テクニカル レポート

NetApp ONTAP 9セキュリティ設定ガイド

ONTAP 9のセキュアな導入のための ガイドライン

ネットアップ製品セキュリティ チーム
2020年12月| TR-4569

概要

このテクニカル レポートでは、組織が情報システムの機密性、整合性、可用性について定めたセキュリティ目標に沿ってNetApp® ONTAP® 9を導入するためのガイダンスと設定を記載します。

<<本レポートは機械翻訳による参考訳です。公式な内容はオリジナルである英語版をご確認ください。>>

目次

表一覧

はじめに

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、難読化やスパイ技術も巧妙化しているため、システム管理者にはデータや情報のセキュリティにプロアクティブに対処することが求められています。このガイドは、セキュリティ部門のオペレータや管理者に対し、ネットアップ ソリューションの中核をなす機密性、整合性、可用性を活用した支援を提供することを目的としています。

ONTAPイメージの検証

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 / 自動無停止イメージ更新、CLI、ZAPIでインストールされたONTAPイメージがネットアップから正式に提供されたものであり、改ざんされていないことを検証するために使用します。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` シグネチャを検証できる以外、他に何も行う必要はありません。

ブート時のイメージ検証

ONTAP 9.4以降、Unified Extensible Firmware Interface（UEFI）のセキュア ブートが導入され、NetApp AFF A800、AFF A220、FAS2750、FAS2720の各システム、およびUEFI BIOSを採用する以降の次世代システムに使用されています。

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。

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

ロールベース アクセス制御（RBAC）を使用すると、ユーザの職責や職務に応じて必要なシステムとオプションにのみアクセスを許可できます。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。表 1 に 、ONTAP の事前定義されたロールを示します。

表 1）クラスタ管理者の事前定義ロール

クラスタ ロール	説明
admin	最上位の管理用アカウント
AutoSupport	NetApp AutoSupport®で使用
バックアップ	コマンド ディレクトリへのアクセスを提供
read-only	すべてのコマンドを取り消し、独自のパスワードをリセット
なし	コマンド ディレクトリへのアクセスを禁止

表 2）Storage Virtual Machine管理者の事前定義ロール

SVM ロール	機能
vsadmin	• 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • ボリューム、クォータ、qtree、NetApp Snapshotコピー、およびファイルの管理 • LUNを管理します。 • NetApp SnapLock®処理の実行（privileged deleteを除く） • プロトコルの設定：NFS、CIFS、iSCSI、FC（FCoEを含む） • サービスの設定：DNS、Lightweight Directory Access Protocol（LDAP）、Network Information Service（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 • Storage Virtual Machine（SVM、旧Vserver）の健全性の監視
vsadmin-volume	• 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • ボリューム、クォータ、qtree、Snapshotコピー、FlexCache、およびファイルの管理 • LUNを管理します。 • プロトコルの設定：NFS、CIFS、iSCSI、FC（FCoEを含む） • 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 の健常性を監視
vsadmin-protocol	• 自身のユーザ アカウント、ローカル パスワード、キー情報の管理 • プロトコルの設定：NFS、CIFS、iSCSI、FC（FCoEを含む） • 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 の健常性を監視
vsadmin-backup	• 自身のユーザ アカウント、ローカル パスワード、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の読み取り / 書き込み許可 • NetApp SnapMirror®関係とSnapshotコピーの管理 • 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、ローカル パスワード、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、およびファイルの管理 • SnapLock処理の実行（privileged deleteも含む） • プロトコルの設定：NFS、CIFS • 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、ローカル パスワード、キー情報の管理 • SVM の健常性を監視

SVM ロール	機能
	• 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

Application Method

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service-processor に設定すると、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。service-processor-authentication-method password このパラメータをに設定すると、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、パラメータをに設定する必要があります。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service-processorに設定されている場合、運用者と管理者は-vserver パラメータを使用できません。

ネットアップではセキュアなリモート アクセスにSecure Shell（SSH）を推奨しているため、セキュリティ上の理由からTelnetとRemote Shell（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。

security protocol modify コマンドは、クラスタ全体にわたる、RSHとTelnetの既存の構成を変更します。クラスタ内でRSHとTelnetを有効にするには、enabledフィールドをtrueに設定します。

Authentication Method

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。表 3 に 、さまざまな認証方式を示します。

表 3）認証方式

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、admin およびpublickey を2つの認証方式として使用することで、チェーン型の2要素認証を使用できます。security login コマンドの-authentication-method フィールドに加え、-second- authentication-method という名前の新しいフィールドが追加されました。- authentication-method または-second-authentication-method. には公開鍵またはパスワードを指定できます。ただし、SSH認証では、公開鍵（部分認証）、パスワード プロンプト（完全認証）の順に表示されます。

```
[sam@centos7 ~]$ ssh ontap9.3.NTAP.LOCAL
Authenticated with partial success.
Password:
cluster1::>
```

