ONTAP hardening guidelines

ONTAP 9

NetApp
July 18, 2024

Table of Contents

ONTAP hardening guidelines

ONTAP security hardening overview

ONTAP provides a set of controls that allow you to harden the ONTAP storage operating system, the industry's leading data management software. Use the guidance and configuration settings for ONTAP to help your organization meet prescribed security objectives for information system confidentiality, integrity, and availability.

The evolution of the current threat landscape presents an organization with unique challenges for protecting its most valuable assets: data and information. The advanced and dynamic threats and vulnerabilities we face are ever increasing in sophistication. Coupled with an increase in the effectiveness of obfuscation and reconnaissance techniques on the part of potential intruders, system managers must address the security of data and information proactively.

> Beginning in July 2024, content from technical reports previously published as PDFs has been integrated with ONTAP product documentation. The ONTAP security documentation now includes content from *TR-4569: Security hardening guide for ONTAP*.

ONTAP image validation

ONTAP provides mechanisms to ensure the ONTAP image is valid at upgrade and at boot time.

Upgrade image validation

Code signing helps verify that ONTAP images installed through nondisruptive image updates or automated nondisruptive image updates, CLIs, or ONTAP APIs are authentically produced by NetApp and have not been tampered with. Upgrade image validation was introduced in ONTAP 9.3.

This feature is a no-touch security enhancement to ONTAP upgrading or reversion. The user is not expected to do anything differently except for optionally verifying the top-level "image.tgz" signature.

Boot-time image validation

Beginning with ONTAP 9.4, Unified Extensible Firmware Interface (UEFI) secure boot is enabled for NetApp AFF A800, AFF A220, FAS2750, and FAS2720 systems and subsequent next-generation systems that employ UEFI BIOS.

During power on, the bootloader validates the whitelist database of secure boot keys with the signature associated with each module that is loaded. After each module is validated and loaded, the boot process continues with the ONTAP initialization. If signature validation fails for any module, the system reboots.

> These items apply to ONTAP images and the platform BIOS.

Local storage administrator accounts

Roles, applications, and authentication

ONTAP provides the security-conscious enterprise with the ability to provide granular access to different administrators through different login applications and methods. This helps customers create a data centric zero-trust model.

These are the roles available for admin and storage virtual machine administrators. The login application methods and login authentication methods are specified.

Roles

With role-based access control (RBAC), users have access to only the systems and options required for their job roles and functions. The RBAC solution in ONTAP limits users' administrative access to the level granted for their defined role, which allows administrators to manage users by assigned role. ONTAP provides several predefined roles. Operators and administrators can create, modify, or delete custom access control roles, and they can specify account restrictions for specific roles.

Predefined roles for cluster administrators

This role…	Has this level of access…	To the following commands or command directories
`admin`	All	All command directories (`DEFAULT`)

`admin-no-fsa` (available beginning in ONTAP 9.12.1)	Read/Write	• All command directories (`DEFAULT`) • `security login rest-role` • `security login role`
	Read only	• `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`
	None	`volume file show-disk-usage`
`autosupport`	All	• `set` • `system node autosupport`
	None	All other command directories (`DEFAULT`)

`backup`	All	`vserver services ndmp`
	Read only	`volume`
	None	All other command directories (`DEFAULT`)
`readonly`	All	• `security login password` For managing own user account local password and key information only • `set`
	None	`security`
	Read only	All other command directories (`DEFAULT`)
`none`	None	All command directories (`DEFAULT`)

The `autosupport` role is assigned to the predefined `autosupport` account, which is used by AutoSupport OnDemand. ONTAP prevents you from modifying or deleting the `autosupport` account. ONTAP also prevents you from assigning the `autosupport` role to other user accounts.

Predefined roles for storage virtual machine (SVM) administrators

Role name	Capabilities

`vsadmin`	• Manage own user account local password and key information • Manage volumes, except volume moves • Manage quotas, qtrees, Snapshot copies, and files • Manage LUNs • Perform SnapLock operations, except privileged delete • Configure protocols: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC and NVMe/TCP • Configure services: DNS, LDAP, and NIS • Monitor jobs • Monitor network connections and network interface • Monitor the health of the SVM
`vsadmin-volume`	• Manage own user account local password and key information • Manage volumes, including volume moves • Manage quotas, qtrees, Snapshot copies, and files • Manage LUNs • Configure protocols: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC and NVMe/TCP • Configure services: DNS, LDAP, and NIS • Monitor network interface • Monitor the health of the SVM
`vsadmin-protocol`	• Manage own user account local password and key information • Configure protocols: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC and NVMe/TCP • Configure services: DNS, LDAP, and NIS • Manage LUNs • Monitor network interface • Monitor the health of the SVM

`vsadmin-backup`	• Manage own user account local password and key information • Manage NDMP operations • Make a restored volume read/write • Manage SnapMirror relationships and Snapshot copies • View volumes and network information
`vsadmin-snaplock`	• Manage own user account local password and key information • Manage volumes, except volume moves • Manage quotas, qtrees, Snapshot copies, and files • Perform SnapLock operations, including privileged delete • Configure protocols: NFS and SMB • Configure services: DNS, LDAP, and NIS • Monitor jobs • Monitor network connections and network interface
`vsadmin-readonly`	• Manage own user account local password and key information • Monitor the health of the SVM • Monitor network interface • View volumes and LUNs • View services and protocols

Application methods

The application method specifies the access type of the login method. Possible values include `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, and `telnet`.

Setting this parameter to `service-processor` grants the user access to the Service Processor. When this parameter is set to `service-processor`, the `-authentication-method` parameter must be set to `password` because the Service Processor only supports password authentication. SVM user accounts cannot access the Service Processor. Therefore, operators and administrators cannot use the `-vserver` parameter when this parameter is set to `service-processor`.

To further restrict access to the `service-processor` use the command `system service-processor ssh add-allowed-addresses`. The command `system service-processor api-service` can be used to update the configurations and certificates.

For security reasons, Telnet and Remote Shell (RSH) are disabled by default because NetApp recommends Secure Shell (SSH) for secure remote access. If there is a requirement or unique need for Telnet or RSH, they must be enabled.

The `security protocol modify` command modifies the existing cluster-wide configuration of RSH and Telnet. Enable RSH and Telnet in the cluster by setting the enabled field to `true`.

Authentication methods

The authentication method parameter specifies the authentication method used for logins.

Authentication method	Description
`cert`	SSL certificate authentication
`community`	SNMP community strings
`domain`	Active Directory authentication
`nsswitch`	LDAP or NIS authentication
`password`	Password
`publickey`	Public key authentication
`usm`	SNMP user security model

> The use of NIS is not recommended due to protocol security weaknesses.

Beginning with ONTAP 9.3, chained two-factor authentication is available for local SSH `admin` accounts using `publickey` and password as the two authentication methods. In addition to the `-authentication-method` field in the `security login` command, a new field named `-second-authentication-method` has been added. Either public key or password can be specified as the `-authentication-method` or the `-second -authentication-method`. However, during SSH authentication, the order is always public key with partial authentication, followed by the password prompt for full authentication.

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

Beginning with ONTAP 9.4, `nsswitch` can be used as a second authentication method with `publickey`.

Beginning with ONTAP 9.12.1, FIDO2 can also be used for SSH authentication using a YubiKey hardware authentication device or other FIDO2 compatible devices.

Beginning with ONTAP 9.13.1:

- `domain` accounts can be used as a second authentication method with `publickey`.
- Time-based one-time password (`totp`) is a temporary passcode generated by an algorithm that uses the current time of day as one of its authentication factors for the second authentication method.
- Public key revocation is supported with SSH publickeys as well as certificates which will be checked for expiration/revocation during SSH.

For more information about multifactor authentication (MFA) for ONTAP System Manager, Active IQ Unified Manager, and SSH, see TR-4647: Multifactor Authentication in ONTAP 9.

Default administrative accounts

The admin account should be restricted because the role of administrator is allowed access using all applications. The diag account allows access to the system shell and should be reserved only for technical support to perform troubleshooting tasks.

There are two default administrative accounts: `admin` and `diag`.

