COHESITY

Version 1.1

May 2024

Deploy and Configure Cohesity to Comply with DoDIN APL

Deployment and configuration settings on Cohesity to comply with DoDIN APL

ABSTRACT

Cohesity 6.6.0d LTS release is DoDIN APL (Department of Defense's Information Network Approved Product List) certified. DoDIN APL provides a single, consolidated list of products that meet the cybersecurity and interoperation certification requirements. Read these practical recommendations for deploying and configuring Cohesity to comply with DoDIN APL. You will find descriptions, technical recommendations, and notes describing the common mistakes to avoid.

Table of Contents

Tables

Introduction

Cohesity 6.6.0d LTS release is DoDIN APL (Department of Defense's Information Network Approved Product List) certified. DoDIN APL provides a single, consolidated list of products that meet the cybersecurity and interoperation certification requirements. To use Cohesity as per DoDIN APL requirements and recommendations, you need to enable DoD mode in the Cohesity cluster and configure security settings listed in Configure Additional Security Settings on Cohesity Cluster.

This implementation guide provides step-by-step instructions to prepare your Cohesity cluster to run effectively in DoD mode.

Plan and Prepare

Conditions of Fielding

Before you begin, refer to and follow the Conditions of Fielding (COF) found in the Cybersecurity Assessment Report (CAR). CAR is available through Approved Product Lists (APLITS). For more information, see Common Access Cards.

Follow the steps below to request a copy.

1. Go to https://aplits.disa.mil/.
2. Select **Browse the DoDIN APL**.
3. From the search menu, select **Cohesity** as the vendor and then click **Search**.
4. From the results, select the link to request a copy of the Cybersecurity Assessment Package (CAP) is available.
5. Once you click on the link, your default mailbox is opened with a new email draft to request a copy.
6. Send the email.

> **NOTE:** To request a copy, you must be US Government and Military personnel with a valid email address.

Common Access Cards

Command Access Cards are smart cards that are the standard identification for active-duty uniformed Service personnel, Selected Reserve, Department of Defense (DoD) civilian employees, and eligible contractor personnel. It is also the principal card used to enable physical access to buildings and controlled spaces, and it provides access to DoD computer networks and systems. For more information, see DoD Common Access Cards (CAC).

Configure Active Directory

You've to join an Active Directory (AD) with your Cohesity cluster to enable AD users with access to Cohesity. For more information, see Join Active Directory.

Before you join AD with the Cohesity cluster, you must meet the following prerequisites. Follow these prerequisite steps:

1. Log into Microsoft Azure Active Directory.
2. Create DNS A, AAAA, and PTR records for Cohesity Cluster VIPs and Nodes. For more information, see Microsoft documentation.
3. Create an Organizational Unit (OU) for the Cohesity cluster. For more information, see Microsoft documentation.
4. Create a Cohesity AD service account user. For more information, see Microsoft documentation.
5. Assign delegated permissions to Cohesity OU. For more information, see Microsoft documentation.
6. Create a Global Security Group for users accessing Cohesity. For more information, see Microsoft documentation.
7. Add NFS client users to the Global Security Group and enable NFS client access for each AD user. For more information, see Microsoft documentation.

After the cluster is joined to AD, modify the service principal name. For more information see Microsoft documentation.

Deploy Cohesity

Cohesity can be deployed on any qualified hardware, supported hypervisor and cloud environments. The following options are available to deploy a Cohesity cluster.

- **On-Premises Cluster Setup**: These clusters are hosted on hardware from Cohesity and other qualified hardware from Cisco, Dell, and HPE.
- **Virtual Edition Cluster Setup**: These clusters are hosted on virtual machines in the hypervisors.

  NOTE: When deployed without the required safeguards, customers introduce a single point of failure into the Cohesity solutions in a virtual environment (virtual edition). To safeguard your cluster, Cohesity strongly recommends hosting virtual edition solutions on resilient underlying storage and having outgoing archival and replication, or both configured to eliminate this risk.

- **Cloud Edition Cluster Setup**: These clusters are hosted in the clouds.

For more information, see Initial Cluster Setup.

Create a Cohesity Cluster

Cohesity cluster creation is a process of connecting three or more independent Cohesity nodes. You must create a Cohesity cluster for primary and disaster recovery purposes. See the relevant setup guide available on the Initial Cluster Setup page for more information.

Change Node Root Password

For DoD mode, console access to the Cohesity nodes is available by login via the 'root' account. If you are locked out of the cluster, have lost connectivity to the cluster, or forgotten your support user password, you can reset your user account's password using the 'root' account user.

When a cluster is accessed via IPMI or console, the username is root. Follow the steps below to change the password.

1. To change the root user password, open an iris_cli session and run the following command from the Cohesity Secure Shell.

   To set a new password

   ```
   [support@nodeIP]$ iris_cli
   admin> user linux-user linux-username=root  linux-password=<password min 15 characters>
   ```

   To update a password

   ```
   [support@nodeIP]$ iris_cli
   admin>user linux-user linux-username=root  current-password=<password min 15 characters>  linux-password=<password min 15 characters>
   ```

Change Support User Password

Cohesity provides a support user account for improved security. Use the support user account to log in to the Cohesity cluster bash shell using SSH. For more information, see Change Support User Password.

Virtual Edition vSphere 6.7 Virtual Machine STIG Application

You must apply VMware vSphere 6.7 Virtual Machine STIG settings to each Cohesity Platform Virtual Edition node. Follow the steps below:

