로컬 스토리지 관리자 계정

ONTAP 9

NetApp
July 18, 2024

목차

로컬 스토리지 관리자 계정

역할, 응용 프로그램 및 인증

ONTAP는 보안을 중시하는 기업에 다양한 로그인 응용 프로그램 및 방법을 통해 다양한 관리자에게 세분화된 액세스를 제공할 수 있는 기능을 제공합니다. 이를 통해 고객은 데이터 중심의 제로 트러스트 모델을 만들 수 있습니다.

다음은 관리자 및 스토리지 가상 머신 관리자가 사용할 수 있는 역할입니다. 로그인 응용 프로그램 방법과 로그인 인증 방법이 지정됩니다.

역할

사용자는 역할 기반 액세스 제어(RBAC)를 사용하여 직무 역할 및 기능에 필요한 시스템 및 옵션에만 액세스할 수 있습니다. ONTAP의 RBAC 솔루션은 사용자의 관리 액세스를 정의된 역할에 허용된 수준으로 제한하므로 관리자가 할당된 역할별로 사용자를 관리할 수 있습니다. ONTAP는 몇 가지 미리 정의된 역할을 제공합니다. 운영자와 관리자는 사용자 지정 액세스 제어 역할을 생성, 수정 또는 삭제할 수 있으며 특정 역할에 대한 계정 제한을 지정할 수 있습니다.

클러스터 관리자를 위한 사전 정의된 역할

이 역할은…	이 수준의 액세스 권한…	명령 또는 명령 디렉토리로 이동합니다
`admin`	모두	모든 명령 디렉토리(기본값)
`admin-no-fsa` (ONTAP 9.12.1부터 사용 가능)	읽기/쓰기	• 모든 명령 디렉토리(기본값) • `security login rest-role` • `security login role`

읽기 전용	• `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`	없음
`volume file show-disk-usage`	`autosupport`	모두
• '세트' • '시스템 노드 AutoSupport	없음	기타 모든 명령 디렉토리(기본값)
`backup`	모두	'vserver services ndmp'
읽기 전용	'볼륨'	없음
기타 모든 명령 디렉토리(기본값)	`readonly`	모두
• '보안 로그인 비밀번호 사용자 계정 로컬 암호 및 키 정보 관리에만 사용됩니다 • '세트'	없음	'보안'
읽기 전용	기타 모든 명령 디렉토리(기본값)	"없음"

AutoSupport 역할은 AutoSupport OnDemand가 사용하는 미리 정의된 AutoSupport 계정에 할당됩니다. ONTAP에서는 AutoSupport 계정을 수정하거나 삭제할 수 없습니다. 또한 ONTAP에서는 다른 사용자 계정에 'AutoSupport' 역할을 할당할 수 없습니다.

스토리지 가상 머신**(SVM)** 관리자를 위한 사전 정의된 역할

역할 이름	제공합니다
`vsadmin`	• 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • 볼륨 이동을 제외하고 볼륨을 관리합니다 • 할당량, Qtree, 스냅샷 복사본 및 파일을 관리합니다 • LUN 관리 • 권한 있는 삭제를 제외하고 SnapLock 작업을 수행합니다 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • DNS, LDAP 및 NIS 서비스 구성 • 작업을 모니터링합니다 • 네트워크 연결 및 네트워크 인터페이스를 모니터링합니다 • SVM의 상태를 모니터링합니다
`vsadmin-volume`	• 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • 볼륨 이동을 포함한 볼륨 관리 • 할당량, Qtree, 스냅샷 복사본 및 파일을 관리합니다 • LUN 관리 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • DNS, LDAP 및 NIS 서비스 구성 • 네트워크 인터페이스를 모니터링합니다 • SVM의 상태를 모니터링합니다
`vsadmin-protocol`	• 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • DNS, LDAP 및 NIS 서비스 구성 • LUN 관리 • 네트워크 인터페이스를 모니터링합니다 • SVM의 상태를 모니터링합니다

