ONTAPセキュリティ強化ガイドライン

ONTAP 9

NetApp
July 19, 2024

目次

ONTAPセキュリティ強化ガイドライン

ONTAPセキュリティ強化の概要

ONTAPには、業界をリードするデータ管理ソフトウェアであるONTAPストレージオペレーティングシステムを強化するための一連の制御機能が用意されています。ONTAPのガイダンスと構成設定を使用して、組織が情報システムの機密性、整合性、可用性に関する所定のセキュリティ目標を達成できるようにします。

現在、進化を続ける脅威から最も価値のある資産であるデータと情報を保護するため、組織は今までに経験したことのない課題に直面しています。日々進化する脅威や脆弱性はますます洗練され、潜在的な侵入者による難読化と偵察の手法の有効性が向上すると同時に、システム管理者はデータと情報のセキュリティにプロアクティブに対処する必要があります。

2024年7月以降、これまでPDFとして公開されていたテクニカルレポートの内容がONTAPの製品ドキュメントに統合されました。ONTAPのセキュリティドキュメントに、_ TR-4569 ：ONTAP _のセキュリティ強化ガイドの内容が追加されました。

ONTAP画像検証

ONTAPには、アップグレード時およびブート時にONTAPイメージが有効であることを確認するメカニズムが用意されています。

アップグレードイメージの検証

コード署名は、無停止イメージ更新または自動無停止イメージ更新、CLI、またはONTAP APIによってインストールされたONTAPイメージがNetAppによって正式に生成され、改ざんされていないことを確認するのに役立ちます。アップグレードイメージの検証はONTAP 9.3で導入されました。

ONTAPのアップグレード時またはリバート時に自動的に適用されます。ユーザは、オプションで最上位レベルの「image.tgz」シグネチャを検証する以外は、これとは異なる処理を行う必要はありません。

ブート時イメージの検証

ONTAP 9.4以降では、NetApp AFF A800、AFF A220、FAS2750、FAS2720システム、およびUEFI BIOSを採用する後続の次世代システムで、Unified Extensible Firmware Interface（UEFI）セキュアブートが有効になります。

電源投入時、ブートローダーによってセキュア ブート キーのホワイトリスト データベースとロードする各モジュールに関連付けられた署名が照合されて検証されます。各モジュールが検証されてロードされると、ONTAPの初期化が実行されます。モジュールが1つでも署名の検証に失敗した場合、システムはリブートします。

これらの項目は、ONTAPイメージおよびプラットフォームBIOSに適用されます。

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

属性	説明	デフォルト	範囲
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
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。

システムカンリホウホウ

これらは、ONTAPシステム管理を強化するための重要なパラメータです。

コマンドラインアクセス

ソリューションの安全性を守るには、システムとの間にセキュアなアクセスを確立することが重要です。コマンドライン アクセスの最も一般的なオプションとしては、SSH、Telnet、RSHがあります。このうちで最も安全なのがSSHであり、リモート コマンドライン アクセス用の業界標準のベストプラクティスとなっています。ONTAPソリューションへのコマンドライン アクセスにはSSHを使用することを強く推奨します。

SSHセツテイ

`security ssh show`コマンドは、クラスタおよびSVMの
SSH鍵交換アルゴリズム、暗号、およびMACアルゴリズムの設定を表示します。鍵交換方式は、これらのアルゴリズムと暗号を使用して、暗号化や認証用の1回限りのセッション
キーの生成方法、およびサーバ認証の実行方法を指定します。

```
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.
```

ロクインハナ

ログイン バナーを使用すると、すべてのオペレータと管理者、さらには不正ユーザにも、システムの利用条件を提示することができます。また、誰がシステムへのアクセスを許可されているかを伝えることもできます。ログイン バナーは、システムに求められるアクセス方法や使用方法を確立するのに役立ちます。
`security login banner modify`コマンドは、ログインバナーを変更します。ログイン バナーは、SSHおよびコンソール デバイスのログイン プロセスで認証ステップの直前に表示されます。バナーのテキストは次の例のように二重引用符（“ ”）で囲む必要があります。

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

ログインバナーのパラメータ

パラメータ	説明
vserver	このパラメータを使用して、バナーを変更するSVMを指定します。クラスタ レベルのメッセージを変更する場合は、クラスタ管理SVMの名前を使用します。クラスタ レベルのメッセージは、メッセージが定義されていないデータSVM用のデフォルトとして使用されます。

パラメータ	説明
`message`	（オプション）このパラメータは、ログインバナーメッセージを指定します。クラスタにログイン バナー メッセージが設定されている場合、データSVMにもクラスタのログイン バナーが使用されます。データSVMのログインバナーを設定すると、クラスタのログインバナーは表示されません。データSVMのログインバナーでクラスタのログインバナーを使用するようにリセットするには、このパラメータに値を指定します。 このパラメータを使用する場合、ログイン バナーに改行（EOL）を含めることはできません。改行付きのログインバナーメッセージを入力する場合は、パラメータを指定しないでください。そうすると、メッセージを入力するためのプロンプトが表示されます。対話形式で入力されたメッセージには改行を含めることができます。 非ASCII文字にはUnicode UTF-8形式を使用する必要があります。
`uri`	`(ftp
http):///(hostname	IPv4` このパラメータを使用して、ログイン バナーのダウンロード元のURIを指定します。 メッセージの長さは2048バイトを超えてはなりません。ASCII以外の文字はUnicode UTF-8で指定する必要があります。

Message Of The Day

コマンドは、 `security login motd modify` Message Of The Day（MOTD；本日のメッセージ）を更新します。

MOTDには、クラスタ レベルのMOTDとデータSVMレベルのMOTDの2種類があります。データSVMのクラスタシェルにログインしたユーザには、クラスタレベルのMOTDに続いて、そのSVMに対するSVMレベルのMOTDが表示されることがあります。

クラスタ管理者は、クラスタ レベルのMOTDを必要に応じてSVM単位で有効または無効にできます。クラスタ管理者がSVMでクラスタ レベルのMOTDを無効にした場合、そのSVMにログインしたユーザにはクラスタレベルのメッセージは表示されません。クラスタレベルのメッセージを有効または無効にできるのは、クラスタ管理者だけです。

MOTDパラメータ	説明
SVM	このパラメータを使用して、MOTDを変更するSVMを指定します。クラスタ レベルのメッセージを変更する場合は、クラスタ管理SVMの名前を使用します。

MOTDパラメータ	説明
メッセージ	（オプション）このパラメータを使用すると、メッセージを指定できます。このパラメータを使用する場合、MOTDに改行を含めることはできません。パラメータ以外のパラメータを指定しない場合は `-vserver` 、メッセージを対話型モードで入力するように求められます。対話形式で入力されたメッセージには改行を含めることができます。ASCII以外の文字はUnicode UTF-8で指定する必要があります。メッセージには、次のエスケープ シーケンスを使用して、動的に生成される内容を含めることもできます。 • `\\` - 1つのバックスラッシュ文字 • `\b` -出力なし（Linuxとの互換性のためのみサポート） • `\C` -クラスタ名 • `\d` -ログインしたノードの現在の日付 • `\t` -ログインしたノードの現在の時刻 • `\I` -受信LIFのIPアドレス（ログインの場合は「console」と出力 `console` ） • `\l` -ログインしたデバイス名（ログインの場合はconsoleと出力 `console` ） • `\L` -ユーザによるクラスタ内のノードへの前回のログイン • `\m` -マシンアーキテクチャ • `\n` -ノードまたはデータSVMの名前 • `\N` -ログインしているユーザの名前 • `\o` -\Oと同じ。Linuxとの互換性を考慮して提供 • `\O` -ノードのDNSドメイン名。出力はネットワーク構成によって異なり、空になる場合もあり • `\r` -ソフトウェアリリース番号 • `\s` -オペレーティングシステム名 • `\u` -ローカルノードのアクティブなクラスタシェルセッションの数。クラスタ管理者の場合：すべてのクラスタシェルユーザ。データSVM管理の場合はそのデータSVMのアクティブなセッションのみが含まれる • `\U` -と同じ `\u` `` ですが、またはが付加されています。 `user users` • `\v` -有効なクラスタバージョン文字列 • `\W` -ログインしているユーザのクラスタ全体でのアクティブなセッション (`who`)