1. From a management workstation, launch Microsoft Powershell with VMWare PowerCLI installed.
2. Enter the following commands in sequence:
   a. Set-PowerCLIConfiguration -InvalidCertificateAction Ignore -Confirm: $false
   b. connect-viserver <ESXi or VCenter Server Address>
3. Login with a VMware administrator account to VMware vSphere.
4. For each Cohesity Virtual Edition VM, run the following script replacing <VM Name> with the name of the Cohesity Virtual Edition VM.

```
Write-Host "VMCH-67-000001"
Get-VM "<VM Name>" | New-AdvancedSetting -Name
isolation.tools.copy.disable - Value true -Confirm:$false -Force
Write-Host "VMCH-67-000002"
Get-VM "<VM Name>" | New-AdvancedSetting -Name
isolation.tools.dnd.disable - Value true -Confirm:$false -Force
Write-Host "VMCH-67-000003"
Get-VM "<VM Name>" | New-AdvancedSetting -Name
isolation.tools.paste.disable - Value true -Confirm:$false -Force
Write-Host "VMCH-67-000004"
Get-VM "<VM Name>" | New-AdvancedSetting -Name
isolation.tools.diskShrink.disable -Value true -Confirm:$false -Force
Write-Host "VMCH-67-000005"
Get-VM "<VM Name>" | New-AdvancedSetting -Name
isolation.tools.diskWiper.disable -Value true -Confirm:$false -Force
Write-Host "VMCH-67-000007"
Get-VM "<VM Name>" | New-AdvancedSetting -Name
isolation.tools.hgfsServerSet.disable -Value true -Confirm:$false -
Force Write-Host "VMCH-67-000008"
Get-VM "<VM Name>" | Get-FloppyDrive | Remove-FloppyDrive -
Confirm:$false Write-Host "VMCH-67-000009"
Get-VM "<VM Name>" | Get-CDDrive | Set-CDDrive -NoMedia -Confirm:$false
Write-Host "VMCH-67-000013"
Get-VM "<VM Name>" | New-AdvancedSetting -Name
RemoteDisplay.maxConnections - Value 1 -Confirm:$false -Force
Write-Host "VMCH-67-000014"
Get-VM "<VM Name>" | New-AdvancedSetting -Name
RemoteDisplay.vnc.enabled - Value false -Confirm:$false -Force
Write-Host "VMCH-67-000015"
```

```
Get-VM "<VM Name>" | New-AdvancedSetting -Name tools.setinfo.sizeLimit -
Value  1048576 -Confirm:$false -Force
Write-Host "VMCH-67-000016"
Get-VM "<VM Name>" | New-AdvancedSetting -Name
isolation.device.connectable.disable -Value true -Confirm:$false -Force
Write-Host "VMCH-67-000017"
Get-VM "<VM Name>" | New-AdvancedSetting -Name
tools.guestlib.enableHostInfo - Value false -Confirm:$false -Force
Write-Host "VMCH-67-000018"
Get-VM "<VM Name>" | Get-AdvancedSetting -Name sched.mem.pshare.salt |
Remove AdvancedSetting -Confirm:$false
Write-Host "VMCH-67-000019"
Get-VM "<VM Name>" | Get-AdvancedSetting -Name ethernetX.filterY.name |
Remove-AdvancedSetting -Confirm:$false
Write-Host "VMCH-67-000022"
Get-VM "<VM Name>" | New-AdvancedSetting -Name
tools.guest.desktop.autolock - Value true -Confirm:$false -Force
Write-Host "VMCH-67-000023"
Get-VM "<VM Name>" | New-AdvancedSetting -Name mks.enable3d -Value false
- Confirm:$false -Force
Write-Host "VMCH-67-000024"
Get-VM "<VM Name>" | New-AdvancedSetting -Name
ExtensionData.Config.MigrateEncryption -Value required -Confirm:$false -
Force
```

5. For Cohesity Virtual Edition VMs that are operated in a vCenter environment utilizing vMotion, run this additional command:

```
Write-Host "VMCH-67-000024"
Get-VM "<VM Name>" | Set-vMotionEncryptionConfig -Encryption
opportunistic - Confirm:$false -Force
```

6. Run the following command to disconnect from the VMware server:

```
Disconnect-VIServer -Server <ESXi or VCenter Server>
```

Configure Cohesity Cluster Certificates

You can replace the Cohesity cluster's self-signed certificate with a Certificate Authority (CA) signed certificate. For more information, see Configuring Cohesity Cluster with a CA Signed Certificate.

Implement Node-to-Node TLS Encryption

DoD mode depends upon the use of certificates to encrypt traffic between Cohesity cluster nodes. This section covers configuring your cluster nodes with certificates, and is a prerequisite step that must be completed before enabling DoD mode.

NOTE: Internal data such as statistics data or other non-critical data is not encrypted.

Configure Certificates for Node-to-Node Encryption

To use a certificate for node-to-node encryption, you must manually create a certificate signing request, generate the certificate, and import the certificate on each node in the Cohesity cluster.

Prerequisites

Before you configure a certificate for node-to-node encryption, ensure the following prerequisites:

- Verify whether the domain name is set for your Cohesity cluster using the following command:

```
$ cluster ls-domains
```

For example:

```
$ cluster ls-domains
CLUSTER ID            : 4759089959284457
CLUSTER NAME          : cohesity
DOMAIN NAMES          : eng.cohesity.com, corp.cohesity.com
```

- Update the hostnames of the nodes in the Cohesity cluster using the following command:

```
$ node-csr update-hostnames node-ids=<node_id1, node_id2>      host-
names=<hostname_1, hostname_2>
```

Output:

Cluster config updated successfully.

Where:

- node-ids - The node id of the nodes in the Cohesity cluster. Provide a comma separated list of the node ids.
- host-names - Define the hostnames for the nodes in the Cohesity cluster. Provide a comma separated list of the hostnames for the node ids.
- You can run the command $ iris_cli cluster status to get node-ids and host-names.

Create a Certificate Signing Request

Perform the following to create a certificate signing request (CSR) on each node in the Cohesity cluster.

1. Start the Cohesity DataPlatform CLI remotely or locally as described in the Cohesity CLI Reference Guide.
2. Run the following command to create a certificate signing request:

```
$ node-csr create city=<city_name> state=<state_name>
country=<country_name> organization=<org_name> organization-
unit=<org_unit_name> dns-names=<dns_name> common-name=<node FQDN>
```