vsadmin-backup	• 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • NDMP 작업을 관리합니다 • 복원된 볼륨을 읽기/쓰기로 만듭니다 • SnapMirror 관계 및 스냅샷 복사본 관리 • 볼륨 및 네트워크 정보를 봅니다
vsadmin-snaplock	• 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • 볼륨 이동을 제외하고 볼륨을 관리합니다 • 할당량, Qtree, 스냅샷 복사본 및 파일을 관리합니다 • 권한 있는 삭제를 포함한 SnapLock 작업을 수행합니다 • 프로토콜 구성: NFS 및 SMB • DNS, LDAP 및 NIS 서비스 구성 • 작업을 모니터링합니다 • 네트워크 연결 및 네트워크 인터페이스를 모니터링합니다
vsadmin-readonly	• 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • SVM의 상태를 모니터링합니다 • 네트워크 인터페이스를 모니터링합니다 • 볼륨 및 LUN 보기 • 서비스 및 프로토콜 보기

응용 프로그램 방법

응용 프로그램 메서드는 로그인 메서드의 액세스 유형을 지정합니다. 가능한 값에는 `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, 및 `telnet`가 포함됩니다.

이 매개 변수를 설정하면 `service-processor` 사용자에게 서비스 프로세서에 대한 액세스 권한이 부여됩니다. 이 매개 변수를 로 설정할 `service-processor -authentication-method` 경우 서비스 프로세서가 암호 인증만 지원하므로 매개 변수를 로 설정해야 `password` 합니다. SVM 사용자 계정은 서비스 프로세서에 액세스할 수 없습니다. 따라서 이 매개 변수가 로 설정된 경우 연산자 및 관리자는 매개 변수를 사용할 수 `-vserver` `service-processor`없습니다.

에 대한 액세스를 더 제한하려면 `service-processor` 명령을 `system service-processor ssh add-allowed-addresses`사용하십시오. 명령을 `system service-processor api-service` 사용하여 구성 및 인증서를 업데이트할 수 있습니다.

NetApp에서는 보안 원격 액세스를 위해 SSH(보안 셸)를 권장하므로 보안상의 이유로 Telnet 및 RSH(원격 셸)는 기본적으로 비활성화되어 있습니다. 텔넷 또는 RSH에 대한 요구 사항이나 고유한 요구 사항이 있는 경우 이를 활성화해야 합니다.

이 `security protocol modify` 명령은 RSH 및 Telnet의 기존 클러스터 전체 구성을 수정합니다. 활성화된 필드를 로 설정하여 클러스터에서 RSH 및 텔넷을 활성화합니다 `true`.

인증 방법

authentication method 매개 변수는 로그인에 사용되는 인증 방법을 지정합니다.

인증 방법	설명
`cert`	SSL 인증서 인증
`community`	SNMP 커뮤니티 문자열
`domain`	Active Directory 인증
`nsswitch`	LDAP 또는 NIS 인증
`password`	암호
`publickey`	공개 키 인증
`usm`	SNMP 사용자 보안 모델입니다

프로토콜 보안의 약점으로 인해 NIS를 사용하지 않는 것이 좋습니다.

ONTAP 9.3부터는 두 가지 인증 방법으로 로컬 SSH 계정에 대해 연결된 2단계 인증을 사용할 수 `admin publickey` 있습니다. 명령의 필드 외에 `-authentication-method security login` 이라는 새 필드가 `-second -authentication-method` 추가되었습니다. 공개 키 또는 암호를 또는 로 지정할 수 `-authentication -method` `-second-authentication-method`있습니다. 그러나 SSH 인증 중에 순서는 부분 인증을 사용하는 공개 키와 전체 인증을 위한 암호 프롬프트가 차례로 표시됩니다.

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

ONTAP 9.4부터 를 `nsswitch` 와 함께 두 번째 인증 방법으로 사용할 수 `publickey`있습니다.

ONTAP 9.12.1부터 FIDO2는 YubiKey 하드웨어 인증 장치 또는 기타 FIDO2 호환 장치를 사용하는 SSH 인증에도 사용할 수 있습니다.

ONTAP 9.13.1부터:

- `domain` 계정은 에서 두 번째 인증 방법으로 사용할 `publickey`수 있습니다.
- 시간 기반 일회용 암호 (`totp`)는 현재 시간을 두 번째 인증 방법의 인증 요소 중 하나로 사용하는 알고리즘에 의해 생성된 임시 암호입니다.
- 공개 키 취소는 SSH 공개 키와 SSH 중에 만료/해지 여부를 확인하는 인증서를 통해 지원됩니다.