ONTAPでのMessage Of The Dayの設定の詳細については、を参照してください "Message Of The Dayに関するONTAPのドキュメント"。

CLIセツシヨンタイムアウト

CLIセッションのデフォルトのタイムアウトは30分です。タイムアウトは古いセッションやセッションのピギーバックを防ぐために重要です。

現在のCLIセッションタイムアウトを表示するには、コマンドを使用し `system timeout show` ます。タイムアウト値を設定するには、コマンドを使用し `system timeout modify -timeout <minutes>` ます。

NetApp ONTAP System ManagerによるWebアクセス

ONTAP管理者がCLIではなくグラフィカル インターフェイスを使用してクラスタにアクセスして管理するには、NetApp ONTAP System Managerを使用します。System ManagerはWebサービスとしてONTAPに搭載されており、デフォルトで有効になっていて、ブラウザからアクセスできます。DNSまたはIPv4またはIPv6アドレスを使用している場合は、ブラウザでホスト名を指定し `https://cluster-management-LIF`ます。

自己署名デジタル証明書がクラスタで使用されている場合、信頼されていない証明書であることを示す警告がブラウザに表示されることがあります。危険を承諾してアクセスを続行するか、認証局（CA）の署名のあるデジタル証明書をクラスタにインストールしてサーバを認証します。

ONTAP 9.3以降では、Security Assertion Markup Language（SAML）認証はONTAP System Managerのオプションです。

ONTAP System ManagerのSAML認証

SAML 2.0は広く採用されている業界標準で、SAMLに準拠したサードパーティのアイデンティティプロバイダ（IdP）が、企業が選択したIdP固有のメカニズムを使用してシングルサインオン（SSO）のソースとしてMFAを実行できるようにします。

SAML仕様では、プリンシパル、IdP、サービスプロバイダの3つのロールが定義されています。ONTAP環境の場合、プリンシパルは、ONTAP System ManagerまたはNetApp Active IQ Unified Managerを通じてONTAPにアクセスするクラスタ管理者です。IdPはサードパーティのIdPソフトウェアです。ONTAP 9.3以降では、Microsoft Active Directoryフェデレーションサービス（ADFS）とオープンソースのシボレスIdPがサポートされます。ONTAP 9.12.1以降では、Cisco Duoがサポートされています。サービスプロバイダは、ONTAPに組み込まれているSAML機能で、ONTAP System ManagerまたはActive IQ Unified Manager Webアプリケーションで使用されます。

SSHの2要素設定プロセスとは異なり、SAML認証をアクティブ化すると、ONTAP System ManagerまたはONTAPサービス プロセッサのアクセスでは既存のすべての管理者にSAML IdPによる認証が要求されます。クラスタ ユーザ アカウントへの変更は必要ありません。SAML認証を有効にすると、およびアプリケーションの管理者ロールを持つ既存のユーザに新しい認証方式が `saml` 追加され `http ontapi` ます。

SAML認証を有効にしたあとに、アプリケーションおよびアプリケーションに対して、SAML IdPアクセスを必要とする追加のアカウントを管理者ロールとSAML認証方式でONTAPで定義する必要があります `http ontapi` 。ある時点でSAML認証が無効になった場合、新しいアカウントに認証方式を定義し、およびアプリケーション用の管理者ロールを割り当て、ローカルONTAP認証用のコンソールアプリケーションをONTAP System Managerに追加する必要があります `password http ontapi` 。

SAML IdPを有効にすると、IdPは、Lightweight Directory Access Protocol（LDAP）、Active Directory（AD）、Kerberos、パスワードなど、IdPで使用可能な方式を使用してONTAP System Managerへのアクセスの認証を実行します。使用可能な方式はIdPごとに異なります。ONTAPで設定したアカウントのユーザIDがIdPの認証方式に対応していることが重要になります。

NetAppによって検証されたIdPは、Microsoft ADFS、Cisco Duo、およびオープンソースのShibboleth IdPです。

ONTAP 9.14.1以降では、Cisco DuoをSSHの2番目の認証ファクターとして使用できます。

ONTAP System Manager、Active IQ Unified Manager、およびSSHの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』"。

ONTAP System Managerの分析情報

ONTAP 9.11.1以降のONTAP System Managerには、クラスタ管理者が日常的なタスクを合理化するための分析情報が用意されています。セキュリティに関する分析情報は、このテクニカルレポートの推奨事項に基づいています。

セキュリティインサイト	決定
Telnetが有効	NetAppでは、セキュアなリモートアクセスにセキュアシェル（SSH）を推奨しています。
Remote Shell（RSH；リモートシェル）が有効	NetAppでは、セキュアなリモートアクセスにSSHを推奨しています。
AutoSupportでセキュアでないプロトコルが使用されています	AutoSupportは、LINK:HTTPS経由で送信されるように設定されていません。
クラスタレベルでログインバナーが設定されていません	警告：クラスタにログインバナーが設定されていません。
SSH でセキュアでない暗号を使用	SSHでセキュアでない暗号が使用されている場合の警告。
設定されているNTPサーバが少なすぎます	Warning：設定されているNTPサーバの数が3つ未満の場合。
デフォルトの管理ユーザがロックされていない	デフォルトの管理アカウント（adminまたはdiag）を使用してSystem Managerにログインしない場合、それらのアカウントがロックされていないときは、ロックすることを推奨します。
ランサムウェア対策—ボリュームにSnapshotポリシーがない	適切なSnapshotポリシーが1つ以上のボリュームに関連付けられていません。
ランサムウェア対策—Snapshotの自動削除を無効にする	Snapshotの自動削除が1つ以上のボリュームに対して設定されています。
ボリュームはランサムウェア攻撃に対して監視されていない	自律型ランサムウェア対策は複数のボリュームでサポートされていますが、まだ設定されていません。
SVMに自律型ランサムウェア対策が設定されていない	自律型ランサムウェア対策は、いくつかのSVMでサポートされますが、まだ設定されていません。
ネイティブFPolicyが設定されていない	NAS SVMに対してはFPolicyが設定されません。
自律型ランサムウェア対策アクティブモードを有効にする	複数のボリュームがラーニングモードを完了しました。アクティブモードをオンにすることができます。
FIPS 140-2へのグローバルな準拠が無効になっている	グローバルなFIPS 140-2準拠が有効になっていません。
通知用のクラスタが設定されていません	Eメール、Webhook、またはSNMPトラップホストは、通知を受信するように設定されていません。

ONTAP System Managerのインサイトの詳細については、を参照して "ONTAP System Managerインサイトドキュメント"ください。

ONTAP自律型ランサムウェア対策

ONTAPの自律型ランサムウェア対策は、ストレージワークロードのセキュリティに関するユーザ行動分析を補完するために、ボリュームのワークロードとエントロピーを分析してランサムウェアを検出し、Snapshotを作成して攻撃の疑いがある場合に管理者に通知します。

ONTAP 9.10.1では、NetApp Cloud Insights / Cloud SecureおよびNetApp FPolicyパートナーエコシステムを使用した外部FPolicyユーザ行動分析（UBA）を使用したランサムウェアの検出と防止に加えて、自律型ランサムウェア対策も導入されています。ONTAP自律型ランサムウェア対策は、組み込みの機械学習（ML）機能を使用して、ボリュームワークロードのアクティビティとデータエントロピーを監視し、ランサムウェアを自動的に検出します。UBAとは異なるアクティビティを監視し、UBAではない攻撃を検出できるようにします。

この機能の詳細については、またはを参照して "TR-4572：『The NetApp Solution for Ransomware』" "ONTAP自律型ランサムウェア対策に関するドキュメント"ください。

ストレージ管理システムの監査

ONTAPイベントをリモートsyslogサーバにオフロードして、イベント監査の整合性を確保します。このサーバは、Splunkなどのセキュリティ情報イベント管理システムである可能性があります。

syslogを送信

ログや監査情報は、サポートやシステム可用性の観点から組織に欠かせません。また、ログ（syslog）や監査レポート、出力結果には、通常、取り扱いに注意を要する情報が含まれています。セキュリティのコントロールと体制を維持するためには、ログと監査データをセキュアな方法で管理することが必要です。