CSR

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC5TCCAc0CAQAwVTELMAkGA1UEBhMCVVMxETAPBgNVBAoMCENvaGVzaXR5MRIw
EAYDVQQLDAlDb3JlSW5mcmExCzAJBgNVBAgMAkNBMRIwEAYDVQQHDAlDdXBlcnRp
bm8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDWDkZokJkovKdSj6Ni
5Shqkjx+BUsgs0DNS6Kfpo1ZlFEeDbwQ9ThgycNU8PWtNyb8bNwzPlMvbPtB1o4C
u+ACukfASH9blJyOBP4JrUAouHTHK73gDU0hlnN+PrVjMNtgRvAh68vJtLudtK8j
3pcGE3eWEMolNC8M3h5bLUF+b9d9UyCvrJIjcwrUkI+9EI5OJNCQIxLdZ1XjTQdf
khSnarh2wNTrF1AuBrmJdTY0S5FG9s0TD8UdDE5c90vfNVVlLN02NK06s3wVtskL
j+eF7DNUJrL1gftx7i0s5ksdLPYxzVo8ap5VW4OqSZDtPv/zllBK9u/6FAqqDbC1
q+nXAgMBAAGgSzBJBgkqhkiG9w0BCQ4xPDA6MDgGA1UdEQQxMC+CLWNvaGVzaXR5
LTAwNTA1Njg5MzFlOC1ub2RlLTQuZW5nLmNvaGVzaXR5LmNvbTANBgkqhkiG9w0B
AQsFAAOCAQEAt+vgpETeZqPKJaQA6I+jEKi6hcHaNUFTHrPrb7QMdzzzB9AIyoYc
onCctHFkpt77NNqmmq+3K3+J2YBlpIwDVjKu5vf1rY3BMeeo6RlOsWJH62cdQbS9
V3xr+dkF2tnVXrsoMizh2IaVBSVfbzllIVLwfayuRZzKeAt13XVQsqAnBFNdSyFO
d9R42rwPMfJ1MzfFz/jRBFIrbknkDKNdOJ+80AyRKFYQSvNvygD+0t+rww9EcBgq
2Jw06WFDmFMNxPnSLe0/Mt7UUt/WCTU5bs9Coq8cat4nBNeebJ7GgubE+7G3QhcZ
KzyUXKkcY/Md/n/k2EHDrF5thGX8X8qugw==
-----END CERTIFICATE REQUEST-----
```

The following table lists the attributes required to create the certificate signing request:

Table 1: Attributes

ATTRIBUTE	REQUIRED/OPTIONAL	DESCRIPTION
city	Required	The city where the company is located.
common-name	Optional	A context for the certificate. For example, the name of the node to which the certificate must be assigned.
country	Required	The country where the state is located. You can specify it as two letter code defined by the ISO standard.
dns-names	Optional	Concatenate the hostname with the first domain name. For more information, see Prerequisites. For example: Cohesity-0050568931e8-node-2.eng.cohesity.com Note: Though dns-names attribute is optional. Cohesity recommends that you use the dns-names attribute.
email-address	Optional	An alternative subject name component that must be included in the certificate.
host-ip	Optional	An alternative subject name component to be included in the certificate. It is used to uniquely identify the node.
organization	Required	The name of the company.
organization-unit	Required	The department or business unit in the company that owns the node.
state	Required	The state where the city is located.

Obtaining and Validating the Certificate

Once the CSR has been created, contact your CA administrator to receive your certificate file.

Each self-installed certificate should have both client and server authorization. You can run the following command to check the certificate:

```
$openssl x509 -in <certificate_path> - text
```

The certificate details are displayed, and you should see the following details under X509v3 Extended Key Usage:

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
```

If the certificate details are not displayed, or the Extended Key Usage does not match above, you may need to create a new CSR, or contact your CA administrator to troubleshoot and generate the appropriate certificate.

NOTE: If you are using an intermediate CA certificate, then you must ensure that the imported CA certificate should contain the intermediate CA certificate and the root CA.
You can also sign the CSR using a third-party Certificate Authority (CA).

Import the Signed Certificates to the Nodes

After the certificate signing request (CSR) corresponding to the node is signed, import the signed certificate and the CA certificate onto each node in the Cohesity cluster.

Perform the following on all the nodes in the Cohesity cluster:

1. Copy the signed certificate to a node in the cluster. Ensure that you copy both the signed and CA certificates to the node.
2. Change the certificate file permission to 644.
3. Import the signed and CA certificates to the node using the following command:

```
$ node-csr import signedcert-path=<signed_cert_path> cacert-
path=<ca_cert_path>
```

Output: Success: Certificates imported successfully.
Where:

- <signed_cert_path> - The absolute path of the signed certificate file that must be imported to the node.
- <ca_cert_path> - The absolute path of the CA certificate that was used to sign the CST for the node.

Once done on all the nodes, run the following command.

```
  $ iris_cli cluster tpenc enable_encryption=true
```

Verify Certificate's Location and Authentication

You can run the following commands to verify certificate location and certificate's server and client authentication.

Verify the location of CA and the signed certificate:

```
$ openssl verify -verbose -CAfile <ca_cert_path>  <signed_cert_path>
```

Where:

- *<signed_cert_path>* - The absolute path of the signed certificate file that must be imported to the node.
- *<ca_cert_path>* - The absolute path of the CA certificate that was used to sign the CST for the node.

Verify the server and client authentication:

```
$ openssl x509 -in <signed certificate> -text -noout
```

Verify Login through DoD Common Access Card

You can follow the steps below to verify login to a Cohesity cluster through a DoD Common Access Card.

1. Insert a DoD smart card mapped to an AD user who is a member of the Cohesity Admins security group.
2. Go to https://<Cluster_FQDN>:9440 and inspect the installed certificate, which should now be the CA issued certificate.
3. Select the smart card certificate associated with the AD user.
4. Enter the smart card pin when prompted.
5. Verify that you are successfully logged in using smart card credentials.

Enable DoD Mode on a Cohesity Cluster

Cohesity is DoDIN APL certified.

To use Cohesity as per DoDIN APL requirements and recommendations, you need to enable DoD mode in the Cohesity cluster and configure the list of security settings mentioned in Configure Additional Security Settings on Cohesity Cluster.

About DoD Mode

You can enable DoD mode using the Cohesity CLI. Once you have enabled DoD mode, you cannot disable it. For node-to-node traffic encryption, you must configure the required certificates before enabling DoD mode. For more information, see Node-to-Node Encryption.

When you enable DoD mode, by default:

- The cohesity user is disabled, and you cannot use the cohesity user account to access the Cohesity bash shell using SSH. Instead, you need to use the support user account to log into the Cohesity bash shell using SSH.
- You can change the support user password only once a day.
- The support user can run the "sudo" prefixed commands only after providing the support user password. The sudo session is valid for 15 minutes, and you will be prompted to enter the password again.
- The cohesity_console account is disabled, and instead, you can use the root account to log into the console.
- The data transfer between the nodes in the Cohesity cluster is encrypted.

Prerequisites

Dedicated partitions are required to support DODIN RHEL STIG requirements for Operating System partitions. Before you enable the DOD mode, you must run a script provided by Cohesity Platform to check if the system disk on the Cohesity node contains the dedicated partitions. To run the script:

1. Log on to the Cohesity node bash shell using SSH.
2. Run the following script:
   /home/cohesity/bin/validate_dodin_compliant_partitions.sh

The script validates if the following partitions are present in the system disk on the Cohesity node:

- /var
- /spare/var
- /var/log/audit
- /cohesity_users_home

If the validation fails, it implies that the Cohesity node does not contain the dedicated partitions. Therefore, you need to perform ISO installation on the Cohesity node to get all the security benefits listed by DODIN RHEL STIG for Operating System partitions.

Enable DOD Mode

To enable DoD mode:

1. Start the Cohesity CLI remotely or locally as described in the Cohesity CLI Reference Guide.
2. Run the following command to enable DoD mode:

   $ iris_cli security-config update-security-mode security-mode-dod=true

   Configuring security mode...Success: Security mode DOD will be turned on after rolling reboot.

   The Cohesity cluster goes into a rolling reboot. Wait until the rolling reboot is complete.