ONTAP System Manager, Active IQ Unified Manager, SSH를 위한 다단계 인증(MFA)에 대한 자세한 내용은 를 참조하십시오. "TR-4647: ONTAP 9의 다단계 인증"

기본 관리 계정

관리자 역할은 모든 응용 프로그램을 사용하여 액세스할 수 있으므로 관리자 계정을 제한해야 합니다. diag 계정은 시스템 쉘에 액세스할 수 있으며 기술 지원 부서의 문제 해결 작업을 수행하기 위한 목적으로만 예약되어야 합니다.

기본 관리 계정에는 및 의 두 `admin` `diag`가지가 있습니다.

고립된 계정은 권한 에스컬레이션을 비롯한 취약점을 유발하는 주요 보안 수단입니다. 이러한 계정은 사용자 계정 저장소에 남아 있는 불필요하고 사용되지 않는 계정입니다. 이러한 계정은 기본적으로 사용되지 않았거나 암호가 업데이트 또는 변경되지 않은 기본 계정입니다. 이 문제를 해결하기 위해 ONTAP에서는 계정 제거 및 이름 변경을 지원합니다.

ONTAP에서 기본 제공 계정을 제거하거나 이름을 바꿀 수 없습니다. 그러나 NetApp에서는 lock 명령을 사용하여 필요하지 않은 기본 제공 계정을 잠그는 것이 좋습니다.

분리된 계정은 중요한 보안 문제이지만 NetApp에서는 로컬 계정 리포지토리에서 계정을 제거할 경우의 영향을 테스트하는 것이 좋습니다.

로컬 계정을 나열합니다

로컬 계정을 나열하려면 `security login show` 명령을 실행합니다.

```
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.
```

기본 관리자 계정을 제거합니다

`admin`계정은 관리자 역할을 가지며 모든 응용 프로그램을 사용하여 액세스할 수 있습니다.

단계

1. 다른 관리자 수준 계정을 만듭니다.

   기본 계정을 완전히 제거하려면 `admin` 먼저 로그인 응용 프로그램을 사용하는 다른 관리자 수준 계정을 만들어야

console 합니다.

> 이러한 변경을 수행하면 원하지 않는 결과가 발생할 수 있습니다. 항상 비운영 클러스터에서 솔루션의 보안 상태에 영향을 줄 수 있는 새 설정을 먼저 테스트하십시오.

예:

```
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. 새 관리자 계정을 만든 후 계정 로그인으로 해당 계정에 대한 액세스를 NewAdmin 테스트합니다. 로그인을 사용하여 NewAdmin 기본 또는 이전 admin 계정(예: , , 또는)과 동일한 로그인 응용 프로그램을 사용하도록 계정을 http ontapi service-processor `ssh`구성합니다. 이 단계를 통해 액세스 제어가 유지됩니다.

   예:

```
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. 모든 기능을 테스트한 후 ONTAP에서 제거하기 전에 모든 응용 프로그램에 대해 admin 계정을 비활성화할 수 있습니다. 이 단계는 이전 관리 계정을 사용하는 반복 기능이 없는지 확인하기 위한 최종 테스트로 사용됩니다.

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

4. 기본 admin 계정과 이 계정에 대한 모든 항목을 제거하려면 다음 명령을 실행합니다.

```
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.
```

진단(diag) 계정 암호를 설정합니다

라는 진단 계정이 diag 스토리지 시스템과 함께 제공됩니다. 계정을 사용하여 에서 문제 해결 작업을 수행할 수 diag systemshell`있습니다. 이 `diag 계정은 권한이 있는 명령을 통해 시스템 쉘에 액세스하는 데 사용할 수 있는 유일한 계정입니다. diag systemshell

> 시스템 셸 및 관련 diag 계정은 저수준 진단 목적으로 사용됩니다. 이러한 액세스 권한은 진단 권한 수준이 필요하며, 기술 지원 부서의 지침에 따라 문제 해결 작업을 수행할 수 있는 경우에만 사용됩니다. 계정과 은 일반 관리 목적으로 사용할 수 diag systemshell 없습니다.