Orphaned accounts are a major security vector that often leads to vulnerabilities, including the escalation of privileges. These are unnecessary and unused accounts that remain in the user account repository. They are primarily default accounts that were never used or for which passwords were never updated or changed. To address this issue, ONTAP supports the removal and renaming of accounts.

> ONTAP cannot remove or rename built-in accounts. However, NetApp recommends locking any unneeded built-in accounts with the lock command.

Although orphaned accounts are a significant security issue, NetApp strongly recommends testing the effect of removing accounts from the local account repository.

List local accounts

To list the local accounts, run the `security login show` command.

```
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.
```

Remove the default admin account

The `admin` account has the role of administrator and is allowed access using all applications.

Steps

1. Create another admin-level account.

   To completely remove the default `admin` account, you must first create another admin-level account that uses the `console` login application.

> Making these changes might cause some undesired effects. Always test new settings that might affect the security status of the solution on a nonproduction cluster first.

Example:

```
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. After you create the new admin account, test access to that account with the `NewAdmin` account login. With the `NewAdmin` login, configure the account to have to same login applications as the default or previous admin account (for example, `http`, `ontapi`, `service-processor`, or `ssh`). This step makes sure that access control is maintained.

   Example:

```
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. After all functions have been tested, you can disable the admin account for all applications before removing it from ONTAP. This step serves as a final test to confirm that there are no lingering functions that rely on the previous admin account.

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

4. To remove the default admin account and all entries for it, run the following command:

```
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.
```

Set the diagnostic (diag) account password

A diagnostic account named `diag` is provided with your storage system. You can use the `diag` account to perform troubleshooting tasks in the `systemshell`. The `diag` account is the only account that can be used to access the systemshell through the `diag` privileged command `systemshell`.

> The systemshell and the associated `diag` account are intended for low-level diagnostic purposes. Their access requires the diagnostic privilege level and is reserved only to be used with guidance from technical support to perform troubleshooting tasks. Neither the `diag` account nor the `systemshell` is intended for general administrative purposes.

Before you begin

Before accessing the `systemshell`, you must set the `diag` account password by using the `security login password` command. You should use strong password principles and change the `diag` password at regular intervals.

Steps

1. Set the `diag` account user password:

```
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%
```

Multi-admin verification

Beginning with ONTAP 9.11.1, you can use multi-admin verification (MAV) to allow certain operations, such as deleting volumes or Snapshot copies, to be executed only after approvals from designated administrators. This prevents compromised, malicious, or inexperienced administrators from making undesirable changes or deleting data.

Configuring MAV consists of the following:

- Creating one or more administrator approval groups.
- Enabling multi-admin verification functionality.
- Adding or modifying rules.

After initial configuration, only administrators in a MAV approval group (MAV administrators) can modify these elements.

When MAV is enabled, the completion of every protected operation requires three steps:

1. When a user initiates the operation, a request is generated.
2. Before it can be executed, the required number of MAV administrators must approve.
3. After approval, the user completes the operation.

MAV is not intended for use with volumes or workflows that involve heavy automation because each automated task requires approval before the operation can be completed. If you want to use automation and MAV together, NetApp recommends that you use queries for specific MAV operations. For example, you can apply `volume delete` MAV rules only to volumes where automation is not involved, and you can designate those volumes with a particular naming scheme.

For more detailed information about MAV, see the ONTAP multi-admin verification documentation.

Snapshot copy locking

Snapshot copy locking is a SnapLock capability where Snapshot copies are rendered indelible manually or automatically with a retention period on the volume Snapshot policy. The purpose of Snapshot copy locking is to prevent rogue or untrusted administrators from deleting Snapshots on primary or secondary ONTAP system.

Snapshot copy locking was introduced in ONTAP 9.12.1. Snapshot copy locking is also referred to as tamper-proof Snapshot locking. Although it does require the SnapLock license and initialization of the compliance clock, Snapshot copy locking is unrelated to SnapLock Compliance or SnapLock Enterprise. There is no trusted storage administrator, as with SnapLock Enterprise and it does not protect the underlying physical storage infrastructure, as with SnapLock Compliance. This is an improvement over SnapVaulting Snapshot copies to a secondary system. Rapid recovery of locked Snapshots on primary systems can be achieved to restore volumes corrupted by ransomware.

For more details on Snapshot copy locking, see the ONTAP documentation.

Set up certificate-based API access

Instead of user ID and password authentication for REST API or NetApp Manageability SDK API access to ONTAP, certificate-based authentication must be used.

> ⓘ As an alternative to certificate-based authentication for REST API, use OAuth 2.0 token-based authentication.)

You can generate and install a self-signed certificate on ONTAP as described in these steps.

Steps

1. Using OpenSSL, generate a certificate by running the following command:

```
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'
```

   This command generates a public certificate named `test.pem` and a private key named `key.out`. The common name, CN, corresponds to the ONTAP user ID.

2. Install the contents of the public certificate in privacy enhanced mail (pem) format in ONTAP by running the following command and pasting the certificate’s contents when prompted:

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

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

3. Enable ONTAP to allow client access through SSL and define the user ID for API access.

   ```
   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
   ```

   In the following example, the user ID `cert_user` is now enabled to use certificate-authenticated API access. A simple Manageability SDK Python script using `cert_user` to display the ONTAP version appears as follows:

   ```
   #!/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)
   ```

   The output of the script displays the ONTAP version.

```
./version.py

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

4. To perform certificate-based authentication with the ONTAP REST API, complete the following steps:
   a. In ONTAP, define the user ID for http access:

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

   b. On your Linux client, run the following command that produces the ONTAP version as output:

   ```
   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"
           }
       }
   }
   ```

More information

- Certificate based authentication with the NetApp Manageability SDK for ONTAP.

ONTAP OAuth 2.0 token-based authentication for REST API

As an alternative to certificate-based authentication, you can use OAuth 2.0 token-based authentication for REST API.

Beginning with ONTAP 9.14.1, you have the option to control access to your ONTAP clusters using the Open Authorization (OAuth 2.0) framework. You can configure this feature using any of the ONTAP administrative interfaces, including the ONTAP CLI, System Manager, and REST API. However, the OAuth 2.0 authorization and access control decisions can only be applied when a client accesses ONTAP using the REST API.

OAuth 2.0 tokens replace passwords for user account authentication.

For more information about using OAuth 2.0, see the ONTAP documentation on authentication and authorization using OAuth 2.0.

Login and password parameters

An effective security posture adheres to established organizational policies, guidelines, and any governance or standards that apply to the organization. Examples of these requirements include user name lifetime, password-length requirements, character requirements, and the storage of such accounts. The ONTAP solution provides features and functions to address these security constructs.

New local account features

To support an organization’s user account policies, guidelines, or standards, including governance, the following functionality is supported in ONTAP:

- Configuring password policies to enforce a minimum number of digits, lowercase characters, or uppercase characters
- Requiring a delay after a failed login attempt
- Defining the account inactive limit
- Expiring a user account
- Displaying a password expiration warning message
- Notification of an invalid login

ⓘ Configurable settings are managed by using the security login role config modify command.

SHA-512 support

To enhance password security, ONTAP 9 supports the SHA-2 password hash function and defaults to using SHA-512 for hashing newly created or changed passwords. Operators and administrators can also expire or lock accounts as needed.

Pre-existing ONTAP 9 user accounts with unchanged passwords continue to use the MD5 hash function after the upgrade to ONTAP 9.0 or later. However, NetApp strongly recommends that these user accounts migrate to the more secure SHA-512 solution by having users change their passwords.

The password hash functionality enables you to perform the following tasks:

- Display user accounts that match the specified hash function:

```
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
```

- Expire accounts that use a specified hash function (for example, MD5), which forces users to change their passwords at the next login:

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

- Lock accounts with passwords that use the specified hash function.

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

The password hash function is unknown for the internal `autosupport` user in your cluster’s administrative SVM. This issue is cosmetic. The hash function is unknown because this internal user does not have a configured password by default.

  - To view the password hash function for the `autosupport` user, run the following commands:

```
::> 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
```

  - To set the password hash function (default: sha512), run the following command:

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

It does not matter what the password is set to.