   Verify if the DoD mode is enabled. Run the following command:
   $ iris_cli cluster info

Configure Additional Security Settings on Cohesity Cluster

To strengthen the security of your Cohesity cluster running on DoD mode, you have to perform the following tasks after enabling DoDIN mode on your new Cohesity cluster.

- Configure Erasure Coding for Multi-Node Clusters
- Configure Node ID
- Set Mapping to AD Users
- Enable Mapping-based Authentication
- Restart Cohesity Services
- Configure SMTP Server
- Configure Login Banner
- Enable Offline Help
- Join the Cohesity Cluster to an AD Domain
- Configure SNMP
- Add Alert Notification Rule

Configure Erasure Coding for Multi-Node Clusters

You can configure erasure coding for multi-node clusters on Cohesity. For more information, see Create or Edit Storage Domains.

Configure IPv6 Addresses

1. Launch your terminal client (ssh), for example, PuTTY.
2. Open an SSH tunnel to the cluster.
3. Login with the support user account.
4. Launch the CLI and enter the command, *iris_cli.*

5. Execute the following commands.

PURPOSE	COMMAND
Capture the node IDs for each node	*node ls*
Configure IPv6 Address	*ip config node-ids=<comma_separated_list of_node IDs> interface-ips=<comma_separated_ list_of_IPv6_node_addresses_same_order_as_node _IDs> interface-name=intf_group1 family=2 subnet-mask-bits=64 subnet-gateway=<IPv6_gateway>*

Set Mapping to AD Users

The DoD personnel can use Common Access Card (CAC) to login only if you set the mapping to AD users. Follow the steps below.

1. Launch your terminal client (ssh), for example, PuTTY.
2. Open an SSH tunnel to the cluster.
3. Login with the support user account.

   Launch the CLI and enter the command, *iris_cli*.
4. Execute the following commands.

PURPOSE	COMMAND
Set the mapping to AD users	*security-config update ad mapping=UserPrincipalName*
Set the mapping to the certificate	*security-config update certificate-mapping=UserPrincipalName*

Enable Mapping-based Authentication

Before you enable mapping-based authentication, you have to integrate Active Directory with Cohesity. For more information, see About Active Directory Integration.

1. Launch your terminal client (ssh), for example, PuTTY.
2. Open an SSH tunnel to the cluster.
3. Login with the support user account.
4. Launch the CLI and enter the command, *iris_cli.*

5. Execute the following commands.

PURPOSE	COMMAND
Enable mapping-based authentication	*security-config update enable-mapping-based-auth=true*

Configure Password Settings

1. Launch your terminal client (ssh), for example, PuTTY.
2. Open an SSH tunnel to the cluster.
3. Login with the support user account.

   Launch the CLI and enter the command, `iris_cli`.
4. Execute the following commands.

PURPOSE	COMMAND
Set password complexity for:	
Lowercase Letter	*security-config update include lower-letter=true*
Uppercase Letter	*security-config update include upper-letter=true*
Numbers	*security-config update include number=true*
Characters	*security-config update include special-char=true*
Set maximum password lifetime	*security-config update max-lifetime-days=60*
Set minimum password lifetime	*security-config update min-lifetime-days=1*
Set minimum password length	*security-config update min-length=15*
Set minimum password reuse	*security-config update num-disallowed-old-pwd=5*

Configure User Session Settings

1. Launch your terminal client (ssh), for example, PuTTY.

   NOTE: You must ensure your terminal client supports the AES-GCM cipher or has been configured to accept AES-GCM.

2. Open an SSH tunnel to the cluster.
3. Login with the support user account.

   Launch the CLI and enter the command, *iris_cli.*

4. Execute the following commands.

PURPOSE	COMMAND	DEFAULT VALUES
Enable session limits	`security-config update limit-sessions=true`	*False*
Set session absolute timeout	`security-config update session-absolute-timeout=3600`	*86400*
Set session inactivity timeout	`security-config update session-inactivity-timeout=600`	*3600*
Set per-user session limit	`security-config update session-limit-per-user=40`	*10*
Set per-system session limit	`security-config update session-limit-system-wide=60000`	*100000*

Configure Classification Banner

1. Launch your terminal client (ssh), for example, PuTTY.
2. Open an SSH tunnel to the cluster.
3. Login with the support user account.
4. Launch the CLI and enter the command, *iris_cli.*

5. Execute the following commands.

PURPOSE	COMMAND
Set the security classification banner	*security-config update classified-data msg=<SYSTEM CLASSIFICATION LABEL>*
Enable classification banner	*security-config update is-data-classified=true*

Enable Cluster Audit Verbosity

You must enable cluster audit verbosity as it's an Application Security STIG requirement. Follow the steps below.

1. Launch your terminal client (ssh), for example, PuTTY.
2. Open an SSH tunnel to the cluster.
3. Login with the support user account.
4. Launch the CLI and enter the command, *iris_cli.*
5. Execute the following command.

PURPOSE	COMMAND
Enable verbose cluster auditing	*cluster update cluster-audit-verbosity=true*

Configure NFS LDAP Objects

1. Launch your terminal client (ssh), for example, PuTTY.
2. Open an SSH tunnel to the cluster.
3. Login with the support user account.
4. Launch the CLI and enter the command, *iris_cli*.
5. Execute the following command.

PURPOSE	COMMAND
NFS LDAP user object	*cluster update-gflag gflag name=bridge_nfs_auth_ldap_user_object_class_name gflag-value=posixAccount service name=bridge effective-now=true reason="test"*
NFS LDAP group object	*cluster update-gflag gflag name=bridge_nfs_auth_ldap_group_object_class_name gflag-value=posixGroup service name=bridge effective-now=true reason="test"*
NFS LDAP group ID object	*cluster update-gflag gflag name=bridge_nfs_auth_ldap_gid_attr_name gflag-value=gidNumber service-name=bridge effective-now=true reason="test"*
NFS LDAP UID object	*cluster update-gflag gflag name=bridge_nfs_auth_ldap_uid_attr_name gflag-value=uidNumber service-name=bridge effective-now=true reason="test"*
NFS LDAP memberUid object	*cluster update-gflag gflag name=bridge_nfs_auth_ldap_member_of_attribute_name gflag-value=memberUid service name=bridge effective-now=true reason="test"*
NFS LDAP username object	*cluster update-gflag gflag name=bridge_nfs_auth_ldap_user_name_attribute_name gflag-value=uid service-name=bridge effective-now=true reason="test"*

Configure Miscellaneous Settings

1. Launch your terminal client (ssh), for example, PuTTY.
2. Open an SSH tunnel to the cluster.
3. Login with the support user account.

