權。

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. 將系統管理員帳戶指派給您在上一個步驟中建立的新 REST API 角色。

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```

如果您想阻止內置 ONTAP 羣集管理員帳戶使用 REST API 進行文件訪問，則需要先 "建立新的系統管理員帳戶、並停用或刪除內建帳戶"執行。

設定並啟用 CIFS SMB 簽署與封裝

您可以設定及啟用 SMB 簽署、以確保儲存系統與用戶端之間的流量不會受到重播或攔截式攻擊的影響、進而保護資料架構的安全性。SMB 簽署可驗證 SMB 訊息是否具有有效的簽章、以保護其安全。

關於這項工作

檔案系統和架構的常見威脅模式、在於 SMB 傳輸協定。為了解決這個問題、 ONTAP 9 解決方案採用業界標準的 SMB 簽署與密封。SMB 簽署可確保儲存系統與用戶端之間的流量不會因為重播或攔截式攻擊而受到影響、進而保護資料架構的安全性。驗證 SMB 訊息是否有有效的簽章、即可完成此作業。

雖然 SMB 簽署依預設為停用、以提高效能、但 NetApp 強烈建議您啟用此功能。此外、 ONTAP 解決方案支援 SMB 加密、也稱為密封。這種方法可讓資料以每個共享區的方式安全傳輸。預設會停用SMB加密。不過、 NetApp 建議您啟用 SMB 加密。

現在 SMB 2.0 及更新版本均支援 LDAP 簽署和封裝。簽署（防止竄改）和密封（加密）可在 SVM 和 Active Directory 伺服器之間實現安全通訊。SMB 3.0 及更新版本均支援加速 AES 新指令（ Intel AES NI ）加密。Intel AES NI 可改善 AES 演算法、並透過支援的處理器系列來加速資料加密。

步驟

1. 若要設定及啟用 SMB 簽署，請使用 `vserver cifs security modify` 命令並確認 `-is-signing-required` 參數已設定為 `true`。請參閱下列組態範例：

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. 若要設定及啟用 SMB 密封與加密，請使用 `vserver cifs security modify` 命令並確認 `-is-smb`

`-encryption-required` 參數已設定為 `true`。請參閱下列組態範例：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

NFS 安全性

匯出規則是匯出原則的功能要素。匯出規則會根據您設定的特定參數、比對磁碟區的用戶端存取要求、以決定如何處理用戶端存取要求。匯出原則必須包含至少一個匯出規則、才能允許存取用戶端。如果匯出原則包含多個規則、則會依照規則在匯出原則中的顯示順序來處理這些規則。

存取控制是維持安全狀態的核心。因此、 ONTAP 使用匯出原則功能、將 NFS Volume 存取限制在符合特定參數的用戶端。匯出原則包含一或多個匯出規則、可處理每個用戶端存取要求。匯出原則會與每個磁碟區相關聯、以設定用戶端對磁碟區的存取。此程序的結果會決定是否授予或拒絕用戶端（使用拒絕權限的訊息）對磁碟區的存取權。此程序也會決定提供給磁碟區的存取層級。

具有匯出規則的匯出原則必須存在於 SVM 上、用戶端才能存取資料。SVM 可以包含多個匯出原則。

規則順序由規則索引編號決定。如果規則符合用戶端、則會使用該規則的權限、而不會處理其他規則。如果沒有符合的規則、用戶端就會被拒絕存取。

匯出規則會套用下列準則來決定用戶端存取權限：

- 傳送要求的用戶端所使用的檔案存取傳輸協定（例如 NFSv4 或 SMB ）
- 用戶端識別碼（例如主機名稱或 IP 位址）
- 用戶端用來驗證的安全性類型（例如 Kerberos v5 、 NTLM 或 AUTH_SYS ）

如果規則指定多個準則、且用戶端不符合其中一或多個準則、則規則將不適用。

匯出原則範例包含具有下列參數的匯出規則：

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

安全性類型決定用戶端接收的存取層級。這三種存取層級分別為唯讀、讀寫及超級使用者（適用於具有使用者

ID 的用戶端 0）。由於會依此順序評估由安全性類型所決定的存取層級、因此您必須遵守列出的規則：

匯出規則中存取層級參數的規則

讓用戶端取得下列存取層級	這些存取參數必須符合用戶端的安全性類型
一般使用者唯讀	唯讀 (-rorule)
一般使用者讀寫	唯讀 (-rorule) 和讀寫 (-rwrule)
超級使用者唯讀	唯讀 (-rorule) 和 -superuser
超級使用者讀寫	唯讀 (-rorule) 和讀寫 (-rwrule) 和 -superuser

