Module 3
Cluster management

About this module

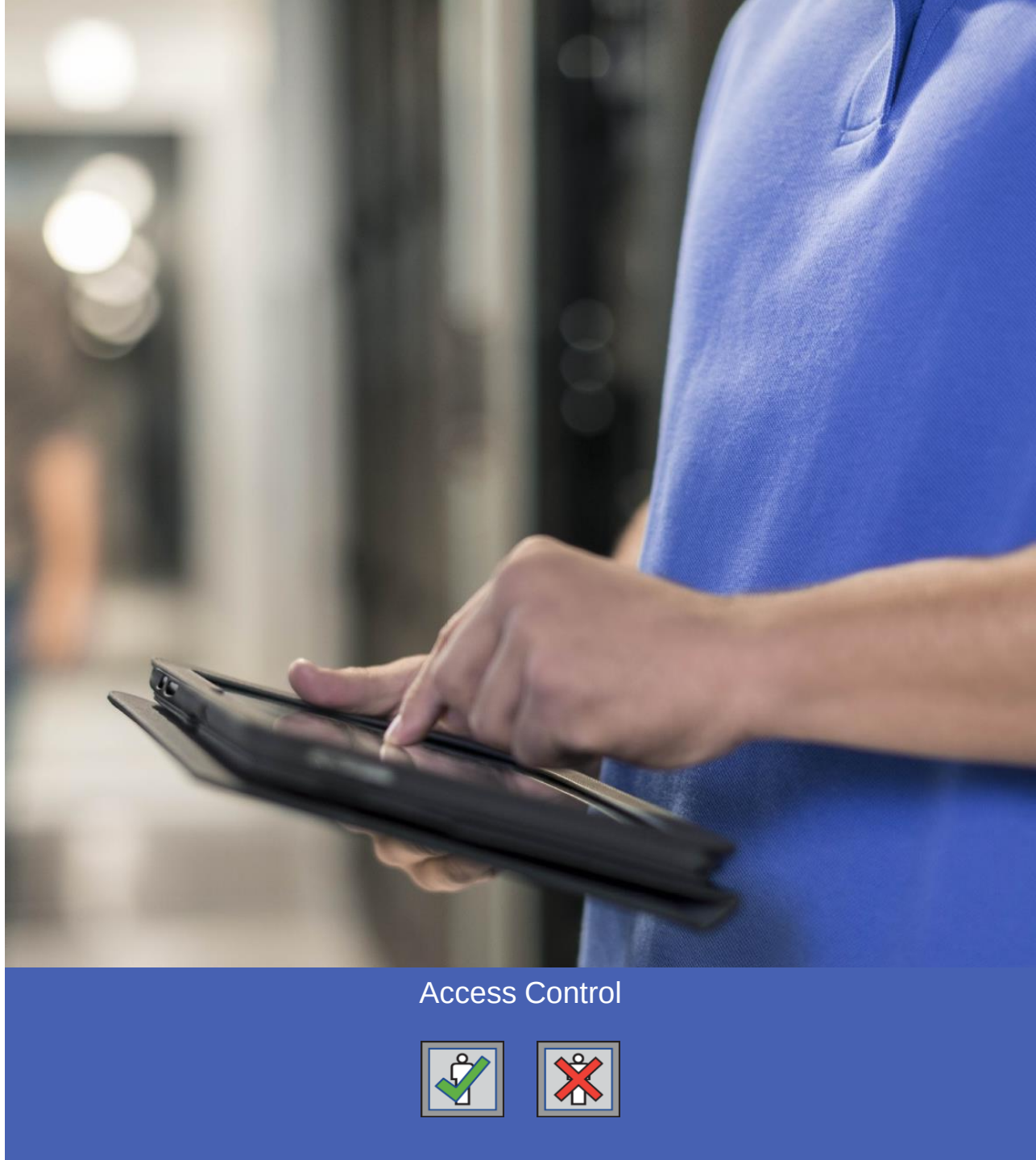
This module focuses on enabling you to do the following:

- Manage access control
- Set the date and time on cluster nodes
- Manage NetApp ONTAP software licenses
- Manage jobs and schedules

