

ECS

Version 3.4.0.1

Administration Guide

302-999-901

02

February 2020

Copyright © 2019-2020 Dell Inc. or its subsidiaries. All rights reserved.

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.” DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

Figures		7
Tables		9
Chapter 1	Overview	11
	Introduction.....	12
	ECS platform.....	12
	ECS data protection.....	14
	Configurations for availability, durability, and resilience.....	15
	ECS network.....	17
	Load balancing considerations.....	17
Chapter 2	Getting Started with ECS	19
	Initial configuration.....	20
	Log in to the ECS Portal.....	20
	View the Getting Started Task Checklist.....	21
	View the ECS Portal Dashboard.....	22
	Upper-right menu bar.....	22
	View requests.....	22
	View capacity utilization.....	22
	View performance.....	23
	View storage efficiency.....	23
	View geo monitoring.....	23
	View node and disk health.....	23
	View alerts.....	23
Chapter 3	Storage Pools, VDCs, and Replication Groups	25
	Introduction to storage pools, VDCs, and replication groups.....	26
	Working with storage pools in the ECS Portal.....	27
	Create a storage pool.....	28
	Edit a storage pool.....	29
	Working with VDCs in the ECS Portal	29
	Create a VDC for a single site.....	31
	Add a VDC to a federation.....	31
	Edit a VDC.....	33
	Remove VDC from a Replication Group.....	35
	Fail a VDC (PSO).....	36
	Guidelines to check failover and bootstrap process.....	36
	Working with replication groups in the ECS Portal.....	37
	Create a replication group.....	38
	Edit a replication group.....	40
Chapter 4	Authentication Providers	41
	Introduction to authentication providers.....	42
	Working with authentication providers in the ECS Portal.....	42
	Considerations when adding Active Directory authentication providers...	42

	AD or LDAP authentication provider settings.....	43
	Add an AD or LDAP authentication provider.....	46
	Add a Keystone authentication provider.....	46
Chapter 5	Namespaces	49
	Introduction to namespaces.....	50
	Namespace tenancy.....	50
	Working with namespaces in the ECS Portal.....	51
	Namespace settings.....	51
	Create a namespace.....	55
	Edit a namespace.....	57
	Delete a namespace.....	58
Chapter 6	Users and Roles	59
	Introduction to users and roles.....	60
	Users in ECS.....	60
	Management users.....	60
	Default management users.....	60
	Object users.....	61
	Domain and local users.....	62
	User scope.....	63
	User tags.....	64
	Management roles in ECS.....	64
	System Administrator.....	64
	System Monitor.....	65
	Namespace Administrator.....	65
	Lock Administrator.....	65
	Tasks performed by role.....	65
	Working with users in the ECS Portal.....	68
	Add an object user.....	70
	Add a domain user as an object user.....	71
	Add domain users into a namespace.....	72
	Create a local management user or assign a domain user or AD group to a management role.....	72
	Assign the Namespace Administrator role to a user or AD group.....	73
Chapter 7	Buckets	75
	Introduction to buckets.....	76
	Working with buckets in the ECS Portal.....	76
	Bucket settings.....	76
	Create a bucket.....	79
	Edit a bucket.....	81
	Set ACLs.....	82
	Set bucket policies.....	85
	Create a bucket using the S3 API (with s3curl).....	89
	Bucket HTTP headers.....	91
	Bucket, object, and namespace naming conventions.....	92
	S3 bucket and object naming in ECS.....	92
	OpenStack Swift container and object naming in ECS.....	93
	Atmos bucket and object naming in ECS.....	93
	CAS pool and object naming in ECS.....	93
	Disable unused services.....	94

Chapter 8	File Access	97
	Introduction to file access.....	98
	ECS multi-protocol access.....	98
	S3/NFS multi-protocol access to directories and files.....	98
	Multi-protocol access permissions.....	99
	Working with NFS exports in the ECS Portal.....	101
	Working with user/group mappings in the ECS Portal.....	101
	ECS NFS configuration tasks.....	102
	Create a bucket for NFS using the ECS Portal.....	102
	Add an NFS export using the ECS Portal.....	104
	Add a user or group mapping using the ECS Portal.....	105
	Configure ECS NFS with Kerberos security.....	106
	Mount an NFS export example.....	112
	Best practices for mounting ECS NFS exports.....	114
	NFS access using the ECS Management REST API.....	114
	NFS WORM (Write Once, Read Many).....	115
	S3A support.....	118
	Configuration at ECS.....	118
	Configuration at Ambari Node.....	118
	Geo-replication status.....	119
Chapter 9	Certificates	121
	Introduction to certificates.....	122
	Generate certificates.....	122
	Create a private key.....	123
	Generate a SAN configuration.....	123
	Create a self-signed certificate.....	124
	Create a certificate signing request.....	126
	Upload a certificate.....	130
	Authenticate with the ECS Management REST API.....	130
	Upload a management certificate.....	131
	Upload a data certificate for data access endpoints.....	132
	Add custom LDAP certificate.....	133
	Verify installed certificates.....	136
	Verify the management certificate.....	136
	Verify the object certificate.....	137
Chapter 10	ECS Settings	139
	Introduction to ECS settings.....	140
	Object base URL.....	140
	Bucket and namespace addressing.....	140
	DNS configuration.....	142
	Add a Base URL.....	142
	Key Management.....	143
	Native Key Management.....	146
	External Key Management.....	146
	External Key Manager Configuration.....	147
	Key Rotation.....	152
	EMC Secure Remote Services.....	152
	ESRS prerequisites	153
	Add an ESRS Server.....	154
	Verify that ESRS call home works.....	155
	Disable call home.....	155
	Alert policy.....	156

	New alert policy.....	156
	Event notification servers.....	157
	SNMP servers.....	157
	Syslog servers.....	162
	Platform locking.....	165
	Lock and unlock nodes using the ECS Portal.....	166
	Lock and unlock nodes using the ECS Management REST API.....	166
	Licensing.....	167
	Obtain the Dell EMC ECS license file.....	168
	Upload the ECS license file.....	168
	Security.....	168
	Password.....	169
	Password Rules.....	169
	Sessions.....	171
	User Agreement.....	171
	About this VDC.....	172
Chapter 11	ECS Outage and Recovery	173
	Introduction to ECS site outage and recovery.....	174
	TSO behavior.....	174
	TSO behavior with the ADO bucket setting turned off.....	174
	TSO behavior with the ADO bucket setting turned on.....	176
	TSO considerations.....	182
	NFS file system access during a TSO.....	182
	PSO behavior.....	182
	Recovery on disk and node failures.....	183
	NFS file system access during a node failure.....	183
	Data rebalancing after adding new nodes.....	184
Chapter 12	Advanced Monitoring	185
	Advanced Monitoring.....	186
	View Advanced Monitoring Dashboards.....	186
	Share Advanced Monitoring Dashboards.....	192
	Flux API.....	192
	List of metrics for performance-related data.....	195
	Dashboard API's to be deprecated or changed in the next release.....	198

FIGURES

1	ECS component layers.....	13
2	Guide icon	21
3	Getting Started Task Checklist.....	21
4	Upper-right menu bar.....	22
5	Replication group spanning three sites and replication group spanning two sites.....	27
6	Adding a subset of domain users into a namespace using one AD attribute.....	62
7	Adding a subset of domain users into a namespace using multiple AD attributes.....	63
8	Bucket Policy Editor code view.....	86
9	Bucket Policy Editor tree view.....	86
10	Data encryption using system-generated keys.....	145
11	Encryption of the master key in a geo-replicated environment.....	145
12	Native key management.....	146
13	Read/write request fails during TSO when data is accessed from non-owner site and owner site is unavailable.....	175
14	Read/write request succeeds during TSO when data is accessed from owner site and non-owner site is unavailable.....	176
15	Read/write request succeeds during TSO when ADO-enabled data is accessed from non-owner site and owner site is unavailable.....	177
16	Object ownership example for a write during a TSO in a two-site federation.....	179
17	Read request workflow example during a TSO in a three-site federation.....	180
18	Passive replication in normal state.....	181
19	TSO for passive replication.....	181