   Launch the CLI and enter the command `iris_cli`.
4. Execute the following command:

PURPOSE	COMMAND
Synchronize nodes from NTP	*cluster update-gflag gflag name=nexus_proxy_ntp_disable_master_slave_schem e gflag-value=true service name=nexus_proxy effective-now=true reason="test"*
Disable the built-in DNS service	*cluster update-gflag gflag name=compass_dns_server_port gflag-value=0 reason=testing effective-now=true service name=compass*
Restart the compass service	*compass.sh stop;compass.sh start*
Enable OCSP revocation checking	*cluster update-gflag service-name=nexus gflag name=cert_ocsp_revoke_check gflag-value=true reason=testing effective-now=true*
Set a low disk percentage threshold for alerting	*cluster update-gflag gflag name=low_disk_info_percentage gflag-value=75 reason=testing effective-now=true service name=nexus*
Create a firewall policy to disable network access to the Plugin Backups services	*firewall-profile create name=DisablePluginBackups ports=11117/tcp,29991/tcp force=true*
Enable firewall policy to disable network access to the Plugin Backups services	*firewall-profile activate profile-name=DisablePluginBackups action=deny*
Enable IPv4 DSCP Markings	*cluster update-gflag gflag*

PURPOSE	COMMAND
	name=enable_egress_ipv4_dscp_marking gflag-value=true service-name=nexus reason="Enable DSCP marking"
Enable IPv6 DSCP Markings	*cluster update-gflag gflag* *name=enable_egress_ipv6_dscp_marking gflag-value=true service-name=nexus reason="Enable DSCP marking"*
Enable IP outbound traffic logging	*cluster update-gflag gflag* *name=enable_traffic_logging gflag-value=true service-name=nexus effective-now=true reason="Enable Traffic Logging"*
Restart the nexus_proxy service	*nexus_proxy.sh stop;nexus_proxy.sh start*
Restart the nexus service	*nexus.sh stop;nexus.sh start*

Configure SMTP Server

You can configure the connection to the SMTP Server and verify the SMTP settings when you save the Cohesity cluster configuration.

1. In the Cohesity Dashboard, select **Settings** > **Summary**.
2. On the **Summary** tab, click **Configure** located at the top right of the page, and provide the following configuration information:

Table 2: Configure SMTP Server

SETTINGS	DESCRIPTION	ADDITIONAL NOTES
Enable SMTP Server	Check the **Enable SMTP Server** option to configure the connection to the SMTP Server. Specify the following SMTP settings: • SMTP Server: Specify the name of an SMTP server that is used to send emails when Warning or Critical Alerts are generated by the Cohesity cluster. Cohesity recommends specifying an SMTP mail server. • Port: Specify the port number used to access the SMTP Server. • SMTP Server uses SSL/TLS without STARTTLS (typically for port 465): Select this option if the SMTP Server uses SSL/TLS without STARTTLS. Typically SSL/TLS without STARTTLS uses port 465. • SMTP Username: Specify the name of the account used to authenticate with the SMTP Server. • Change SMTP Password: Specify the password of the account used to authenticate with the SMTP Server. Make sure an email address is specified for the local System Admin account (admin) of the Cohesity cluster. The SMTP server uses this address as the sender's address to send alert notification emails. Select Settings > Access Management and if necessary, edit the local admin user to provide an email address.	The SMTP Server is used to send emails when Warning or Critical Alerts are generated by the Cohesity cluster. Cohesity recommends that you configure the SMTP Server.
Test Email on Save	Enable the Test Email on Save option to verify the SMTP settings when you save the Cohesity cluster configuration. In the Test Email Recipient field, enter an email address to receive the test email.	

Configure Login Banner

You can customize the login banner of Cohesity Dashboard to present a statement to users during the login process, requiring them to acknowledge and agree to the message before logging in.

When you configure the login banner, the message will appear before the user logs on to the Cohesity Dashboard. To configure a login banner, see **Optional Settings** in Configure Settings.

After you've enabled the login banner, enter the following DoD warning banner text.

You are accessing the U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the USG may inspect and seize data stored on this IS.

Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work products are private and confidential. See User Agreement for details.

Enable Offline Help

You can use the documentation help that is included directly on the Cohesity cluster without internet access.

1. In the Cohesity Dashboard, select **Settings** > **Summary**.
2. On the **Summary** tab, click **Configure** located at the top right of the page, and provide the following configuration information:

Table 3: Configuration Info

SETTINGS	DESCRIPTION	ADDITIONAL NOTES
Documentation	Select The **No Internet Access? Access Help Directly From The Cluster** Option To Use The Documentation Help That Is Included Directly On The Cohesity Cluster Without Internet Access.	The Cohesity Dashboard Has Context-Sensitive Links To Help Pages Available From The Cohesity Web Site Or Directly From The Cohesity Cluster. Click The **Help** Icon In The Upper Right Corner Of The Dashboard To Load The Help Topic For The Page You Are Currently Viewing. If Prompted, Enter Your Cohesity Support Portal Credentials.

Join the Cohesity Cluster to an AD Domain

You can join the Cohesity cluster to one or more AD domains to enable:

- Existing AD users can access Cohesity cluster SMB shares based on their AD credentials.
- Existing AD users and groups can be assigned Cohesity roles and access the Cohesity Dashboard.

Follow the steps below.

1. Go to **Settings** > **Access Management** and click the **Active Directory** tab.
2. Click **Add Active Directory**.
3. **Domain Name**: Provide the fully qualified domain name (FQDN) of the Active Directory domain to join.
4. **Username**: Provide the samAccountName.
5. **Password**: Provide the password for the username.
6. **Preferred Domain Controllers**: Add preferred domain controllers to the AD domain to ensure that the Cohesity cluster uses a local domain controller (when possible) to speed up AD queries. The preferred domain controllers are assigned to both the domain and its trusted domains.
    - The SRV records must exist for the domain (the list of domain controllers displayed in the Cohesity Dashboard is generated by querying the SRV records).
    - You can add any number of preferred domain controllers.
7. The Cohesity cluster uses these domain controllers to join the AD domain and for all future communication with the AD domain.