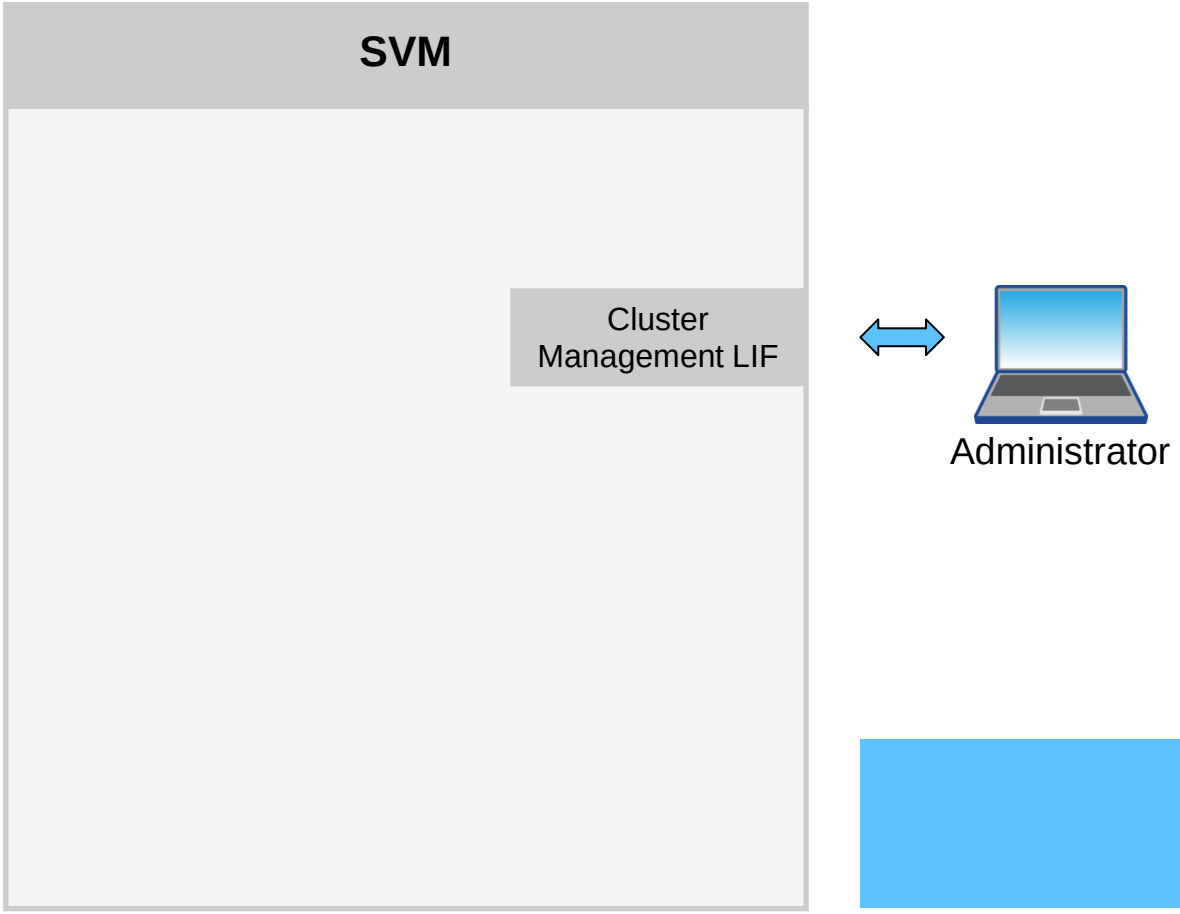
Lesson 1
Access control

Cluster administrators and SVM administrators

- Tasks of cluster administrators:
  - Administer the entire cluster
  - Administer storage VMs (storage virtual machines, also known as SVMs) on the cluster
  - Create and delegate aggregates for SVM administrator use
  - Set up data SVMs and delegate SVM administration to SVM administrators
- Tasks of SVM administrators:
  - Administer only their own data SVMs
  - Set up storage and network resources, such as volumes, protocols, LIFs, and services



Admin storage VM



Admin SVM:

- Created automatically during the cluster setup process
- Representation of the cluster
- *Not* a data server.

  A cluster must have at least one data SVM to serve data to clients.
- Primary access point for administration of nodes, resources, and data SVMs

The cluster management LIF is configured to fail over to any node in the cluster.

Admin access

An administrator account is for a predefined cluster administrator:

- Uses the CLI or NetApp ONTAP System Manager
- Is associated with cluster or data SVMs

You can create additional administrator accounts with role-based access control (RBAC):

```
cluster1::> security login
```


RBAC

RBAC users, roles, and capabilities

Capability

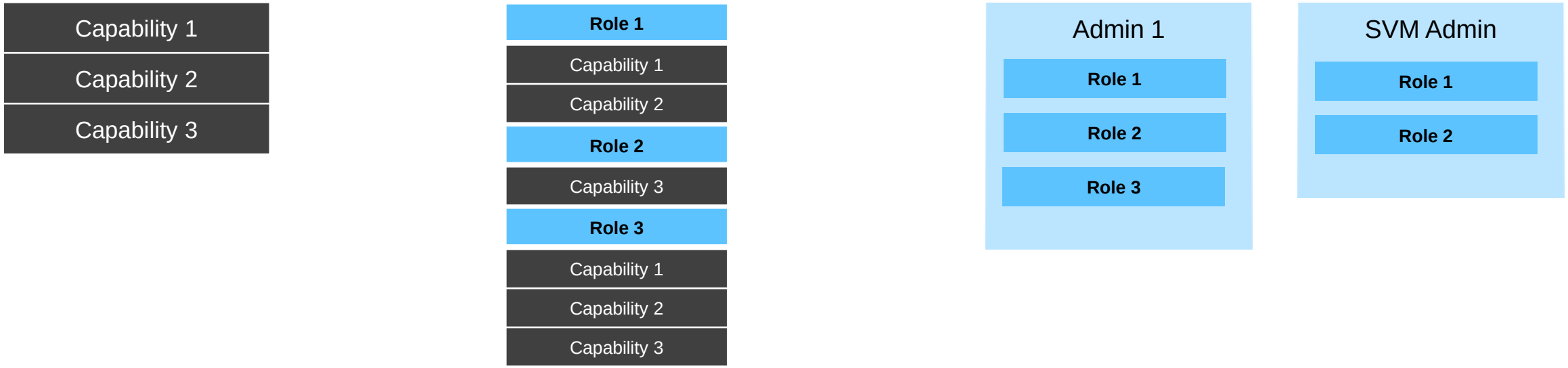
- Includes a command or API endpoint
- Includes an access level:
  - all
  - readonly
  - none