TABLES

1	ECS supported data services.....	13
2	Erasure encoding requirements for regular and cold archives	14
3	Storage overhead.....	15
4	ECS data protection schemes.....	16
5	Storage pool properties.....	27
6	VDC properties.....	30
7	Replication Group properties.....	38
8	Authentication provider properties.....	42
9	AD or LDAP authentication provider settings.....	43
10	Keystone authentication provider settings.....	47
11	Namespace properties.....	51
12	Namespace settings.....	51
13	Default management users.....	61
14	Tasks performed by ECS management user role.....	66
15	Object user properties.....	69
16	Management user properties.....	69
17	Bucket settings.....	77
18	Bucket ACLs.....	83
19	Bucket headers.....	91
20	NFS export properties.....	101
21	ECS Management REST API calls for managing NFS access.....	114
22	Autocommit terms.....	115
23	Key Management properties.....	148
24	Create cluster.....	148
25	New external key servers.....	149
26	Key Management properties.....	151
27	ESRS properties.....	152
28	Syslog facilities used by ECS.....	164
29	Syslog severity keywords.....	164
30	ECS Management REST API calls for managing node locking	167
31	Password rules.....	169
32	Sessions.....	171
33	User agreement.....	171
34	Advanced monitoring dashboards.....	186
35	Advanced monitoring dashboard fields.....	186
36	Metrics for performance-related data.....	195
37	API - Remove.....	198
38	API - Change.....	198
39	API - No change.....	199

CHAPTER 1

Overview

- [Introduction](#)..... 12
- [ECS platform](#)..... 12
- [ECS data protection](#).....14
- [ECS network](#)..... 17
- [Load balancing considerations](#).....17

Introduction

Dell EMC ECS provides a complete software-defined cloud storage platform that supports the storage, manipulation, and analysis of unstructured data on a massive scale on commodity hardware. You can deploy ECS as a turnkey storage appliance or as a software product that is installed on a set of qualified commodity servers and disks. ECS offers the cost advantages of a commodity infrastructure and the enterprise reliability, availability, and serviceability of traditional arrays.

ECS uses a scalable architecture that includes multiple nodes and attached storage devices. The nodes and storage devices are commodity components, similar to devices that are generally available, and are housed in one or more racks.

A rack and its components that are supplied by Dell EMC and that have preinstalled software, is referred to as an ECS *appliance*. A rack and commodity nodes that are not supplied by Dell EMC, is referred to as a Dell EMC ECS *software only solution*. Multiple racks are referred to as a *cluster*.

A rack, or multiple joined racks, with processing and storage that is handled as a coherent unit by the ECS infrastructure software is referred to as a *site*, and at the ECS software level as a *Virtual Data Center* (VDC).

Management users can access the ECS UI, which is referred to as the ECS Portal, to perform administration tasks. Management users include the System Administrator, Namespace Administrator, and System Monitor roles. Management tasks that can be performed in the ECS Portal can also be performed by using the ECS Management REST API.

ECS administrators can perform the following tasks in the ECS Portal:

- Configure and manage the object store infrastructure (compute and storage resources) for object users.
- Manage users, roles, and buckets within namespaces. Namespaces are equivalent to tenants.

Object users cannot access the ECS Portal, but can access the object store to read and write objects and buckets by using clients that support the following data access protocols:

- Amazon Simple Storage Service (Amazon S3)
- EMC Atmos
- OpenStack Swift
- ECS CAS (content-addressable storage)

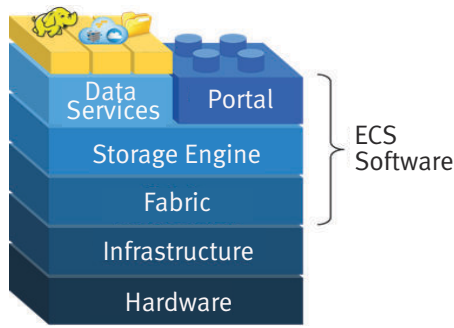
For more information about object user tasks, see the *ECS Data Access Guide*, available from the [ECS Product Documentation page](#).

For more information about System Monitor tasks, see the *ECS Monitoring Guide*, available from the [ECS Product Documentation page](#).

ECS platform

The ECS platform is composed of the data services, portal, storage engine, fabric, infrastructure, and hardware component layers.

Figure 1 ECS component layers



Data services

The data services component layer provides support for access to the ECS object store through object, HDFS, and NFS v3 protocols. In general, ECS provides multi-protocol access, data that is ingested through one protocol can be accessed through another. For example, data that is ingested through S3 can be modified through Swift, NFS v3, or HDFS. This multi-protocol access has some exceptions due to protocol semantics and representations of how the protocol was designed.

The following table shows the object APIs and the protocols that are supported and that interoperate.

Table 1 ECS supported data services

Protocols		Support	Interoperability
Object	S3	Additional capabilities such as byte range updates and rich ACLS	File systems (HDFS and NFS), Swift
	Atmos	Version 2.0	NFS (only path-based objects, not object ID style objects)
	Swift	V2 APIs, Swift, and Keystone v3 authentication	File systems (HDFS and NFS), S3
	CAS	SDK v3.1.544 and later	Not applicable
HDFS		Hadoop 2.6.2 compatibility	S3, Swift*
NFS		NFSv3	S3, Swift, Atmos (only path-based objects)
* When a bucket is enabled for file system access, permissions set using HDFS are in effect when you access the bucket as an NFS file system, and vice versa.			

Portal

The ECS Portal component layer provides a Web-based GUI that allows you to manage, license, and provision ECS nodes. The portal has the following comprehensive reporting capabilities:

- Capacity utilization for each site, storage pool, node, and disk
- Performance monitoring on latency, throughput, transactions per second, and replication progress and rate
- Diagnostic information, such as node and disk recovery status and statistics on hardware and process health for each node, which helps identify performance and system bottlenecks

Storage engine

The storage engine component layer provides an unstructured storage engine that is responsible for storing and retrieving data, managing transactions, and protecting and replicating data. The storage engine provides access to objects ingested using multiple object storage protocols and the NFS and HDFS file protocols.

Fabric

The fabric component layer provides cluster health management, software management, configuration management, upgrade capabilities, and alerting. The fabric layer is responsible for keeping the services running and managing resources such as the disks, containers, firewall, and network. It tracks and reacts to environment changes such as failure detection and provides alerts that are related to system health. The 9069 and 9099 ports are public IP ports protected by Fabric Firewall manager. Port is not available outside of the cluster.

Infrastructure

The infrastructure component layer uses SUSE Linux Enterprise Server 12 as the base operating system for the ECS appliance, or qualified Linux operating systems for commodity hardware configurations. Docker is installed on the infrastructure to deploy the other ECS component layers. The Java Virtual Machine (JVM) is installed as part of the infrastructure because ECS software is written in Java.

Hardware

The hardware component layer is an ECS appliance or qualified industry standard hardware. For more information about ECS hardware, see the *ECS Hardware and Cabling Guide*, available from the [ECS Product Documentation page](#).

ECS data protection

ECS protects data within a site by mirroring the data onto multiple nodes, and by using erasure coding to break down data chunks into multiple fragments and distribute the fragments across nodes. Erasure coding (EC) reduces the storage overhead and ensures data durability and resilience against disk and node failures.

By default, the storage engine implements the Reed-Solomon 12 + 4 erasure coding scheme in which an object is broken into 12 data fragments and 4 coding fragments. The resulting 16 fragments are dispersed across the nodes in the local site. When an object is erasure-coded, ECS can read the object directly from the 12 data fragments without any decoding or reconstruction. The code fragments are used only for object reconstruction when a hardware failure occurs. ECS also supports a 10 + 2 scheme for use with cold storage archives to store objects that do not change frequently and do not require the more robust default EC scheme.

