ローカルストレージ管理者アカウント
ONTAP 9

NetApp
July 19, 2024

目次

ローカルストレージ管理者アカウント

ロール、アプリケーション、認証

ONTAPは、セキュリティを重視する企業に、さまざまなログインアプリケーションやログイン方法を使用して、さまざまな管理者にきめ細かくアクセスできる機能を提供します。これにより、お客様はデータ中心のゼロトラストモデルを構築できます。

管理者とStorage Virtual Machine管理者が使用できるロールです。ログインアプリケーション方式とログイン認証方式が指定されています。

ロール

Role-Based Access Control（RBAC；ロールベースアクセス制御）を使用すると、ユーザは自分のジョブロールと機能に必要なシステムとオプションにのみアクセスできます。ONTAPのRBACソリューションではユーザの管理アクセスがそのユーザのロールに付与されたレベルに制限されるため、管理者は割り当てられたロールに基づいてユーザを管理できます。ONTAPには、複数の事前定義されたロールが用意されています。オペレータや管理者はカスタムのアクセス制御ロールを作成、変更、削除したり、特定のロールに対してアカウント制限を指定したりできます。

クラスタ管理者の事前定義されたロール

ロール	アクセスレベル	コマンドまたはコマンドディレクトリに移動します
`admin`	すべて	すべてのコマンドディレクトリ（`DEFAULT`）
`admin-no-fsa` （ONTAP 9.12.1以降で使用可能）	読み取り / 書き込み	• すべてのコマンドディレクトリ（`DEFAULT`） • `security login rest-role` • `security login role`

読み取り専用です	• 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	なし
volume file show-disk-usage	autosupport	すべて
• set • system node autosupport	なし	その他すべてのコマンドディレクトリ (DEFAULT)
backup	すべて	vserver services ndmp
読み取り専用です	volume	なし
その他すべてのコマンドディレクトリ (DEFAULT)	readonly	すべて
• security login password 自身のユーザアカウントのローカルパスワードとキー情報のみを管理する場合 • set	なし	security

読み取り専用です	その他すべてのコマンドディレクトリ (DEFAULT)	none

。 autosupport ロールは事前定義されたに割り当てられます autosupport AutoSupport OnDemandで使用されるアカウント。ONTAP では、を変更または削除することはできません autosupport アカウント：また、ONTAP ではを割り当てることもできません autosupport 他のユーザアカウントへのロール。

Storage Virtual Machine（SVM）管理者の事前定義されたロール

ロール名	機能
vsadmin	• 自身のユーザアカウントのローカルパスワードとキー情報の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshotコピー、およびファイルを管理します。 • LUNを管理します • SnapLock処理の実行（privileged deleteを除く） • プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、 NVMe/FCとNVMe/TCP • サービスの設定：DNS、LDAP、NIS • ジョブの監視 • ネットワーク接続とネットワーク インターフェイスの監視 • SVMの健全性の監視
vsadmin-volume	• 自身のユーザアカウントのローカルパスワードとキー情報の管理 • ボリュームの管理（ボリュームの移動を含む） • クォータ、qtree、Snapshotコピー、およびファイルを管理します。 • LUNを管理します • プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、 NVMe/FCとNVMe/TCP • サービスの設定：DNS、LDAP、NIS • ネットワーク インターフェイスの監視 • SVMの健全性の監視

`vsadmin-protocol`	• 自身のユーザアカウントのローカルパスワードとキー情報の管理 • プロトコルの設定：NFS、SMB、iSCSI、FC、FCoE、 NVMe/FCとNVMe/TCP • サービスの設定：DNS、LDAP、NIS • LUNを管理します • ネットワーク インターフェイスの監視 • SVMの健全性の監視
`vsadmin-backup`	• 自身のユーザアカウントのローカルパスワードとキー情報の管理 • NDMP処理を管理します。 • リストアしたボリュームを読み取り/書き込み可能にします。 • SnapMirror関係とSnapshotコピーを管理します。 • ボリュームとネットワーク情報の表示
`vsadmin-snaplock`	• 自身のユーザアカウントのローカルパスワードとキー情報の管理 • ボリュームの管理（ボリュームの移動を除く） • クォータ、qtree、Snapshotコピー、およびファイルを管理します。 • privileged deleteなどのSnapLock処理の実行 • プロトコルの設定：NFSとSMB • サービスの設定：DNS、LDAP、NIS • ジョブの監視 • ネットワーク接続とネットワーク インターフェイスの監視
`vsadmin-readonly`	• 自身のユーザアカウントのローカルパスワードとキー情報の管理 • SVMの健全性の監視 • ネットワーク インターフェイスの監視 • ボリュームとLUNの表示 • サービスとプロトコルの表示