違反の範囲やフットプリントを単一のシステムまたはソリューションに限定するには、syslog情報のオフロードが必要です。そのため、NetAppでは、syslog情報を安全なストレージまたは保持場所に安全にオフロードすることを推奨しています。

ログの転送先を作成する

リモートロギングのログ転送先を作成するには、コマンドを使用し `cluster log-forwarding create` ます。

パラメータ

コマンドを設定するには、次のパラメータを使用し `cluster log-forwarding create` ます。

- *デスティネーションホスト*ログの転送先サーバのホスト名、IPv4アドレス、またはIPv6アドレスを指定します。

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

- *宛先ポート*転送先サーバがリスンするポートを指定します。

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

- *ログ転送プロトコル。*転送先へのメッセージの送信に使用するプロトコルを指定します。

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

ログ転送プロトコルには、次のいずれかの値を指定できます。

  - `udp-unencrypted`です。User Datagram Protocol、セキュリティなし。
  - `tcp-unencrypted`です。TCP、セキュリティなし。
  - `tcp-encrypted`です。TCP、Transport Layer Security（TLS）を使用。

- *宛先サーバーIDを確認します。*このパラメータをtrueに設定すると、証明書を検証してログの転送先の識別情報が確認されます。この値をtrueに設定できるのは、protocolフィールドで値が選択されている場合だけ `tcpencrypted` です。

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

- * Syslogファシリティ。*転送対象のログに使用するsyslog機能を指定します。

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

- *接続テストをスキップします。*通常、この `cluster log-forwarding create` コマンドは、Internet Control Message Protocol（ICMP）pingを送信して宛先に到達できるかどうかを確認し、到達できない場合は失敗します。この値をに設定する `true` と、pingチェックが省略され、到達不能なデスティネーションを設定できるようになります。

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

NetAppでは、コマンドを使用してタイプへの接続を強制することを推奨しています `cluster log-forwarding -tcp-encrypted` 。

イベント通知

システムから送信される情報とデータを保護することは、システムのセキュリティ体制を維持および管理するために不可欠です。ONTAPソリューションで生成されるイベントは、ソリューションで発生している状況や処理されている情報など、豊富な情報を提供します。このデータは非常に重要なものであり、安全な方法で管理および移行する必要があります。

コマンドは `event notification create` 、イベントフィルタで定義した一連のイベントの新しい通知を1つ以上の通知先に送信します。次の例は、イベント通知の設定と、設定されているイベント通知フィルタと送信先を表示するコマンドを示して `event notification show` います。

```
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
```

ストレージ暗号化

ディスクが盗難、返却、転用された場合に機密データを保護するには、ハードウェアベースのNetAppストレージ暗号化またはソフトウェアベースのNetAppボリューム暗号化/ネットアップアグリゲート暗号化を使用してください。どちらのメカニズムもFIPS-140-2検証済みであり、ハードウェアベースのメカニズムとソフトウェアベースのメカニズムを使用する場合、このソリューションはCommercial Solutions for Classified（CSfC）Programの対象となります。ハードウェアレイヤとソフトウェアレイヤの両方に保存されている機密データと最高機密データのセキュリティ保護を強化できます。

保管データの暗号化は、ディスクが盗難、返却、転用された場合に機密データを保護するために重要です。

ONTAP 9には、連邦情報処理標準（FIPS）140-2に準拠した保管データ暗号化ソリューションが3つあります。

- NetAppストレージ暗号化（NSE）は、自己暗号化ドライブを使用するハードウェアソリューションです。
- NetApp Volume Encryption（NVE）は、ボリュームごとに一意のキーを使用して、あらゆるタイプのドライブのあらゆるデータ ボリュームを暗号化できるソフトウェア ソリューションです。
- NetApp Aggregate Encryption（NAE）は、アグリゲートごとに一意のキーを使用して、あらゆるタイプのドライブのあらゆるデータ ボリュームを暗号化できるソフトウェア ソリューションです。

NSE、NVE、NAEは、外部キー管理またはオンボードキーマネージャ（OKM）のいずれかを使用できます。NSE、NVE、およびNAEを使用しても、ONTAPのストレージ効率化機能には影響はありません。ただし、NVEボリュームはアグリゲート重複排除の対象外です。NAEボリュームはアグリゲート重複排除の対象であり、重複排除のメリットが得られます。

OKMは、NSE、NVE、またはNAEを使用した保存データに対する自己完結型の暗号化ソリューションです。

NVE、NAE、OKMでは、ONTAP CryptoModが使用されます。CryptoModは、CMVP FIPS 140-2の検証済みモジュールのリストに表示されています。を参照して "FIPS 140-2証明書番号4144"

OKMの設定を開始するには、コマンドを使用し `security key-manager onboard enable` ます。外部のKey Management Interoperability Protocol（KMIP）キー管理ツールを設定するには、コマンドを使用し `security key-manager external enable` ます。ONTAP 9.6以降では、外部キー マネージャでマルチテナンシーがサポートされます。パラメータを使用し `-vserver <vserver name>` て、特定のSVMで外部キー管理を有効にします。9.6より前のバージョンでは `security key-manager setup` 、コマンドを使用してOKMと外部キーマネージャの両方を設定していました。オンボード キー管理の場合、オペレータや管理者は、このコマンドの指示に従ってパスフレーズやOKMのその他のパラメータを順に設定できます。

以下はその一部です。

```
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.
```

ONTAP 9.4以降では、でtrueオプションを使用して、リブート後にユーザにパスフレーズの入力を求めることができます `-enable-cc-mode` `security key-manager setup` 。ONTAP 9.6以降では、コマンド構文はです `security key-manager onboard enable -cc-mode-enabled yes`。

ONTAP 9.4以降では、advanced権限で機能を使用して、NVE対応ボリュームのデータを無停止で「スクラビング」でき `secure-purge` ます。暗号化されたボリュームのデータをスクラビングすると、物理メディアからもリカバリできなくなります。次のコマンドは、SVM vs1のvol1にある削除済みファイルを安全にパージします。

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

ONTAP 9.7以降では、VEライセンスが設定されていて、OKMまたは外部キー管理ツールが設定されていてNSEが使用されていない場合、NAEとNVEがデフォルトで有効になります。NAEアグリゲートにはNAEボリュームがデフォルトで作成され、NAE以外のアグリゲートにはNVEボリュームがデフォルトで作成されます。これを無効にするには、次のコマンドを入力します。

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

ONTAP 9.6以降では、SVMスコープを使用して、クラスタ内のデータSVMに対して外部キー管理を設定できます。この方法は、各テナントが異なるSVM（または一連のSVM）を使用してデータを提供するマルチテナント環境に最適です。特定のテナントのSVM管理者のみが、そのテナントのキーにアクセスできます。詳細については、ONTAPのドキュメントのを参照してください "ONTAP 9.6以降で外部キー管理を有効にする" 。

ONTAP 9.11.1以降では、SVMでプライマリキーサーバとセカンダリキーサーバを指定することで、クラスタ化された外部キー管理サーバへの接続を設定できます。詳細については、ONTAPのドキュメントのを参照してください "クラスタ化された外部キーサーバの設定" 。

ONTAP 9.13.1以降では、System Managerで外部キー管理サーバを設定できます。詳細については、ONTAPのドキュメントのを参照してください "外部キー管理ツールを管理します。" 。

データレプリケーションの暗号化

保存データの暗号化を補うために、SnapMirror、SnapVault、またはFlexCacheの事前共有キーを使用して、TLS 1.2を使用してクラスタ間のONTAPデータレプリケーショントラフィックを暗号化できます。

ディザスタリカバリ、キャッシュ、またはバックアップのためにデータをレプリケートする場合は、ONTAPクラスタ間でネットワークを介して転送するときに、そのデータを保護する必要があります。これにより、転送中の機密データに対する悪意のある中間者攻撃を防ぐことができます。