The following table shows the requirements for the supported erasure coding schemes.

Table 2 Erasure encoding requirements for regular and cold archives

Use case	Minimum required nodes	Minimum required disks	Recommended disks	EC efficiency	EC scheme
Regular archive	4	16	32	1.33	12 + 4
Cold archive	6	12	24	1.2	10 + 2

Sites can be federated, so that data is replicated to another site to increase availability and data durability, and to ensure that ECS is resilient against site failure. For three or more sites, in addition to the erasure coding of chunks at a site, chunks that are replicated to other sites are combined using a technique called XOR to provide increased storage efficiency.

The following table shows the storage efficiency that can be achieved by ECS where multiple sites are used.

Table 3 Storage overhead

Number of sites in replication group	Storage overhead	
	Default (Erasure Code: 12+4)	Cold archive (Erasure Code: 10+2)
1	1.33	1.2
2	2.67	2.4
3	2.00	1.8
4	1.77	1.6
5	1.67	1.5
6	1.60	1.44
7	1.55	1.40
8	1.52	1.37

If you have one site, with erasure coding the object data chunks use more space (1.33 or 1.2 times storage overhead) than the raw data bytes require. If you have two sites, the storage overhead is doubled (2.67 or 2.4 times storage overhead) because both sites store a replica of the data, and the data is erasure coded at both sites. If you have three or more sites, ECS combines the replicated chunks so that, counter intuitively, the storage overhead reduces.

When one node is down in a four nodes system, ECS starts to rebuild the EC on priority to avoid DU. As one node is down, EC segment separates to other three nodes, which results in segment number being greater than the EC code number. If the down node comes back, things go back to normal. When another node with the most number of EC segments goes down, the DU window is as large as the node NA window, when the node does not recover it causes DL.

EC retiring feature converts unsaved EC chunk into three mirror copies chunk for data safety. However, EC retiring has some limitations:

- It increases system capacity, and protection overhead from 1.33 to 3.
- When there is no node down situation, EC retiring introduce unnecessary IO.
- The feature applies to four nodes system. EC retiring does not automatically trigger, you need to trigger it on demand using an API through service console.

For a detailed description of the mechanism used by ECS to provide data durability, resilience, and availability, see the *ECS High Availability Design White Paper*.

Configurations for availability, durability, and resilience

Depending on the number of sites in the ECS system, different data protection schemes can increase availability and balance the data protection requirements against performance. ECS uses the replication group to configure the data protection schemes (see [Introduction to storage pools, VDCs, and replication groups](#) on page 26). The following table shows the data protection schemes that are available.

Table 4 ECS data protection schemes

Number of sites	Data protection scheme			
	Local Protection	Full Copy Protection*	Active	Passive
1	Yes	Not applicable	Not applicable	Not applicable
2	Yes	Always	Not applicable	Not applicable
3 or more	Yes	Optional	Normal	Optional
* Full Copy Protection can be selected with Active. Full Copy Protection is not available if Passive is selected.				

Local Protection

Data is protected locally by using triple mirroring and erasure coding which provides resilience against disk and node failures, but not against site failure.

Full Copy Protection

When the **Replicate to All Sites** setting is turned on for a replication group, the replication group makes a full readable copy of all objects to all sites within the replication group. Having full readable copies of objects on all VDCs in the replication group provides data durability and improves local performance at all sites at the cost of storage efficiency.

Active

Active is the default ECS configuration. When a replication group is configured as Active, data is replicated to federated sites and can be accessed from all sites with strong consistency. If you have two sites, full copies of data chunks are copied to the other site. If you have three or more sites, the replicated chunks are combined (XOR'ed) to provide increased storage efficiency.

When data is accessed from a site that is not the owner of the data, until that data is cached at the non-owner site, the access time increases. Similarly, if the owner site that contains the primary copy of the data fails, and if you have a global load balancer that directs requests to a non-owner site, the non-owner site must recreate the data from XOR'ed chunks, and the access time increases.

Passive

The Passive configuration includes two, three, or four active sites with an additional passive site that is a replication target (backup site). The minimum number of sites for a Passive configuration is three (two active, one passive) and the maximum number of sites is five (four active, one passive). Passive configurations have the same storage efficiency as Active configurations. For example, the Passive three-site configuration has the same storage efficiency as the Active three-site configuration (2.0 times storage overhead).

In the Passive configuration, all replication data chunks are sent to the passive site and XOR operations occur only at the passive site. In the Active configuration, the XOR operations occur at all sites.

If all sites are on-premise, you can designate any of the sites as the replication target.


If there is a backup site hosted off-premise by a third-party data center, ECS automatically selects it as the replication target when you create a Passive geo replication group (see [Create a replication group](#) on page 38). If you want to change the replication target from a hosted site to an on-premise site, you can do so using the ECS Management REST API.

ECS network

ECS network infrastructure consists of top of rack switches allowing for the following types of network connections:

- Public network – connects ECS nodes to your organization's network, providing data.
- Internal private network – manages nodes and switches within the rack and across racks.

For more information about ECS networking, see the *ECS Networking and Best Practices White Paper*.

 **CAUTION** It is required to have connections from the customer's network to both front end switches (rabbit and hare) in order to maintain the high availability architecture of the ECS appliance. If the customer chooses not to connect to their network in the required HA manner, there is no guarantee of high data availability for the use of this product.

Load balancing considerations

It is recommended that a load balancer is used in front of ECS.

In addition to distributing the load across ECS cluster nodes, a load balancer provides High Availability (HA) for the ECS cluster by routing traffic to healthy nodes. Where network separation is implemented, and data and management traffic are separated, the load balancer must be configured so that user requests, using the supported data access protocols, are balanced across the IP addresses of the data network. ECS Management REST API requests can be made directly to a node IP on the management network or can be load balanced across the management network for HA.

The load balancer configuration is dependent on the load balancer type. For information about tested configurations and best practice, contact your customer support representative.

CHAPTER 2

Getting Started with ECS

- [Initial configuration](#).....20
- [Log in to the ECS Portal](#).....20
- [View the Getting Started Task Checklist](#)..... 21
- [View the ECS Portal Dashboard](#)..... 22

Initial configuration

The initial configuration steps that are required to get started with ECS include logging in to the ECS Portal for the first time, using the ECS Portal Getting Started Task Checklist and Dashboard, uploading a license, and setting up an ECS virtual data center (VDC).

About this task

To initially configure ECS, the root user or System Administrator must at a minimum:

Procedure

1. Upload an ECS license.
See [Licensing](#) on page 167.
 2. Select a set of nodes to create at least one storage pool.
See [Create a storage pool](#) on page 28.
 3. Create a VDC.
See [Create a VDC for a single site](#) on page 31.
 4. Create at least one replication group.
See [Create a replication group](#) on page 38.
 - a. Optional: Set authentication.
You can add Active Directory (AD), LDAP, or Keystone authentication providers to ECS to enable users to be authenticated by systems external to ECS. See [Introduction to authentication providers](#) on page 42.
 5. Create at least one namespace. A namespace is the equivalent of a tenant.
See [Create a namespace](#) on page 55.
 - a. Optional: Create object and/or management users.
See [Working with users in the ECS Portal](#) on page 68.
 6. Create at least one bucket.
See [Create a bucket](#) on page 79.
- After you configure the initial VDC, if you want to create an additional VDC and federate it with the first VDC, see [Add a VDC to a federation](#) on page 31.

Log in to the ECS Portal

Log in to the ECS Portal to set up the initial configuration of a VDC. Log in to the ECS Portal from the browser by specifying the IP address or fully qualified domain name (FQDN) of any node, or the load balancer that acts as the front end to ECS. The login procedure is described below.

Before you begin

Logging in to the ECS Portal requires the System Administrator, System Monitor, Lock Administrator (`emcsecurity` user), or Namespace Administrator role.