以下是這三種存取參數的有效安全類型：

- 任何
- 無
- 永不

這些安全性類型不適用於 -superuser 下列參數：

- KRB5
- NTLM
- 系統

存取參數結果規則

如果用戶端的安全性類型...	然後...
符合存取參數中指定的安全性類型。	用戶端會以自己的使用者 ID 接收該層級的存取權。
與指定的安全類型不匹配，但訪問參數包括選項 none。	用戶端會接收該層級的存取權、並接收使用參數所指定之使用者 ID 的匿名使用者 -anon 。
與指定的安全類型不匹配，訪問參數不包括選項 none。	用戶端無法接收該層級的任何存取權。 此限制不適用於 -superuser 參數、因為即使未指定、此參數也一律包含無。

Kerberos 5 和 Krb5p

從 ONTAP 9 開始、支援使用隱私權服務（ krb5p ）進行 Kerberos 5 驗證。krbp5 驗證模式是安全的、使用校驗和來加密用戶端和伺服器之間的所有流量、可防止資料竄改和窺探。ONTAP 解決方案支援 Kerberos 的 128 位元和 256 位元 AES 加密。隱私權服務包括驗證所接收資料的完整性、驗證使用者、以及在傳輸前加密資料。

krb5p 選項最常出現在匯出原則功能中、其設定為加密選項。krb5p 驗證方法可用作驗證參數、如下列範例所示：

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

啟用輕量型目錄存取傳輸協定簽署與密封

支援簽署和封裝、以在查詢 LDAP 伺服器時提供工作階段安全性。此方法可替代 LDAP over TLS 工作階段安全性。

簽署可確認使用秘密金鑰技術的 LDAP 有效負載資料完整性。「密封」會加密LDAP有效負載資料、以避免以純文字傳輸敏感資訊。SVM 上的工作階段安全性設定對應於 LDAP 伺服器上可用的設定。依預設、 LDAP 簽署和密封會停用。

步驟

1. 若要啟用此功能、請使用參數執行 `vserver cifs security modify` 命令 `session-security-for-ad-ldap` 。

   LDAP 安全功能選項：

   - * 無 * ：預設、無簽署或密封
   - * 簽署 * ：簽署 LDAP 流量
   - * 認證標章 * ：簽署及加密 LDAP 流量

   > 符號和認證標章參數是累積的、表示如果使用簽署選項、結果是 LDAP 加上簽署。不過、如果使用密封選項、結果會同時是簽署和密封。此外、如果未指定此命令的參數、則預設值為無。

   以下是組態範例：

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

建立及使用 **NetApp FPolicy**

您可以建立及使用 FPolicy 、這是 ONTAP 解決方案的基礎架構元件、可讓合作夥伴應用程式監控及設定檔案存取權限。其中一個功能更強大的應用程式是儲存工作負載安全、這是 NetApp SaaS 應用程式、可在混合雲環境中集中可見度及控制所有企業資料存取、確保安全性與法規遵循目標得以達成。

存取控制是一項重要的安全概念。可見度和回應檔案存取和檔案作業的能力、對於維持您的安全狀態至關重要。為了提供檔案的可見度和存取控制、 ONTAP 解決方案使用 NetApp FPolicy 功能。

檔案原則可以根據檔案類型來設定。FPolicy 決定儲存系統如何處理個別用戶端系統的要求、以執行建立、開啟、重新命名及刪除等作業。從 ONTAP 9 開始、 FPolicy 檔案存取通知架構就會透過篩選控制和恢復功能來增

強、以避免短暫的網路中斷。

步驟

1. 若要使用 FPolicy 功能、您必須先使用命令建立 FPolicy 原則 `vserver fpolicy policy create` 。

   此外、如果您使用 FPolicy 來查看和收集事件、請使用此 `-events` 參數。ONTAP 提供的額外精細度可讓您篩選及存取控制的使用者名稱層級。若要使用使用者名稱來控制權限和存取、請指定 `-privilege-user-name` 參數。