Role

- Is a named set of capabilities and commands
- Is defined for cluster or SVM administration

User

- Is authenticated by the cluster or domain
- Is authenticated for administration, not for data access
- Is created as a cluster admin or SVM admin



RBAC

Predefined roles in ONTAP software

Cluster SVM roles:

- admin
- readonly
- none
- backup
- autosupport

```
::> security login role show -vserver cluster1
```

Data SVM roles:

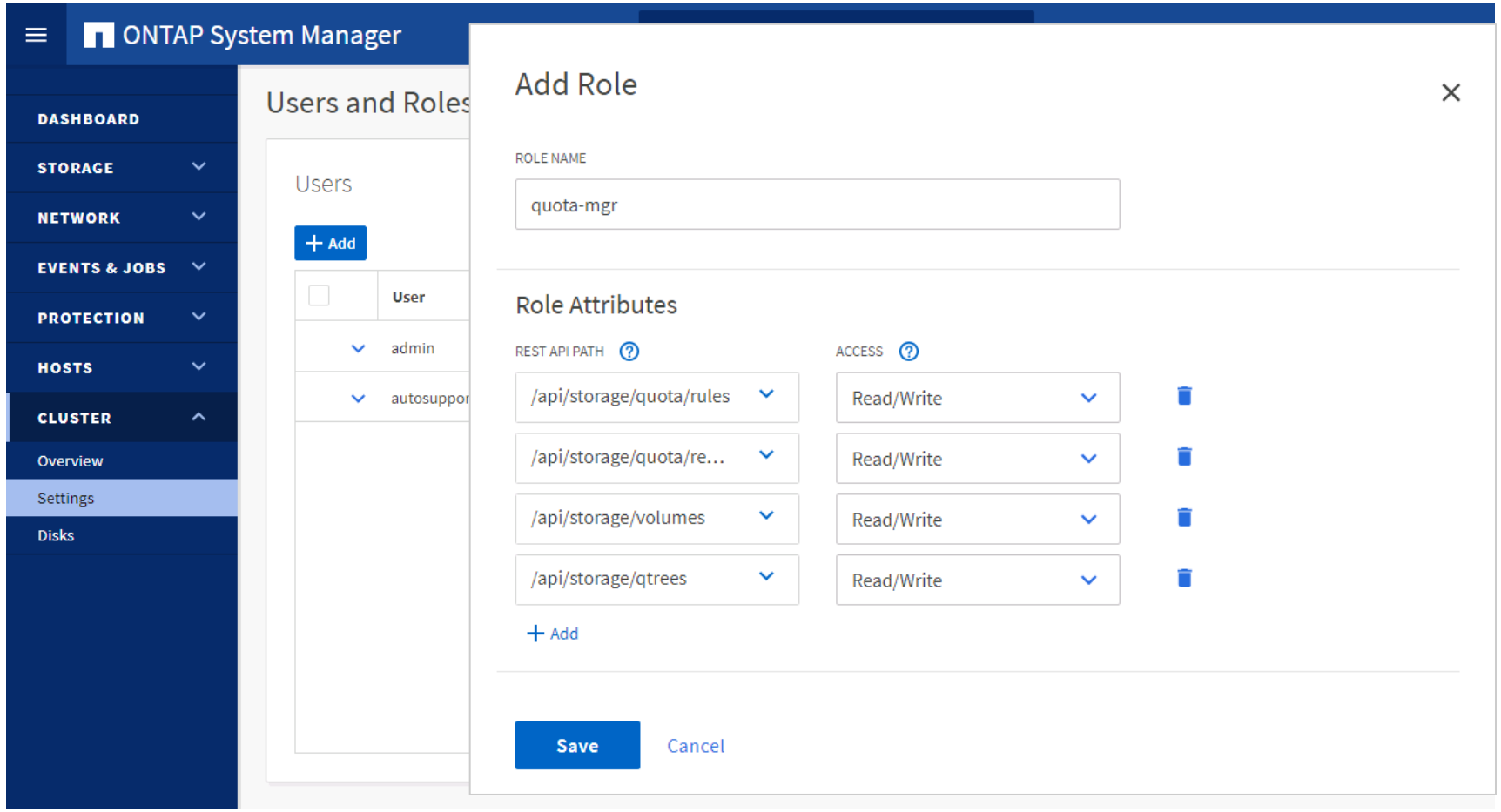
- vsadmin
- vsadmin-volume
- vsadmin-protocol
- vsadmin-backup
- vsadmin-snaplock
- vsadmin-readonly

```
::> security login role show -vserver svm1
```


RBAC

Custom roles

- Role name
- Command directory or API resource
- Optional query or object identifier
- Access level




```
::> security login role create -vserver svm1 -role svm1vols -cmddirname volume -access all
```

```
::> security login modify -vserver svm1 -role svm1vols -user ken
```


Creating ONTAP administrator accounts

- Use the `security login` command to configure role-based administrative access to the cluster.
- Specify the application (access method):
  console, HTTP, SNMP, Secure Shell (SSH), and the API interface.
- Specify the authentication method:
  password, Secure Sockets Layer (SSL) certificate, SNMP community string, Active Directory authentication, Lightweight Directory Access Protocol (LDAP) or Network Information Service (NIS) authentication, public-key authentication, or Security Assertion Markup Language (SAML) authentication.
- Optionally, specify an access-control role.

```
::> security login create -vserver cluster1 -user-or-group-name elsa –role admin
-application http -authentication-method password

Please enter a password for user ‘elsa’: ********
Please enter it again: ********
```