Note: You can login to the ECS Portal for the first time with any valid login. However, you can configure the system, only with the System Administrator role.

Procedure

1. Type the public IP address of the first node in the system, or the address of the load balancer that is configured as the front-end, in the address bar of your browser:
`https://<node1_public_ip>`.
2. Log in with the default root credentials:
 - **User Name:** `root`
 - **Password:** `ChangeMe`
 You are prompted to change the password for the `root` user immediately.
3. After you change the password at first login, click **Save**.
You are logged out and the ECS login screen is displayed.
4. Type the **User Name** and **Password**.
5. To log out of the ECS Portal, in the upper-right menu bar, click the arrow beside your user name, and then click **logout**.

View the Getting Started Task Checklist

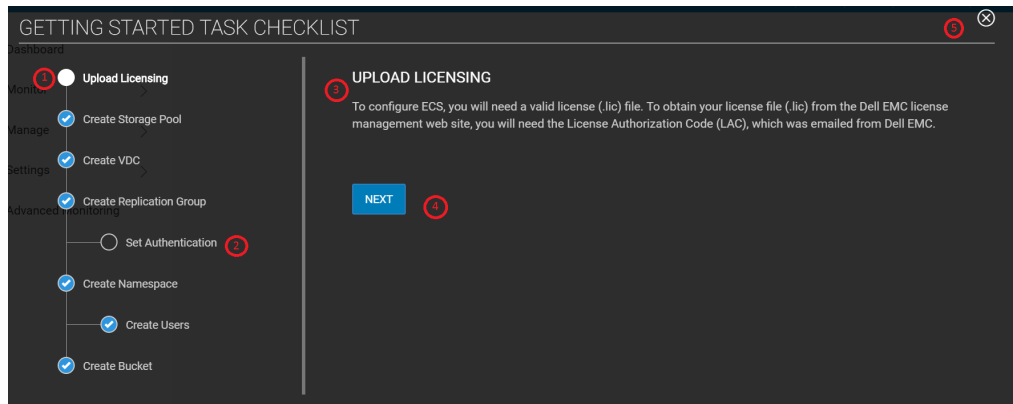
The Getting Started Task Checklist in the ECS Portal guides you through the initial ECS configuration. The checklist appears when you first log in and when the portal detects that the initial configuration is not complete. The checklist automatically appears until you dismiss it. On any ECS Portal page, in the upper-right menu bar, click the Guide icon to open the checklist.

Figure 2 Guide icon



The Getting Started Task Checklist displays in the portal.

Figure 3 Getting Started Task Checklist



1. The current step in the checklist.
2. An optional step. This step does not display a check mark even if you have completed the step.
3. Information about the current step.
4. Available actions.
5. Dismiss the checklist.

A completed step appears in green color.

A completed checklist gives you the option to browse the list again or recheck your configuration.

View the ECS Portal Dashboard

The ECS Portal Dashboard provides critical information about the ECS processes on the VDC you are currently logged in to.

The Dashboard is the first page you see after you log in. The title of each panel (box) links to the portal monitoring page that shows more detail for the monitoring area.

Upper-right menu bar

The upper-right menu bar appears on each ECS Portal page.

Figure 4 Upper-right menu bar



Menu items include the following icons and menus:

1. The Alert icon displays a number that indicates how many unacknowledged alerts are pending for the current VDC. The number displays 99+ if there are more than 99 alerts. You can click the Alert icon to see the Alert menu, which shows the five most recent alerts for the current VDC.
2. The Help icon brings up the online documentation for the current portal page.
3. The Guide icon brings up the Getting Started Task Checklist.
4. The VDC menu displays the name of the current VDC. If your AD or LDAP credentials allow you to access more than one VDC, you can switch the portal view to the other VDCs without entering your credentials.
5. The User menu displays the current user and allows you to log out. The User menu displays the last login time for the user.

View requests

The **Requests** panel displays the total requests, successful requests, and failed requests.

Failed requests are organized by system error and user error. User failures are typically HTTP 400 errors. System failures are typically HTTP 500 errors. Click **Requests** to see more request metrics.

Request statistics do not include replication traffic.

View capacity utilization

The **Capacity Utilization** panel displays the total, used, available, reserved, and percent full capacity.

Capacity amounts are shown in gibibytes (GiB) and tibibytes (TiB). One GiB is approximately equal to 1.074 gigabytes (GB). One TiB is approximately equal to 1.1 terabytes (TB).

The **Used** capacity indicates the amount of capacity that is in use. Click **Capacity Utilization** to see more capacity metrics.

The capacity metrics are available in the left menu.

View performance

The **Performance** panel displays how network read and write operations are currently performing, and the average read/write performance statistics over the last 24 hours for the VDC.

Click **Performance** to see more comprehensive performance metrics.

View storage efficiency

The **Storage Efficiency** panel displays the efficiency of the erasure coding (EC) process.

The chart shows the progress of the current EC process, and the other values show the total amount of data that is subject to EC, the amount of EC data waiting for the EC process, and the current rate of the EC process. Click **Storage Efficiency** to see more storage efficiency metrics.

View geo monitoring

The **Geo Monitoring** panel displays how much data from the local VDC is waiting for geo-replication, and the rate of the replication.

Recovery Point Objective (**RPO**) refers to the point in time in the past to which you can recover. The value is the oldest data at risk of being lost if a local VDC fails before replication is complete. **Failover Progress** shows the progress of any active failover that is occurring in the federation involving the local VDC. **Bootstrap Progress** shows the progress of any active process to add a new VDC to the federation. Click **Geo Monitoring** to see more geo-replication metrics.

View node and disk health

The **Node & Disks** panel displays the health status of disks and nodes.

A green check mark beside the node or disk number indicates the number of nodes or disks in good health. A red x indicates bad health. Click **Node & Disks** to see more hardware health metrics. If the number of bad disks or nodes is a number other than zero, clicking on the count takes you to the corresponding **Hardware Health** tab (**Offline Disks** or **Offline Nodes**) on the **System Health** page.

View alerts

The **Alerts** panel displays a count of critical alerts and errors.

Click **Alerts** to see the full list of current alerts. Any Critical or Error alerts are linked to the **Alerts** tab on the **Events** page where only the alerts with a severity of Critical or Error are filtered and displayed.

CHAPTER 3

Storage Pools, VDCs, and Replication Groups

- [Introduction to storage pools, VDCs, and replication groups](#)..... 26
- [Working with storage pools in the ECS Portal](#)..... 27
- [Working with VDCs in the ECS Portal](#) 29
- [Working with replication groups in the ECS Portal](#)..... 37

Introduction to storage pools, VDCs, and replication groups

This topic provides conceptual information on storage pools, virtual data centers (VDCs), and replication groups and the following topics describe the operations required to configure them:

- [Working with storage pools at the ECS Portal](#)
- [Working with VDCs at the ECS Portal](#)
- [Working with replication groups at the ECS Portal](#)

The storage that is associated with a VDC must be assigned to a storage pool and the storage pool must be assigned to one or more replication groups to allow the creation of buckets and objects.

A storage pool can be associated with more than one replication group. A best practice is to have a single storage pool for a site. However, you can have as many storage pools as required, with a minimum of four nodes (and 16 disks) in each pool.