アプリケーションメソッド

Application Methodはログイン方法のアクセス タイプを指定します。指定できる値は `console`, `http`,

ontapi, rsh, snmp, service-processor, ssh, 、および `telnet`です。

このパラメータをに設定すると service-processor 、サービスプロセッサへのアクセスがユーザに付与されます。サービスプロセッサではパスワード認証のみがサポートされるため、このパラメータを service-processor -authentication-method に設定する必要があります password 。SVMユーザ アカウントではサービス プロセッサにアクセスできません。したがって、このパラメータがに設定されている場合、オペレータや管理者はパラメータを使用できません -vserver service-processor。

へのアクセスをさらに制限するには service-processor 、コマンドを使用し system service-processor ssh add-allowed-addresses`ます。コマンドを `system service-processor api-service 使用すると、設定と証明書を更新できます。

セキュリティ上の理由から、NetAppはセキュアなリモートアクセスにセキュアシェル（SSH）を推奨しているため、Telnetとリモートシェル（RSH）はデフォルトで無効になっています。要件や独自のニーズに従ってTelnetまたはRSHを使用する必要がある場合は、それらを有効にする必要があります。

コマンドは security protocol modify 、クラスタ全体のRSHおよびTelnetの既存の設定を変更します。[Enabled]フィールドをに設定して、クラスタでRSHとTelnetを有効にします true。

ニンショウホウ

Authentication Methodパラメータは、ログインに使用する認証方式を指定します。

認証方式	説明
cert	SSL証明書認証
community	SNMPコミュニティ ストリング
domain	Active Directory認証
nsswitch	LDAP認証またはNIS認証
password	パスワード
publickey	公開鍵認証
usm	SNMPユーザ セキュリティ モデル

NISプロトコルはセキュリティが脆弱であるため、推奨されません。

ONTAP 9.3以降では、ローカルSSHアカウントに対して、とpasswordの2つの認証方式を使用してチェーン型の2要素認証を使用でき admin publickey ます。コマンドのフィールドに加えて -authentication -method security login 、という名前の新しいフィールドが -second-authentication-method 追加されました。またはとして公開鍵またはパスワードを指定できます -authentication-method -second -authentication-method。ただし、SSH認証では、公開鍵で部分認証が行われ、その後にパスワードプロンプトが表示されて完全認証が行われます。

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

ONTAP 9.4以降では、を `nsswitch` 使用して2つ目の認証方式として使用できます `publickey`。

ONTAP 9.12.1以降では、YubiKeyハードウェア認証デバイスまたは他のFIDO2互換デバイスを使用したSSH認証にもFIDO2を使用できます。

ONTAP 9.13.1以降：

- `domain` アカウントは、を使用して2番目の認証方法として使用でき `publickey`ます。
- 時間ベースのワンタイムパスワード (`totp`）は、現在の時刻を2番目の認証方法の認証要素の1つとして使用するアルゴリズムによって生成される一時パスコードです。
- 公開鍵の失効は、SSH公開鍵と、SSH中に有効期限や失効がチェックされる証明書でサポートされます。

ONTAP System Manager、Active IQ Unified Manager、およびSSHの多要素認証（MFA）の詳細については、を参照してください "TR-4647：『Multifactor Authentication in ONTAP 9』"。

デフォルトノカンリアカウント

管理者ロールにはすべてのアプリケーションを使用したアクセスが許可されているため、adminアカウントは制限する必要があります。diagアカウントはシステムシェルへのアクセスを許可します。テクニカルサポートがトラブルシューティングタスクを実行する場合にのみ使用してください。

デフォルトの管理アカウントには、との2つがあります。 `admin` `diag`

アカウントの孤立は重大なセキュリティ ベクターで、権限の昇格などの脆弱性を招くことが珍しくありません。孤立したアカウントとは、ユーザ アカウント リポジトリに残っている使用されていない不要なアカウントのことです。孤立したアカウントの多くは、使用されたことがないかパスワードが更新または変更されていないデフォルト アカウントです。この問題に対処するために、ONTAPではアカウントの削除と名前変更がサポートされています。