```
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
```

Password parameters

The ONTAP solution supports password parameters that address and support organizational policy requirements and guidelines.

Table 1. Restrictions for management utility user accounts

Attribute	Description	Default	Range
`username-minlength`	Minimum user name length required	3	3-16
`username-alphanum`	User name alphanumeric	disabled	Enabled/disabled
`passwd-minlength`	Minimum password length required	8	3-64
`passwd-alphanum`	Password alphanumeric	enabled	Enabled/disabled
`passwd-min-special-chars`	Minimum number of special characters required in the password	0	0-64
`passwd-expiry-time`	Password expiration time (in days)	Unlimited, which means the passwords never expire	0-unlimited 0 == expire now
`require-initial-passwd-update`	Require initial password update on first login	Disabled	Enabled/disabled Changes allowed through console or SSH

Attribute	Description	Default	Range
`max-failed-login-attempts`	Maximum number of failed attempts	0, do not lock account	-
`lockout-duration`	Maximum lockout period (in days)	The default is 0, which means the account is locked for one day	-
`disallowed-reuse`	Disallow last N passwords	6	Minimum is 6
`change-delay`	Delay between password changes (in days)	0	-
`delay-after-failed-login`	Delay after each failed login attempt (in seconds)	4	-
`passwd-min-lowercase-chars`	Minimum number of lowercase alphabetic characters required in the password	0, which requires no lowercase characters	0-64
`passwd-min-uppercase-chars`	Minimum number of uppercase alphabetic characters required	0, which requires no uppercase characters	0-64
`passwd-min-digits`	Minimum number of digits required in the password	0, which requires no digits	0-64
`passwd-expiry-warn-time`	Display warning message before password expiration (in days)	Unlimited, which means never warn about password expiration	0, which means warn user about password expiration upon every successful login
`account-expiry-time`	Account expires in N days	Unlimited, which means the accounts never expire	The account expiration time must be greater than the account inactive limit
`account-inactive-limit`	Maximum duration of inactivity before account expiration (in days)	Unlimited, which means the inactive accounts never expire	The account inactive limit must be less than the account expiration time

Example

```
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
```

Beginning in 9.14.1, there are increased complexity and lockout rules for passwords. This applies only to new installs of ONTAP.

System administration methods

These are important parameters to strengthen ONTAP system administration.

Command-line access

Establishing secure access to systems is a critical part of maintaining a secure solution. The most common command-line access options are SSH, Telnet, and RSH. Of these, SSH is the most secure, industry-standard best practice for remote command-line access. NetApp highly recommends using SSH for command-line access to the ONTAP solution.

SSH configurations

The `security ssh show` command shows the configurations of the SSH key exchange algorithms, ciphers, and MAC algorithms for the cluster and SVMs. The key exchange method uses these algorithms and ciphers to specify how the one-time session keys are generated for encryption and authentication and how server authentication takes place.