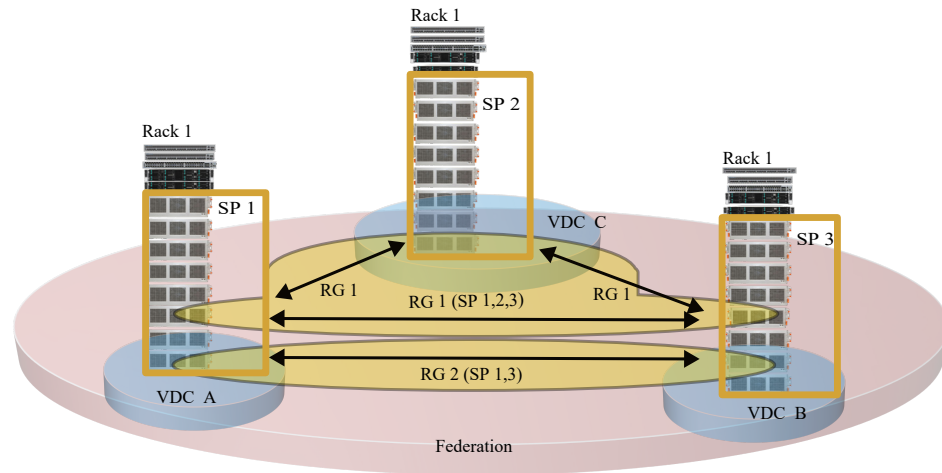
You might need to create more than one storage pool at a site for the following reasons:

- The storage pool is used for Cold Archive. The erasure coding scheme used for cold archive uses 10+2 coding rather than the default ECS 12+4 scheme.
- A tenant requires the data to be stored on separate physical media.

A storage pool must have a minimum of four nodes and must have three or more nodes with more than 10% free capacity in order to allow writes. This reserved space is required to ensure that ECS does not run out of space while persisting system metadata. If this criteria is not met, the write will fail. The ability of a storage pool to accept writes does not affect the ability of other pools to accept writes. For example, if you have a load balancer that detects a failed write, the load balancer can redirect the write to another VDC.

The replication group is used by ECS for replicating data to other sites so that the data is protected and can be accessed from other, active sites. When you create a bucket, you specify the replication group it is in. ECS ensures that the bucket and the objects in the bucket are replicated to all the sites in the replication group.

ECS can be configured to use more than one replication scheme, depending on the requirements to access and protect the data. The following figure shows a replication group (RG 1) that spans all three sites. RG 1 takes advantage of the XOR storage efficiency provided by ECS when using three or more sites. In the figure, the replication group that spans two sites (RG 2), contains full copies of the object data chunks and does not use XOR'ing to improve storage efficiency.

Figure 5 Replication group spanning three sites and replication group spanning two sites

The physical storage that the replication group uses at each site is determined by the storage pool that is included in the replication group. The storage pool aggregates the disk storage of each of the minimum of four nodes to ensure that it can handle the placement of erasure coding fragments. A node cannot exist in more than one storage pool. The storage pool can span racks, but it is always within a site.

Working with storage pools in the ECS Portal

You can use storage pools to organize storage resources based on business requirements. For example, if you require physical separation of data, you can partition the storage into multiple storage pools.

You can use the **Storage Pool Management** page available from **Manage > Storage Pools** to view the details of existing storage pools, to create storage pools, and to edit existing storage pools. You cannot delete storage pools in this release.

Table 5 Storage pool properties

Field	Description
Name	The name of the storage pool.
Nodes	The number of nodes that are assigned to the storage pool.
Status	The state of the storage pool and of the nodes. <ul style="list-style-type: none"> Ready: At least four nodes are installed and all nodes are in the <code>ready to use</code> state. Not Ready: A node in the storage pool is not in the <code>ready to use</code> state. Partially Ready: Less than four nodes, and all nodes are in the <code>ready to use</code> state.
Host	The fully qualified host name that is assigned to the node.
Data IP	The public IP address that is assigned to the node or the data IP address in network separation environment.
Rack ID	The name that is assigned to the rack that contains the nodes.
Actions	The actions that can be completed for the storage pool.

Table 5 Storage pool properties (continued)

Field	Description
	<ul style="list-style-type: none"> • Edit: Change the storage pool name or modify the set of nodes that are included in the storage pool. • Delete: Used by Customer Support to delete the storage pool. System Administrators or root users should not attempt to delete the storage pool. If you attempt this operation in the ECS Portal, you receive an error message that states this operation is not supported. If you must delete a storage pool, contact your customer support representative.
Cold Storage	A storage pool that is specified as Cold Storage. Cold Storage pools use an erasure coding (EC) scheme that is more efficient for infrequently accessed objects. Cold Storage is also known as a Cold Archive. After a storage pool is created, this setting cannot be changed.

Create a storage pool


Storage pools must contain a minimum of four nodes. The first storage pool that is created is known as the system storage pool because it stores system metadata.

Before you begin

This operation requires the System Administrator role in ECS.

Procedure

1. In the ECS Portal, select **Manage > Storage Pools**.
2. On the **Storage Pool Management** page, click **New Storage Pool**.
3. On the **New Storage Pool** page, in the **Name** field, type the storage pool name (for example, `storagePool1`).
4. In the **Cold Storage** field, specify if this storage pool is Cold Storage. Cold storage contains infrequently accessed data. The ECS data protection scheme for cold storage is optimized to increase storage efficiency. After a storage pool is created, this setting cannot be changed.

 **Note:** Cold storage requires a minimum hardware configuration of six nodes. For more information, see [ECS data protection](#) on page 14.

5. From the **Available Nodes** list, select the nodes to add to the storage pool.
 - a. To select nodes one-by-one, click the **+** icon beside each node.
 - b. To select all available nodes, click the **+** icon at the top of the **Available Nodes** list.
 - c. To narrow the list of available nodes, in the **search** field, type the public IP address for the node or the host name.
6. In the **Available Capacity Alerting** fields, select the applicable available capacity thresholds that will trigger storage pool capacity alerts:
 - a. In the **Critical** field, select **10 %**, **15 %**, or **No Alert**.
For example, if you select **10 %**, that means a Critical alert will be triggered when the available storage pool capacity is less than 10 percent.
 - b. In the **Error** field, select **20 %**, **25 %**, **30 %**, or **No Alert**.
For example, if you select **25 %**, that means an Error alert will be triggered when the available storage pool capacity is less than 25 percent.

- c. In the **Warning** field, select **35 %**, **40 %**, or **No Alert**.

For example, if you select **40 %**, that means a Warning alert will be triggered when the available storage pool capacity is less than 40 percent.

When a capacity alert is generated, a call home alert is also generated that alerts ECS customer support that the ECS system is reaching its capacity limit.

7. Click **Save**.
8. Wait 10 minutes after the storage pool is in the **Ready** state before you perform other configuration tasks, to allow the storage pool time to initialize.

If you receive the following error, wait a few more minutes before you attempt any further configuration. `Error 7000 (http: 500): An error occurred in the API Service. An error occurred in the API service.Cause: error insertVdcInfo. Virtual Data Center creation failure may occur when Data Services has not completed initialization.`

Edit a storage pool

You can change the name of a storage pool or change the set of nodes included in the storage pool.

Before you begin

This operation requires the System Administrator role in ECS.

Procedure



1. In the ECS Portal, select **Manage > Storage Pools**.
2. On the **Storage Pool Management** page, locate the storage pool you want to edit in the table. Click **Edit** in the **Actions** column beside the storage pool you want to edit.
3. On the **Edit Storage Pool** page:
 - To modify the storage pool name, in the **Name** field, type the new name.
 - To modify the nodes included in the storage pool:
 - In the **Selected Nodes** list, remove an existing node in the storage pool by clicking the **-** icon beside the node.
 - In the **Available Nodes** list, add a node to the storage pool by clicking the **+** icon beside the node.
 - To modify the available capacity thresholds that will trigger storage pool capacity alerts, select the applicable alert thresholds in the **Available Capacity Alerting** fields.
4. Click **Save**.

Working with VDCs in the ECS Portal

An ECS virtual data center (VDC) is the top-level resource that represents the collection of ECS infrastructure components to manage as a unit.

You can use the **Virtual Data Center Management** page available from **Manage > Virtual Data Center** to view VDC details, to create a VDC, to edit an existing VDC, to update endpoints in multiple VDCs, delete VDCs, and to federate multiple VDCs for a multisite deployment. The following example shows the **Virtual Data Center Management** page for a federated deployment. It is configured with two VDCs named vdc1 and vdc2.