ONTAP 9.6以降では、クラスタピアリング暗号化によって、SnapMirror、SnapVault、FlexCacheなどのONTAPデータレプリケーション機能でTLS 1.2 AES-256 GCM暗号化がサポートされます。暗号化は、2つのクラスタピア間で事前共有キー（PSK）を使用してセットアップされます。

NSE、NVE、NAEなどのテクノロジを使用して保存データを保護している場合は、ONTAP 9.6以降にアップグレードしてクラスタ ピアリング暗号化を使用すると、エンドツーエンドのデータ暗号化も実装できます。

クラスタ ピアリング暗号化では、クラスタ ピア間のすべてのデータが暗号化されます。たとえば、SnapMirrorを使用している場合、ソース クラスタとデスティネーション クラスタのピア間のすべてのピアリング情報とすべてのSnapMirror関係が暗号化されます。クラスタ ピアリング暗号化が有効な場合、クラスタ ピア間でクリアテキストのデータを送信することはできません。

ONTAP 9.6以降では、新しいクラスタピア関係で暗号化がデフォルトで有効になっています。ONTAP 9.6より前に作成されたクラスタピア関係で暗号化を有効にするには、ソースクラスタとデスティネーションクラスタを9.6にアップグレードする必要があります。また、コマンドを使用して、クラスタピアリング暗号化を使用するようにソースとデスティネーション両方のクラスタピアを変更する必要があり `cluster peer modify` ます。

次の例に示すように、ONTAP 9.6でクラスタピアリング暗号化を使用するように既存のピア関係を変換できます。

```
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転送中データの暗号化

データレプリケーショントラフィックにNetApp Storage Encryption（NSE）やNetApp Volume Encryption（NVE）やクラスタピアリング暗号化（CPE）などの保存データ暗号化テクノロジを使用しているお客様は、ONTAP 9.8以降にアップグレードして次を使用することで、ハイブリッドマルチクラウドデータファブリック全体でクライアントとストレージの間でエンドツーエンドの暗号化を使用できるようになりました。 IPSec ：IPSecは、NFS暗号化またはSMB / CIFS暗号化の代替手段であり、iSCSIトラフィックの唯一の転送中暗号化オプションです。

状況によっては、ネットワークを介してONTAP SVMに転送される（または転送中の）すべてのクライアントデータの保護が必要になることがあります。これにより、転送中の機密データに対するリプレイや悪意のある中間者攻撃を防ぐことができます。

ONTAP 9.8以降では、インターネットプロトコルセキュリティ（IPsec）で、クライアントとONTAP SVMの間のすべてのIPトラフィックをエンドツーエンドで暗号化できます。すべての IP トラフィックの IPSec データ暗号化には、 NFS 、 iSCSI 、 SMB/CIFS の各プロトコルが含まれます。IPSecは、iSCSIトラフィックに対して唯一の転送中暗号化オプションを提供します。

ネットワークを介したNFS暗号化は、IPsecの主なユースケースの1つです。ONTAP 9.8より前のバージョンでは、ネットワーク上でのNFS暗号化では、krb5pを使用して転送中のNFSデータを暗号化するためにKerberosのセットアップと設定が必要でした。これは、すべてのお客様の環境で、必ずしも簡単ではありません。

データレプリケーショントラフィックにNetApp Storage Encryption（NSE）やNetApp Volume Encryption（NVE）やクラスタピアリング暗号化（CPE）などの保存データ暗号化テクノロジを使用しているお客様は、ONTAP 9.8以降にアップグレードして次を使用することで、ハイブリッドマルチクラウドデータファブリック全体でクライアントとストレージの間でエンドツーエンドの暗号化を使用できるようになりました。 IPSec ：

IPSecはIETF標準です。ONTAPはトランスポートモードでIPsecを使用します。また、Internet Key Exchange（IKE;インターネットキー交換）プロトコルバージョン2も利用します。IKEプロトコルバージョン2では、事前共有キー（PSK）を使用して、クライアントとONTAP間でIPv4またはIPv6のいずれかでキー素材をネゴシエートします。デフォルトでは、IPsecはSuite-B AES-GCM 256ビット暗号化を使用します。Suite-B AES-GMAC256およびAES-CBC256（256ビット暗号化）もサポートされています。

IPSec機能はクラスタで有効にする必要がありますが、Security Policy Database（SPD；セキュリティポリシーデータベース）エントリを使用して個 々 のSVMのIPアドレスに適用されます。ポリシー（SPD）エントリには、クライアントIPアドレス（リモートIPサブネット）、SVM IPアドレス（ローカルIPサブネット）、使用する暗号スイート、およびIKEv2を介した認証とIPsec接続の確立に必要な事前共有シークレット（PSK）が含まれます。IPsecポリシーエントリに加えて、トラフィックがIPsec接続を通過する前に、クライアントに同じ情報（ローカルおよびリモートIP、PSK、および暗号スイート）を設定する必要があります。ONTAP 9.10.1以降では、IPsec証明書認証のサポートが追加されています。これにより、IPsecポリシーの制限がなくなり、Windows OSでIPsecがサポートされるようになります。

クライアントとSVMのIPアドレスの間にファイアウォールがある場合は、IKEv2ネゴシエーションが成功し、IPsecトラフィックが許可されるように、ESPおよびUDP（ポート500および4500）プロトコル（インバウンド（入力）とアウトバウンド（出力）の両方）を許可する必要があります。

NetApp SnapMirrorおよびクラスタピアリングトラフィックの暗号化では、引き続きIPSecよりもクラスタピアリング暗号化（CPE）が推奨され、ネットワークを介してセキュアに転送されます。CPEは、IPsecよりもこれらのワークロードに対して優れたパフォーマンスを発揮します。IPsecのライセンスは必要ありません。また、輸出入に関する制限もありません。

次の例に示すように、クラスタでIPSecを有効にし、単一のクライアントおよび単一のSVM IPアドレスに対してSPDエントリを作成できます。

```
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とSSLの管理

コントロールプレーンインターフェイスのFIPS 140-2 / 3準拠モードを有効にするには、ONTAPコマンドでパラメータをtrueに設定し `is-fips-enabled` `security config modify` ます。

ONTAP 9以降では、クラスタ全体のコントロールプレーンインターフェイスに対してFIPS 140-2準拠モードを有効にすることができます。デフォルトでは、FIPS 140-2のみのモードは無効になっています。FIPS 140-2準拠モードを有効にするには、コマンドのパラメータをに設定し `is-fips-enabled` `true` `security config modify` ます。その後、を使用してオンラインステータスを確認できます `security config show command` 。

FIPS 140-2への準拠を有効にすると、TLSv1とSSLv3は無効になり、TLSv1.1とTLSv1.2のみが引き続き有効になります。ONTAPでは、FIPS 140-2への準拠が有効な場合、TLSv1とSSLv3を有効にすることはできません。FIPS 140-2を有効にし、そのあとに無効にした場合、TLSv1とSSLv3は無効なままになりますが、以前の設定に応じて、TLSv1.2またはTLSv1.1とTLSv1.2の両方が有効なままになります。

コマンドは `security config modify` 、クラスタ全体の既存のセキュリティ設定を変更します。FIPS準拠モードを有効にしたクラスタでは、自動的にTLSプロトコルのみが選択されます。パラメータを使用する

`-supported-protocols` と、FIPSモードとは関係なくTLSプロトコルを追加または除外できます。デフォルトではFIPSモードは無効で、ONTAPはTLSv1.2、TLSv1.1、およびTLSv1の各プロトコルをサポートします。

下位互換性を維持するため、ONTAPでは、FIPSモードが無効な場合にSSLv3をリストに追加できます `supported-protocols`。パラメータを使用し `-supported-cipher-suites` て、Advanced Encryption Standard（AES）またはAESと3DESのみを設定します。「!RC4」のように指定してRC4などの弱い暗号を無効にすることもできます。デフォルトでは、サポートされる暗号設定はです `ALL:!LOW:!aNULL:!EXP:!eNULL`。この設定では、認証なし、暗号なし、エクスポートなし、および弱い暗号化の暗号スイートを除く、プロトコルに対してサポートされるすべての暗号スイートが有効になります。64ビットまたは56ビットの暗号化アルゴリズムを使用するスイートが当てはまります。