```
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.
```

Login banners

Login banners allow an organization to present any operators, administrators, and even miscreants with terms and conditions of acceptable use, and they indicate who is permitted access to the system. This approach is helpful for establishing expectations for access and use of the system. The `security login banner modify` command modifies the login banner. The login banner is displayed just before the authentication step during the SSH and console device login process. The banner text must be in double quotes (“ ”), as shown in the following example.

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

Login banner parameters

Parameter	Description
`vserver`	Use this parameter to specify the SVM with the modified banner. Use the name of the cluster admin SVM to modify the cluster-level message. The cluster-level message is used as the default for data SVMs that do not have a message defined.

Parameter	Description
`message`	This optional parameter can be used to specify a login banner message. If the cluster has a login banner message set, the cluster login banner is used by all data SVMs as well. Setting a data SVM's login banner overrides the display of the cluster login banner. To reset a data SVM login banner to use the cluster login banner, use this parameter with the value "-". If you use this parameter, the login banner cannot contain newlines (also known as ends of lines [EOLs] or line breaks). To enter a login banner message with newlines, do not specify any parameter. You are prompted to enter the message interactively. Messages entered interactively can contain newlines. Non-ASCII characters must use Unicode UTF-8.
`uri`	`(ftp|http)://(hostname|IPv4` Use this parameter to specify the URI from which the login banner is downloaded. The message must not exceed 2048 bytes in length. Non-ASCII characters must be provided as Unicode UTF-8.

Message of the day

The `security login motd modify` command updates the message of the day (MOTD).

There are two categories of MOTD: the cluster-level MOTD and the data SVM-level MOTD. A user logging in to a data SVM's clustershell might see two messages: the cluster-level MOTD followed by the SVM-level MOTD for that SVM.

The cluster administrator can enable or disable the cluster-level MOTD on each SVM individually if needed. If the cluster administrator disables the cluster-level MOTD for an SVM, a user logging in to the SVM does not see the cluster-level message. Only a cluster administrator can enable or disable the cluster-level message.

MOTD Parameter	Description
Vserver	Use this parameter to specify the SVM for which the MOTD is modified. Use the name of the cluster admin SVM to modify the cluster-level message.

MOTD Parameter	Description
message	This optional parameter can be used to specify a message. If you use this parameter, the MOTD cannot contain newlines. If you do not specify any parameter other than the `-vserver` parameter, you are prompted to enter the message interactively. Messages entered interactively can contain newlines. Non-ASCII characters must be provided as Unicode UTF-8. The message can contain dynamically generated content using the following escape sequences: • `\\` - A single backlash character • `\b` - No output (supported for compatibility with Linux only) • `\C` - Cluster name • `\d` - Current date as set on the login node • `\t` - Current time as set on the login node • `\I` - Incoming LIF IP address (prints console for a `console` login) • `\l` - Login device name (prints console for a `console` login) • `\L` - Last login for the user on any node in the cluster • `\m` - Machine architecture • `\n` - Node or data SVM name • `\N` - Name of user logging in • `\o` - Same as \O. Provided for Linux compatibility. • `\O` - DNS domain name of the node. Note that the output depends on the network configuration and may be empty. • `\r` - Software release number • `\s` - Operating system name • `\u` - Number of active clustershell sessions on the local node. For the cluster admin: all clustershell users. For the data SVM admin: only active sessions for that data SVM. • `\U` - Same as `\u`, but has `user` or `users` appended • `\v` - Effective cluster version string • `\W` - Active sessions across the cluster for the user logging in (`who`)

For more information on configuring the Message of the Day in ONTAP, see the ONTAP documentation on message of the day.

CLI session timeout

The default CLI session timeout is 30 minutes. The timeout is important to prevent stale sessions and session piggybacking.

Use the `system timeout show` command to view the current CLI session timeout. To set the timeout value, use the `system timeout modify -timeout <minutes>` command.

Web access with NetApp ONTAP System Manager

If an ONTAP administrator prefers to use a graphical interface instead of the CLI for accessing and managing a cluster, use NetApp ONTAP System Manager. It is included with ONTAP as a web service, enabled by default, and accessible by using a browser. Point the browser to the host name if using DNS or the IPv4 or IPv6 address through `https://cluster-management-LIF`.

If the cluster uses a self-signed digital certificate, the browser might display a warning indicating that the certificate is not trusted. You can either acknowledge the risk to continue access or install a certificate authority (CA) signed digital certificate on the cluster for server authentication.

Beginning with ONTAP 9.3, Security Assertion Markup Language (SAML) authentication is an option for ONTAP System Manager.

SAML authentication for ONTAP System Manager

SAML 2.0 is a widely adopted industry standard that allows any third-party SAML-compliant identity provider (IdP) to perform MFA using mechanisms unique to the IdP of the enterprise’s choosing and as a source of single sign-on (SSO).

There are three roles defined in the SAML specification: the principal, the IdP, and the service provider. In the ONTAP implementation, a principal is the cluster administrator gaining access to ONTAP through ONTAP System Manager or NetApp Active IQ Unified Manager. The IdP is third-party IdP software. Beginning with ONTAP 9.3, Microsoft Active Directory Federated Services (ADFS) and the open-source Shibboleth IdP are supported IdPs. Beginning with ONTAP 9.12.1, Cisco DUO is a supported IdP. The service provider is the SAML capability built into ONTAP that is used by ONTAP System Manager or the Active IQ Unified Manager web application.

Unlike the SSH two-factor configuration process, after SAML authentication is activated, ONTAP System Manager or ONTAP Service Processor access requires all existing administrators to authenticate through the SAML IdP. No changes are required to the cluster user accounts. When SAML authentication is enabled, a new authentication method of `saml` is added to existing users with administrator roles for `http` and `ontapi` applications.

After SAML authentication is enabled, additional new accounts requiring SAML IdP access should be defined in ONTAP with the administrator role and the saml authentication method for `http` and `ontapi` applications. If SAML authentication is disabled at some point, these new accounts require the `password` authentication method to be defined with the administrator role for `http` and `ontapi` applications and addition of the console application for local ONTAP authentication to ONTAP System Manager.

After the SAML IdP is enabled, the IdP performs authentication for ONTAP System Manager access by using methods available to the IdP, such as Lightweight Directory Access Protocol (LDAP), Active Directory (AD), Kerberos, password, and so on. The methods available are unique to the IdP. It is important that the accounts configured in ONTAP have user IDs that map to the IdP authentication methods.

IdPs that have been validated by NetApp are Microsoft ADFS, Cisco DUO, and open-source Shibboleth IdP.

Beginning with ONTAP 9.14.1, Cisco DUO can be used as a second authentication factor for SSH.

For more information about MFA for ONTAP System Manager, Active IQ Unified Manager, and SSH, see TR-4647: Multifactor Authentication in ONTAP 9.

ONTAP System Manager insights

Beginning with ONTAP 9.11.1, ONTAP System Manager provides insights to help cluster administrators streamline their day-to-day tasks. The security insights are based on the recommendations of this technical report.

Security Insight	Determination
Telnet is enabled	NetApp recommends Secure Shell (SSH) for secure remote access.
Remote Shell (RSH) is enabled	NetApp recommends SSH for secure remote access.
AutoSupport is using an insecure protocol	AutoSupport is not configured to be sent over xref:./ontap-hardening/httpS.
Login banner is not configured on the cluster at cluster level	Warning if login banner is not configured for the cluster.
SSH is using insecure ciphers	Warning if SSH uses insecure ciphers.
Too few NTP servers are configured	Warning if the number of NTP servers configured is less than three.
Default admin user not locked	When not using any default administrative accounts (admin or diag) to log in to System Manager, and these accounts are not locked, the recommendation is to lock them.
Ransomware defense — volumes don’t have Snapshot policies	No adequate Snapshot policy is attached to one or more volumes.
Ransomware defense — disable Snapshot auto-delete	Snapshot auto-delete is set for one or more volumes.
Volumes are not being monitored for ransomware attacks	Autonomic ransomware protection is supported on several volumes but not yet configured.
SVMs are not configured for autonomic ransomware protection	Autonomic ransomware protection is supported on several SVMs but not yet configured.
Native FPolicy is not configured	FPolicy is not set for NAS SVMs.
Enable autonomic ransomware protection active mode	Several volumes have completed their learning mode and you can switch on active mode
Global FIPS 140-2 compliance is disabled	Global FIPS 140-2 compliance is not enabled.
Cluster is not configured for notifications	Emails, webhooks or SNMP traphosts are not configured to receive notifications.

For more information about ONTAP System Manager insights, see the ONTAP System Manager insights documentation.

ONTAP autonomous ransomware protection

To supplement user behavior analytics for Storage Workload Security, the ONTAP autonomous ransomware protection analyzes volume workloads and entropy to detect ransomware and takes a Snapshot and notifies the administrator when an attack is suspected.

In addition to ransomware detection and prevention using external FPolicy user behavioral analytics (UBA) with NetApp Cloud Insights / Cloud Secure and the NetApp FPolicy partner ecosystem, ONTAP 9.10.1 introduces autonomous ransomware protection. ONTAP autonomous ransomware protection uses a built-in on-box machine learning (ML) capability that looks at volume workload activity plus data entropy to automatically detect ransomware. It monitors for activity that is different from UBA so that it can detect attacks that UBA does not.

For more detailed information about this capability, see TR-4572: The NetApp Solution for Ransomware or the ONTAP autonomous ransomware protection documentation.

Storage administrative system auditing

Ensure the integrity of event auditing by offloading ONTAP events to a remote syslog server. This server could be a security information event management system such as Splunk.

Send out syslog

Log and audit information is invaluable to an organization from a support and availability standpoint. In addition, the information and details contained in logs (syslog) and audit reports and outputs are generally of a sensitive nature. To maintain security controls and posture, it is imperative that organizations manage log and audit data in a secure manner.

Offloading of syslog information is necessary for limiting the scope or footprint of a breach to a single system or solution. Therefore, NetApp recommends securely offloading syslog information to a secure storage or retention location.

Create a log-forwarding destination

Use the `cluster log-forwarding create` command to create log-forwarding destinations for remote logging.

Parameters

Use the following parameters to configure the `cluster log-forwarding create` command:

- **Destination host.** This name is the host name or IPv4 or IPv6 address of the server to which to forward the logs.

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

- **Destination port.** This is the port on which the destination server listens.

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

- **Log-forwarding protocol.** This protocol is used for sending messages to the destination.

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

The log-forwarding protocol can use one of the following values:

  - `udp-unencrypted`. User Datagram Protocol with no security.
  - `tcp-unencrypted`. TCP with no security.
  - `tcp-encrypted`. TCP with Transport Layer Security (TLS).

- **Verify destination server identity.** When this parameter is set to true, the identity of the log-forwarding destination is verified by validating its certificate. The value can be set to true only when the `tcpencrypted` value is selected in the protocol field.

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

- **Syslog facility.** This value is the syslog facility to use for the forwarded logs.

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

- **Skip the connectivity test.** Normally, the `cluster log-forwarding create` command checks that the destination is reachable by sending an Internet Control Message Protocol (ICMP) ping and fails if it is not reachable. Setting this value to `true` bypasses the ping check so that you can configure the destination when it is unreachable.

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

NetApp recommends using the `cluster log-forwarding` command to force the connection to a `-tcp-encrypted` type.

Event notification

Securing the information and data leaving a system is vital to maintaining and managing the system's security posture. The events generated by the ONTAP solution provide a wealth of information about what the solution is encountering, the information processed, and more. The vitality of this data highlights the need to manage and migrate it in a secure manner.

The `event notification create` command sends a new notification of a set of events defined by an event filter to one or more notification destinations. The following examples depict the event notification configuration and the `event notification show` command, which displays the configured event notification filters and destinations.

```
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
```

Storage encryption

To protect sensitive data in the event of a disk that is stolen, returned, or repurposed use hardware-based NetApp Storage Encryption or software-based NetApp Volume Encryption/NetApp Aggregate Encryption. Both mechanisms are FIPS-140-2 validated and when using hardware-based mechanisms with software-based mechanisms, the solution qualifies for Commercial Solutions for Classified (CSfC) Program. It enables enhanced security protection for secret and top-secret data at rest at both the hardware and software layers.

Data-at-rest encryption is important to protect sensitive data in the event of a disk that is stolen, returned, or repurposed.

ONTAP 9 has three Federal Information Processing Standard (FIPS) 140-2-compliant data-at-rest encryption solutions:

- NetApp Storage Encryption (NSE) is a hardware solution that uses self-encrypting drives.
- NetApp Volume Encryption (NVE) is a software solution that enables encryption of any data volume on any drive type where it is enabled with a unique key for each volume.
- NetApp Aggregate Encryption (NAE) is a software solution that enables encryption of any data volume on any drive type where it is enabled with unique keys for each aggregate.

NSE, NVE, and NAE can use either external key management or the onboard key manager (OKM). Use of NSE, NVE, and NAE does not affect ONTAP storage efficiency features. However, NVE volumes are excluded from aggregate deduplication. NAE volumes participate in and benefit from aggregate deduplication.

The OKM provides a self-contained encryption solution for data at rest with NSE, NVE, or NAE.

NVE, NAE, and OKM use the ONTAP CryptoMod. CryptoMod is listed on the CMVP FIPS 140-2 validated modules list. See FIPS 140-2 Cert# 4144.

To begin OKM configuration, use the `security key-manager onboard enable` command. To configure external Key Management Interoperability Protocol (KMIP) key managers, use the `security key-manager external enable` command. Starting with ONTAP 9.6, multitenancy is supported for external key managers. Use the `-vserver <vserver name>` parameter to enable external key management for a specific SVM. Prior to 9.6, the `security key-manager setup` command was used to configure both OKM and external key managers. For onboard key management, this configuration walks the operator or administrator through the passphrase setup and additional parameters for configuring OKM.

A part of the configuration is provided in the following example:

```
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.
```

Beginning with ONTAP 9.4, You can use the `-enable-cc-mode` true option with `security key-manager setup` to require that users enter the passphrase after a reboot. For ONTAP 9.6 and later, the command syntax is `security key-manager onboard enable -cc-mode-enabled yes`.

Beginning with ONTAP 9.4, you can use the `secure-purge` feature with advanced privilege to nondisruptively “scrub” data on NVE-enabled volumes. Scrubbing data on an encrypted volume ensures that it cannot be recovered from the physical media. The following command securely purges the deleted files on vol1 on SVM vs1:

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

Beginning with ONTAP 9.7, NAE and NVE are enabled by default if the VE license is in place, either OKM or external key managers are configured, and NSE is not used. NAE volumes are created by default on NAE aggregates, and NVE volumes are created by default on non-NAE aggregates. You can override this by entering the following command:

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

Beginning with ONTAP 9.6, you can use an SVM scope to configure external key management for a data SVM in the cluster. This is best for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data. Only the SVM administrator for a given tenant has access to the keys for that tenant. For more information, see enable external key management in ONTAP 9.6 and later in the ONTAP documentation.

Beginning in ONTAP 9.11.1, you can configure connectivity to clustered external key management servers by designating primary and secondary key servers on an SVM. For more information, see configure clustered external key servers in the ONTAP documentation.

Beginning in ONTAP 9.13.1, you can configure external key manager servers in system manager. For more information, see Manage external key managers in the ONTAP documentation.

Data replication encryption

To supplement data at rest encryption, you can encrypt ONTAP data replication traffic between clusters using TLS 1.2 with a pre-shared key for SnapMirror, SnapVault, or FlexCache.

When replicating data for disaster recovery, caching, or backup, you must protect that data during transport over the wire from one ONTAP cluster to another. Doing so prevents malicious man-in-the-middle attacks against sensitive data while it is in flight.

Beginning with ONTAP 9.6, Cluster Peering Encryption provides TLS 1.2 AES-256 GCM encryption support for ONTAP data replication features such as SnapMirror, SnapVault, and FlexCache. Encryption is setup by way of a pre-shared key (PSK) between two cluster peers.

Customers who use technologies like NSE, NVE, and NAE to protect data at rest can also use end-to-end data encryption by upgrading to ONTAP 9.6 or later to use Cluster Peering Encryption.

Cluster peering encrypts all data between the cluster peers. For example, when using SnapMirror, all peering information as well as all SnapMirror relationships between the source and destination cluster peer are encrypted. You cannot send clear-text data between cluster peers with Cluster Peering Encryption enabled.

Beginning with ONTAP 9.6, new cluster-peer relationships have encryption enabled by default. To enable encryption on cluster peer relationships that were created before ONTAP 9.6, you must upgrade the source and destination cluster to 9.6. In addition, you must use the `cluster peer modify` command to change both the source and destination cluster peers to use Cluster Peering Encryption.

You can convert an existing peer relationship to use Cluster Peering Encryption in ONTAP 9.6 as shown in the following example:

```
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 data-in-flight encryption

Customers who use data-at-rest encryption technologies such as NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) and Cluster Peering Encryption (CPE) for data replication traffic can now use end-to-end encryption between client and storage across their hybrid multi-cloud data fabric by upgrading to ONTAP 9.8 or later and using IPsec. IPsec provides an alternative to NFS or SMB/CIFS encryption and is the only encryption in flight option for iSCSI traffic.

In some situations, there might be a requirement to protect all client data transported over the wire (or in flight) to the ONTAP SVM. Doing so prevents replay and malicious man-in-the-middle attacks against sensitive data while it is in flight.

Starting with ONTAP 9.8, Internet Protocol Security (IPsec) provides end-to-end encryption support for all IP traffic between a client and an ONTAP SVM. IPsec data encryption for all IP traffic includes NFS, iSCSI, and SMB/CIFS protocols. IPsec provides the only encryption in flight option for iSCSI traffic.

Providing NFS encryption over the wire is one of the main use cases for IPsec. Prior to ONTAP 9.8, NFS over-the-wire encryption required the setup and configuration of Kerberos to utilize krb5p to encrypt NFS data in flight. This is not always simple or easy to accomplish in every customer environment.

Customers who use data-at-rest encryption technologies such as NetApp Storage Encryption (NSE) or NetApp Volume Encryption (NVE) and Cluster Peering Encryption (CPE) for data replication traffic can now use end-to-end encryption between client and storage across their hybrid multi-cloud data fabric by upgrading to ONTAP 9.8 or later and using IPsec.

IPsec is an IETF standard. ONTAP uses IPsec in transport mode. It also leverages the Internet Key Exchange (IKE) protocol version 2, which uses a pre-shared key (PSK) for negotiating key material between the client and ONTAP with either IPv4 or IPv6. By default, IPsec uses Suite-B AES-GCM 256-bit encryption. Suite-B AES-GMAC256 and AES-CBC256 with 256-bit encryption are also supported.

Although the IPsec capability must be enabled on the cluster, it applies to individual SVM IP addresses through the use of a Security Policy Database (SPD) entry. The policy (SPD) entry contains the client IP address (remote IP subnet), SVM IP address (local IP subnet), the encryption cipher suite to use, and the pre-shared secret (PSK) needed to authenticate via IKEv2 and establish the IPsec connection. In addition to the IPsec policy entry, the client must be configured with the same information (local and remote IP, PSK, and cipher suite) before traffic can flow over the IPsec connection. Beginning with ONTAP 9.10.1, IPsec certificate authentication support is added. This removes IPsec policy limits and enables Windows OS support for IPsec.

If there is a firewall between the client and the SVM IP address, then it must allow the ESP and UDP (port 500 and 4500) protocols, both inbound (ingress) and outbound (egress), for the IKEv2 negotiation to succeed and thus allow IPsec traffic.

For NetApp SnapMirror and cluster peering traffic encryption, cluster peering encryption (CPE) is still recommended over IPsec for secure in-transit over the wire. CPE performs better for these workloads than IPsec. You do not need a license for IPsec, and there are no import or export restrictions.