시작하기 전에

에 액세스하기 전에 systemshell`명령을 사용하여 계정 암호를 설정해야 `diag security login password 합니다. 강력한 암호 원칙을 사용하고 정기적으로 암호를 변경해야 diag 합니다.

단계

1. 계정 사용자 암호 설정 diag :

```
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%
```

다중 관리 검증

ONTAP 9.11.1부터 MAV(다중 관리자 검증)를 사용하여 지정된 관리자의 승인 후에만 볼륨 또는 스냅샷 복사본 삭제 같은 특정 작업이 실행되도록 할 수 있습니다. 따라서 손상되거나 악의적이거나 경험이 부족한 관리자가 원치 않는 변경 또는 데이터 삭제를 방지할 수 있습니다.

MAV 구성은 다음과 같이 구성됩니다.

- "하나 이상의 관리자 승인 그룹을 생성합니다."
- "다중 관리 확인 기능 활성화."
- "규칙 추가 또는 수정"

초기 구성 후 MAV 승인 그룹(MAV 관리자)의 관리자만 이러한 요소를 수정할 수 있습니다.

MAV가 활성화된 경우 모든 보호된 작업을 완료하려면 다음 세 단계를 수행해야 합니다.

1. 사용자가 작업을 시작하면 가 나타납니다 "요청이 생성되었습니다."
2. 이 명령을 실행하기 전에 필요한 개수 "MAV 관리자가 승인해야 합니다."
3. 승인 후 사용자가 작업을 완료합니다.

MAV는 자동화 작업이 완료되기 전에 승인이 필요하기 때문에 높은 자동화가 필요한 볼륨이나 워크플로에는 사용할 수 없습니다. 자동화와 MAV를 함께 사용하려는 경우 NetApp에서는 특정 MAV 작업에 대해 쿼리를 사용하는 것이 좋습니다. 예를 들어, 자동화가 관련되지 않은 볼륨에만 MAV 규칙을 적용할 수 `volume delete` 있으며 특정 명명 체계를 사용하여 해당 볼륨을 지정할 수 있습니다.

MAV에 대한 자세한 내용은 를 "ONTAP 다중 관리자 인증 문서"참조하십시오.

스냅샷 복사본 잠금

스냅샷 복사본 잠금은 볼륨 스냅샷 정책의 보존 기간 동안 수동으로 또는 자동으로 스냅샷 복사본을 지울 수 없는 SnapLock 기능입니다. 스냅샷 복사본 잠금의 목적은 악성 또는 신뢰할 수 없는 관리자가 1차 또는 2차 ONTAP 시스템에서 스냅샷을 삭제하지 못하도록 방지하는 것입니다.

스냅샷 복사본 잠금은 ONTAP 9.12.1에 도입되었습니다. 스냅샷 복사본 잠금은 무단 조작 방지 스냅샷 잠금이라고도 합니다. SnapLock 라이센스와 규정 준수 클록의 초기화가 필요하지만, 스냅샷 복사본 잠금은 SnapLock Compliance 또는 SnapLock Enterprise와 관련이 없습니다. SnapLock Enterprise에서와 같이 신뢰할 수 있는 스토리지 관리자는 없으며 SnapLock 규정 준수와 같이 기본 물리적 스토리지 인프라를 보호하지 않습니다. 이것은 보조 시스템에 Snapshot 복사본을 SnapVaulting에 비해 향상된 기능입니다. 기본 시스템에서 잠긴 스냅샷을 빠르게 복구하여 랜섬웨어에 의해 손상된 볼륨을 복원할 수 있습니다.

스냅샷 복사본 잠금에 대한 자세한 내용은 를 참조하십시오 "ONTAP 설명서".

인증서 기반 **API** 액세스를 설정합니다

REST API 또는 ONTAP에 대한 NetApp Manageability SDK API 액세스에 대한 사용자 ID 및 암호 인증 대신 인증서 기반 인증을 사용해야 합니다.

REST API에 대한 인증서 기반 인증 대신 사용 "OAuth 2.0 토큰 기반 인증")

이 단계에 설명된 대로 ONTAP에서 자체 서명된 인증서를 생성하고 설치할 수 있습니다.