Active Directory authentication for administrators

- You must configure access to an Active Directory domain controller to authenticate domain accounts.
- If you have already configured a CIFS server for a data SVM, you can configure the SVM as a gateway, or *tunnel*, for Active Directory access by the cluster.

```
::> security login domain-tunnel create -vserver svm3
```

- If you have not configured a CIFS server, you can create a computer account for the cluster in the Active Directory domain.

```
::> vserver active-directory create -vserver cluster1 -account-name CLUSTER1 -domain demo.com
```

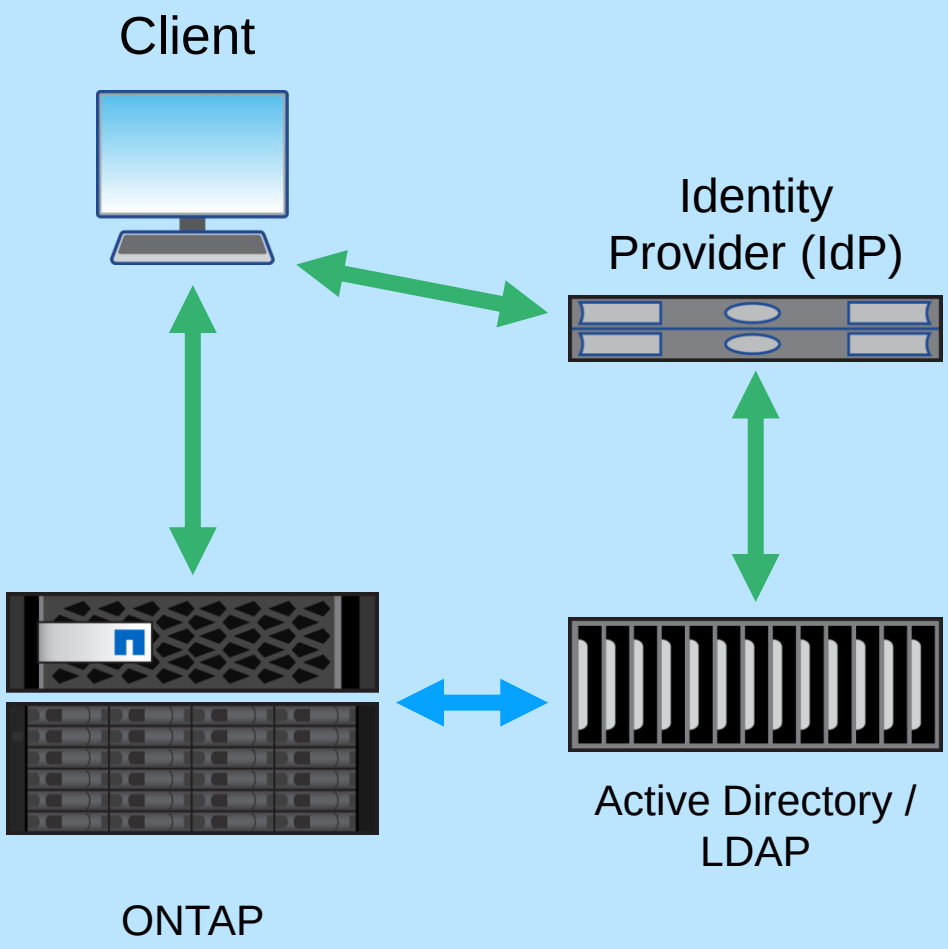
- When a login is created for an Active Directory group, all group members share access privileges.

```
::> security login create -vserver cluster1 –role admin -application ssh
-user-or-group-name demo\Administrators -authentication-method domain
```


Securing administrator access

Multifactor Authentication

- Secure access to System Manager and the ONTAP APIs
  - Use an external identity provider to authenticate users and enforce multifactor authentication.
  - Validated with Microsoft Active Directory Federated Services (ADFS) IdP and open source Shibboleth IdP.
- Secure access to the ONTAP CLI
  - Require both a SSH public key and a password for multifactor authentication.
  - You must associate the public key with the account before the account can access the SVM.
- Require FIPS 140-2 compliant encryption



Administrative auditing

- You can monitor administrator activity for compliance and accountability.
- To enable and disable security audit logging, use the following command:

```
::> security audit modify -cliget on -ontapiget on
```

- Audited commands go to the management log.
- The `security audit log show` command displays cluster-wide audit log messages.

```
::> security audit log show –user elsa
```

- Nodes track local SSH and console commands in the command history log.

Security login banner and message of the day

For legal purposes, some computer systems must display a warning to unauthorized users who are connecting to the system.