選択したプロトコルで使用可能な暗号スイートを選択してください。設定が無効な場合、一部の機能が適切に動作しなくなる可能性があります。

正しい暗号文字列構文については、OpenSSL（OpenSSLソフトウェア財団が公開）のページを参照してください "アンコウ" 。ONTAP 9.9.1以降のリリースでは、セキュリティ設定の変更後にすべてのノードを手動でリブートする必要がなくなりました。

FIPS 140-2への準拠を有効にすると、ONTAP 9内外の他のシステムや通信に影響します。コンソール アクセスが可能な非本番環境のシステムで、これらの設定をテストすることを強く推奨します。

> ONTAP 9の管理にSSHを使用する場合は、OpenSSH 5.7以降のクライアントを使用する必要があります。SSHクライアントは、接続を成功させるために、Elliptic Curve Digital Signature Algorithm（ECDSA）公開鍵アルゴリズムとネゴシエートする必要があります。

TLSセキュリティは、TLS 1.2のみを有効にし、Perfect Forward Secrecy（PFS）対応の暗号スイートを使用することで、さらに強化できます。PFSは鍵交換の方法で、TLS 1.2などの暗号化プロトコルと組み合わせて使用すると、攻撃者がクライアントとサーバ間のすべてのネットワークセッションを復号化するのを防ぐことができます。TLS 1.2およびPFS対応の暗号スイートのみを有効にするには、次の例に示すように、advanced権限レベルでコマンドを使用します `security config modify`。

> SSLインターフェイス設定を変更する前に、クライアントがONTAPに接続するときに、前述の暗号（DHE、ECDHE）をサポートしている必要があることに注意してください。それ以外の場合、接続は許可されません。

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

プロンプトごとに確認し `y` ます。PFSの詳細については、を参照してください "このNetAppブログ"。

ONTAP 9.11.1およびTLS 1.3のサポート以降では、FIPS 140-3を検証できます。

> FIPSの設定は、ONTAPとプラットフォームBMCに適用されます。

CA署名デジタル証明書の作成

ONTAP Webアクセス用の自己署名デジタル証明書が、組織の情報セキュリティ ポリシーに準拠していないことは珍しくありません。本番用システムでは、NetAppのベストプラクティスとしてCA署名デジタル証明書をインストールし、クラスタまたはSVMをSSLサーバとして認証する際に使用することを推奨します。

コマンドを使用して証明書署名要求（CSR）を生成し、コマンドを使用してCAから返された証明書をインストールできます `security certificate generate-csr` `security certificate install` 。

手順

1. 組織のCAによって署名されたデジタル証明書を作成するには、次の手順を実行します。
   a. CSRを生成します。
   b. 組織の手順に従って、組織のCAからCSRを使用してデジタル証明書を要求します。たとえば、Microsoft Active Directory証明書サービスWebインターフェイスを使用してに移動し `<CA_server_name>/certsrv` 、証明書を要求します。
   c. デジタル証明書をONTAPにインストールします。

オンライン証明書ステータスプロトコル

Online Certificate Status Protocol（OCSP）を有効にすると、TLS通信（LDAP、TLSなど）を使用するONTAPアプリケーションがデジタル証明書のステータスを受信できるようになります。アプリケーションは、要求した証明書が「有効」、「失効」、「不明」のどのステータスであるかを示す署名済みの応答を受け取ります。

OCSPを使用すると、証明書失効リスト（CRL）がなくてもデジタル証明書の現在のステータスを特定することができます。

デフォルトでは、OCSPによる証明書のステータスチェックは無効になっています。オンにするには、コマンドを使用し `security config ocsp enable -app name`ます。アプリケーション名は `autosupport`、、 `audit_log` `fabricpool`、、 `ems` `kmip`、、 `ldap_ad` `ldap_nis_namemap`、またはall。このコマンドにはadvanced権限レベルが必要です。

SSHv2の管理

コマンドは `security ssh modify` 、クラスタまたはSVMのSSH鍵交換アルゴリズム、暗号、またはMACアルゴリズムの既存の設定を、指定した設定で置き換えます。

NetAppの推奨事項は次のとおりです。

- ユーザ セッションにはパスワードを使用する。
- マシン アクセスには公開鍵を使用する。

サポートされる暗号とキー交換

暗号	キー交換
aes256-ctr	diffie-hellman-group-exchange-sha256（SHA-2）
aes192-ctr	diffie-hellman-group-exchange-sha1（SHA-1）
aes128-ctr	diffie-hellman-group14-sha1（SHA-1）
aes256-cbc	diffie-hellman-group1-sha1（SHA-1）
aes192-cbc	-
aes128-cbc	-
aes128-gcm	-
aes256-gcm	-
3des-cbc	-

サポートされる**AES**および**3DES**対称暗号化

ONTAPでは、次のタイプのAESおよび3DESの対称暗号化（暗号）もサポートしています。

- 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管理設定は、ONTAPおよびプラットフォームBMCに適用されます。

NetApp AutoSupport

ONTAPのAutoSupport機能を使用すると、システムの健全性をプロアクティブに監視し、NetAppテクニカルサポート、組織内のサポートチーム、またはサポートパートナーにメッセージと詳細を自動的に送信できます。ストレージシステムの初回設定時には、NetAppテクニカルサポートへのAutoSupportメッセージがデフォルトで有効になります。また、AutoSupportは有効になってから24時間後にNetAppテクニカルサポートへのメッセージ送信を開始します。この24時間という設定は変更可能です。組織の社内サポートチームとのコミュニケーションを活用するには、メールホストの設定が完了している必要があります。

AutoSupportを管理（設定）できるのはクラスタ管理者だけです。SVM管理者にはAutoSupportへのアクセス権はありません。AutoSupport機能は無効にできます。ただし、NetAppでは、AutoSupportを有効にすることを推奨しています。これは、ストレージシステムで問題が発生した場合に、迅速に問題を特定して解決できるためです。デフォルトでは、AutoSupportを無効にした場合でも、AutoSupport情報は収集されてローカルに格納されます。

さまざまなメッセージに含まれる内容や、さまざまな種類のメッセージが送信される場所など、AutoSupportメッセージの詳細については、ドキュメントを参照して "NetApp Active IQ Digital Advisor" ください。

AutoSupportメッセージには、次のような機密データが含まれます。

- ログファイル
- 特定のサブシステムについての状況に応じたデータ
- 設定データおよびステータスデータ
- パフォーマンスデータ

AutoSupportでは、転送プロトコルとしてHTTPS、HTTP、およびSMTPがサポートされます。AutoSupportメッセージは機密性が高いため、NetAppでは、AutoSupportメッセージをNetAppサポートに送信するためのデフォルトの転送プロトコルとしてHTTPSを使用することを強く推奨します。

また、コマンドを使用して、AutoSupportデータのターゲット（NetAppテクニカルサポート、組織内の業務、パートナーなど）を指定する必要があります `system node autosupport modify`。このコマンドでは、AutoSupportで送信する内容（パフォーマンス データやログ ファイルなど）も指定できます。

AutoSupportを完全に無効にするには、コマンドを使用し `system node autosupport modify -state disable` ます。

Network Time Protocol の略

ONTAPではクラスタのタイムゾーン、日付、および時刻を手動で設定できますが、クラスタ時間を3つ以上の外部NTPサーバと同期するようにネットワークタイムプロトコル（NTP）サーバを設定する必要があります。

クラスタ時間が不正確だと問題が発生する可能性があります。ONTAPではクラスタのタイム ゾーン、日付、時刻を手動で設定できますが、ネットワーク タイム プロトコル（NTP）サーバを設定してクラスタ時間を外部のNTPサーバと同期する必要があります。

ONTAP 9.5 以降では、対称認証を使用して NTP サーバを設定できます。

コマンドを使用すると、最大10台の外部NTPサーバを関連付けることができます `cluster time-service ntp server create` 。タイムサービスの冗長性と品質を高めるには、少なくとも3台の外部NTPサーバをクラスタに関連付ける必要があります。