단계

1. OpenSSL을 사용하여 다음 명령을 실행하여 인증서를 생성합니다.

```
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'
```

이 명령은 라는 공용 인증서와 `test.pem` 라는 개인 키를 `key.out`생성합니다. 일반 이름인 CN은 ONTAP 사용자 ID에 해당합니다.

2. 다음 명령을 실행하고 메시지가 표시되면 인증서의 내용을 붙여 넣어 ONTAP의 PEM(Privacy Enhanced mail) 형식으로 공용 인증서 내용을 설치합니다.

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

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

3. ONTAP를 활성화하여 SSL을 통한 클라이언트 액세스를 허용하고 API 액세스에 대한 사용자 ID를 정의합니다.

```
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
```

다음 예에서는 사용자 ID가 `cert_user` 인증서 인증 API 액세스를 사용할 수 있게 되었습니다. ONTAP 버전을 표시하기 위해 사용하는 간단한 관리 SDK Python 스크립트는 `cert_user` 다음과 같습니다.

```
#!/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)
```

스크립트의 출력에 ONTAP 버전이 표시됩니다.

```
./version.py

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

4. ONTAP REST API를 사용하여 인증서 기반 인증을 수행하려면 다음 단계를 완료하십시오.
   a. ONTAP에서 http 액세스에 대한 사용자 ID를 정의합니다.

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

   b. Linux 클라이언트에서 다음 명령을 실행하여 ONTAP 버전을 출력으로 생성합니다.

```
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"
        }
    }
}
```

추가 정보

- "ONTAP용 NetApp 관리 SDK를 사용한 인증서 기반 인증"..

REST API에 대한 ONTAP OAuth 2.0 토큰 기반 인증

인증서 기반 인증 대신 REST API에 OAuth 2.0 토큰 기반 인증을 사용할 수 있습니다.

ONTAP 9.14.1부터 OAuth 2.0(Open Authorization 2.0) 프레임워크를 사용하여 ONTAP 클러스터에 대한 액세스를 제어할 수 있습니다. 이 기능은 ONTAP CLI, System Manager, REST API를 포함한 모든 ONTAP 관리 인터페이스를 사용하여 구성할 수 있습니다. 그러나 OAuth 2.0 권한 부여 및 액세스 제어 결정은 클라이언트가 REST API를 사용하여 ONTAP에 액세스할 때만 적용할 수 있습니다.

OAuth 2.0 토큰은 사용자 계정 인증을 위한 암호를 대체합니다.

OAuth 2.0 사용에 대한 자세한 내용은 를 "OAuth 2.0을 사용한 인증 및 권한 부여에 대한 ONTAP 문서"참조하십시오.

로그인 및 암호 매개 변수

효과적인 보안 체계는 확립된 조직 정책, 지침 및 조직에 적용되는 모든 거버넌스 또는 표준을 준수합니다. 이러한 요구 사항의 예로는 사용자 이름 수명, 암호 길이 요구 사항, 문자 요구 사항 및 이러한 계정의 저장 등이 있습니다. ONTAP 솔루션은 이러한 보안 구조를 처리하는 기능을 제공합니다.

새로운 로컬 계정 기능

거버넌스를 포함하여 조직의 사용자 계정 정책, 지침 또는 표준을 지원하기 위해 ONTAP에서 지원되는 기능은 다음과 같습니다.

- 최소 숫자, 소문자 또는 대문자를 사용하도록 암호 정책 구성
- 로그인 시도 실패 후 지연이 필요합니다
- 계정 비활성 한도 정의
- 사용자 계정 만료
- 암호 만료 경고 메시지 표시
- 잘못된 로그인에 대한 알림입니다

ⓘ 구성 가능한 설정은 보안 로그인 역할 config modify 명령을 사용하여 관리합니다.

SHA-512 지원

암호 보안을 강화하기 위해 ONTAP 9에서는 SHA-2 암호 해시 기능을 지원하며, 새로 생성되거나 변경된 암호를 해시하는 데 기본적으로 SHA-512를 사용합니다. 운영자와 관리자는 필요에 따라 계정을 만료하거나 잠글 수도 있습니다.

암호가 변경되지 않은 기존 ONTAP 9 사용자 계정은 ONTAP 9.0 이상으로 업그레이드한 후에도 MD5 해시 기능을 계속 사용합니다. 그러나 NetApp에서는 사용자가 암호를 변경하도록 하여 이러한 사용자 계정을 보다 안전한 SHA-512 솔루션으로 마이그레이션할 것을 적극 권장합니다.

암호 해시 기능을 사용하면 다음 작업을 수행할 수 있습니다.

- 지정된 해시 함수와 일치하는 사용자 계정 표시:

```
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
```

- 지정된 해시 함수(예: MD5)를 사용하는 계정을 만료시켜 사용자가 다음 로그인 시 암호를 변경해야 합니다.

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

- 지정된 해시 함수를 사용하는 암호로 계정을 잠급니다.

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

클러스터의 관리 SVM에서 내부 사용자가 암호 해시 기능을 알 수 없습니다 `autosupport` . 이 문제는 외관상 문제입니다. 이 내부 사용자에게는 기본적으로 구성된 암호가 없으므로 해시 기능을 알 수 없습니다.

  - 사용자의 암호 해시 기능을 보려면 `autosupport` 다음 명령을 실행합니다.

```
::> 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
```

  - 암호 해시 기능(기본값: SHA512)을 설정하려면 다음 명령을 실행합니다.

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

암호가 무엇으로 설정되어 있는지는 중요하지 않습니다.

```
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
```

암호 매개 변수

ONTAP 솔루션은 조직 정책 요구 사항 및 지침을 다루고 지원하는 암호 매개 변수를 지원합니다.

속성	설명	기본값	범위
username-minlength	최소 사용자 이름 길이가 필요합니다	3	3-16 을 참조하십시오
username-alphanum	사용자 이름 영숫자	사용 안 함	활성화/비활성화
passwd-minlength	최소 암호 길이가 필요합니다	8	3-64 을 참조하십시오
passwd-alphanum	암호 영숫자	활성화됨	활성화/비활성화
passwd-min-special-chars	암호에 필요한 최소 특수 문자 수입니다	0	0-64 을 참조하십시오
passwd-expiry-time	암호 만료 시간(일)	무제한 - 암호가 만료되지 않습니다	0 - 무제한 0 = 지금 만료
require-initial-passwd-update	첫 번째 로그인 시 초기 암호 업데이트가 필요합니다	사용 안 함	활성화/비활성화 콘솔 또는 SSH를 통해 변경이 허용됩니다
max-failed-login-attempts	최대 시도 실패 횟수입니다	0, 계정을 잠그지 마십시오	-
lockout-duration	최대 잠금 기간(일)	기본값은 0입니다. 즉, 계정이 하루 동안 잠겨 있습니다	-
disallowed-reuse	마지막 N 암호를 허용하지 않습니다	6	최소값은 6입니다

속성	설명	기본값	범위
`change-delay`	암호 변경 간격(일)	0	-
`delay-after-failed-login`	로그인 시도 실패 후 지연(초)	4	-
`passwd-min-lowercase-chars`	암호에 필요한 최소 소문자 알파벳 문자 수입니다	0으로, 소문자가 필요하지 않습니다	0-64 을 참조하십시오
`passwd-min-uppercase-chars`	알파벳 대문자 최소 개수여야 합니다	0 - 대문자가 필요하지 않습니다	0-64 을 참조하십시오
`passwd-min-digits`	암호에 필요한 최소 자릿수입니다	0으로, 숫자가 필요하지 않습니다	0-64 을 참조하십시오
`passwd-expiry-warn-time`	암호 만료 전에 경고 메시지 표시(일)	Unlimited(무제한) - 암호 만료에 대해 경고하지 않습니다	0: 로그인할 때마다 암호 만료에 대해 사용자에게 경고합니다
`account-expiry-time`	계정이 N일 후에 만료됩니다	무제한. 즉, 계정이 만료되지 않습니다	계정 만료 시간은 계정 비활성 제한보다 커야 합니다
`account-inactive-limit`	계정 만료 전 최대 비활성 기간(일)	무제한 - 비활성 계정은 만료되지 않습니다	계정 비활성 한도는 계정 만료 시간보다 작아야 합니다

예

```
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
```

9.14.1부터는 암호에 대한 복잡성과 잠금 규칙이 증가합니다. 이는 ONTAP의 신규 설치에만 적용됩니다.