8. **Machine Accounts**: Click Add and specify the following details:
   - Provide at least one machine account to identify the Cohesity cluster on the domain. For example, you can use the Cohesity cluster name.
   - Optionally, specify the DNS hostname of the machine account. For AD to work with the internal DNS server, apart from machine account names, you should add DNS hostnames you want to configure for each machine account. The DNS hostnames should have one of the In Bound DNS zone suffix configured for the internal DNS server. For more information, see Internal DNS for Load Balancing.
     If the DNS hostname is specified, Kerberos authentication succeeds only with the specified DNS hostname.
   - Optionally, select the encryption type(s) that must be used by the machine account. You can select multiple encryption types. The following encryption types are supported:
     - DES-CBC-CRC
     - DES-CBC-MD5
     - RC4-HMAC
     - AES128-CTS-HMAC-SHA1-96
     - AES256-CTS-HMAC-SHA1-96
   - If either DNS Hostname or Encryption Type is modified when editing the machine accounts, all existing configuration of the machine account is overwritten on the Active Directory.
9. All (or a subset) of the VIPs will resolve to the machine account. You can optionally add multiple machine accounts, which creates aliases for the same cluster. You can map these aliases to a subset (or all) of the VIPs to direct I/O to a subset (or all) of the nodes. Separate names with commas. For example: cluster1, cluster1-vip1, cluster1-vip2, cluster1-vip3, cluster1-vip4.
   If using VLANs—One of the machine accounts must be a DNS hostname for a virtual IP (VIP) of a VLAN configured on the cluster in order to recover to servers within that VLAN.
   The machine account must follow NetBIOS naming conventions of 15 maximum character length, those described in Naming conventions in Active Directory for computers, domains, sites, and OUs and the additional restriction that the ! @ ( ) characters are not supported.
   - After adding a Cohesity cluster to an AD, ensure the machine account used to register the Cohesity cluster in AD has the "Read membership" permissions across all users and groups.
   - The same configuration must be done on every additional domain to which the Cohesity cluster is joined.
10. Use the above Machine Accounts even if they already exist in AD Domain: Optionally toggle on to use the machine accounts that you specified above even if they already exist in the Active Directory domain.
11. **Mapped Provider**: Select the type of mapped provider to join the domain. By default, no mapped provider is selected. Optionally, select LDAP or NIS. If you select the LDAP option, you can select the provider from the LDAP Provider drop-down list. If you select the NIS option, you can select the NIS provider from the NIS Provider drop-down list.
12. **Organizational Unit**: Provide the organizational unit if applicable. Use the format: OUName or OUName/SubOUName. For example: Engineering or Sales/West or West Coast Sales/ North California.

13. **AD Workgroup / NetBIOS Name**: Provide the workgroup / NetBIOS name if applicable.
14. **Discover Trusted Domains**: Optionally, turn on this toggle to discover the trusted domains associated with an AD. You can exclude certain trusted domains after the Cohesity cluster is joined to the AD domain. For more information, see Trusted Domains.
15. Click **Join**.

For more information, see Join Active Directory.

Configure SNMP

You can enable Simple Network Management Protocol (SNMP) on the Cohesity cluster to further integrate Cohesity into your data center and enterprise management solutions. Whenever events occur on the Cohesity cluster, SNMP notifications are sent to your network management system. For more information, see Configure and Test SNMP.

Add Alert Notification Rule

You can add different alert notification rules that send emails, SNMP, Syslog, and/or cURL HTTP POST requests to a webhook URL based on the alert categories, severities, and names. Rules can be configured at both the service provider and the tenancy level.

Prerequisites

Before you add an alert notification rule, make sure that you:

- Configure an SMTP Server on the Cohesity cluster, if you plan to send email notifications when an alert is triggered. For details on configuring the SMTP server, see Configure Settings.
- Configure the SNMP setting on the Cohesity cluster, if you plan to send SNMP notifications to your network management system when an alert is triggered. For details on configuring SNMP settings, see Configure and Test SNMP.
- Add a Syslog server to the Cohesity cluster, if you plan to send Syslog notifications to the server when an alert is triggered. For details on configuring the Syslog server, see Add a Syslog Server.

To add an alert notification rule:

1. In the Cohesity Dashboard, select **System** > **Health** and click the **Settings** tab.
2. Click **Add Alert Notification Rule**.
3. In the **Add Alert Notification Rule** page, do the following:
    a. **Rule Name**: Type a descriptive name for the rule, for example, Cluster Disk Offline or Backup Job Failure.
    b. **Alert Category**: (Optional) Select one or more categories from the drop-down. Otherwise, all alerts in any category will trigger the rule.
    c. **Alert Severities**: (Optional) Select one or more severities from the drop-down. Otherwise, all alerts with any severity will trigger the rule.

d. **Alert Name**: (Optional) Select one or more names from the drop-down. Otherwise, any Alert name will trigger the rule. If you selected any categories, the list includes only alerts in those categories.

e. **Email**: (Optional) Click Add and from the drop-down menu, perform the following:

    i. Select To and type an email address or distribution list of the recipients to whom you plan to send the email notification.
    ii. Select CC and type an email address or distribution list of the recipients to whom you plan to send a copy of the email notification.

f. **SNMP**: (Optional) **Toggle** on if you want the rule to send SNMP notifications when the alert is triggered.

g. **Syslog**: (Optional) Toggle on if you want the rule to send Syslog notifications when the alert is triggered.

h. **Webhook**: (Optional) Toggle on and provide the URL and cURL details if you want the rule to send a web callback to a server. Type the URL for the server and type any cURL options you want to use. When an alert is triggered, the Cohesity cluster sends an HTTP request to the server. Your application can then interpret the request. For example, the webhook might notify the server about a critical disk alert, and your application might open a trouble ticket to track the problem. For more information, see Configuring Webhooks.

4. Click **Save**.

Guidelines for Cohesity Views

When configuring Cohesity Views, please take the following guidelines into consideration to be compliant with the DoDIN requirements.

- Enable File Services Audit
- Configure Global Settings for Views
- Update Authentication Provider for Storage Domain
- Add a Remote Cohesity Cluster
- Create a Replication Policy

Enable File Services Audit

File logs and Syslog are recorded to understand the activity at a particular time.

To enable or disable File Services Audit, do the following:

1. In the Cohesity Dashboard, navigate to **System** > **Audit Logs** > **Log Settings**.
2. In the **Log Settings** tab, turn on the toggle **File Services Audit** to enable it.

After enabling the **File Services Audit**, the **Log Retention Period** audit information option appears. Use this option to set the audit logs retention period.

Configure Global Settings for Views

When you configure global settings for Cohesity Views, it allows you to restrict unknown IP addresses to access the system.

Before you can mount and access a view, the system's IP address must be in a subnet that has been added to a Cohesity **Global Allowlist**. The global allowlist applies to all views on the Cohesity cluster but is overridden by a view allowlist or view share allowlist if they exist.

To add a subnet to the Cohesity cluster's global allowlist, follow the steps below.

1. Navigate to **File Services** > **Views**.
2. Select the **Global Settings** tab.
3. In the **Global Subnet Allowlist** section, click **Add**.
4. In the **Add Allowlist** screen, enter a **Subnet IP** in CIDR format (IPv4 - 10.0.0.0/24 or IPv6 - FE80:CD00::211E:729C/60).