ONTAP 9.4以降では、publickeyを指定したnsswitch を第2の認証方式として使用できます。

デフォルトの管理アカウント

デフォルトでは、admin とdiagの2つの管理アカウントがあります。

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。

注： 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、ネットアップでは、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 アカウントを一覧表示するには、コマンドを使用します。

```
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.
```

adminアカウント

adminアカウントにはadminロールが割り当てられており、すべてのアプリケーションにアクセスできます。

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

注： ただしその結果として想定外の状況が生じることがあります。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。

```
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.
```

新しいadminアカウントが作成されたら、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、デフォルトまたは以前のadminアカウントと同じログイン アプリケーションを使用するようにアカウントを設定します（http、ontapi、service-processor、sshなど）。これによってアクセス制御が維持されます。

```
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
```

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 *
```

次のコマンドを使用して、デフォルトのadminアカウントと対応するすべてのエントリを削除します。

```
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.
```

diagアカウント

ストレージ システムには、diag という名前の診断アカウントが用意されています。diag アカウントを使用すると、systemshellでトラブルシューティングの作業を実行できます。diag アカウントとsystemshell は、簡単な診断だけを目的としています。使用する場合は、必ずテクニカル サポートの指示に従ってください。

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。アクセスするには、診断権限付きコマンドのdiag を使用します。systemshellにアクセスする前に、security login password コマンドを使用して、diag アカウントのパスワードを設定する必要があります。diag のパスワードは、強力なパスワードの原則に基づいて作成し、定期的に変更する必要があります。diag アカウントとsystemshell は、どちらも一般的な管理目的で使用するものではありません。

```
ontap9-tme-8040::> set -privilege diag

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

ontap9-tme-8040::*> systemshell -node ontap9-tme-8040-01
  (system node systemshell)
diag@169.254.185.32'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.

ontap9-tme-8040-01%
```

証明書ベースのAPIアクセス

ONTAPへのアクセスにNetApp Manageability SDK APIを使用する場合は、ユーザIDとパスワードによる認証の代わりに、証明書ベースの認証を使用する必要があります。

次の方法で自己署名証明書を生成してONTAPにインストールできます。

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。
   このコマンドは、test.pem という名前のパブリック証明書と、key.outという名前の秘密鍵を生成します。共通名のは、ONTAPのユーザIDに対応しています。
2. Privacy Enhanced Mail（PEM）形式のパブリック証明書の内容をONTAPにインストールします。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貼り付けます。

```
security certificate install -type client-ca -vserver ontap9-tme-8040

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 ontap9-tme-8040 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi -authmethod cert -role
admin -vserver ontap9-tme-8040
```

次の例では、証明書認証を使用したAPIアクセスが使用できるようにユーザID_certが有効になっています。ONTAPのバージョンを表示するための、cert_user を使用した簡単なManageability SDK Pythonスクリプトは、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 = "ontap9-tme-8040"
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 アクセス用のユーザ ID を定義します。

```
security login create -user-or-group-name cert_user -application http -authmethod cert -role
admin -vserver ontap9-tme-8040
```

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

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key ./test.key -X GET "https://ontap9-
tme-8040/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"
    }
  }
}
```

詳細については、「Certificate based authentication with the NetApp Manageability SDK for ONTAP」を参照してください。

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。

ローカル アカウントの新機能

ユーザ アカウントに関する組織のポリシー、ガイドライン、標準（ガバナンスを含む）に対応するために、ONTAP 9では次の機能がサポートされます。

- 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

  注：構成可能な設定は、セキュリティ ログイン ロールの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 アカウントには、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。ユーザにパスワードの変更を指示して、該当するユーザ アカウントをより安全なSHA-512ソリューションに移行することを強く推奨します。

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 アカウントを表示する

```
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）を使用しているアカウントを失効させて次回ログイン時にパスワードの変更を求める

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

- 指定したハッシュ関数を使用しているアカウントをロックする

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

パスワードのハッシュ関数 autosupport が、クラスタの管理 SVM で内部ユーザのものではありません。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。

autosupport ユーザのパスワードハッシュ関数を表示するには、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
```

パスワードをに設定しても問題はありません。

```
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。は、アカウントに関する情報を表示するsecurity login role config show コマンドの説明です。

表 4）管理ユーティリティのユーザ アカウントの制限

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	enabled	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～unlimited 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	過去*N*個のパスワードを禁止	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	アカウントの有効期間（日数）	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

```
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
```

システム管理方法

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。

コマンドは、クラスタとSVMのSSHキー交換アルゴリズム、暗号、およびMACアルゴリズムの構成を表示します。ONTAPのSSHでサポートされるアルゴリズムと暗号については、を参照してください。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.
```

