本機儲存管理員帳戶
ONTAP 9

NetApp
July 19, 2024

目錄

本機儲存管理員帳戶 . . . 1
角色、應用程式和驗證 . . . 1
預設管理帳戶 . . . 6
多管理員驗證 . . . 9
Snapshot 複本鎖定 . . . 10
設定憑證型 API 存取 . . . 10
REST API 的 ONTAP OAuth 2.0 權杖型驗證 . . . 12
登入和密碼參數 . . . 12

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。