You can enable IPsec on the cluster and create an SPD entry for a single client and a single SVM IP address as shown in the following example:

```
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 and SSL management

You can enable FIPS 140-2/3 compliance mode for control plane interfaces by setting the `is-fips-enabled` parameter to true with the ONTAP `security config modify` command.

Beginning with ONTAP 9, you can enable the FIPS 140-2 compliance mode for cluster-wide control plane interfaces. By default, the FIPS 140-2-only mode is disabled. You can enable the FIPS 140-2 compliance mode by setting the `is-fips-enabled` parameter to `true` for the `security config modify` command. You can then use the `security config show command` to confirm the online status.

When FIPS 140-2 compliance is enabled, TLSv1 and SSLv3 are disabled, and only TLSv1.1 and TLSv1.2 remain enabled. ONTAP prevents you from enabling TLSv1 and SSLv3 when FIPS 140-2 compliance is enabled. If you enable FIPS 140-2 and then subsequently disable it, TLSv1 and SSLv3 remain disabled, but TLSv1.2 or both TLSv1.1 and TLSv1.2 remain enabled, depending on the previous configuration.

The `security config modify` command modifies the existing cluster-wide security configuration. If you enable the FIPS-compliant mode, the cluster automatically selects only TLS protocols. Use the `-supported -protocols` parameter to include or exclude TLS protocols independently from FIPS mode. By default, FIPS mode is disabled, and ONTAP supports the TLSv1.2, TLSv1.1, and TLSv1 protocols.

For backward compatibility, ONTAP supports adding SSLv3 to the `supported-protocols` list when FIPS mode is disabled. Use the `-supported-cipher-suites` parameter to configure only the Advanced Encryption Standard (AES) or AES and 3DES. You can also disable weak ciphers such as RC4 by specifying !RC4. By default, the supported cipher setting is `ALL:!LOW:!aNULL:!EXP:!eNULL`. This setting means that all supported cipher suites for the protocols are enabled, except for the ones with no authentication, no encryption, no exports, and low-encryption cipher suites. These are suites using 64-bit or 56-bit encryption algorithms.

Select a cipher suite that is available with the corresponding selected protocol. An invalid configuration might cause some functionality to fail to operate properly.

For the correct cipher string syntax, see the ciphers page on OpenSSL (published by the OpenSSL software foundation). Beginning with ONTAP 9.9.1 and later releases, you are no longer required to reboot all the nodes manually after modifying the security configuration.

Enabling FIPS 140-2 compliance has effects on other systems and communications internal and external to ONTAP 9. NetApp highly recommends testing these settings on a nonproduction system that has console access.

> If SSH is used to administer ONTAP 9, then you must use an OpenSSH 5.7 or later client. SSH clients must negotiate with the Elliptic Curve Digital Signature Algorithm (ECDSA) public key algorithm for the connection to be successful.

TLS security can be further hardened by only enabling TLS 1.2 and using Perfect Forward Secrecy (PFS)-capable cipher suites. PFS is a method of key exchange that, when used in combination with encryption protocols like TLS 1.2, helps prevent an attacker from decrypting all network sessions between a client and server. To enable only TLS 1.2 and PFS-capable ciphers suites, use the `security config modify` command from the advanced privilege level as shown in the following example.

> Before changing the SSL interface configuration, it is important to remember that the client must support the cipher’s mentioned (DHE, ECDHE) when connecting to ONTAP. Otherwise, the connection is not allowed.

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

Confirm `y` for each prompt. For more information on PFS, see this NetApp blog.

Beginning with ONTAP 9.11.1 and TLS 1.3 support, you can validate FIPS 140-3.

> The FIPS configuration applies to ONTAP and the platform BMC.

Create a CA-signed digital certificate

For many organizations, the self-signed digital certificate for ONTAP web access is not compliant with their InfoSec policies. On production systems, it is a NetApp best practice to install a CA-signed digital certificate for use in authenticating the cluster or SVM as an SSL server.

You can use the `security certificate generate-csr` command to generate a certificate signing request (CSR), and the `security certificate install` command to install the certificate you receive back from the CA.

Steps

1. To create a digital certificate that is signed by the organization's CA, do the following:
   a. Generate a CSR.
   b. Follow your organization's procedure to request a digital certificate using the CSR from your organization's CA. For example, using Microsoft Active Directory Certificate Services web interface, go to `<CA_server_name>/certsrv` and request a certificate.
   c. Install the digital certificate in ONTAP.

Online certificate status protocol

Online Certificate Status Protocol (OCSP) enables ONTAP applications that use TLS communications, such as LDAP or TLS, to receive digital certificate status when OCSP is enabled. The application receives a signed response signifying that the certificate requested is good, revoked, or unknown.

OCSP enables determination of the current status of a digital certificate without requiring certificate revocation lists (CRLs).

By default, OCSP certificate status checking is disabled. It can be turned on with the command `security config ocsp enable -app name`, where the app name can be `autosupport`, `audit_log`, `fabricpool`, `ems`, `kmip`, `ldap_ad`, `ldap_nis_namemap`, or all. The command requires advanced privilege level.

SSHv2 management

The `security ssh modify` command replaces the existing configurations of the SSH key exchange algorithms, ciphers, or MAC algorithms for the cluster or an SVM with the configuration settings you specify.

NetApp recommends the following:

- Use passwords for user sessions.
- Use a public key for machine access.

Supported ciphers and key exchanges

Ciphers	Key exchange
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	-

Ciphers	Key exchange
aes256-gcm	-
3des-cbc	-

Supported AES and 3DES symmetric encryptions

ONTAP also supports the following types of AES and 3DES symmetric encryptions (also known as ciphers):

- 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

ⓘ The SSH management configuration applies to ONTAP and the platform BMC.

NetApp AutoSupport

The AutoSupport feature of ONTAP allows you to proactively monitor the health of your system and automatically send messages and details to NetApp technical support, your organization’s internal support team, or a support partner. By default, AutoSupport messages to NetApp technical support are enabled when the storage system is configured for the first time. In addition, AutoSupport begins sending messages to NetApp technical support 24 hours after it is enabled. This 24-hour period is configurable. To leverage the communication to an organization’s internal support team, the mail host configuration must be completed.

Only the cluster administrator can perform AutoSupport management (configuration). The SVM administrator has no access to AutoSupport. The AutoSupport feature can be disabled. However, NetApp recommends enabling it because AutoSupport helps speed problem identification and resolution should an issue arise on the storage system. By default, the system collects AutoSupport information and stores it locally even if you disable AutoSupport.

For more details regarding AutoSupport messages, including what is contained in the various messages and where different types of messages are sent, see the NetApp Active IQ Digital Advisor documentation.

AutoSupport messages contain sensitive data including, but not limited to, the following items:

- Log files
- Context-sensitive data regarding specific subsystems
- Configuration and status data
- Performance data

AutoSupport supports HTTPS, HTTP, and SMTP for transport protocols. Because of the sensitive nature of AutoSupport messages, NetApp strongly recommends using HTTPS as the default transport protocol for sending AutoSupport messages to NetApp support.

In addition, you should leverage the `system node autosupport modify` command to specify the targets of AutoSupport data (for example, NetApp technical support, an organization's internal operations, or partners). This command also allows you to specify what specific AutoSupport details to send (for example, performance data, log files, and so on).

To entirely disable AutoSupport, use the `system node autosupport modify -state disable` command.

Network Time Protocol

Although ONTAP enables you to manually set the time zone, date, and time on the cluster, you must configure the Network Time Protocol (NTP) servers to synchronize the cluster time with at least three external NTP servers.

Problems can occur when the cluster time is inaccurate. Although ONTAP enables you to manually set the time zone, date, and time on the cluster, you must configure the Network Time Protocol (NTP) servers to synchronize the cluster time with external NTP servers.

Beginning with ONTAP 9.5, you can configure your NTP server with symmetric authentication.

You can associate a maximum of 10 external NTP servers by using the `cluster time-service ntp server create` command. For redundancy and quality of time service, you should associate at least three external NTP servers with the cluster.

For details about the configuration of NTP in ONTAP, see Managing the cluster time (cluster administrators only).

NAS file system local accounts (CIFS workgroup)

Workgroup client authentication provides an extra layer of security to the ONTAP solution that is consistent with a traditional domain authentication posture. Use the `vserver` `cifs session show` command to display numerous posture-related details, including IP information, the authentication mechanism, the protocol version, and the authentication type.

Starting with ONTAP 9, you can configure a CIFS server in a workgroup with CIFS clients that authenticate to the server by using locally defined users and groups. Workgroup client authentication provides an extra layer of security to the ONTAP solution that is consistent with a traditional domain authentication posture. To configure the CIFS server, use the `vserver cifs create` command. After the CIFS server is created, you can join it to a CIFS domain or join it to a workgroup. To join a workgroup, use the `-workgroup` parameter. Here is an example configuration:

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

> A CIFS server in workgroup mode supports only Windows NT LAN Manager (NTLM) authentication and does not support Kerberos authentication.

NetApp recommends using the NTLM authentication function with CIFS workgroups to maintain your organization's security posture. To validate the CIFS security posture, NetApp recommends using the `vserver cifs session show` command to display numerous posture-related details, including IP information, the authentication mechanism, the protocol version, and the authentication type.

NAS file system auditing

NAS file systems occupy an increased footprint in today's threat landscape, audit functions are critical to support visibility.

Security requires validation. ONTAP 9 provides increased auditing events and details across the solution. Because NAS file systems occupy an increased footprint in today's threat landscape, audit functions are critical to support visibility. Because of the improved audit capability in ONTAP 9, CIFS audit details are more plentiful than ever. Key details, including the following, are logged with events created:

- File, folder, and share access
- Files created, modified, or deleted
- Successful file read access
- Failed attempts to read or write files
- Folder permission changes

Create an audit configuration

You must enable CIFS auditing to generate auditing events. Use the `vserver audit create` command to create an audit configuration. By default, the audit log uses a rotation method based on size. You can use a time-based rotation option if specified in the Rotation Parameters field. Additional log audit rotation configuration details include the rotation schedule, the rotation limits, the rotation days of the week, and the rotation size. The following text provides an example configuration depicting an audit configuration using a monthly time-based rotation scheduled for all days of the week at 12:30.