   NOTE: CIDR prefix values are allowed from 0 to 32.

5. Select all permissions.
6. In the **Description** field, type a description for the allowlist.

7. Click **Add**.
8. Repeat the preceding steps for specifying additional subnets in the global allowlist.

For more information on **Global Settings** for SMB, NFS, and S3 Views, see:

- Global Settings for SMB
- Global Settings for NFS
- Global Settings for S3

Update Authentication Provider for Storage Domain

1. In the Cohesity Dashboard, select **Settings** > **Summary** and select the **Storage Domains** tab.
2. In the **Storage Domains** page, select **Actions Menu** and then **Edit** to edit an existing Storage Domain.
3. **Authentication Provider**: You can map the Storage Domain to an AD domain if the Cohesity cluster, version 6.5.1d or higher, is AD domain-joined. Mapping to a specific AD domain means that users from only that AD domain have permission to view the Storage Domain's contents when accessing through SMB. By default, a Storage Domain is accessible to users from all joined AD domains.

Add a Remote Cohesity Cluster

You have to establish the connection to a remote Cohesity cluster from your primary cluster. For more information, Create a Connection to the Remote Cohesity Cluster.

Create a Replication Policy

You can refer to Create or Edit Standard Policy to learn more about creating a policy on Cohesity cluster and adding replication settings to it.

1. In the Cohesity Dashboard, go to **Data Protection** > **Policies**.
2. Click **Create Policy** located at the top right of the page.
   To edit an existing policy in the list, click the actions menu and select **Edit**.
3. **Policy Name**: Specify a protection policy name. The name can contain the alphanumerics, underscores, hyphens, periods, and spaces. This field is required and can be changed later.
4. **Replication**: Click the Replication icon from the floating menu to replicate snapshots to another Cohesity cluster. The copied snapshots are stored in the storage domain of the remote cluster. (The storage domain, however, is specified in the Protection Group.) The replication schedule for copying Snapshots cannot be more often than the protection schedule for capturing Snapshots. For example, if Snapshots are captured hourly, the Cohesity cluster cannot replicate them every 30 minutes but it can replicate them hourly or any value over one hour.

> **NOTE**: For CloudArchive Direct, you should not add Replication.

5. Click **Save** to save your changes and return to the Policy Manager page.

The policy is immediately available to use in Protection Groups. You can now create a view and assign this replication policy to it.

Create & Protect Cohesity Views

This topic describes how you can create and protect a Cohesity view.

Create a Cohesity View for File Shares

After creating a replication policy, you have to create a Cohesity View. You can create a View for SMB or NFS file share.

> **NOTE:** To be DoDIN APL compliant, NFS shares must only use NFS version 4 or higher. This is required to support RPCSEC_GSS with Kerberos 5. Also, the SMB share must be v2 or higher.

1. In the Cohesity Dashboard, go to **SmartFiles** > **Views**.
2. Select **Create View**.
3. Enter the **View Name**.
4. Select **More Options** to update the settings. For more information about the available options, see About Cohesity View Options.
5. Select **Create** to create the view.

> **NOTE:** Select **Create View & Save as Template** to create the view and save the settings as a custom view template. On the **Template Name** dialog, enter the template name and click **Done**. The customized template is created.

Protect the View

You have to create a protection group with Cohesity View for SMB or NFS file share. Follow the steps below.

1. In the Cohesity Dashboard, go to **SmartFiles** > **Views**.
2. Choose a View and select the ellipsis icon.
3. Select **Protect**. The **Create Protection Group** page is displayed.
4. **Views**: Select the view that you want to protect and then click Save Selection. The list shows the Storage Domain that contains the view. View Snapshots are always stored in the same Storage Domain as the original view.
5. **Name**: Enter a name for the Protection Group. The name can contain alphanumeric characters, underscores, dashes, and periods.

6. **Policy**: Select an existing protection policy or create a new one by selecting New Policy.
7. **Remote View**: This option is available only if the policy you selected has replication enabled. In the Remote cluster fields, enter a name for each view that will be created on the remote Cohesity cluster corresponding to the views on the primary Cohesity cluster. Ensure that the names provided for the views are unique and are not the same as any other view names on the remote Cohesity cluster. If the name provided is not unique, then on the remote Cohesity cluster, a new view will be created with"-1" appended to the provided name. In the next protection run, the views in the remote Cohesity cluster will be overwritten by the latest replicated snapshot of the view on the primary Cohesity cluster.
8. **End Date**: (Optional) Toggle on and select the date when the Protection Group stops capturing snapshots. A protection run that starts prior to this date runs until completion even if it completes after this date.
9. **Start Time**: Available only if the selected policy is set to Backup Daily. Indicates when the Protection Group should run. The current time is displayed by default but you can change it. Enter the hour and minutes or use the up and down arrows on your keyboard. Verify the AM or PM setting.
   The default time zone is the browser's time zone. You can change the time zone by selecting a different time zone.
10. **Indexing**: Indexing is enabled by default and is required for file recovery. Optionally customize by adding indexing rules. Type index text. Click Add under Include and Exclude fields to add more index terms.
11. **Priority**: Select a priority for the Protection Group execution. Cohesity supports concurrent backups, but if the number of Protection Groups exceeds the ability to process them, those with High priority are given the highest priority to execute, Medium the second-highest priority, and Low the lowest priority.
12. **Cancel Runs at Quiet Time Start**: Available only if the selected policy has at least one quiet time period. Toggle it on to specify that all currently executing protection runs should abort if a quiet time period specified for the Protection Group starts. By default this toggle is off, which means after a protection run starts, it continues to execute even when a quiet time period specified for this protection run starts. However, a new protection run will not start during a quiet time period.
13. **Alerts**: Optional. Select one or more of the following settings if you want Alerts to be created for the following triggers:
    a. **Success**: Create an Informational Alert when a Protection Group completes successfully. Emails are not sent when Informational Alerts are created.
    b. **Failure**: Create a Critical Alert if the Protection Group fails to complete. Emails are sent when Critical Alerts are created.
       For more information about Alerts, see Alerts.
14. **Description**: Optional. Click the plus sign and enter a description for the Protection Group.
15. Select **Protect**.

The **Protection** page is displayed and includes the new Protection Group.

Mark Differentiated Services Code Point (DSCP) for an Active QoS Profile

The Quality of Service (QoS) feature in Cohesity supports Differentiated Services Code Point (DSCP) marking for outgoing packets based on the TCP/UDP ports and IP address. It enables the users to assign a QoS policy to a view.

A Cohesity view offers a storage location with NFS, SMB, and S3 mount paths within a storage domain on the Cohesity cluster. QoS policies optimize the performance of the view in terms of throughput, IOPS (Input/Output Operations Per Second), and latency for various workloads. Additionally, these policies enable users to prioritize I/O operations for specific views above others.