   下列文字提供 FPolicy 建立範例：

   ```
   cluster1::> vserver fpolicy policy create -vserver vs1.example.com
   -policy-name vs1_pol -events cserver_evt,v1e1 -engine native -is
   -mandatory true -allow-privileged-access no -is-passthrough-read-enabled
   false
   ```

2. 建立 FPolicy 原則之後、您必須使用命令加以啟用 `vserver fpolicy enable` 。此命令也會設定 FPolicy 項目的優先順序或順序。

   FPolicy 順序很重要、因為如果多個原則已訂閱相同的檔案存取事件、則順序會指示存取的授與或拒絕順序。

   下列文字提供啟用 FPolicy 原則和使用命令驗證組態的範例組態 `vserver fpolicy show` ：

   ```
   cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
   vs2_pol -sequence-number 5

   cluster1::> vserver fpolicy show
   Vserver                 Policy Name                  Sequence  Status
   Engine
   ----------------------- ---------------------------- --------  -------
   -------
   vs1.example.com         vs1_pol
   vs2.example.com         vs2_pol
    external
   2 entries were displayed.
   ```

FPolicy 增強功能

ONTAP 9 包括以下各節所述的 FPolicy 增強功能。

篩選控制項

新的篩選器可用於 `SetAttr` 和移除目錄活動的通知。

非同步恢復能力

如果以非同步模式運作的FPolicy伺服器發生網路中斷、則中斷期間產生的FPolicy通知會儲存在儲存節點上。當FPolicy伺服器重新連線時、系統會警示已儲存的通知、並從儲存節點擷取通知。在停機期間可儲存通知的時間長度可設定為10分鐘。

LIF安全性

LIF 是 IP 位址或全球連接埠名稱（ WWPN ）、具有相關特性、例如角色、主連接埠、主節點、容錯移轉至的連接埠清單、以及防火牆原則。您可以在叢集透過網路傳送和接收通訊的連接埠上設定LIF。瞭解每個 LIF 角色的安全性特性非常重要。

LIF 角色

LIF 角色可以是：

- * Data LIF* ：與 SVM 相關的 LIF 、用於與用戶端通訊。
- * 叢集 LIF* ： LIF 用於在叢集中的節點之間傳輸叢集內的流量。
- * 節點管理 LIF* ：提供專用 IP 位址的 LIF 、用於管理叢集中的特定節點。
- * 叢集管理 LIF* ：為整個叢集提供單一管理介面的 LIF 。
- * 叢集間 LIF* ：用於跨叢集通訊、備份及複寫的 LIF 。

每個 LIF 角色的安全特性

	資料LIF	叢集LIF	節點管理 LIF	叢集管理LIF	叢集間 LIF
需要私有 IP 子網路？	否	是的	否	否	否
需要安全的網路？	否	是的	否	否	是的
預設防火牆原則	非常嚴格	完全開放	中	中	非常嚴格
防火牆是否可自訂？	是的	否	是的	是的	是的

- 由於叢集 LIF 完全開啟、而且沒有可設定的防火牆原則、因此它必須位於安全隔離網路上的私有 IP 子網路上。
- 在任何情況下、 LIF 角色都不應暴露在網際網路上。

如需更多關於保護生命安全的資訊，請參閱 "設定lifs的防火牆原則"。

傳輸協定與連接埠安全性

除了執行隨裝即用的安全作業和功能外、解決方案的強化還必須包括隨裝即用的安全機制。利用其他基礎架構裝置（例如防火牆、入侵防禦系統（ IPS ）和其他安全裝置）來篩選和限制對 ONTAP 的存取、是建立和維持嚴苛安全狀態的有效方法。此資訊是篩選及限制環境及其資源存取的關鍵元件。