ログイン バナー

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。表 5 に、ログインバナーのパラメータを示します。

表 5）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。
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にログイン バナーを設定すると、クラスタのログイン バナーの代わりにそのログイン バナーが表示されます。データSVMのログイン バナーではなく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、このパラメータを「-」に指定します。 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。改行を含むログイン バナー メッセージを入力するには、この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。プロンプトに対して入力する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	バナー メッセージのダウンロードURIを(ftp|http)://(hostname|IPv4 Address|'['IPv6 Address']'の形式で指定します。 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2,048バイト以内にする必要があります。非ASCII文字はUnicode UTF-8形式で入力する必要があります。

Message Of The Day

`security login motd modify` コマンドは、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も表示され、メッセージが2回表示される可能性があります。

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。

表 6） MOTD のパラメータ

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。

パラメータ	説明
message	（オプション）このパラメータは、メッセージを指定します。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せずにコマンドを実行すると、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。プロンプトに対して入力するメッセージには改行を含めることができます。非ASCII文字はUnicode UTF-8形式で入力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との互換性のみを目的としてサポート） • \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（コンソールへのログインの場合は「」と出力） • \l - ログインしたデバイスの名前（コンソールへのログインの場合は「」と出力） • \L - ユーザによるクラスタ内ノードへの前回のログイン • \m - マシンのアーキテクチャ • \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 - と同じ。（Linuxとの互換性のためにサポート） • \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。クラスタ管理の場合はすべてのクラスタシェル ユーザが含まれ、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。ただし、\uまたはuser が追加されます。 • \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（）のクラスタ全体におけるアクティブなセッション。

CLIセッションのタイムアウト

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、`system timeout show command` を使用します。タイムアウト値を設定するには、`system timeout modify -timeout <minutes>` コマンドを使用します。

Webアクセス

NetApp ONTAP System Manager

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

か、IPv4またはIPv6アドレス（`https://cluster-management-LIF`）を使用している場合は、ブラウザでホスト名を指定します。

自己署名の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伝える警告がブラウザ画面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以降のSystem ManagerではSecurity Assertion Markup Language（SAML）認証も使用できます。

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に準拠した外部のアイデンティティ プロバイダ（IdP）による多要素認証（MFA）を可能にします。企業が選んだIdP独自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を実行できます。

SAMLの仕様では、プリンシパル、IdP、およびサービス プロバイダ（SP）の3つの役割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、Microsoft Active Directory Federated Services（ADFS）やオープンソースのShibboleth IdPなど、組織側が用意した他社製のIdPソフトウェアです。SPはONTAPに搭載された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認証が有効になると、新しい認証方式である`saml` が、`http` と`ontapi` 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追加されます。

SAML認証が有効になった後は、ONTAPで、`http` および`ontapi` アプリケーション用の管理者ロールと`saml` 認証方式を指定した、SAML IdPアクセスを必要とする新しいアカウントを追加で定義する必要があります。ある時点でSAML認証が無効になった場合は、これらの新しいアカウントに、`http` および`ontapi` アプリケーション用の管理者ロールを指定した`password` 認証方式を定義し、ローカルONTAP認証用の`console` アプリケーションをONTAP System Managerに追加する必要があります。

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。

ネットアップで検証済みのIdPは、Microsoft ADFSとオープンソースのShibboleth IdPです。

ONTAP System Manager、Active IQ Unified Manager、およびSSHのMFAの詳細については、TR-4647：『Multifactor Authentication in ONTAP 9.3』を参照してください。

ストレージ管理システムの監査

syslogの送信

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。

情報の流出を単一のシステムまたはソリューションに限定するためには、syslog情報をオフロードする必要があります。そのため、syslog情報を安全な保管場所にオフロードすることを推奨します。

ログの転送先を作成します。

cluster log-forwarding create コマンドは、リモート ロギングのログ転送先を作成します。

パラメータ

cluster log-forwarding create コマンドを構成するには、次のパラメータを使用します。

- 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>
```

- **転送先ポート。**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』User Datagram Protocol、セキュリティなし。
  - 『tcp-unencrypted』TCP、セキュリティなし。
  - 『tcp-encrypted』TCP、Transport Layer Security（TLS）を使用。
- 転送先サーバの識別情報を検証。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。値をtrueに設定できるのは、protocolフィールドでtcpencrypted値が選択されている場合だけです。

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

- **syslog機能。**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。通常、cluster log-forwarding create コマンドは、Internet Control Message Protocol（ICMP）のpingを送信してデスティネーションに到達できるかどうかをチェックし、到達できない場合は失敗します。この値をtrue に設定すると、pingチェックがバイパスされ、デスティネーションが到達不能でも設定できるようになります。

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

  ネットアップでは、cluster log-forwarding コマンドを使用して、-tcp-encrypted タイプへの接続を強制的に行うことを推奨しています。

イベント通知

システムのセキュリティ体制を維持および管理するには、システムから送信される情報やデータを保護することが不可欠です。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、イベント フィルタで定義され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、イベント通知の構成、および構成済みのイベント通知フィルタとデスティネーションを表示するevent notification show コマンドを示しています。