- This legal warning is configured in ONTAP software by using the `security login banner` command.

```
::> security login banner modify
```

- The message of the day (MOTD) subcommand enables you to show a message to all cluster and SVM administrators when they open a console session:

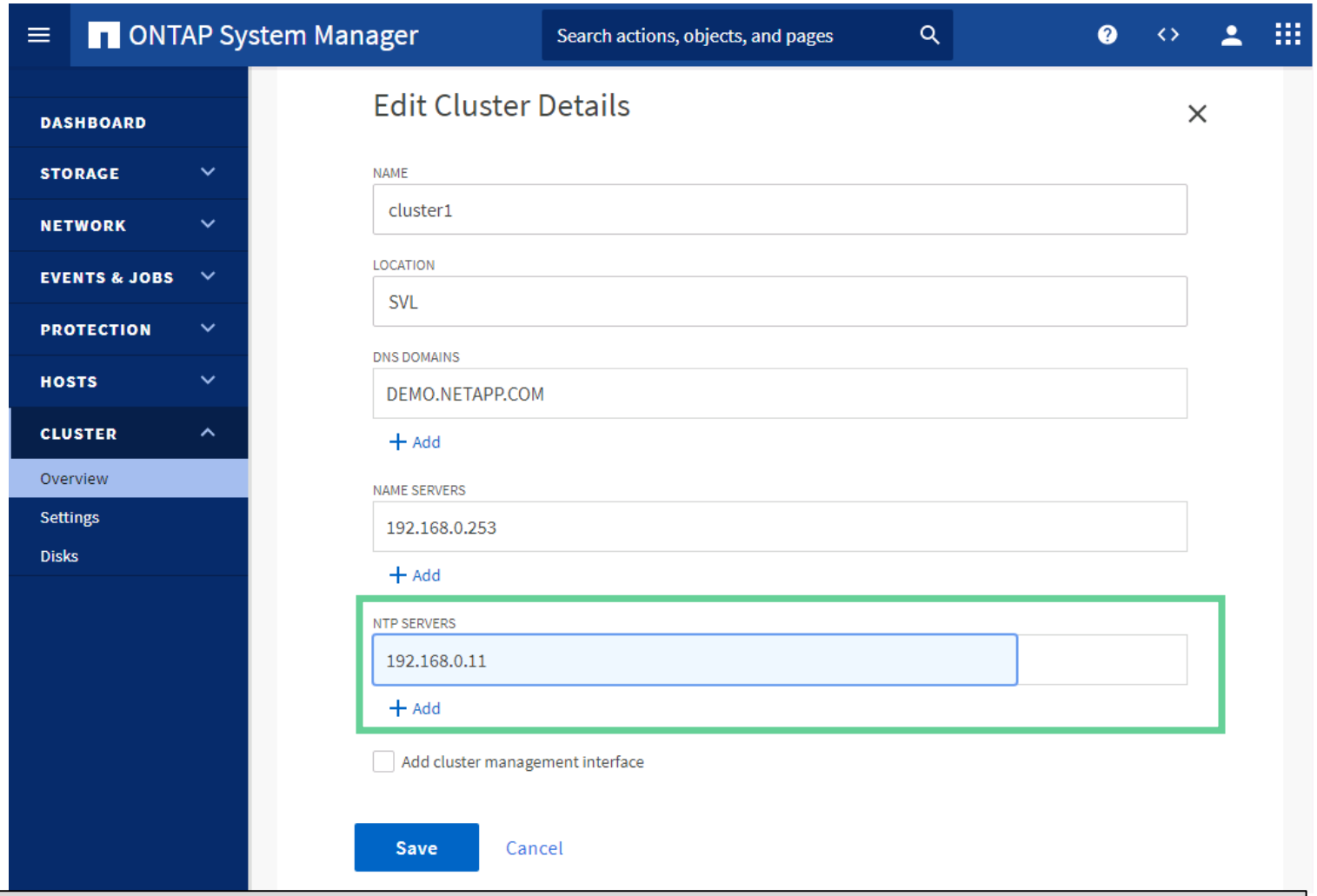
```
::> security login motd modify
```


Date and time

Ways to configure date and time:

- Manually, with CLI
- Automatically, with Network Time Protocol (NTP) servers

After you add an NTP server, the nodes require time to synchronize.

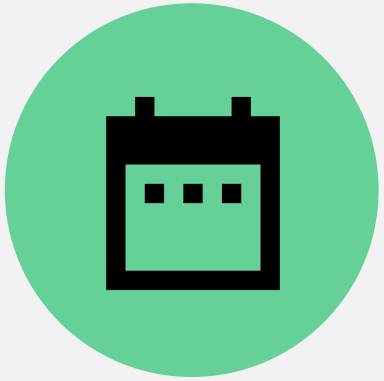



```
::> cluster time-service ntp server create -server xx.xx.xx.xx
::> date
```