NOTE: Make sure to assign the QoS policy when creating a view.

For more information, see QoS Policies.

Default Configurations for Active QoS Profile

These are the default configurations for an Active QoS profile,

- By default, the QoS DSCP marking feature is disabled.
- Pre-created default profiles are available for immediate application if enabled.
- Access the default configuration details using the "`iris_cli qos-profile ls`" command.

Mark DSCP for an Active Profile

Follow the steps below to mark the DSCP for an Active Profile.

1. Log in to the cluster using the Linux support user account through your SSH client, ie. PuTTY.
2. Launch the CLI by entering the command, `iris_cli`.
3. Login with a valid administrator's account.
4. If you have not done so prior, enable the QoS DSCP marking feature by entering the following command:

   ```
   qos-profile feature enable=true
   ```

   The application of the command also triggers the QoS rules to the kernel.

   NOTE: The process occurs in the background and may take a few minutes to apply all the rules.

5. To confirm the QoS profiles are now available, enter the following command:

   ```
   qos-profile ls-active
   ```

   You can see a list of profiles (ie. Management, Operations) in the following format:

   PROFILE NAME : Default
   PRIORITY : 32676
   DIRECTION : "OUTPUT"

6. To activate or modify the DSCP value for an active QoS profile, enter the following command:

```
qos-profile activate name=<Profile Name> mark-dscp=<DSCP value>
```

For more information, see qos-profile and qos-profile activate.

Default Active QoS Profiles

The table below represents the list of active QoS profiles by default.

Table 4: Active QoS Profiles

Profile Name	RFC Mapping	Match	Direction	Action	DSCP Value
Management (ssh/http/https/ Teleport)	OAM	TCP/22, 443, 80, 3025, 3080, 3022, 3023, 3024	OUTPUT (dport OR sport)	Set DSCP	16
Operations (snmp/dhcp/dns/ntp/SMTP/LLDP)	OAM	UDP/161, 162, 68, 53, 123, 389 TCP/53, 25, 465, 587, 636, 389, 3268, 3269	OUTPUT (dport)	Set DSCP	16
Avahi	OAM	UDP/5353	OUTPUT (dport OR sport)	Set DSCP	16
Replication	High-Throughput Data (AF13)	TCP/11111, 20000, 24444	OUTPUT (dport OR sport)	Set DSCP	14
Data Protection	High-Throughput Data (AF13)	TCP/20004, 11113, 11117	OUTPUT (dport OR sport)	Set DSCP	14
S3/NFS/SMB	High-Throughput Data (AF12)	TCP/3000, 135, 445 TCP/111, 2049 UDP/111, 2049	OUTPUT (dport OR sport)	Set DSCP	12

Profile Name	RFC Mapping	Match	Direction	Action	DSCP Value
Routing Protocol	Network Control	protocol: tcp port 89,179,520	OUTPUT (dport OR sport)	Set DSCP	48
Internal Data	High-Throughput Data (AF11)	DIP: node_ipset	OUTPUT (DestIP)	Set DSCP	10
Others	Standard				0

Disable DSCP Marking Feature

Execute the following command to disable the DSCP marking feature:

```
iris_cli qos-profile feature enable=false
```

NOTE: Disabling may take a few minutes to complete and also removes the rules from the kernel.

Create and Delete QoS DSCP Marking Profile

To create a new QoS DSCP Marking profile,

1. Execute the following command:

   ```
   qos-profile add name=<Name> ports=<port> direction=<direction>
   ```

   NOTE: Ensure the name is unique. Currently, only output direction is supported.

2. List the ports and separate them with the commas.

   To delete a QoS DSCP Marking profile,

   Execute the following command:

   ```
   qos-profile delete name=<Name>
   ```

   IMPORTANT: Ensure to deactivate the profile before deletion.

Activate and Deactivate DSCP for QoS Profile

To activate DSCP for a QoS profile,

Execute the following command:

```
qos-profile activate name=<Name> mark-dscp=<DSCP value>
```

IMPORTANT: Ensure the name is unique and exists in the profile.

The IP set entries are limited to existing firewall IP set entries.

For more information, see qos-profile and qos-profile activate.

To deactivate DSCP for a QoS profile,

Execute the following command:

```
qos-profile deactivate profile-names=<profile name>
```

Restore Default QoS DSCP Marking Profile

To restore the QoS DSCP Marking profiles to default values,

Execute the following command:

```
qos-profile revert-to-default=true
```

IMPORTANT: Execution may take a few minutes to complete, depending on the previous configuration that needs to be cleaned.

FAQs

How to add a new QoS profile with higher priority than the default QoS profile?

To add a new QoS profile with higher priority than default QoS profile, execute the following command:

```
#iris_cli qos-profile add name=Custom_Profile ports="22/tcp"
direction=OUTPUT priority=1

#iris_cli qos-profile activate profile_names=Custom_Profile mark-dscp=20
```

How to change the priority on the default QoS profile?

To change the priority on default, execute the following command:

```
#iris_cli qos-profile deactivate profile_names=Management priority=10

#iris_cli qos-profile activate profile_names=Management mark-dscp=20
```

How do you create an override on default profile ports?

To create an override on default profile ports, execute the following command:

```
#iris_cli qos-profile create name=Custom_Profile ports=443/tcp
direction=OUTPUT priority=1 force=true

#iris_cli qos-profile activate profile-name=Custom_Profile mark-dscp=0x5
```

How do you activate the QoS profile matching IP Address/Port?

To activate the QoS profile matching IP Address/Port, execute the following command:

```
#iris_cli firewall-ipset ls

[support@haswell2-bqkp91500082-node-1 ~]$ iris_cli firewall-ipset ls

IPSET NAME                    : customize_1_ipset

IPSET ENTRIES                 : 20.1.4.0/24


#iris_cli qos-profile create name=Custom_Profile ports=9999/tcp
direction=OUTPUT priority=1 force=true

#iris_cli qos-profile activate profile-name=Custom_Profile mark-dscp=0x5
ipset-entries=customize_1_ipset
```

Appendix A: Cohesity Ports and Protocols

You can refer to the topic Manage Firewall Rules to learn more about the ports and protocols that are open on the Cohesity system.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Seethamsu S is a Technical Writer at Cohesity. In his role, Seethamsu focuses on security and multitenancy components of the platform, and FortKnox.

Other essential contributors include:

- Luke Walker, Product Management
- Venkatesh Pallipadi, Technical Director
- Gauri Gokhale, Member of Technical Staff
- Subash Babu, Staff Technology Editor at Cohesity

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.1	May 2024	Content Updates
1.0	Mar 2023	First Release

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 44 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.