ONTAPでのNTPの設定の詳細については、を参照してください "クラスタ時間の管理（クラスタ管理者のみ）"。

NASファイルシステムのローカルアカウント（CIFSワークグループ）

ワークグループによるクライアント認証は、従来のドメイン認証の仕組みに反しないセキュリティ レイヤをONTAPソリューションに追加します。IP情報、認証メカニズム、プロトコルバージョン、認証タイプなど、ポスチャ関連の詳細情報を多数表示するには、コマンドを使用し `vserver cifs session show` ます。

ONTAP 9以降では、ローカルで定義されたユーザとグループを使用してサーバに認証するCIFSクライアントを含むワークグループ内にCIFSサーバを設定できます。ワークグループによるクライアント認証は、従来のドメイン認証の仕組みに反しないセキュリティ レイヤをONTAPソリューションに追加します。CIFSサーバを設定するには、コマンドを使用し `vserver cifs create` ます。CIFSサーバを作成したら、CIFSドメインに追加するかワークグループに追加できます。ワークグループに参加するには、パラメータを使用し `-workgroup` ます。次に設定例を示します。

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

ワークグループ モードのCIFSサーバでは、Windows NT LAN Manager（NTLM）認証のみがサポートされ、Kerberos認証はサポートされません。

NetAppでは、組織のセキュリティ体制を維持するために、CIFSワークグループでNTLM認証機能を使用することを推奨しています。NetAppでは、CIFSのセキュリティ体制を検証するために、コマンドを使用して、IP情報、認証メカニズム、プロトコルバージョン、認証タイプなど、ポスチャ関連の詳細を表示することを推奨してい `vserver cifs session show` ます。

NASフアイルシステムノカンサ

NASファイル・システムは'今日の脅威の状況で使用量が増加しています監査機能は'可視性をサポートするために不可欠です

セキュリティの維持には検証が欠かせません。ONTAP 9では、ソリューション全体をとおしてさらに多くの監査イベントや詳細が記録されます。今日の脅威の状況ではNASファイルシステムが占める割合が増加しているため、可視性を維持するには監査機能が不可欠です。ONTAP 9で強化された監査機能により、CIFS監査ではこれまでになく詳細な情報が提供されます。作成されるイベントには、次のような重要な情報が記録されます。

- ファイル、フォルダ、共有へのアクセス

- ファイルの作成、変更、削除
- ファイル読み取りアクセスの成功
- ファイルの読み取りまたは書き込みの失敗
- フォルダ権限の変更

監査設定を作成します

監査イベントを生成するには、CIFS監査を有効にする必要があります。監査設定を作成するには、コマンドを使用し `vserver audit create` ます。デフォルトでは、監査ログのローテーションはサイズに基づいて行われます。ローテーション パラメータのフィールドにオプションを指定すれば、時間に基づくローテーションも使用できます。監査ログのローテーション設定には、ローテーションのスケジュール、ローテーション上限、実行する曜日、サイズなどの詳細を指定できます。次のテキストは、すべての曜日の12：30にスケジュールされた月単位の時間ベースのローテーションを使用した監査設定の例を示しています。

```
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監査イベント

CIFS監査イベントは次のとおりです。

- ファイル共有：関連するコマンドを使用してCIFSネットワーク共有が追加、変更、または削除されたときに監査イベントを生成します `vserver cifs share` 。
- 監査ポリシーの変更：関連するコマンドを使用して監査ポリシーが無効化、有効化、または変更された場合に、監査イベントを生成します `vserver audit` 。
- ユーザアカウント：ローカルのCIFSまたはUNIXユーザが作成または削除されたとき、ローカルユーザアカウントが有効化、無効化、変更されたとき、パスワードがリセットまたは変更されたときに監査イベントを生成します。このイベントは、コマンドまたは関連するコマンドを使用し `vserver cifs users-and-groups local-group` `vserver services name-service unix-user` ます。
- セキュリティグループ：コマンドまたは関連するコマンドを使用してローカルのCIFSまたはUNIXセキュリティグループが作成または削除されたときに監査イベントを生成します `vserver cifs users-and-groups local-group` `vserver services name-service unix-group` 。
- 認証ポリシーの変更：コマンドを使用してCIFSユーザまたはCIFSグループの権限が付与または取り消されたときに、監査イベントを生成します `vserver cifs users-and-groups privilege` 。

これはシステムの監査機能に基づく機能であり、管理者は、システムが何を許可および実行しているかをデータ ユーザの視点で確認することができます。

NASノカンサヘノRESTAPIノエイキヨウ

ONTAPには、管理者アカウントがREST APIを使用してSMB / CIFSまたはNFSファイルにアクセスして操作する機能が含まれています。REST APIはONTAP管理者のみが実行できますが、REST APIコマンドはシステムNAS監査ログをバイパスします。また、ONTAP管理者がREST APIを使用する際にファイル権限をバイパスすることもできます。ただし、ファイルに対するREST APIを使用した管理者の操作は、システムコマンド履

歴ログに記録されます。

アクセスなし**REST API**ロールの作成

RESTを使用してONTAPボリュームにアクセスできないREST APIロールを作成することで、ONTAP管理者がREST APIをファイルアクセスに使用できないようにすることができます。このロールをプロビジョニングするには、次の手順を実行します。

手順

1. ストレージボリュームへのアクセスは許可されず、他のすべてのREST APIアクセスを許可する新しいRESTロールを作成します。

```
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. 前の手順で作成した新しいREST APIロールに管理者アカウントを割り当てます。

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

組み込みのONTAPクラスタ管理者アカウントがREST APIをファイルアクセスに使用しないようにするには、まずを実行する必要があり "新しい管理者アカウントを作成し、組み込みアカウントを無効化または削除する"ます。

CIFS SMBの署名と封印の設定と有効化

ストレージシステムとクライアント間のトラフィックがリプレイ攻撃や中間者攻撃によって危険にさらされないようにすることで、データファブリックのセキュリティを保護するSMB署名を設定して有効にすることができます。SMB署名は、SMBメッセージに有効な署名があることを確認することで保護します。

このタスクについて

ファイルシステムやアーキテクチャの代表的な脅威ベクターは、SMBプロトコルです。このベクターに対処するために、ONTAP 9は業界標準のSMB署名と封印を使用ます。SMB署名は、ストレージシステムとクライアント間のトラフィックがリプレイ攻撃や中間者攻撃によって危険にさらされないようにすることで、データファブリックのセキュリティを保護します。具体的には、SMBメッセージに有効な署名があることが確認されます。

パフォーマンス上の理由からSMB署名はデフォルトでは無効になっていますが、NetAppでは有効にすることを強く推奨します。さらに、ONTAPではSMB暗号化（封印）もサポートしています。SMB暗号化は共有単位でのセキュアなデータ転送を実現します。デフォルトでは、SMB暗号化は無効になっています。ただし、NetAppではSMB暗号化を有効にすることを推奨します。

SMB 2.0以降ではLDAPの署名と封印がサポートされるようになりました。署名（改ざんに対する保護）と封

印（暗号化）により、SVMとActive Directoryサーバ間のセキュアな通信が実現します。SMB 3.0以降では、アクセラレーション用の新しいAES命令セット（Intel AES NI）がサポートされます。Intel AES NIはAESアルゴリズムの改良版で、サポートされるプロセッサ ファミリでのデータ暗号化を加速します。

手順

1. SMB署名を設定して有効にするには、コマンドを使用し `vserver cifs security modify` て、パラメータがに設定されていることを確認し `-is-signing-required` `true`ます。次の設定例を参照してください。

