Local storage administrator accounts

ONTAP Technical Reports

NetApp
January 23, 2026

Table of Contents

Local storage administrator accounts

ONTAP 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 with 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, snapshots, 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, except volume moves • Manage quotas, qtrees, snapshots, 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 snapshots • View volumes and network information
`vsadmin-snaplock`	• Manage own user account local password and key information • Manage volumes, except volume moves • Manage quotas, qtrees, snapshots, 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 `publickey` or `password` can be specified as the `-authentication-method` or the `-second-authentication-method`. However, during SSH authentication, the order is always `publickey` 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.

> You cannot remove or rename built-in accounts. If an administrator removes the account, upon reboot, the built-in account will be recreated. **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.
```

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 snapshots, 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 locking

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

Snapshot locking was introduced in ONTAP 9.12.1. Snapshot locking is also referred to as tamper-proof snapshot locking. Although it does require the SnapLock license and initialization of the compliance clock, snapshot 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 snapshots to a secondary system. Rapid recovery of locked snapshots on primary systems can be achieved to restore volumes corrupted by ransomware.

For more details, see the snapshot locking 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.

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

All passwords must be distinct from the user name.

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
```

Copyright information

Trademark information