Lesson 2
ONTAP licensing

License types

- Standard license
- Enterprise license



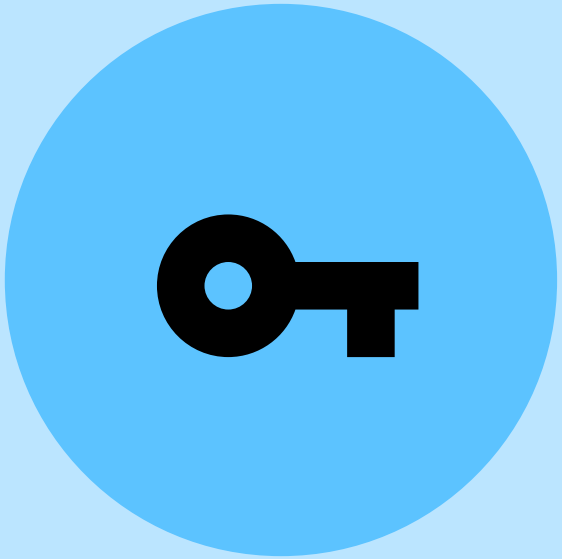
Evaluation license

Capacity license

Standard and enterprise licenses

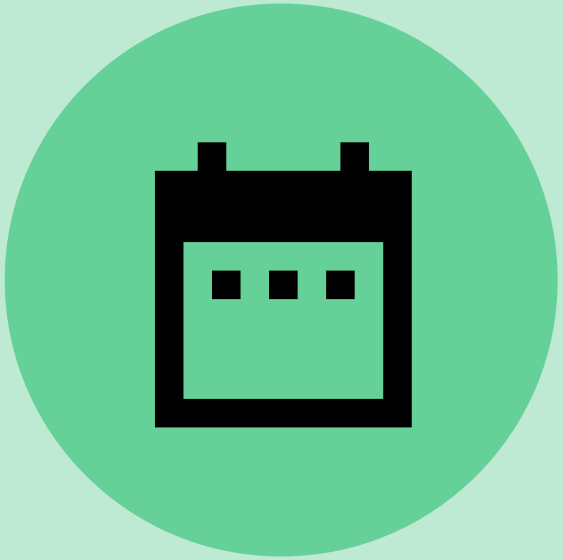
- Proof of sale is recorded as a license entitlement record.
- License keys are 28 characters long.
- Standard licenses are linked to the controller serial number (node locked).
- Features are licensed on every node and continue to function if one licensed node is running.
- Enterprise licenses enable the feature on the entire cluster.

  An enterprise license is not carried with nodes that are removed from the cluster.



Evaluation license

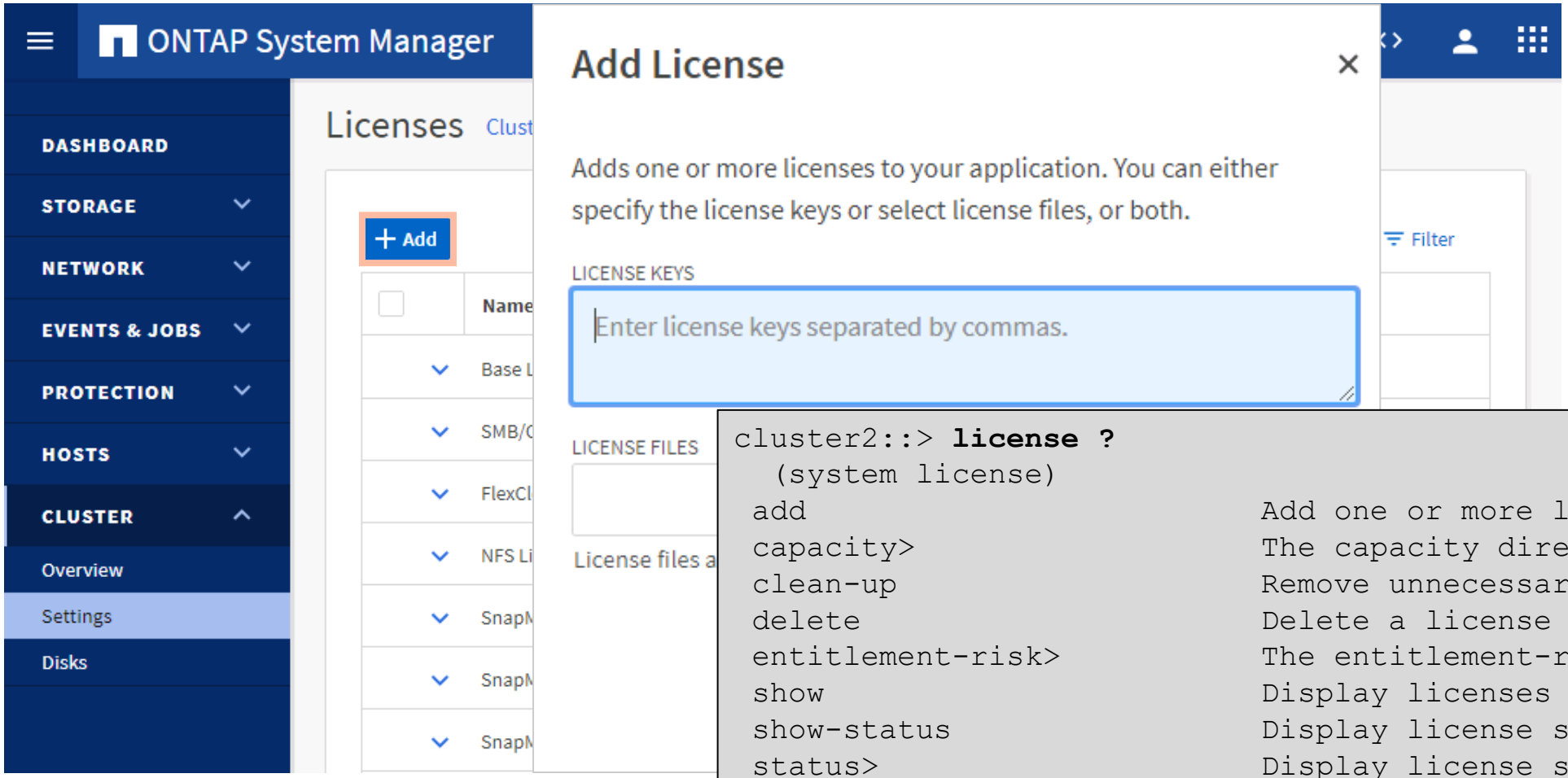
- Enables testing of software functionality before purchasing the license
- Is a time-limited license
- Can be renewed but only a limited number of times before requiring a purchase



Capacity licenses

- Capacity licenses are sold individually for increments of storage capacity (500TB, 100TB, 50TB, and so on).
- These licenses are used with NetApp ONTAP Select, Cloud Volumes ONTAP, and FabricPool functionality.
- Additional capacity can be added to a capacity pool license at any time.
- Enforcement is performed at the aggregate level and relies on an aggregate lease.
- An expired lease prevents users from bringing aggregates back online after a manual reboot.
- License codes are shorter than 28 characters.