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

2. SMBの封印と暗号化を設定して有効にするには、コマンドを使用し `vserver cifs security modify` て、パラメータがに設定されていることを確認し `-is-smb-encryption-required` `true`ます。次の設定例を参照してください。

```
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のセキュリティ保護

エクスポートルールは、エクスポートポリシーの機能要素です。エクスポート ルールでは、ボリュームへのクライアント アクセス要求が設定済みの特定のパラメータと照合され、クライアント アクセス要求の処理方法が決定されます。エクスポートポリシーには、クライアントへのアクセスを許可するエクスポートルールが少なくとも1つ含まれている必要があります。エクスポートポリシーに複数のルールが含まれている場合、ルールはエクスポートポリシーに表示される順序で処理されます。

アクセス制御は、セキュアな体制を維持するうえで中心的な役割を果たします。そのためONTAPでは、エクスポート ポリシー機能を使用して、NFSボリュームへのアクセスを特定のパラメータに一致するクライアントだけに制限します。エクスポートポリシーには、各クライアントアクセス要求を処理するエクスポートルールが 1 つ以上含まれています。ボリュームへのクライアント アクセスを設定するため、各ボリュームにはエクスポート ポリシーが関連付けられています。エクスポート ポリシーの結果に基づいて、クライアントにボリュームへのアクセスが許可されるか拒否されるか（「permission denied」メッセージが表示される）が決まります。また、ボリュームに対するアクセス レベルも決まります。

クライアントがデータにアクセスするためには、エクスポート ルールを含むエクスポート ポリシーがSVMに割り当てられている必要があります。SVMには複数のエクスポート ポリシーを割り当てることができます。

ルールの順序は、ルールインデックス番号によって決まります。ルールがクライアントに一致すると、そのルールのアクセス権が使用され、それ以降のルールは処理されません。一致するルールがない場合、クライアントはアクセスを拒否されます。

エクスポート ルールは、次の条件を適用することでクライアントのアクセス権を決定します。

- クライアントが要求の送信に使用したファイル アクセス プロトコル（NFSv4やSMBなど）
- クライアント識別子（ホスト名やIPアドレスなど）
- クライアントが認証に使用したセキュリティ タイプ（Kerberos v5、NTLM、AUTH_SYSなど）

ルールに複数の条件が指定されている場合、クライアントが1つでも条件に一致しないとそのルールは適用されません。

エクスポート ポリシーに、次のパラメータが指定されたエクスポート ルールが含まれているとします。

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

クライアントに付与されるアクセス レベルはセキュリティ タイプで決まります。アクセスレベルには、読み取り専用、読み取り/書き込み、およびスーパーユーザ（ユーザIDを持つクライアントの場合）の3つがあります `0`。セキュリティタイプによって決定されたアクセスレベルはこの順序で評価されるため、次のルールに従う必要があります。

エクスポートルールのアクセスレベルパラメータのルール

クライアントが次のアクセスレベルを取得する場合	これらのアクセスパラメータは、クライアントのセキュリティタイプと一致している必要があります。
標準ユーザの読み取り専用	読み取り専用です (`-rorule`)
標準ユーザの読み取り / 書き込み	読み取り専用です (`-rorule`）および読み取り/書き込み (`-rwrule`)
スーパーユーザの読み取り専用です	読み取り専用です (`-rorule`）および `-superuser`
スーパーユーザの読み取り / 書き込み	読み取り専用です (`-rorule`）および読み取り/書き込み (`-rwrule`）および `-superuser`

次に、これらの 3 つのアクセスパラメータのそれぞれで有効なセキュリティタイプを示します。

- 任意
- なし
- なし

次のセキュリティタイプは、パラメータでは使用できません `-superuser` 。

- krb5

- ntlm
- システム

アクセスパラメータの結果のルール

クライアントのセキュリティタイプ	結果
アクセス パラメータに指定されたセキュリティ タイプと一致する。	クライアントは、自身のユーザIDでそのレベルのアクセス権を受け取ります。
指定したセキュリティタイプと一致しないが、アクセスパラメータにオプションが指定されている `none`。	クライアントは、そのレベルのアクセス権を受け取り、パラメータで指定されたユーザIDを持つ匿名ユーザを受け取り `-anon` ます。
指定したセキュリティタイプと一致しないため、アクセスパラメータにオプションが含まれていません `none`。	クライアントは、そのレベルのアクセス権を受け取りません。 この制限はパラメータには適用され `-superuser` ません。このパラメータには、指定しなくても常にnoneが指定されるためです。

Kerberos 5とkrb5p

ONTAP 9以降では、プライバシー サービス（krb5p）を使用したKerberos 5認証がサポートされます。krbp5認証は安全で、チェックサムを使用してクライアントとサーバの間のすべてのトラフィックを暗号化することでデータの改ざんやスヌーピングを防止します。ONTAPでは、Kerberos用に128ビットおよび256ビットのAES暗号化をサポートしています。プライバシー サービスには、受信データの整合性検証、ユーザの認証、送信前のデータの暗号化が含まれます。

krb5pオプションはエクスポート ポリシー機能で最もよく使用され、暗号化オプションとして設定されます。次の例に示すように、krb5p認証方式を認証パラメータとして使用できます。

```
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
```

Lightweight Directory Access Protocolの署名と封印を有効にする

署名と封印は、LDAPサーバへのクエリでセッションセキュリティを有効にするためにサポートされています。これは、LDAP over TLSに代わるセッション セキュリティを提供します。

署名は、シークレット キー技術を使用してLDAPペイロード データの整合性を確保します。封印は、LDAPペイロードデータを暗号化して、機密情報がクリアテキストで送信されないようにします。SVMのセッション セキュリティ設定は、LDAPサーバで使用可能な設定に対応しています。デフォルトでは、LDAPの署名と封

印は無効になっています。

手順

1. この機能を有効にするには、パラメータを指定してコマンドを実行し `vserver cifs security modify session-security-for-ad-ldap` ます。

   LDAPセキュリティ機能のオプション：

   - なし:デフォルト、署名または封印なし
   - 署名：LDAPトラフィックに署名します。
   - 封印：LDAPトラフィックの署名と暗号化

   > signとsealは累積的に適用されます。つまり、signオプションを使用した場合はLDAPが署名され、sealオプションを使用した場合は署名されたうえで封印（暗号化）されます。また、このコマンドにパラメータを指定しない場合、デフォルトはnoneです。

   次に、設定例を示します。

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

NetApp FPolicyの作成と使用

ONTAPソリューションのインフラコンポーネントであるFPolicyを作成して使用できます。FPolicyを使用すると、パートナーアプリケーションからファイルアクセス権限を監視および設定できます。その中でも強力なアプリケーションの1つが、NetApp SaaSアプリケーションであるストレージワークロードセキュリティです。ハイブリッドクラウド環境全体にわたるすべての企業データアクセスを一元的に可視化して制御できるため、セキュリティとコンプライアンスの目標を確実に達成できます。

アクセス制御はセキュリティの中核をなす概念です。ファイルアクセスやファイル操作を可視化し、応答できるようにすることは、セキュリティ体制の維持に欠かせません。可視性とファイルアクセス制御を提供するために、ONTAPソリューションではNetApp FPolicy機能を使用しています。

ファイル ポリシーはファイル タイプに基づいて設定できます。FPolicyは、ファイルを作成する、開く、名前を変更する、削除するといった、個々のクライアント システムからの操作の要求をストレージ システムがどのように処理するかを決定します。ONTAP 9以降ではFPolicyのファイル アクセス通知フレームワークが強化され、フィルタによる制御および短時間のネットワーク停止に対する耐障害性が追加されました。

手順

1. FPolicy機能を利用するには、まずコマンドを使用してFPolicyポリシーを作成する必要があります `vserver fpolicy policy create` 。

FPolicyを使用してイベントを表示したり収集したりする場合は、パラメータも使用し `-events` ます。ONTAPには、フィルタ処理やアクセスをユーザ名レベルで制御するより細かな機能が用意されています。ユーザ名で権限とアクセスを制御するには、パラメータを指定します `-privilege-user-name` 。

次にFPolicyの作成例を示します。

```
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. FPolicyポリシーを作成したら、コマンドを使用して有効にする必要があります `vserver fpolicy enable` 。このコマンドではFPolicyエントリの優先度（順序）も設定します。

同じファイル アクセス イベントに複数のポリシーが割り当てられている場合、優先度に基づいてアクセスが許可または拒否される順序が決まるため、FPolicyのシーケンスが重要になります。