```
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

ディスクの盗難、返却、転用に際して保存されている機密データを保護するには、保存データ暗号化が重要です。

ONTAP 9には、連邦情報処理標準（FIPS）140-2に準拠した保存データ暗号化ソリューションが3つ用意されています。

- NetApp Storage Encryption（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、およびNAEでは、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、およびOKMでは、ONTAP CryptoModを使用します。CryptoModはCMVP FIPS 140-2の認定モジュールです。FIPS 140-2認定番号3387を参照してください。

OKMの構成を開始するには、`security key-manager onboard enable` コマンドを使用します。外部のKey Management Interoperability Protocol（KMIP）キー マネージャを設定するには、`security key-manager external enable` コマンドを使用します。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。特定のSVMに対して外部キー管理を有効にするには、`-vserver <vserver name>` パラメータを使用します。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構成していました。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、`-enable-cc-mode true` オプションを`security key- manager setup` で使用して、リブート後にパスフレーズの入力をユーザに求めることができます。ONTAP 9.6以降で

は、コマンド構文は`security key-manager onboard enable -cc-mode-enabled yes.`です。

ONTAP 9.4以降では、高度な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 ライセンスが導入されており、OKM または外部キーマネージャが設定されていて、NSE が使用されていない場合、NAE および NVE がデフォルトで有効になります。NAE ボリュームはデフォルトで NAE アグリゲートで作成され、NVE ボリュームはデフォルトで非 NAE アグリ

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

ゲートで作成されます。次のコマンドを入力して、この設定を上書きできます。

NSE、NVE、NAE、OKM、および外部KMIPサーバの詳細については、ONTAP 9ドキュメント センターの『NetApp Encryptionパワー ガイド』を参照してください。

データ レプリケーションにおける暗号化

ディザスタ リカバリ、キャッシュ、またはバックアップの目的でデータをレプリケートする場合は、あるONTAPクラスタから別のONTAPクラスタへの転送時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不正な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 ピアリング暗号化で、SnapMirror、SnapVault、FlexCacheなどのONTAPデータ レプリケーション機能に対する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 ピア間の事前共有キー（PSK）を使用して設定されます。

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、新しいクラスタ ピア関係では暗号化がデフォルトで有効になります。ONTAP 9.6よりも前に作成したクラスタ ピア関係で暗号化を有効にするには、ソースとデスティネーションの両方のクラスタを9.6にアップグレードする必要があります。さらに、`cluster peer modify` 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 クラスタ ピアとデスティネーション クラスタ ピアの両方を変更する必要があります。

9.6で既存のピア関係をクラスタ ピアリング暗号化を使用するように変換する例を次に示します。

```
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.
```

クラスタ ピアリング暗号化の詳細については、ONTAP 9ドキュメント センターの『クラスタ / SVMピアリング パワー ガイド』を参照してください。

IPSec の転送中データ暗号化

状況によっては、ネットワーク経由（または転送中）で ONTAP SVM に転送されるすべてのクライアント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不正な中間者攻撃を防ぐことができます。

ONTAP 9.8 以降では、Internet Protocol Security（IPsec ；インターネットプロトコルセキュリティ）により、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 では、iSCSI トラフィックに対して転送中の暗号化オプションのみが提供されます。

ネットワーク上で NFS 暗号化を提供することは、IPSec の主なユースケースの 1 つです。ONTAP 9.8 よりも前のバージョンでは、転送中の NFS データを暗号化するために krb5p を使用するには、NFS のネットワーク経由での暗号化を行うために、Kerberos の設定と構成が必要でした。これは、すべてのお客様の環境で、必ずしもシンプルであるとは限らず、達成も容易ではありません。

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（、Cluster Peering Encryption（CPE（などの保存データ暗号化テクノロジを使用するお客様は、ONTAP 9.8 以降にアップグレードしてを使用することで、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の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、IPsecを非同期モードで使用します。また、Internet Key Exchange（IKE; インターネットキーエクスチェンジ）プロトコルバージョン 2 も利用します。このプロトコルでは、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 のどちらかを使用してキーマテリアル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。また、スイート B の AES-GMAC256 および 256 ビットの暗号化をサポートします。

クラスタで IPSec 機能を有効にする必要がありますが、SPD エントリを使用することにより、環境の個々の SVM IP アドレスを使用できます。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秘密鍵（PSK（が含まれています。IPsec ポリシーエントリに加えて、トラフィックが IPsec 接続を通過できるようにするには、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。

クライアントと SVM 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て IPsec トラフィックを許可するために、ESP プロトコルと UDP プロトコル（ポート 500 と 4500（を許可する必要があります（着信（入力）と発信（出力）の両方）。

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 経由でクラスタピアリング暗号化（CPE（を使用して、ネットワーク経由でセキュアな転送を実現することを推奨します。CPE は、IPsec よりもこれらのワークロードの方が優れています。IPsec のライセンスは不要で、インポートやエクスポートの制限もありません。