常用的通訊協定和連接埠

服務	連接埠/傳輸協定	說明
SSH	22TCP	SSH 登入
telnet	23個TCP	遠端登入
Domain	53/TCP	網域名稱伺服器
HTTP	80/TCP 80/udp	HTTP
rpcbind	111/TCP 111/UDP	遠端程序呼叫
NTP	123/UDP	網路時間傳輸協定
msrpc	135/UDP	Microsoft 遠端程序呼叫
Netbios-name	137/TCP 137/UDP	NetBios 名稱服務
netbios-ssn	139/TCP	NetBios 服務工作階段
SNMP	161/UDP	SNMP
HTTPS	443/TCP	安全連結： http
microsoft-ds	445/TCP	Microsoft 目錄服務
IPsec	500/udp	網際網路傳輸協定安全性
mount	635/UDP	NFS 掛載
named	953/udp	名稱精靈
NFS	2049/UDP 2049/TCP	NFS 伺服器精靈
nrv	2050/TCP	NetApp 遠端 Volume 傳輸協定
iscsi	3260/TCP	iSCSI目標連接埠
Lockd	4045/TCP 4045/UDP	NFS 鎖定精靈
NFS	4046/TCP	NFS mountd 傳輸協定
acp-proto	4046/UDP	會計傳輸協定
rquotad	4049/UDP	NFS rquotad 傳輸協定
krb524	4444 / udp	Kerberos 524
IPsec	4500/udp	網際網路傳輸協定安全性
acp	5125/UDP 5133/UDP 544/TCP	磁碟的替代控制連接埠
Mdns	533/udp	多點傳送DNS

服務	連接埠/傳輸協定	說明
HTTPS	5986/UDP	HTTPS 連接埠：正在接聽二進位傳輸協定
TELNET	8023/TCP	節點範圍 Telnet
HTTPS	8433/TCP	7MTT GUI 工具、透過連結： HTTPS
RSH	8514/TCP	節點範圍 RSH
KMIP	9877/TCP	KMIP 用戶端連接埠（僅限內部本機主機）
ndmp	1000/TCP	NDMP
cifs 見證連接埠	40001/TCP	CIFS 見證連接埠
TLS	50000/TCP	傳輸層安全性
Iscsi	65200/TCP	iSCSI 連接埠
SSH	65502/TCP	安全Shell
vsun	65503/TCP	Vsun

NetApp 內部連接埠

連接埠/傳輸協定	說明
900	NetApp 叢集 RPC
902.	NetApp 叢集 RPC
904	NetApp 叢集 RPC
905)	NetApp 叢集 RPC
910	NetApp 叢集 RPC
911	NetApp 叢集 RPC
913	NetApp 叢集 RPC
914	NetApp 叢集 RPC
159.15	NetApp 叢集 RPC
918	NetApp 叢集 RPC
920	NetApp 叢集 RPC
921.	NetApp 叢集 RPC
924	NetApp 叢集 RPC
925	NetApp 叢集 RPC
927	NetApp 叢集 RPC
928	NetApp 叢集 RPC
929	NetApp 叢集 RPC
931	NetApp 叢集 RPC
932.	NetApp 叢集 RPC

連接埠/傳輸協定	說明
933	NetApp 叢集 RPC
934	NetApp 叢集 RPC
935	NetApp 叢集 RPC
936.	NetApp 叢集 RPC
937	NetApp 叢集 RPC
939	NetApp 叢集 RPC
940	NetApp 叢集 RPC
951.	NetApp 叢集 RPC
954	NetApp 叢集 RPC
95	NetApp 叢集 RPC
956.	NetApp 叢集 RPC
958	NetApp 叢集 RPC
961.	NetApp 叢集 RPC
963,	NetApp 叢集 RPC
969.64	NetApp 叢集 RPC
9666	NetApp 叢集 RPC
967	NetApp 叢集 RPC
7810.	NetApp 叢集 RPC
7811.	NetApp 叢集 RPC
7812.	NetApp 叢集 RPC
7813.	NetApp 叢集 RPC
7814	NetApp 叢集 RPC
（—	NetApp 叢集 RPC
7816	NetApp 叢集 RPC
7817.	NetApp 叢集 RPC
7818.	NetApp 叢集 RPC
7819	NetApp 叢集 RPC
7820	NetApp 叢集 RPC
7821	NetApp 叢集 RPC
7822.	NetApp 叢集 RPC
7823	NetApp 叢集 RPC
7824	NetApp 叢集 RPC

安全資源

若要深入瞭解本 ONTAP 安全性文件中所述的資訊、請參閱下列其他資訊和安全概念。

有關報告漏洞和事件、 NetApp 安全響應和客戶機密性的信息，請參閱 "NetApp 安全入口網站"。

- "發行說明ONTAP"
- "ONTAP 9 命令參考"
- "系統管理"
- "系統管理員驗證和 RBAC"
- "NetApp 加密"
- "TR-4647 ： ONTAP 9.3 中的多因素驗證"
- "OpenSSL 密碼"
- "CryptoMod FIPS-140-2 第 1 級"
- "憑證型驗證、搭配 NetApp Manageability SDK for ONTAP"
- "網路管理"