次のテキストは、コマンドを使用してFPolicyポリシーを有効にし、その設定を検証する設定例を示してい `vserver fpolicy show` ます。

```
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の機能拡張

以降のセクションで、ONTAP 9で強化されたFPolicyの機能について説明します。

フィルタリングコントロール

ディレクトリアクティビティに関する通知を削除するための新しいフィルタが追加されました `SetAttr` 。

非同期の耐障害性

非同期モードで動作している FPolicy サーバでネットワーク停止が発生した場合、停止中に生成された FPolicy 通知はストレージノードに格納されます。FPolicy サーバがオンラインに戻ると、サーバは格納された通知に関するアラートを受け取り、ストレージノードから通知を読み込むことができます。停止中に通知を保存できる期間は、最大 10 分に設定できます。

LIF セキュリティ

LIFは、ロール、ホームポート、ホームノード、フェイルオーバー先のポートのリスト、ファイアウォールポリシーなどの特性が関連付けられているIPアドレスまたはWorld Wide Port Name（WWPN）です。LIFは、クラスタでネットワーク経由の通信の送受信に使用するポートに設定できます。LIFの各ロールのセキュリティ特性を理解することが重要です。

LIFロール

LIFのロールは次のとおりです。

- *データLIF *：SVMに関連付けられ、クライアントとの通信に使用されるLIFです。
- *クラスタLIF *：クラスタ内のノード間のトラフィックの伝送に使用されるLIFです。
- *ノード管理LIF *：クラスタ内の特定のノードを管理するための専用IPアドレスを提供するLIFです。
- *クラスタ管理LIF *：クラスタ全体に対して単一の管理インターフェイスを提供するLIFです。
- *クラスタ間LIF *：クラスタ間の通信、バックアップ、およびレプリケーションに使用されるLIFです。

各LIFロールのセキュリティ特性

	データ **LIF**	クラスタ **LIF**	ノード管理 **LIF**	クラスタ管理**LIF**	クラスタ間 **LIF**
プライベートIPサブネットが必要	いいえ	はい。	いいえ	いいえ	いいえ
セキュアなネットワークが必要	いいえ	はい。	いいえ	いいえ	はい。
デフォルトのファイアウォールポリシー	非常に厳しい	完全にオープン	中	中	非常に厳しい
ファイアウォールをカスタマイズ可能	はい。	いいえ	はい。	はい。	はい。

- クラスタLIFは完全にオープンで設定可能なファイアウォール ポリシーがないため、分離されたセキュアなネットワークのプライベートIPサブネットに配置する必要があります。
- どのような状況下でも、LIFのロールをインターネットに公開しないでください。

LIFの保護の詳細については、を参照して "LIF のファイアウォールポリシーを設定します"ください。

プロトコルおよびポートセキュリティ

ソリューションのセキュリティを強化するには、組み込みのセキュリティ処理や機能に加え、外部のセキュリティ メカニズムも必要になります。ファイアウォール、不正侵入防御（IPS）、その他のセキュリティ デバイスなど、追加のインフラ デバイスを利用してONTAPへのアクセスをフィルタおよび制限することで、厳しいセキュリティ体制を効果的に確立して維持することができます。この情報を基づいて、環境とリソースへのアクセスをフィルタして制限します。

よく使用されるプロトコルとポート

サービス	ポート / プロトコル	説明
SSH	22 / TCP	SSHロクイン
telnet	23 / TCP	リモートログイン
Domain	53 / TCP	ドメイン ネーム サーバ
HTTP	80 / TCP 80 / UDP	HTTP
rpcbind	111/TCP 111/UDP	リモート手順コール
NTP	123 / UDP	Network Time Protocol の略
msrpc	135 / UDP	Microsoftリモート プロシージャ コール
Netbios-name	137 / TCP 137 / UDP	NetBIOSネームサービス
netbios-ssn	139 / TCP	NetBIOS サービスセッション
SNMP	161 / UDP	SNMP
HTTPS	443 tcp	セキュアリンク：http
microsoft-ds	445 / TCP	Microsoftディレクトリ サービス
IPsec	500 / UDP	インターネットプロトコルセキュリティ
mount	635/UDP	NFS マウント
named	953 / UDP	名前デーモン
NFS	2049 / UDP 2049 / TCP	NFSサーバデーモン
nrv	2050 / TCP	NetAppリモート ボリューム プロトコル
iscsi	3260 / TCP	iSCSI ターゲットポート
Lockd	4045 / TCP 4045 / UDP	NFS ロックデーモン
NFS	4046 / TCP	NFS mountdプロトコル

サービス	ポート / プロトコル	説明
acp-proto	4046 / UDP	アカウント プロトコル
rquotad	4049/UDP	NFS rquotad プロトコル
krb524	444/UDP	Kerberos 524
IPsec	4500/UDP	インターネットプロトコルセキュリティ
acp	5125 / UDP 5133 / UDP 5144 / TCP	ディスク用の代替制御ポート
Mdns	533/UDP	マルチキャスト DNS
HTTPS	5986/UDP	HTTPSポート：バイナリ プロトコルをリスン
TELNET	8023/tcp のようになります	ノードを対象としたTelnet
HTTPS	8443 / TCP	7MTT GUIツール（リンク経由）：HTTPS
RSH	8514/tcp のようになります	ノードを対象としたRSH
KMIP	9877/tcp のようになります	KMIPクライアント ポート（内部ローカル ホストのみ）
ndmp	10000 / TCP	NDMP
cifs 監視ポート	40001/tcp のようになります	CIFS監視ポート
TLS	50000 / TCP	トランスポートレイヤのセキュリティ
Iscsi	65200/TCP	iSCSIポート
SSH	65502/tcp のようになります	セキュアシェル
vsun	65503/tcp のようになります	vsun

NetApp内部ポート

ポート / プロトコル	説明
900	NetAppクラスタRPC
902	NetAppクラスタRPC
904	NetAppクラスタRPC
905	NetAppクラスタRPC
910	NetAppクラスタRPC
911	NetAppクラスタRPC
913	NetAppクラスタRPC
914	NetAppクラスタRPC
915	NetAppクラスタRPC

ポート / プロトコル	説明
918	NetAppクラスタRPC
920	NetAppクラスタRPC
921	NetAppクラスタRPC
924	NetAppクラスタRPC
925	NetAppクラスタRPC
927	NetAppクラスタRPC
928	NetAppクラスタRPC
929	NetAppクラスタRPC
931	NetAppクラスタRPC
932	NetAppクラスタRPC
933	NetAppクラスタRPC
934	NetAppクラスタRPC
935	NetAppクラスタRPC
936	NetAppクラスタRPC
937	NetAppクラスタRPC
939	NetAppクラスタRPC
940	NetAppクラスタRPC
951	NetAppクラスタRPC
954	NetAppクラスタRPC
九五五	NetAppクラスタRPC
956	NetAppクラスタRPC
958	NetAppクラスタRPC
961	NetAppクラスタRPC
九六三	NetAppクラスタRPC
九六四	NetAppクラスタRPC
九六六	NetAppクラスタRPC
967	NetAppクラスタRPC
7810	NetAppクラスタRPC
7811	NetAppクラスタRPC
7812	NetAppクラスタRPC
7813	NetAppクラスタRPC
7814	NetAppクラスタRPC
7815	NetAppクラスタRPC

ポート / プロトコル	説明
7816	NetAppクラスタRPC
7817	NetAppクラスタRPC
7818	NetAppクラスタRPC
7819	NetAppクラスタRPC
7820	NetAppクラスタRPC
7821	NetAppクラスタRPC
7822	NetAppクラスタRPC
7823	NetAppクラスタRPC
7824	NetAppクラスタRPC

セキュリティリソース

このONTAPセキュリティマニュアルに記載されている情報の詳細については、次の追加情報およびセキュリティの概念を参照してください。

脆弱性とインシデントの報告、NetAppのセキュリティ対応、および顧客の機密性の詳細については、を参照してください "NetAppセキュリティポータル"。

- "ONTAP 9リリースノート"
- "ONTAP 9コマンドリファレンス"
- "システム管理"
- "管理者認証とRBAC"
- "NetApp暗号化"
- "TR-4647：『Multifactor Authentication in ONTAP 9.3』"
- "OPENSSL暗号"
- "CryptoMod FIPS-140-2レベル1"
- "Certificate-Based Authentication with the NetApp Manageability SDK for ONTAP"
- "Network Management の略"