Table 6 VDC properties

Field	Description
Name	The name of the VDC.
Type	The type of VDC is automatically set and can be either Hosted or On-Premise. <ul style="list-style-type: none"> A Hosted VDC is hosted off-premise by a third-party data center (a backup site).
Replication Endpoints	Endpoints for communication of replication data between VDCs when an ECS federation is configured. <ul style="list-style-type: none"> By default, replication traffic runs between VDCs over the public network. By default the public network IP address for each node is used as the Replication Endpoints. If a separate replication network is configured, the network IP address that is configured for replication traffic of each node is used as the Replication Endpoints. If a load balancer is configured to distribute the load between the replication IP addresses of the nodes, the address that is configured on the load balancer is displayed.
Management Endpoints	Endpoints for communication of management commands between VDCs when an ECS federation is configured. <ul style="list-style-type: none"> By default, management traffic runs between VDCs over the public network. By default the public network IP address for each node is used as the Management Endpoints. If a separate management network is configured, the network IP address that is configured for management traffic of each node is used for the Management Endpoints.
Status	The state of the VDC. <ul style="list-style-type: none"> Online Permanently Failed: The VDC was deleted.
Actions	The actions that can be completed for the VDC. <ul style="list-style-type: none"> Edit: Change the name of a VDC, the VDC access key, and the VDC replication and management endpoints. Delete: Delete the VDC. The delete operation triggers permanent failover of the VDC, You cannot add the VDC again by using the same name. You cannot delete a VDC that is part of a replication group until you first remove it from the replication group. You cannot delete a VDC when you are logged in to the VDC you are trying to delete. Fail this VDC: <ul style="list-style-type: none">  WARNING Failing a VDC is permanent. The site cannot be added back.  Note: Fail this VDC is available when there is more than one VDC. <ul style="list-style-type: none"> Ensure that Geo replication is up-to-date. Stop all writes to the VDC. Ensure that all nodes of the VDC are shutdown. Replication to/from the VDC will be disabled for all replication groups. Recovery is initiated only when the VDC is removed from the replication group. Proceed to do that next. This VDC will display a status of <code>Permanently Failed</code> in any replication group to which it belongs. To Reconstruct this VDC, it must be added as a new site. Any previous data will be lost, as that data will have failed over to other sites in the federation.

Create a VDC for a single site

You can create a VDC for a single-site deployment, or when you create the first VDC in a multi-site federation.

Before you begin

This operation requires the System Administrator role in ECS.

Ensure that one or more storage pools are available and in the `Ready` state.

Procedure

1. In the ECS Portal, select **Manage > Virtual Data Center**.
2. On the **Virtual Data Center Management** page, click **New Virtual Data Center**.
3. On the **New Virtual Data Center** page, in the **Name** field, type the VDC name (for example: `vdc1`).
4. To create an access key for the VDC, either:
 - Type the VDC access key value in the **Key** field, or
 - Click **Generate** to generate a VDC access key.

The VDC Access Key is used as a symmetric key for encrypting replication traffic between VDCs in a multi-site federation.

5. In the **Replication Endpoints** field, type the replication IP address of each node assigned to the VDC. Type them as a comma-separated list.

By default replication traffic runs on the public network. Therefore by default, the IP address configured for the public network on each node is entered here. If the replication network was separated from the public or management network, each node's replication IP address is entered here.

If a load balancer is configured to distribute the load between the replication IP addresses of the nodes, the address configured on the load balancer is displayed.

6. In the **Management Endpoints** field, type the management IP address of each node assigned to the VDC. Type them as a comma-separated list.

By default management traffic runs on the public network. Therefore by default, the IP address configured for the public network on each node is entered here. If the management network was separated from the public or replication network, each node's management IP address is entered here.

7. Click **Save**.

When the VDC is created, ECS automatically sets the VDC's **Type** to either **On-Premise** or **Hosted**.

A **Hosted** VDC is hosted off-premise by a third-party data center (a backup site).

Add a VDC to a federation

You can add a VDC to an existing VDC (for example, `VDC1`) to create a federation. It is important when you perform this procedure that you **DO NOT** create a VDC on the rack you want to add. Retrieve only the VDC Access Key from it, and then proceed from the existing VDC (`VDC1`).

Before you begin

Obtain the ECS Portal credentials for the root user, or for a user with System Administrator credentials, to log in to both VDCs.

In an ECS geo-federated system with multiple VDCs, the IP addresses for the replication and management networks are used for connectivity of replication and management traffic between VDC endpoints. If the VDC you are adding to the federation is configured with:

- Replication or management traffic running on the public network (default), you need the public network IP address that is used by each node.
- Separate networks for replication or management traffic, you need the IP addresses of the separated network for each node.

If a load balancer is configured to distribute the load between the replication IP addresses of the nodes, you need the IP address that is configured on the load balancer.

Ensure that the VDC you are adding has a valid ECS license that is uploaded and has at least one storage pool in the `Ready` state.

Procedure

1. On the VDC you want to add (for example, VDC2):
 - a. Log in to the ECS Portal.
 - b. In the ECS Portal, select **Manage > Virtual Data Center**.
 - c. On the **Virtual Data Center Management** page, click **Get VDC Access Key**.
 - d. Select the key, and press `Ctrl-C` to copy it.

Important: You are only obtaining and copying the key of the VDC you want to add, you are not creating a VDC on the site you are logged in to.
 - e. Log out of the ECS Portal on the site you are adding.
2. On the existing VDC (for example, VDC1):
 - a. Log in to the ECS Portal.
 - b. Select **Manage > Virtual Data Center**.
 - c. On the **Virtual Data Center Management** page, click **New Virtual Data Center**.
 - d. On the **New Virtual Data Center** page, in the **Name** field, type the name of the new VDC you are adding.
 - e. Click in the **Key** field, and then press `Ctrl-V` to paste the access key you copied from the VDC you are adding (from step 1d).
3. In the **Replication Endpoints** field, enter the replication IP address of each node in the storage pools that are assigned to the site you are adding (for example, VDC2). Use the:
 - Public IP addresses for the network if the replication network has not been separated.
 - IP address configured for replication traffic, if you have separated the replication network.
 - If a load balancer is configured to distribute the load between the replication IP addresses of the nodes, the replication endpoint is the IP address that is configured on the load balancer.

Use a comma to separate IP addresses within the text box.
4. In the **Management Endpoints** fields, enter the management IP address of each node in the storage pools that are assigned to the site you are adding (for example, VDC2). Use the:
 - Public IP addresses for the network if the management network has not been separated.
 - IP address configured for management traffic, if you have separated the management network.


Use a comma to separate IP addresses within the text box.

5. Click **Save**.

Results

The new VDC is added to the existing federation. The ECS system is now a geo-federated system. When you add the VDC to the federation, ECS automatically sets the type of the VDC to either **On-Premise** or **Hosted**.

After you finish

 **Note:** If External Key Manager (EKM) feature is activated for the federation, and then you have to add the necessary VDC to EKM mapping for the newly added VDC in the key management section.

To complete the configuration of the geo-federated system, you must create a replication group that spans multiple VDCs so that data can be replicated between the VDCs. To do this, you must ensure that:

- You have created storage pools in the VDCs that will be in the replication group (see [Create a storage pool](#) on page 28).
- You create the replication group, selecting the VDCs that provide the storage pools for the replication group (see [Create a replication group](#) on page 38).
- After you create the replication group, you can monitor the copying of user data and metadata to the new VDC that you added to the replication group on the **Monitor > Geo Replication > Geo Bootstrap Processing** tab. When all the user data and metadata are successfully replicated to the new VDC, the **Bootstrap State** is **Done** and the **Bootstrap Progress (%)** is **100** on all the VDCs.

Edit a VDC

You can change the name, the access key, or the replication and management endpoints of the VDC.

Before you begin

This operation requires the System Administrator role in ECS.