クラスタで IPSec を有効にし、単一クライアントおよび単一 SVM の IP アドレス用に SPD エントリを作成する例を次に示します。

```
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 confimr the pre shared secret (PSK).
```

LIFの保護の詳細については、ONTAP 9ドキュメント センターの『ONTAP 9ネットワーク管理ガイド』を参照してください。

TLSとSSLの管理

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準拠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、`security config modify` コマンドの`is-fips-enabled` パラメータを`true` に設定します。その後、`security config show` コマンドを使用して、オンライン ステータスを確認できます。

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。

`security config modify` コマンドは、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。`-supported-protocols` パラメータを使用すると、FIPSモードとは関係なく、TLSプロトコルを含める、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。

下位互換性のため、ONTAPでは、FIPSモードが無効の場合、SSLv3を`supported-protocols` のリストに追加できます。Advanced Encryption Standard（AES）またはAESと3DESのみを設定するには、`-supported-ciphers` パラメータを使用します。「!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`ALL:!LOW:!aNULL:!EXP:!eNULL`です。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。

正しい暗号文字列の構文について は、OpenSSL Software Foundation が公開しているこのサイトを参照してください。セキュリティ設定を変更したら、すべてのノードを手動でリブートします。

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。

注： 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 クライアントを接続するには、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 1.2 を有効にし、PFS（Perfect Forward Secrecy（対応の暗号スイートを使用するだけで、TLS セキュリティをさらに強化できます。PFS は、と組み合わせて使用する場合のキー交換方式です
TLS 1.2 などの暗号化プロトコルを使用すると、攻撃者がクライアントとサーバー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だけをイネ `security config modify` ーブルにするには、次の例に示すように、advanced 権限レベルからコマンドを使用します。

注 ： SSL インターフェイスの設定を変更する前に、ONTAP に接続する際にクライアントが言及した暗号（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-
ciphers PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNull:!3DES:!kdH:!kECDH
```

y 各プロンプトを確認します。セキュリティ設定を変更したら、すべてのノードを手動でリブートします。PFS の詳細について は、こちらの NetApp ブログを参照してください。

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。本番システムでは、クラスタまたはSVMのSSLサーバとしての認証用にCA署名デジタル証明書をインストールすることを推奨します。`security certificate generate-csr` `security certificate install` コマンドを使用してCertificate Signing Request（CSR;証明書署名要求）を生成し、コマンドを使用して、CAから受信した証明書をインストールできます。

組織のCAの署名入りのデジタル証明書を作成するには、次の手順を実行します。

1. CSR を生成します。
2. 2. 組織で定められた手順に従って、CSRを使用して組織のCAにデジタル証明書を要求します。たとえば、Microsoft Active Directory証明書サービスのWebインターフェイスを使用してに移動し、証明書を要求します。
3. ONTAPにデジタル証明書をインストールします。

Online Certificate Status Protocol

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による証明書ステータス チェックは無効になっています。これを有効にするには、`security config ocsp enable -app app name,` コマンドを使用します。ここで、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.` になります。このコマンドには高度なレベルの権限が必要です。

SSHv2の管理

推奨
• 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。

`security ssh modify` コマンドは、クラスタまたはSVMのSSHキー交換アルゴリズム、暗号、またはMACアルゴリズムの既存の構成を、指定した構成に置き換えます。に、ONTAPでサポートされるSSHの暗号と鍵交換を示します。

表 7）サポートされる暗号と鍵交換

暗号	鍵交換方式
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	-

暗号	鍵交換方式
aes256-gcm	-
3des-cbc	-

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

NetApp AutoSupport

ONTAPのAutoSupport機能を使用すると、システム ヘルスをプロアクティブに監視し、ネットアップ テクニカル サポート、組織内のサポート チーム、およびサポート 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。ネットアップ テクニカル サポートへのAutoSupportメッセージの送信は、ストレージ システムの初回設定時にデフォルトで有効になります。また、ネットアップ テクニカル サポートへのメッセージ送信はAutoSupportを有効にしてから24時間後に開始されます。この24時間という設定は変更可能です。組織内のサポート チームへの通信を利用するには、メール ホストを設定しておく必要があります。

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機能は無効にすることもできます。ただし、AutoSupportはストレージ システムで発生した問題の迅速な特定と解決に役立つため、有効にしておくことを推奨します。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。

メッセージに含まれる内容やメッセージ タイプ別の送信先など、AutoSupportメッセージの詳細については、ネットアップ サポート ポータルを参照してください。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は、転送プロトコルとしてHTTPS、HTTP、およびSMTPをサポートします。AutoSupport メッセージには機密的な情報が含まれているため、AutoSupportメッセージをネットアップ サポートに送信する際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。

さらに、`system node autosupport modify` コマンドを使用して、AutoSupportデータの送信先（ネットアップ テクニカル サポート、組織の社内チーム、パートナーなど）を指定する必要があります。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、`system node autosupport modify -state disable` コマンドを使用します。

ネットワーク タイム プロトコル

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、NTPサーバに対称認証を設定できます。

`cluster time- service ntp server create` 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。タイム サービスの冗長性と品質を高めるためには、最低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、ONTAP 9ドキュメント センターの「クラスタ時間の管理（クラスタ管理者のみ）」を参照してください。

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）

ONTAP 9以降ではCIFSサーバをワークグループ内に設定できます。ワークグループには、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クライアントが含まれます。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サーバを構成するには、`vserver cifs create` コマンドを使用します。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させるには、`-workgroup` パラメータを使用します。次に設定例を示します。

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

注： 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。

組織のセキュリティ体制を維持するために、CIFSワークグループとNTLM認証機能を使用することを推奨します。CIFSのセキュリティ体制を検証するため、`vserver cifs session show` コマンドを使用して、セキュリティ体制関連の詳細情報（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）を表示することを推奨します。

NASファイルシステムの監査

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。近年NASファイルシステムに対する脅威が増えており、可視

化という側面からも監査機能が非常に重要になります。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、`vserver audit create` コマンドを使用します。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。次の監査設定例では、時間に基づくローテーションを使用して、毎月すべての曜日の12時30分にローテーションを行うようにスケジュールしています。