```
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 audit events

The CIFS audit events are as follows:

- **File share**: Generates an audit event when a CIFS network share is added, modified, or deleted using the related `vserver cifs share` commands.
- **Audit policy change**: Generates an audit event when the audit policy is disabled, enabled, or modified using the related `vserver audit` commands.
- **User account**: Generates an audit event when a local CIFS or UNIX user is created or deleted; a local user account is enabled, disabled, or modified; or a password is reset or changed. This event uses the `vserver cifs users-and-groups local-group` command or the related `vserver services name-service unix-user` command.
- **Security group**: Generates an audit event when a local CIFS or UNIX security group is created or deleted using the `vserver cifs users-and-groups local-group` command or the related `vserver services name-service unix-group` command.
- **Authorization policy change**: Generates an audit event when rights are granted or revoked for a CIFS user or a CIFS group using the `vserver cifs users-and-groups privilege` command.

ⓘ This functionality is based on the system audit function, which enables an administrator to review what the system is allowing and performing from the perspective of a data user.

Effect of REST APIs on NAS auditing

ONTAP includes the ability for administrator accounts to access and manipulate SMB/CIFS or NFS files using REST APIs. Although REST APIs can only be run by ONTAP administrators, REST API commands do bypass the system NAS audit log. Additionally, file permissions can also be bypassed by ONTAP administrators when using REST APIs. However, the administrator’s actions with REST APIs on files are captured in the system command history log.

Create no-access REST API role

You can prevent ONTAP administrators from using REST APIs for file access by creating a REST API role that does not have access to ONTAP volumes via REST. To provision this role, complete the following steps.

Steps

1. Create a new REST role that has no access to storage volumes but has all other REST API access.

   ```
   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. Assign the administrator account to the new REST API role you created in the previous step.

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

> If you want to prevent the built-in ONTAP cluster administrator account from using REST APIs for file access, you need to first create a new administrator account and disable or delete the built-in account.

Configure and enable CIFS SMB signing and sealing

You can configure and enable SMB signing that protects the security of the data fabric by making sure that traffic between storage systems and clients is not compromised by replay or man-in-the-middle attacks. SMB signing protects by verifying that SMB messages have valid signatures.

About this task

A common threat vector for file systems and architectures lies in the SMB protocol. To address this vector, the ONTAP 9 solution uses industry-standard SMB signing and sealing. SMB signing protects the security of the data fabric by making sure that traffic between storage systems and clients is not compromised by replay or man-in-the-middle attacks. It does so by verifying that SMB messages have valid signatures.

Although SMB signing is disabled by default in the interest of performance, NetApp highly recommends that you enable it. In addition, the ONTAP solution supports SMB encryption, which is also known as sealing. This approach enables the secure transport of data on a share-by-share basis. By default, SMB encryption is disabled. However, NetApp recommends that you enable SMB encryption.

LDAP signing and sealing are now supported in SMB 2.0 and later. Signing (protection against tampering) and sealing (encryption) enable secure communication between SVMs and Active Directory servers. Accelerated AES new instructions (Intel AES NI) encryption is now supported in SMB 3.0 and later. Intel AES NI improves on the AES algorithm and accelerates data encryption with supported processor families.

Steps

1. To configure and enable SMB signing, use the `vserver cifs security modify` command and verify that the `-is-signing-required` parameter is set to `true`. See the following example configuration:

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

2. To configure and enable SMB sealing and encryption, use the `vserver cifs security modify` command and verify that the `-is-smb-encryption-required` parameter is set to `true`. See the following example configuration:

```
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 securing

Export rules are the functional elements of an export policy. Export rules match client access requests for a volume against specific parameters you configure to determine how to handle the client access requests. An export policy must contain at least one export rule to allow access to clients. If an export policy contains more than one rule, the rules are processed in the order in which they appear in the export policy.

Access control is central to maintaining a secure posture. Therefore, ONTAP uses the export policy feature to limit NFS volume access to clients that match specific parameters. Export policies contain one or more export rules that process each client access request. An export policy is associated with each volume to configure client access to the volume. The result of this process determines whether the client is granted or denied (with a permission-denied message) access to the volume. This process also determines what level of access is provided to the volume.

> An export policy with export rules must exist on an SVM for clients to access data. An SVM can contain multiple export policies.

The rule order is dictated by the rule index number. If a rule matches a client, the permissions of that rule are used, and no further rules are processed. If no rules match, the client is denied access.

Export rules determine client access permissions by applying the following criteria:

- The file access protocol used by the client sending the request (for example, NFSv4 or SMB)
- A client identifier (for example, host name or IP address)
- The security type used by the client to authenticate (for example, Kerberos v5, NTLM, or AUTH_SYS)

If a rule specifies multiple criteria, and the client does not match one or more of them, the rule does not apply.

An example export policy contains an export rule with the following parameters:

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

The security type determines which level of access a client receives. The three access levels are read-only, read-write, and superuser (for clients with the user ID `0`). Because the access level determined by the security type is evaluated in this order, you must observe the rules listed:

Rules for access-level parameters in export rules

For a client to obtain the following access levels	These access parameters must match the client's security type
Normal user read-only	Read-only (`-rorule`)
Normal user read-write	Read-only (`-rorule`) and read-write (`-rwrule`)
Superuser read-only	Read-only (`-rorule`) and `-superuser`
Superuser read-write	Read-only (`-rorule`) and read-write (`-rwrule`) and `-superuser`

The following are valid security types for each of these three access parameters:

- Any
- None
- Never

These security types are not valid for use with the `-superuser` parameter:

- krb5
- ntlm
- sys

Rules for access parameter outcomes

If the client's security type …	Then …
Matches a security type specified in the access parameter.	The client receives access for that level with its own user ID.
Does not match a specified security type, but the access parameter includes the option `none`.	The client receives access for that level and receives the anonymous user with the user ID specified by the `-anon` parameter.
Does not match a security type specified, and the access parameter does not include the option `none`.	The client does not receive any access for that level. ⓘ This restriction does not apply to the `-superuser` parameter because this parameter always includes none, even when not specified.

Kerberos 5 and Krb5p

Beginning with ONTAP 9, Kerberos 5 authentication with privacy service (krb5p) is supported. The krbp5 authentication mode is secure, and it protects against data tampering and snooping by using checksums to encrypt all traffic between client and server. The ONTAP solution supports 128-bit and 256-bit AES encryption for Kerberos. The privacy service includes verifying the integrity of the received data, authenticating users, and encrypting data before transmission.

The krb5p option is most present in the export policy feature, where it is set as an encryption option. The krb5p authentication method can be used as an authentication parameter, as shown in the following example:

```
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
```

Enable Lightweight Directory Access Protocol signing and sealing

Signing and sealing are supported to enable session security on queries to an LDAP server. This approach provides an alternative to LDAP-over-TLS session security.

Signing confirms the integrity of LDAP payload data using secret key technology. Sealing encrypts the LDAP payload data to avoid transmitting sensitive information in clear text. The session security settings on an SVM correspond to those available on the LDAP server. By default, LDAP signing and sealing are disabled.

Steps

1. To enable this function, run the `vserver cifs security modify` command with the `session-security-for-ad-ldap` parameter.

   Options for LDAP security functions:

   - **None**: Default, no signing or sealing
   - **Sign**: Sign LDAP traffic
   - **Seal**: Sign and encrypt LDAP traffic

   > The sign and seal parameters are cumulative, meaning that if the sign option is used, the outcome is LDAP with signing. However, if the seal option is used, the outcome is both sign and seal. In addition, if a parameter is not specified for this command, the default is none.

   The following is an example configuration:

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

Create and use a NetApp FPolicy

You can create and use an FPolicy, an infrastructure component of the ONTAP solution, that allows partner applications to monitor and set file access permissions. One of the more powerful applications is Storage Workload Security, a NetApp SaaS application that provides centralized visibility and control of all corporate data access across hybrid cloud environments to ensure security and compliance goals are met.