License commands




```
cluster2::> license ?
  (system license)
 add                          Add one or more licenses
 capacity>                    The capacity directory
 clean-up                     Remove unnecessary licenses
 delete                       Delete a license
 entitlement-risk>            The entitlement-risk directory
 show                         Display licenses
 show-status                  Display license status
 status>                      Display license status
```


Lesson 3
Policies and schedules

Policy-based storage services

Policy:

- A collection of rules that the cluster or SVM administrator creates and manages
- Predefined or created for managing data access

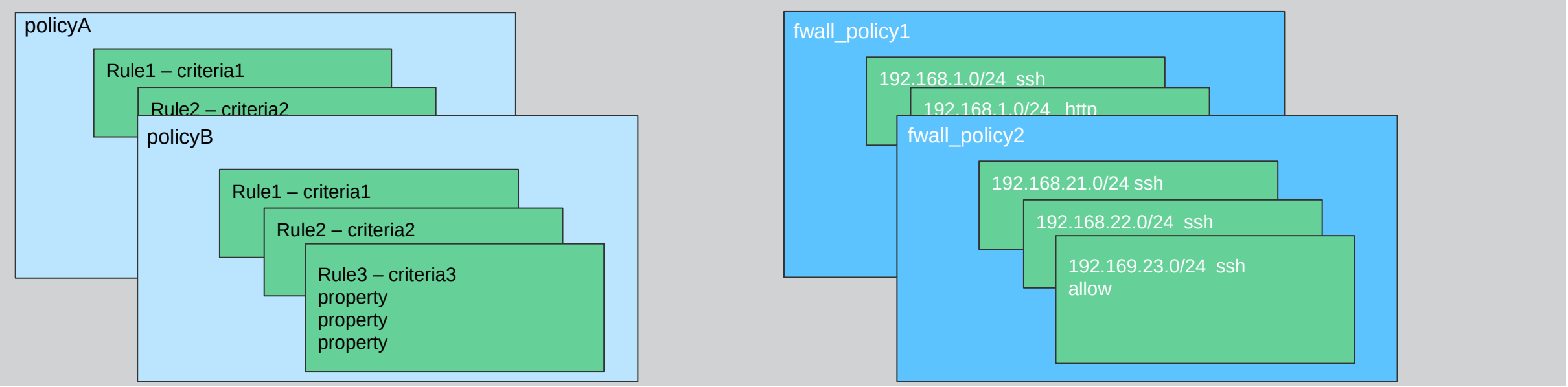
Policy examples:

- Firewall and security
- Export, quota, file, and data
- Snapshot and SnapMirror
- Quality of service (QoS)

Jobs and Schedules

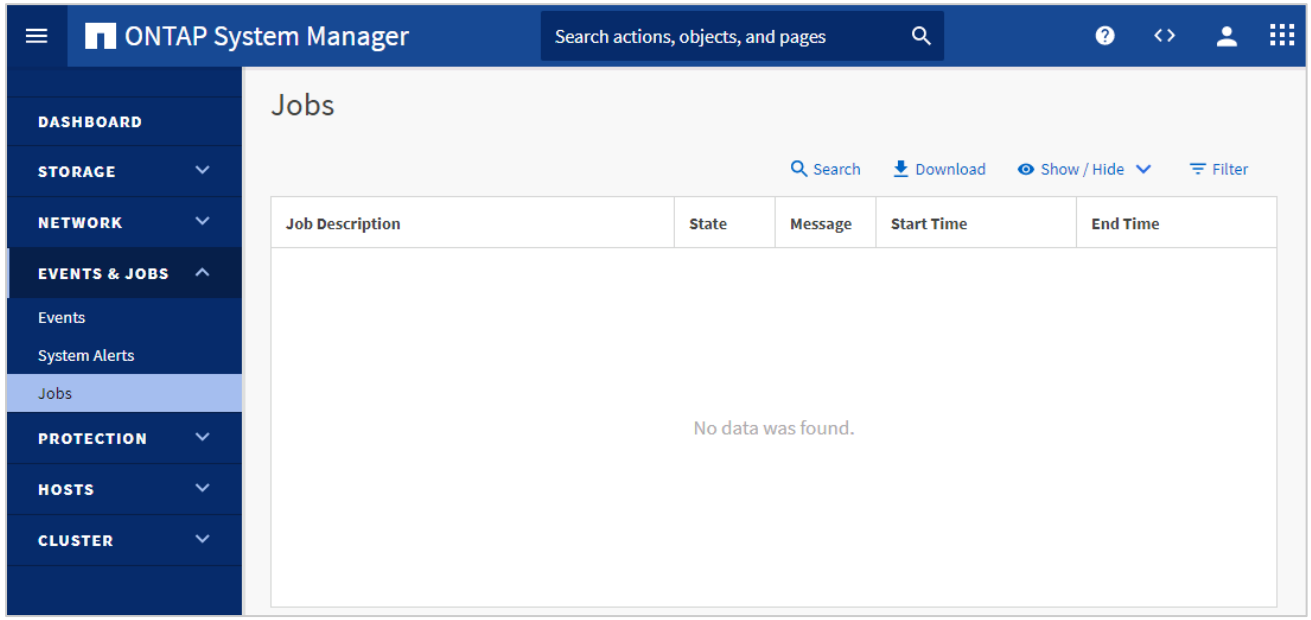
Policy-based management

- You assign a policy to a service or resource.
- A rule criterion in the policy matches the service or resource.
- The matching rule properties apply to the service or resource.
- The example is a firewall that permits or denies access to a protocol for specific IP address ranges.