If you have an ECS geo-federated system and you want to update VDC endpoints after you:

- separated the replication or management networks for a VDC, or
- changed the IP addresses of multiple nodes in a VDC

you must use the [update endpoints in multiple VDCs](#) procedure. If you attempt to update the VDC endpoints by editing the settings for an individual VDC from the **Edit Virtual Data Center <VDC name>** page, you will lose connectivity between VDCs.

Procedure

1. In the ECS Portal, select **Manage > Virtual Data Center**.
2. On the **Virtual Data Center Management** page, locate the VDC you want to edit in the table. Click **Edit** in the **Actions** column beside the VDC you want to edit.
3. On the **Edit Virtual Data Center <VDC name>** page:
 - to modify the VDC name, in the **Name** field, type the new name.
 - to modify the VDC access key for the node you are logged into, in the **Key** field, type the new key value, or click **Generate** to generate a new VDC access key.
 - To modify the replication and management endpoints:

Option	Description
for a single VDC that is not part of an ECS federation	<p>a. In the Replication Endpoints field, enter the IP addresses for the replication endpoints. Use the:</p> <ul style="list-style-type: none"> • Public IP addresses for the network, if you did not separate the replication network. • IP address configured for replication traffic, if you separated the replication network. • IP address configured on the load balancer, if you configured a load balancer to distribute the load between the replication IP addresses of the nodes. <p>b. In the Management Endpoints field, enter the IP addresses for the management endpoints. Use the:</p> <ul style="list-style-type: none"> • Public IP addresses for the network, if you did not separate the management network. • IP address configured for management traffic, if you separated the management network. <p>Use a comma to separate IP addresses within the text boxes.</p>
for a VDC that is part of an ECS federation, and for which you have separated the replication or management networks or changed multiple node IP addresses	Do not modify endpoints on the Edit Virtual Data Center <VDC name> page, you must modify the endpoints on the Update All VDC Endpoints page as described in Update replication and management endpoints in multiple VDCs on page 34.

4. Click **Save**.

Update replication and management endpoints in multiple VDCs

In an ECS geo-federated system, you can use the **Update All VDC Endpoints** page to update replication and management endpoints in multiple VDCs.

Before you begin

This operation requires the System Administrator role in ECS.

You must update the VDC endpoints from the **Update All VDC Endpoints** page after you have:

- Separated the replication or management networks of a VDC in an existing ECS federation.
- Changed the IP address of multiple nodes in a VDC.

If you attempt to update the VDC endpoints by editing the settings for an individual VDC from the **Edit Virtual Data Center <VDC name>** page, you will lose connectivity between VDCs.

About this task

In an ECS geo-federated system with multiple VDCs, the IP addresses configured for ECS replication and management networks are used for connectivity of replication and management traffic between VDC endpoints. By default, all of the ECS replication and management traffic is configured to run on the ECS public network, and by default the IP addresses of the public network configured for each node are used as the replication and management endpoints.

Optionally, you can separate the replication and management networks, and therefore must reconfigure the replication and management endpoints for a VDC.

Procedure

1. In the ECS Portal, select **Manage > Virtual Data Center**.
2. On the **Virtual Data Center Management** page, click **Update All VDC Endpoints**.

3. On the **Update All VDC Endpoints** page, if the replication network was separated, or if the IP address for the node was changed, type the replication IP address of each node in the **Replication Endpoints** field for the VDC. Type them as a comma-separated list.
4. On the **Update All VDC Endpoints** page, if the management network was separated, or if the IP address for the node was changed, type the management IP address of each node in the **Management Endpoints** field for the VDC. Type them as a comma-separated list.
5. Click **Update Endpoints**.

Remove VDC from a Replication Group

You can remove a VDC from a replication group (RG) in a multi VDC federation without affecting the VDC or other RGs associated with the VDC. Removing VDC from RG no longer initiates PSO. Removing a VDC from RG initiates recovery.

Before you begin


This operation requires the System Administrator role in ECS.

Restrictions to Remove VDC

- You cannot log in to a VDC and remove the same VDC.
- If any VDC in the replication group is off, you cannot remove a VDC .
- If it is the only VDC in a replication group, you cannot remove a VDC.
- If any VDC in the replication group has Bootstrap or Failover process in progress, you cannot remove a VDC.
- You cannot remove more than one VDC at a time.
- If the system is not fully upgraded, you cannot remove a VDC.

You cannot delete a VDC when it is still associated with any replication groups.

It is a prerequisite to stop any workload to the system and wait until data replication is complete between the VDCs.

 **Note:** The time taken to complete data replication depends on the workload and network condition.

Procedure

1. Log in to the ECS Portal.
2. In the ECS Portal, select **Manage > Virtual Data Center**, check to ensure the VDC you want to remove is online and working correctly.
3. Select **Manage > Replication Group** and click **Edit** for the corresponding replication group. The **Edit Replication Group** window opens.
4. Click **Delete...** for the VDC you want to delete.

Confirm Remove VDC window opens. Read all the important notes before you click the check box to confirm removal of VDC. Click **ok**.
5. Click **Save** in the Replication Group Management Window.
6. Select **Monitoring > Geo Replication > Failover Processing**. The **Failover Progress** column must show 100% done on all remaining VDCs in the replication group.

Refer to [Guidelines to check failover and bootstrap process](#) procedure for details.
7. Select **Monitoring > Geo Replication > Bootstrap Processing**. The **Bootstrap Progress (%)** column must show 100% done on all remaining VDCs in the replication group.

The time that is taken for both the Failover process and the Bootstrap Process to complete depends on the amount of data on the failed VDC.

Refer to [Guidelines to check failover and bootstrap process](#) procedure for details.

After you finish

- Note:** You may have to wait for 5 to 10 minutes before the Failover and the Bootstrap process show the status on the page.

Fail a VDC (PSO)

Failing a VDC or permanent site outage (PSO) is done from the VDC level. Removing a VDC from replication group (RG) initiates recovery, but failed VDC does not initiate recovery.

Before you begin

This operation requires the System Administrator role in ECS.

Stop any workload to the system and wait until data replication is complete between the VDCs.

- Note:** The time taken to complete data replication depends on the workload and network condition.

Wait for more than 15 minutes after you power off the VDC for the system to confirm that the VDC is off. For unplanned PSO, ensure the VDC is not accessible for more than 15 minutes.

Restrictions to fail a VDC

- You cannot fail a VDC that is powered on. If a VDC is powered off for less than 15 minutes, the system does not detect that the VDC is off, which results in Fail VDC operation to fail.
- You cannot fail a VDC if it is the only VDC in a replication group.

Procedure

- Log in to the ECS Portal.
- In the ECS Portal, select **Manage > Virtual Data Center**. Click **Edit** and select **Fail this VDC**. Wait for a few minutes to ensure the VDC status shows **Permanent Site Outage**.
Refer to the restrictions in the prerequisites section for limitations of this operation.
- Select **Manage > Replication Group**, click **Edit** and remove the failed VDC from each replication group.
Refer to the restrictions in the prerequisites section for limitations of this operation.
- Select **Monitoring > Geo Replication > Failover Processing**. The **Failover Progress** column must show 100% done on all remaining VDCs in the replication group.
- Select **Monitoring > Geo Replication > Bootstrap Processing**. The **Bootstrap Progress (%)** column must show 100% done on all remaining VDCs in the replication group.
The time that is taken for both the Failover process and the Bootstrap Process to complete depends on the amount of data on the failed VDC.
Note: You may have to wait for 5 to 10 minutes before the Failover and the Bootstrap process show the status on the page.
- Select **Manage > Virtual Data Center**, click **Edit** and delete the Permanently failed VDC. If the VDC is still associated with any of the replication groups, this operation fails.

Guidelines to check failover and bootstrap process

The following section describes the procedure to check the failover and bootstrap process completion:

Before you begin

This operation requires the System Administrator role in ECS.