> ⓘ 組み込みアカウントの削除と名前変更はONTAPではサポートされていません。ただし、NetAppでは、lockコマンドを使用して不要な組み込みアカウントをロックすることを推奨しています。

孤立したアカウントはセキュリティ上の重大な問題となりますが、ローカル アカウント リポジトリから削除する場合はその影響についてテストすることを強く推奨します。

ローカルアカウントをリスト表示

ローカルアカウントを一覧表示するには、コマンドを実行し `security login show` ます。

```
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.
```

デフォルトの管理者アカウントを削除する

この admin アカウントには管理者のロールが割り当てられ、すべてのアプリケーションを使用したアクセスが許可されます。

手順

1. 別の管理者レベルアカウントを作成します。

   デフォルトアカウントを完全に削除するには admin 、まずログインアプリケーションを使用する別の管理者レベルアカウントを作成する必要があります console 。

   > これらの変更を行うと、望ましくない影響が生じる可能性があります。ソリューションのセキュリティ ステータスに影響する可能性がある新しい設定は、適用する前に必ず非本番環境のクラスタでテストしてください。

   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. 新しいadminアカウントを作成したら、アカウントログインを使用してそのアカウントへのアクセスをテストします `NewAdmin` 。ログインを使用して `NewAdmin` 、デフォルトまたは以前のadminアカウントと同じログインアプリケーション（、、、、など）を使用するようにアカウントを設定し `http` `ontapi` `service-processor` `ssh`ます。これによってアクセス制御が維持されます。

   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. すべての機能についてテストしたら、ONTAPから削除する前にすべてのアプリケーションでadminアカウントを無効にします。この手順で、前のadminアカウントに依存する機能が残っていないことを最後にもう一度確認します。

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

4. デフォルトのadminアカウントとそのすべてのエントリを削除するには、次のコマンドを実行します。

```
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.
```

診断（diag）アカウントのパスワードを設定する

ストレージシステムには、という名前の診断アカウントが `diag` 用意されています。アカウントを使用して、でトラブルシューティングタスクを実行できます `diag systemshell`。 `diag`システムシェルへのアクセスに使用できるアカウントはアカウントだけです。アクセスには、特権コマンドを使用し `diag systemshell` ます。

> ⚠ システムシェルと関連する `diag` アカウントは、簡単な診断を目的としています。このアクセスにはdiagnostic権限レベルが必要で、テクニカルサポートからの指示に従ってトラブルシューティングタスクを実行する場合にのみ使用されます。アカウントとは、いずれも `diag systemshell` 一般的な管理目的で使用するものではありません。

作業を開始する前に

にアクセスする前に `systemshell`、コマンドを使用してアカウントパスワードを設定する必要があります `diag security login password`。強力なパスワード原則を使用し、定期的にパスワードを変更する必要があります `diag`。

手順

1. アカウントのユーザパスワードを設定し `diag` ます。

```
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%
```

管理者による検証が複数必要です

ONTAP 9.11.1以降では、Multi-Admin Verification（MAV；マルチ管理者検証）を使用して、ボリュームやSnapshotコピーの削除などの特定の処理を、指定した管理者の承認後にのみ実行することができます。これにより、侵害された管理者や悪意のある管理者、経験の浅い管理者が望ましくない変更やデータ削除を行うのを防ぐことができます。

MAVの設定は、次の内容で構成されます。

- "1つ以上の管理者承認グループを作成します。"
- "マルチ管理者検証機能の有効化。"
- "ルールを追加または変更する。"

初期設定後は、MAV承認グループの管理者（MAV管理者）のみがこれらの要素を変更できます。

MAVがイネーブルの場合、保護されたすべての動作を完了するには、次の3つのステップが必要です。

1. ユーザが処理を開始すると、 "要求が生成されます。"
2. 実行する前に、必要な数の "MAV管理者は承認する必要があります。"
3. 承認後、ユーザーは操作を完了します。

MAVは、高度な自動化を伴うボリュームやワークフローでは使用しません。自動化された各タスクは、操作を完了する前に承認を必要とするためです。自動化とMAVを一緒に使用する場合はNetApp、特定のMAV操作にクエリを使用することをお勧めします。たとえば、自動化が関係していないボリュームにのみMAVルールを適用し `volume delete` 、特定の命名規則を使用してそれらのボリュームを指定できます。