```
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
```

新しい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vserver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。
- **監査ポリシーの変更。**関連するvserverコマンドを使用して、監査ポリシーが無効化、有効化、または変更されたときに、監査イベントを生成します。
- **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、vserverコマンドまたは関連する コマンドを使用します。
- **セキュリティ グループ。**vserverコマンドまたは関連する コマンドを使用して、ローカル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。
- **認証ポリシーの変更。**vserver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。

  注： 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。

REST API が NAS の監査に与える影響

ONTAP には、管理者アカウントが REST API を使用して SMB / CIFS ファイルまたは NFS ファイルにアクセスして操作する機能があります。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の 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省略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ています。

REST を使用して ONTAP ボリュームにアクセスできない REST API ロールを作成すると、ONTAP 管理者がファイルアクセスに REST API を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。

1. ストレージボリュームへのアクセスは許可せず、REST API によるその他のアクセスもすべて許可する新しい REST ロールを作成します。

```
cluster1::> security login rest-role create nofiles -vserver ontap9-tme-8040
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver ontap9-tme-8040 "/api" -access all
```

2. 手順 1 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 ontap9-tme-8040 -role nofile
```

メモ　：組み込みの ONTAP クラスタ管理者アカウントでファイルアクセスに REST API を使用できないようにするには、まず新しい管理者アカウントを作成し、「デフォルトの管理アカウント」の手順に従って組み込みのアカウントを無効にするか削除する必要があります。

CIFS SMBの署名と封印

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の間のトラフィックをリプレイ アタック（中間者攻撃）から守ることでデータ 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。

パフォーマンスを重視するためにSMB署名はデフォルトでは無効になっていますが、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、ネットアップでは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。

SMB署名を設定して有効にするには、コマンドを使用して、`vserver cifs security modify` パラメータが`-is-signing-required` に設定されていることを確認します。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
```

SMBのシーリングと暗号化を設定して有効にするには、`vserver cifs security modify` コマンドを使用して、`-is-smb-encryption-required` パラメータがtrueに設定されていることを確認します。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
----------- ----------------------------------
```

NFSの保護

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。

注： 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。

エクスポート ルールは、エクスポート ポリシーが機能するための要素です。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、クライアントにアクセスを許可するエクスポート ルールを少なくとも1つ含める必要があります。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に処理されます。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、スーパーユーザ（ユーザIDが0のクライアントの場合）の3つがあります。セキュリティ タイプに基づくアクセス レベルはこの順序で評価されるため、アクセス レベルを設定するときは、のルールに従う必要があります。

表 8）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

クライアントが必要とするアクセス レベル	クライアントのセキュリティ タイプと一致する必要があるアクセス パラメータ
標準ユーザの読み取り専用	read-only
標準ユーザの読み取り / 書き込み	読み取り専用（）および読み取り / 書き込み（`-rorule`）
スーパーユーザの読み取り専用	読み取り専用（）および`-rorule`
スーパーユーザの読み取り / 書き込み	読み取り専用（）、読み取り / 書き込み（`-rorule`）、および

次に、3つそれぞれのアクセス パラメータで有効なセキュリティ タイプを示します。

- any
- なし
- 更新しない

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

- krb5
- ntlm
- sys

は、クライアントのセキュリティ タイプを有効な3つのアクセス パラメータと照合したときの結果です。

表 9）アクセス パラメータのルール結果

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 パラメータにはオプションが含まれる	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ます。
指定したセキュリティ タイプとは一致せず、アクセス パラメータにオプションも含まれない	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。 **注：** この制限はパラメータには適用されません。このパラメータには、指定されていなくても常にが含まれるためです。