Access control is a key security concept. Visibility and the ability to respond to file access and file operations are critical for maintaining your security posture. To provide visibility and access control for files, the ONTAP solution uses the NetApp FPolicy feature.

File policies can be set based on file type. FPolicy determines how the storage system handles requests from individual client systems for operations such as create, open, rename, and delete. Beginning with ONTAP 9, the FPolicy file access notification framework is enhanced with filtering controls and resiliency against short network outages.

Steps

1. To leverage the FPolicy feature, you must first create the FPolicy policy with the `vserver fpolicy policy create` command.

   > ⓘ In addition, use the `-events` parameter if you use FPolicy for visibility and the collection of events. The additional granularity provided by ONTAP enables filtering and access down to the user name level of control. To control privileges and access with user names, specify the `-privilege-user-name` parameter.

   The following text provides an example of FPolicy creation:

   ```
   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. After you create the FPolicy policy, you must enable it with the `vserver fpolicy enable` command. This command also sets the priority or sequence of the FPolicy entry.

   > ⓘ The FPolicy sequence is important because, if multiple policies have subscribed to the same file access event, the sequence dictates the order in which access is granted or denied.

   The following text provides a sample configuration for enabling the FPolicy policy and validating the configuration with the `vserver fpolicy show` command:

```
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 enhancements

ONTAP 9 includes the FPolicy enhancements described in the following sections.

Filtering controls

New filters are available for `SetAttr` and for removing notifications on directory activities.

Async resiliency

If an FPolicy server operating in asynchronous mode experiences a network outage, FPolicy notifications generated during the outage are stored on the storage node. When the FPolicy server comes back online, it is alerted of the stored notifications and can fetch them from the storage node. The length of time the notifications can be stored during an outage is configurable up to 10 minutes.

LIF security

A LIF is an IP address or worldwide port name (WWPN) with associated characteristics, such as a role, a home port, a home node, a list of ports to fail over to, and a firewall policy. You can configure LIFs on ports over which the cluster sends and receives communications over the network. It is critical to understand the security characteristics of each LIF role.

LIF roles

LIF roles can be the following:

- **Data LIF**: A LIF associated with an SVM and used for communicating with clients.
- **Cluster LIF**: A LIF used to carry intracluster traffic between nodes in a cluster.
- **Node management LIF**: A LIF that provides a dedicated IP address for managing a particular node in a cluster.
- **Cluster management LIF**: A LIF that provides a single management interface for the entire cluster.
- **Intercluster LIF**: A LIF used for cross-cluster communication, backup, and replication.

Security characteristics of each LIF role

	Data LIF	Cluster LIF	Node management LIF	Cluster Management LIF	Intercluster LIF
Requires private IP subnet?	No	Yes	No	No	No
Requires secure network?	No	Yes	No	No	Yes
Default firewall policy	Very restrictive	Completely open	Medium	Medium	Very restrictive
Is the firewall customizable?	Yes	No	Yes	Yes	Yes

- Because the cluster LIF is completely open with no configurable firewall policy, it must be on a private IP subnet on a secure isolated network.
- Under no circumstance should any LIF roles be exposed to the internet.

Learn more about securing LIFs, see the Configure firewall policies for LIFs.

Protocol and port security

In addition to performing on-box security operations and functions, the hardening of a solution must also include off-box security mechanisms. Leveraging additional infrastructure devices, such as firewalls, intrusion prevention systems (IPSs), and other security devices, for filtering and limiting access to ONTAP is an effective way to establish and maintain a stringent security posture. This information is a key component for filtering and limiting access to the environment and its resources.

Commonly used protocols and ports

Service	Port/Protocol	Description
`SSH`	22/TCP	SSH login
`telnet`	23/TCP	Remote login
`Domain`	53/TCP	Domain Name Server
`HTTP`	80/TCP 80/UDP	HTTP
`rpcbind`	111/TCP 111/UDP	Remote procedure call
`NTP`	123/UDP	Network Time Protocol
`msrpc`	135/UDP	Microsoft Remote Procedure Call

Service	Port/Protocol	Description
Netbios-name	137/TCP 137/UDP	NetBIOS name service
netbios-ssn	139/TCP	NetBIOS service session
SNMP	161/UDP	SNMP
HTTPS	443/TCP	Secure xref:./ontap-hardening/http
microsoft-ds	445/TCP	Microsoft directory services
IPsec	500/UDP	Internet Protocol Security
mount	635/UDP	NFS mount
named	953/UDP	Name daemon
NFS	2049/UDP 2049/TCP	NFS server daemon
nrv	2050/TCP	NetApp remote volume protocol
iscsi	3260/TCP	iSCSI target port
Lockd	4045/TCP 4045/UDP	NFS lock daemon
NFS	4046/TCP	NFS mountd protocol
acp-proto	4046/UDP	Accounting protocol
rquotad	4049/UDP	NFS rquotad protocol
krb524	4444/UDP	Kerberos 524
IPsec	4500/UDP	Internet Protocol Security
acp	5125/UDP 5133/UDP 5144/TCP	Alternate control port for disk
Mdns	5353/UDP	Multicast DNS
HTTPS	5986/UDP	HTTPS port: listening binary protocol
TELNET	8023/TCP	Node-scope Telnet
HTTPS	8443/TCP	7MTT GUI tool through xref:./ontap-hardening/httpS
RSH	8514/TCP	Node-scope RSH
KMIP	9877/TCP	KMIP client port (internal local host only)
ndmp	10000/TCP	NDMP
cifs witness port	40001/TCP	CIFS witness port

Service	Port/Protocol	Description
TLS	50000/TCP	Transport layer security
Iscsi	65200/TCP	iSCSI port
SSH	65502/TCP	Secure Shell
vsun	65503/TCP	vsun

NetApp internal ports

Port/Protocol	Description
900	NetApp cluster RPC
902	NetApp cluster RPC
904	NetApp cluster RPC
905	NetApp cluster RPC
910	NetApp cluster RPC
911	NetApp cluster RPC
913	NetApp cluster RPC
914	NetApp cluster RPC
915	NetApp cluster RPC
918	NetApp cluster RPC
920	NetApp cluster RPC
921	NetApp cluster RPC
924	NetApp cluster RPC
925	NetApp cluster RPC
927	NetApp cluster RPC
928	NetApp cluster RPC
929	NetApp cluster RPC
931	NetApp cluster RPC
932	NetApp cluster RPC
933	NetApp cluster RPC
934	NetApp cluster RPC
935	NetApp cluster RPC
936	NetApp cluster RPC
937	NetApp cluster RPC
939	NetApp cluster RPC
940	NetApp cluster RPC

Port/Protocol	Description
951	NetApp cluster RPC
954	NetApp cluster RPC
955	NetApp cluster RPC
956	NetApp cluster RPC
958	NetApp cluster RPC
961	NetApp cluster RPC
963	NetApp cluster RPC
964	NetApp cluster RPC
966	NetApp cluster RPC
967	NetApp cluster RPC
7810	NetApp cluster RPC
7811	NetApp cluster RPC
7812	NetApp cluster RPC
7813	NetApp cluster RPC
7814	NetApp cluster RPC
7815	NetApp cluster RPC
7816	NetApp cluster RPC
7817	NetApp cluster RPC
7818	NetApp cluster RPC
7819	NetApp cluster RPC
7820	NetApp cluster RPC
7821	NetApp cluster RPC
7822	NetApp cluster RPC
7823	NetApp cluster RPC
7824	NetApp cluster RPC

Security resources

To learn more about the information described in this ONTAP security documentation, refer to the following additional information and security concepts.

For information about reporting vulnerabilities and incidents, NetApp security responses, and customer confidentiality, see the NetApp security portal.

- ONTAP 9 Release Notes
- ONTAP 9 Command References

- System Administration
- Administrator Authentication and RBAC
- NetApp Encryption
- TR-4647: Multifactor Authentication in ONTAP 9.3
- OPENSSL Ciphers
- CryptoMod FIPS-140-2 Level 1
- Certificate-Based Authentication with the NetApp Manageability SDK for ONTAP
- Network management

Copyright information

Trademark information