MAVの詳細については、を参照してください "ONTAPのマルチ管理者認証に関するドキュメント"。

Snapshotコピーロック

Snapshotコピーロックは、ボリュームSnapshotポリシーの保持期間に応じて手動または自動でSnapshotコピーを消去できないようにするSnapLock機能です。Snapshotコピーロックの目的は、悪意のある管理者や信頼されていない管理者が、プライマリまたはセカンダリONTAPシステム上のSnapshotを削除しないようにすることです。

SnapshotコピーロックはONTAP 9.12.1で導入されました。Snapshotコピーロックは、改ざん防止Snapshotロックとも呼ばれます。Snapshotコピーのロックは、SnapLockライセンスとコンプライアンスクロックの初期化が必要ですが、SnapLock ComplianceやSnapLock Enterpriseとは関係ありません。SnapLock Enterpriseのように信頼できるストレージ管理者は存在せず、SnapLockコンプライアンスのように基盤となる物理ストレージインフラを保護することもできません。この機能は、Snapshotコピーをセカンダリシステムに保存する場合に比べて強化されています。プライマリシステム上のロックされたSnapshotの迅速なリカバリを実現し、ランサムウェアによって破損したボリュームをリストアできます。

Snapshotコピーロックの詳細については、を参照して "ONTAPのドキュメント"ください。

証明書ベースのAPIアクセスのセットアップ

REST APIまたはNetApp Manageability SDK APIによるONTAPへのアクセスでは、ユーザIDとパスワード認証の代わりに、証明書ベースの認証を使用する必要があります。

REST APIの証明書ベースの認証の代わりにを使用し "OAuth 2.0トークンベースの認証"ます）。

次の手順の説明に従って、自己署名証明書を生成してONTAPにインストールできます。

手順

1. OpenSSLを使用して、次のコマンドを実行して証明書を生成します。

```
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'
```

   このコマンドは、というパブリック証明書とという名前の秘密鍵を生成します `test.pem` `key.out`。共通名CNは、ONTAPユーザIDに対応します。

2. 次のコマンドを実行し、プロンプトが表示されたら証明書の内容をONTAPに貼り付けて、パブリック証明書の内容をPrivacy Enhanced Mail（PEM）形式でインストールします。

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

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

3. ONTAPがSSL経由のアクセスをクライアントに許可し、APIアクセスに使用するユーザIDを定義できるようにします。

```
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
```

次の例では、証明書で認証されたAPIアクセスの使用をユーザIDで `cert_user` 有効にしています。ONTAPのバージョンを表示するためにを使用する簡単なManageability SDK Pythonスクリプトは `cert_user` 、次のようになります。

```
#!/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)
```

スクリプトからONTAPのバージョンが出力されます。

```
./version.py

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

4. ONTAP REST APIを使用して証明書ベースの認証を実行するには、次の手順を実行します。
   a. ONTAPで、httpアクセスのユーザIDを定義します。

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

b. Linuxクライアントで、次のコマンドを実行してONTAPバージョンを出力します。

```
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"
        }
    }
}
```

詳細情報

- "NetApp Manageability SDK for ONTAPを使用した証明書ベースの認証"です。

REST APIのONTAP OAuth 2.0トークンベース認証

証明書ベースの認証の代わりに、REST APIにOAuth 2.0トークンベースの認証を使用できます。

ONTAP 9.14.1以降では、Open Authorization（OAuth 2.0）フレームワークを使用してONTAPクラスタへのアクセスを制御するオプションが用意されています。この機能は、ONTAP CLI、System Manager、REST APIなど、ONTAP管理インターフェイスを使用して設定できます。ただし、OAuth 2.0の承認とアクセス制御の決定は、クライアントがREST APIを使用してONTAPにアクセスする場合にのみ適用できます。

OAuth 2.0トークンは、ユーザーアカウント認証用のパスワードを置き換えます。

OAuth 2.0の使用方法の詳細については、を参照してください "OAuth 2.0を使用した認証と許可に関するONTAPドキュメント"。

ログインとパスワードのパラメータ

セキュリティ体制は、組織が規定したポリシーやガイドライン、および組織に適用されるガバナンスや標準に準拠していなければ効果的とはいえません。例としては、ユーザ名の有効期間、パスワードの長さ、使用できる文字、アカウントの保存などの要件があります。ONTAPソリューションには、これらのセキュリティ要素に対応する機能が用意されています。

新しいローカルアカウント機能

組織のユーザーアカウントポリシー、ガイドライン、またはガバナンスを含む標準をサポートするために、ONTAPでは次の機能がサポートされています。

- パスワード ポリシーを設定して最小文字数や大文字小文字の条件を適用する
- ログインに失敗したあとに遅延させる
- アカウントがアクティブでない状態を維持できる最大期間を定義する
- ユーザ アカウントを期限切れにする
- パスワード失効の警告メッセージを表示する
- 無効なログインを通知する

設定可能な設定は、security login role config modifyコマンドを使用して管理します。

SHA-512のサポート

パスワードのセキュリティを強化するために、ONTAP 9ではSHA-2パスワード ハッシュ関数をサポートしており、新規作成または変更されたパスワードのハッシュ化にSHA-512をデフォルトで使用します。必要に応じて、オペレータや管理者がアカウントを期限切れにしたり、ロックしたりすることもできます。

パスワードが変更されていない既存のONTAP 9ユーザアカウントでは、ONTAP 9.0以降へのアップグレード後も引き続きMD5ハッシュ関数が使用されます。ただし、NetAppでは、これらのユーザアカウントをより安全なSHA-512ソリューションに移行し、ユーザにパスワードを変更させることを強く推奨しています。

パスワード ハッシュ機能を使用して、次の作業を実行できます。

- 指定したハッシュ関数に一致するユーザアカウントを表示します。