Jobs

- Asynchronous tasks
- Managed by the Job Manager
- Long-running operations
- In a job queue



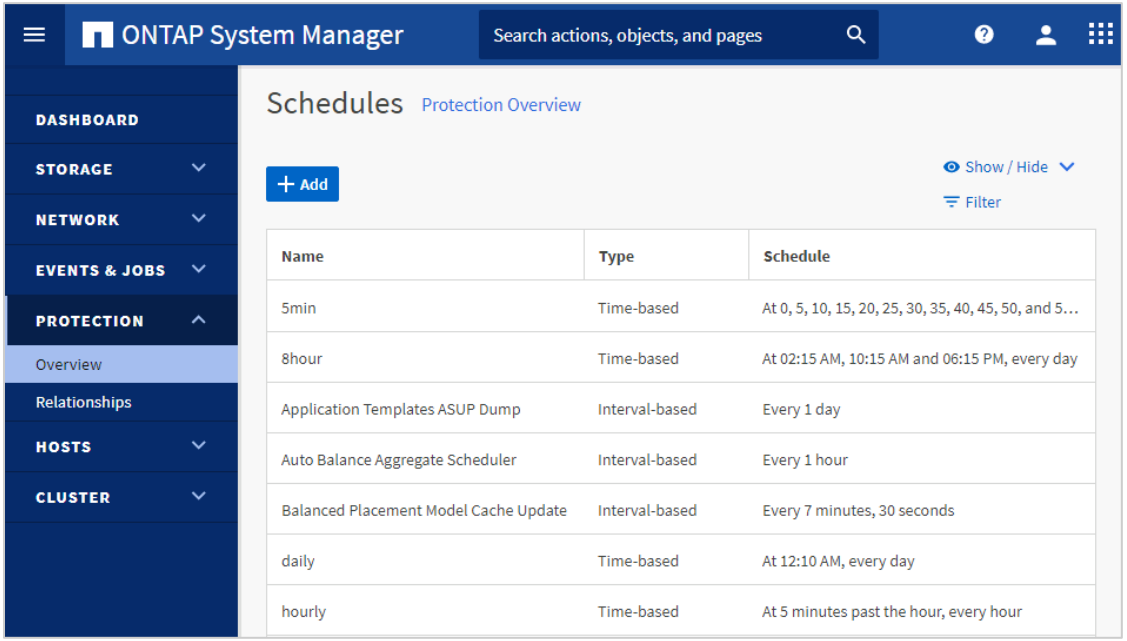

```
::> job show
                                          Owning
Job ID Name                               Vserver     Node            State
------ ---------------------------        ----------  --------------  ----------
1      SnapMirror Service Job.            cluster1    cluster1-01     Dormant
       Description: SnapMirror Service Job
3      Certificate Expiry Check           cluster1    -               Queued
       Description: Certificate Expiry Check
5      Auto Balance Aggregate Analyzer    cluster1    -               Paused
```


Schedules

Schedules for tasks:

- Time-based schedules, which run at specific times (similar to UNIX cron schedules)
- Interval-based schedules, which run at intervals

```
::> job schedule show
Name          Type      Description
-----------   --------- -------------------------------
5min          cron      @:00,:05,:10,:15,:20,:25,:30,:35
8hour         cron      @2:15,10:15,18:15
Auto Balance Aggregate Scheduler
              interval  Every 1h
RepositoryBalanceMonitorJobSchedule
              interval  Every 10m
daily         cron      @0:10
hourly        cron      @:05
monthly       cron      1@0:20
weekly        cron      Sun@0:15
```



Module summary

This module focused on enabling you to do the following:

- Manage access control
- Configure cluster settings
- Manage cluster-level features of ONTAP software

Knowledge check

Module 3: Cluster management

Knowledge check

The admin SVM manages the cluster and serves data.

a. true

b. false

Knowledge check

The admin SVM manages the cluster and serves data.

a. true

b. false

Knowledge check

Which are valid types of ONTAP licenses? (Choose four.)

a. capacity

b. enterprise

c. evaluation

d. expansionary

e. provisional

f. standard

Knowledge check

Which are valid types of ONTAP licenses? (Choose four.)

a. capacity

b. enterprise

c. evaluation

d. expansionary

e. provisional

f. standard

Complete an exercise

Module 3
Cluster management

Managing ONTAP clusters and administrators

- Access your lab equipment.
- Open your Exercise Guide, Module 3.
- Complete the specified tasks.
- Share your results.

This exercise requires approximately
45 minutes.

Share your experiences

Roundtable discussion

- How did the cluster behave after you specified the NTP server?
- Did the time synchronize immediately?