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。krb5p認証方式は認証パラメータとして次のように使用できます。

```
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

ONTAP 9以降では、LDAPサーバへの照会で署名と封印を使用してセッション セキュリティを有効にすることができます。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。この機能を有効にするには、-session-security-for-ad-ldap パラメータを指定してvserver cifs security modify コマンドを実行します。LDAPセキュリティ機能には次のオプションがあります。

- none（デフォルト、署名も封印もなし）
- sign（LDAPトラフィックを署名）
- seal（LDAPトラフィックを署名して暗号化）

注： 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が指定されない場合、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

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 アクセスとファイル操作を可視化して対処できるようにすることは、セキュリティ体制を維持するために不可欠です。ファイルの可視化とアクセス制御を可能にするために、ONTAPではFPolicy™機能を使用しています。FPolicyは、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する機能を備えたONTAPソリューションのインフラ コンポーネントです。

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。

FPolicy機能を利用するには、まずvserver fpolicy policy create 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。また、FPolicyを使用してイベントの表示と収集を行う場合は、-events パラメータを使用します。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。ユーザ名の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。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
```

FPolicyポリシーを作成したら、vserver fpolicy enable コマンドを使用して有効にする必要があります。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、vserver fpolicy show コマンドを使用して、FPolicyポリシーを有効にし、設定を検証する設定例を示しています。

```
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.
```

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。

フィルタによる制御

SetAttrおよびディレクトリ操作に対する通知の削除に使用できるフィルタが新たに追加されました。

非同期の耐障害性

FPolicyサーバが非同期モードで動作している場合にネットワークが停止すると、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。停止中に通知を格納できる期間は、10分までの範囲で設定可能です。

論理インターフェイスの保護

論理インターフェイス（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されるポートに設定できます。

LIFのロールは次のとおりです。

- **データLIF**：SVMに関連付けられたLIF。クライアントとの通信に使用されます。
- **クラスタLIF**：クラスタ内のノード間トラフィックに使用される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に専用のIPアドレスを提供するLIFです。
- **クラスタ管理LIF**：クラスタ全体に対する単一の管理インターフェイスを提供するLIFです。
- **インタークラスタ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。

それぞれのLIFロールのセキュリティ特性については、を参照してください。

表10）LIFのセキュリティ

	データLIF	クラスタLIF	ノード管理LIF	クラスタ管理LIF	インタークラスタ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

注： 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。

LIFの保護の詳細については、ONTAP 9ドキュメント センターの『ONTAP 9ネットワーク管理ガイド』を参照してください。

プロトコルとポートの保護

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。表10は、ONTAPで使用される代表的なプロトコルとポートの一覧です。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。

表 10）広く使用されてい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	Secure Shellログイン
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 プロシージャ コール
NTP	123 / UDP	ネットワーク タイム プロトコル
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HTTP
microsoft-ds	445 / TCP	Microsoftディレクトリ サービス
IPsec	500/UDP	Internet Protocol Securityの略。
mount	635 / UDP	NFSマウント
named	953 / UDP	ネーム デーモン
NFS	2049 / UDP 2049 / TCP	NFSサーバ デーモン
nrv	2050 / TCP	ネットアップ 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
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	4444 / UDP	Kerberos 524
IPsec	4、500 / UDP	Internet Protocol Securityの略。
acp	5125 / UDP 5133 / UDP 5144 / TCP	ディスク用の代替制御ポート
Mdns	5353 / 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	ノードを対象としたTelnet
HTTPS	8443 / TCP	HTTPSを使用した7MTT GUIツール
RSH	8514 / TCP	ノードを対象としたRSH
KMIP	9877 / TCP	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 witness port	40001 / TCP	CIFS監視ポート
TLS	50000 / TCP	Transport Layer Security

サービス	ポート / プロトコル	説明
Iscsi	65200 / TCP	iSCSIポート
SSH	65502 / TCP	Secure Shell
vsun	65503 / TCP	vsun

表 11）ネットアップ内部ポート

ポート / プロトコル	説明
900	ネットアップ クラスタRPC
902	ネットアップ クラスタRPC
904	ネットアップ クラスタRPC
905	ネットアップ クラスタRPC
910	ネットアップ クラスタRPC
911	ネットアップ クラスタRPC
913	ネットアップ クラスタRPC
914	ネットアップ クラスタRPC
915	ネットアップ クラスタRPC
918	ネットアップ クラスタRPC
920	ネットアップ クラスタRPC
921	ネットアップ クラスタRPC
924	ネットアップ クラスタRPC
925	ネットアップ クラスタRPC
927	ネットアップ クラスタRPC
928	ネットアップ クラスタRPC
929	ネットアップ クラスタRPC
931	ネットアップ クラスタRPC
932	ネットアップ クラスタRPC
933	ネットアップ クラスタRPC
934	ネットアップ クラスタRPC
935	ネットアップ クラスタRPC
936	ネットアップ クラスタRPC
937	ネットアップ クラスタRPC
939	ネットアップ クラスタRPC
940	ネットアップ クラスタRPC
951	ネットアップ クラスタRPC
954	ネットアップ クラスタRPC
955	ネットアップ クラスタRPC
956	ネットアップ クラスタRPC
958	ネットアップ クラスタRPC
961	ネットアップ クラスタRPC
963	ネットアップ クラスタRPC
964	ネットアップ クラスタRPC
966	ネットアップ クラスタRPC
967	ネットアップ クラスタRPC