```
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
```

- 指定したハッシュ関数（MD5など）を使用するアカウントを期限切れにします。これにより、ユーザは次回のログイン時にパスワードを変更する必要があります。

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

- 指定したハッシュ関数を使用するパスワードでアカウントをロックします。

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

クラスタの管理SVMにある内部ユーザのパスワードハッシュ関数が不明 `autosupport` です。これは問題のない問題です。この内部ユーザにはデフォルトでパスワードが設定されていないため、ハッシュ関数は不明です。

  - ユーザのパスワードハッシュ関数を表示するには `autosupport` 、次のコマンドを実行します。

```
::> 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
```

  - パスワードハッシュ関数（デフォルト：SHA512）を設定するには、次のコマンドを実行します。

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

パスワードが何に設定されているかは関係ありません。

```
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
```

パスワードパラメータ

ONTAPでは、組織のポリシーやガイドラインに対応するパスワード パラメータをサポートしています。

属性	説明	デフォルト	範囲
username-minlength	ユーザ名の最小文字数	3.	3-16
username-alphanum	ユーザ名のアルファベットと数字の混在	無効	enabled / disabled
passwd-minlength	パスワードの最大文字数	8	3-64
passwd-alphanum	パスワードのアルファベットと数字の混在	有効	enabled / disabled
passwd-min-special-chars	パスワードに必要な特殊文字の最小数	0	0 ~ 64
passwd-expiry-time	パスワードの有効期限（日数）	unlimited（パスワードは失効しない）	0 -無制限 0 == 直ちに失効
require-initial-passwd-update	初回ログイン時に初期パスワードの更新が必要	無効	enabled / disabled コンソールまたはSSHから変更可能
max-failed-login-attempts	最大失敗回数	0（アカウントをロックしない）	-
lockout-duration	最大ロックアウト期間（日数）	0（アカウントをその日だけロックする）	-
disallowed-reuse	直近のN個のパスワードを許可しない	6.	6以上

属性	説明	デフォルト	範囲
change-delay	次回のパスワード変更までに必要な間隔（日数）	0	-
delay-after-failed-login	失敗したログイン後の再試行間隔（秒数）	4.	-
passwd-min-lowercase-chars	パスワードに必要な小文字の最小数	0（小文字は不要）	0 ~ 64
passwd-min-uppercase-chars	パスワードに必要な大文字の最小数	0（大文字は不要）	0 ~ 64
passwd-min-digits	パスワードに必要な数字の最小数	0（数字は不要）	0 ~ 64
passwd-expiry-warn-time	パスワードの失効何日前に警告を表示するか（日数）	unlimited（パスワードの失効について警告しない）	0（ログインのたびにパスワードの失効について警告）
account-expiry-time	N日後にアカウントの有効期限が切れます	unlimited（アカウントは失効しない）	アクティブでないアカウントが失効となるまでの期間よりも長くする必要がある
account-inactive-limit	アクティブでないアカウントが失効となるまでの期間（日数）	unlimited（アクティブでないアカウントは失効しない）	アカウントの有効期間よりも短くする必要がある

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
```

9.14.1以降では、パスワードの複雑さが増し、ロックアウトルールが追加されました。これは、ONTAPの新規インストールにのみ適用されます。

著作権に関する情報

商標に関する情報