ポート / プロトコル	説明
7810	ネットアップ クラスタRPC
7811	ネットアップ クラスタRPC
7812	ネットアップ クラスタRPC
7813	ネットアップ クラスタRPC
7814	ネットアップ クラスタRPC
7815	ネットアップ クラスタRPC
7816	ネットアップ クラスタRPC
7817	ネットアップ クラスタRPC
7818	ネットアップ クラスタRPC
7819	ネットアップ クラスタRPC
7820	ネットアップ クラスタRPC
7821	ネットアップ クラスタRPC
7822	ネットアップ クラスタRPC
7823	ネットアップ クラスタRPC
7824	ネットアップ クラスタRPC

セキュリティ関連リソース

脆弱性やインシデントの報告、ネットアップのセキュリティ対応、およびお客様の機密保持に関する詳細については、ネットアップ セキュリティ ポータルを参照してください。

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントやWebサイトを参照してください。

- ONTAP 9 ドキュメントセンター
  http://docs.netapp.com/ontap-9/index.jsp
- ONTAP 9リリース ノート
  http://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.dot-cm-rn%2Fhome.html
- ONTAP 9のコマンド リファレンス
  http://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.dot-cm-cmpr-930%2Fhome.html
- システム アドミニストレーション リファレンス
  http://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.dot-cm-sag%2Fhome.html
- 管理者認証とRBACパワー ガイド
  http://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-adm-auth-rbac%2Fhome.html
- NetApp Encryptionパワー ガイド
  http://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html
- TR-4647 ：『 Multifactor Authentication in ONTAP 9.3 』
  https://www.netapp.com/us/media/tr-4647.pdf
- OpenSSL Ciphers
  https://www.openssl.org/docs/man1.0.2/man1/ciphers.html

- CryptoMod FIPS-140-2レベル1
  https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3387
- NetApp Manageability SDK for ONTAP
  https://netapp.io/2016/11/08/certificate-based-authentication-netapp-manageability-sdk-ontap/
  を使用した証明書ベースの認証
- ONTAP 9ネットワーク管理ガイド
  http://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-nmg/home.html
- ONTAP 9 CA署名済みサーバ証明書の生成とインストール
  https://docs.netapp.com/ontap-9/topic/com.netapp.doc.pow-adm-auth-rbac/GUID-7D65DCFE-A3F7-4898-BFA6-1E4DE6C60DE7.html
- Perfect Forwarding Secrecy ブログ
  https://blog.netapp.com/protecting-your-data-perfect-forward-secrecy-pfs-with-netapp-ontap/

バージョン履歴

バージョン	日付	ドキュメント バージョン履歴
バージョン1.0	2016年12月	初版リリース
バージョン1.1	2017年12月	ONTAP 9.2、9.3、およびFIPS-140-2に関する更新
バージョン1.2	2018年3月	ONTAP 9.4用に更新しました。
バージョン1.3	2019年2月	更新：API証明書認証、イメージ検証、およびNTP
バージョン1.4	2019年3月	LIFのセキュリティおよびNISに関する更新
バージョン1.5	2019年5月	ONTAP 9.6用に更新しました。
バージョン1.6	2019年6月	更新：ポートのセクションとCA署名証明書のプロセスを追加
バージョン1.7	2019年7月	LIF セキュリティが更新されました
バージョン1.8	2019年11月	AutoSupport セクション 9.7 ソフトウェアの暗号化をデフォルトで変更
バージョン1.9	2020年1月	AutoSupport パスワードが SHA512 ハッシュを取得するように設定されました
バージョン1.10	2020年4月	ONTAP REST API による証明書認証が更新されました
バージョン1.11	2020年6月	PFS 暗号設定を追加し、FIPS モードの SSH クライアント要件を明確にしました。
バージョン1.12	2020年7月	セクション 22 の表 10 にあるポート 635 の rlzdbase を削除。
バージョン1.13	2020年10月	IPSec、ONTAP 9.8、および REST 証明書認証に関する説明を追加
バージョン1.14	2020年12月	サービスプロセッサのログイン方法に対する REST API およびファイルシステム監査および変更に対する更新

本ドキュメントに記載されている、特定バージョンの製品と機能がお客様の環境でサポートされるかどうかは、ネットアップ サポート サイトにあるInteroperability Matrix Tool（IMT）で確認してください。NetApp IMTには、ネットアップがサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4569-1020-JP

NetApp