Procedure

1. Log in to each of the VDC in the replication group (RG) and check the following:
2. Select **Monitoring > Geo Replication > Failover Processing** and check the failover process column for the VDCs. One more row which shows the failed VDC and the failover process is shown. The **Failover Progress** column shows 100% when the process is complete.
3. Select **Monitoring > Geo Replication > Bootstrap Processing**. Addition rows for each of the remaining VDCs except for the VDC you have logged in is shown. The process is complete when bootstrap process shows 100%.

Example 1 Checking failover and bootstrap process in different cases

2 Site Case (We have vdc1 and vdc2. Vdc2 is removed from the RG).

Failover process: According to the guidelines in the procedure, you see that one other row shows that VDC2 as failed and the failover status from VDC1's UI.

Bootstrap process: According to the guidelines, there are no other remaining zones in the RG except VDC1. So no addition row is shown.

3 Site Case (We have vdc1, vdc2 and vdc3. Vdc3 is removed from the RG)

Failover process: According to the guidelines in the procedure, you see that one other row shows that VDC3 as failed and the failover status from VDC1 and VDC2's UI.

Bootstrap process: According to the guidelines, if you log in to VDC1, VDC2 is the remaining zone. As a result, you can see an extra row showing the bootstrap process of VDC2. Similarly, you can see an extra row showing bootstrap process of VDC1 while you log in to VDC2.

4 Site Case (We have vdc1, vdc2, vdc3 and vdc4. Vdc4 is removed from the RG)

Failover process: According to the guidelines in the procedure, you see that one other row shows that VDC4 as failed and the failover status from VDC1, VDC2, and VDC3's UI.

Bootstrap process:

If you log in to VDC1, then VDC2 and VDC3 are the remaining zone except VDC1. As a result, you see two extra rows showing the bootstrap process of VDC2 and VDC3.

If you log in to VDC2, then VDC1 and VDC3 are the remaining zone except VDC2. As a result, you see two extra rows showing the bootstrap process of VDC1 and VDC3

If you log in to VDC3, then VDC1 and VDC2 are the remaining zone except VDC3. As a result, you see two extra rows showing the bootstrap process of VDC1 and VDC2.

Working with replication groups in the ECS Portal

You can use replication groups to define where storage pool content is protected. Replication groups can be local or global. Local replication groups do not replicate data to other VDCs, but protect objects within the same VDC against disk or node failures using mirroring and erasure coding techniques. Global replication groups protect objects by replicating them to another site within an ECS federation and, by doing so, protect against site failures.

You can use the **Replication Group Management** page to view replication group details, to create replication groups, and to edit existing replication groups. You cannot delete replication groups in this release.


 **Note:** Do not create more than eight replication groups in a cluster. If there is a requirement to have more than eight replication groups in a cluster, contact ECS Remote Support.

Table 7 Replication Group properties

Field	Description
Name	The name of the replication group.
Type	The replication type can be Active or Passive . Passive means that a site is designated as the target for replication data and is only available when there is a minimum of three sites. Passive cannot be selected if Replicate to All Sites is On . If you have a Hosted site, it will automatically be selected as the target for replication in a Passive configuration.
VDC	The number of VDCs in the replication group and the names of the VDCs where the storage pools are located.
Storage Pool	The names of the storage pools and their associated VDCs. A replication group can contain a storage pool from each VDC in a federation.
Target	The storage pool in the replication group that is the replication target in a Passive configuration.
Status	The state of the replication group. <ul style="list-style-type: none"> Online Temp Unavailable: Replication traffic to this VDC has failed. If all replication traffic to the same VDC is in the Temp Unavailable state, further investigation about the cause of the failure is recommended.
Actions	The actions that can be completed for the replication group. Edit: Modify the replication group name and the set of VDCs and storage pools in the replication group.

Create a replication group

Replication groups can be local to a VDC or can protect data by replicating data across sites.

Before you begin

This operation requires the System Administrator role in ECS.

If you want the replication group to span multiple VDCs, you must ensure that the VDCs are federated (joined) to the primary VDC, and that storage pools have been created in the VDCs that will be included in the replication group.

Procedure

1. In the ECS Portal, select **Manage > Replication Group**.
2. On the **Replication Group Management** page, click **New Replication Group**.
3. On the **New Replication Group** page, in the **Name** field, type a name (for example, `ReplicationGroup1`).
4. Optionally, in the **Replicate to All Sites** field, click **On** for this replication group. You can only turn this setting on when you create the replication group; you cannot turn it off later.

For a Passive configuration, leave this setting **Off**.

Option	Description
Replicate to All Sites Off	The replication group uses default replication. With default replication, data is stored at the primary site and a full copy is stored at a secondary site chosen from the sites within the replication group. The secondary copy is protected by triple-mirroring and erasure coding. This process provides data durability with storage efficiency.
Replicate to All Sites On	The replication group makes a full readable copy of all objects to all sites (VDCs) within the replication group. Having full readable copies of objects on all VDCs in the replication group provides data durability and improves local performance at all sites at the cost of storage efficiency.

5. In the **Geo Replication Type** field, click **Active** or **Passive**. Active is the default ECS configuration. You cannot change this setting after you create the replication group.

Passive is available only when you have three or more sites.

Passive cannot be selected if **Replicate to All Sites** is **On**.

For more information on Active and Passive data protection schemes, see [Configurations for availability, durability, and resilience](#) on page 15
6. Click **Add VDC** to add storage pools from VDCs to the replication group.

The steps to add storage pools to a replication group depends on whether you have a single VDC, an Active, or Passive environment.
7. To add storage pools to an Active (or to a single site) configuration, use the steps below.
 - a. From the **Virtual Data Center** list, select the VDC that will provide a storage pool for the replication group.
 - b. From the **Storage Pool** list, select the storage pool that belongs to the selected VDC.
 - c. To include other sites in the replication group, click **Add VDC**.
 - d. Repeat these steps for each storage pool that you want to add to the replication group.
8. To add storage pools for a Passive configuration, complete the following steps.
 - a. In the **Target VDC for Replication Virtual Data Center** list, select the VDC that you want to add as the replication target.

If you have a Hosted VDC that is hosted off-premise by a third-party data center (a backup site), it is automatically selected as the replication target.
 - b. In the **Target VDC for Replication Storage Pool** list, select the storage pool that belongs to the selected VDC.
 - c. In each of the two **Source VDC for Replication Virtual Data Center** lists, select the VDC that you want to add as the active site.
 - d. In each of the two **Source VDC for Replication Storage Pool** lists, select the storage pool that belongs to each selected VDC. These storage pools will provide storage at the two active sites.
9. Click **Save**.

After you finish

After you create the replication group, you can monitor the copying of user data and metadata to the new VDC that you added to the replication group on the **Monitor > Geo Replication > Geo Bootstrap Processing** tab. When all the user data and metadata is successfully replicated to the new VDC, the **Bootstrap State** is **Done** and the **Bootstrap Progress (%)** is **100**.

Edit a replication group

You can change the name of the replication group or change the set of VDCs and storage pools in the replication group.

Before you begin

This operation requires the System Administrator role in ECS.

About this task

CAUTION In a multisite federation, you can edit a replication group (RG) and choose to delete a VDC from one or more replication groups to which it belongs. Removing a VDC from a RG no longer removes the VDC from the federation. It only removes it from the RG and triggers recovery for that RG. In ECS, each object has a primary, or owning VDC. The time that is taken to complete this failover process depends on the amount of data that must be moved. If you created the replication group with the **Replicate to All Sites** setting turned on, the time taken to move all data to the remaining sites is short, as a copy exists at all sites.

You cannot edit the **Replicate to All Sites** or **Geo Replication Type** settings. After you set these options when you first create the replication group, they cannot be changed.

Procedure

1. In the ECS Portal, select **Manage > Replication Group**.
2. On the **Replication Group Management** page, beside the replication group you want to edit, click **Edit**.
3. On the **Edit Replication Group** page,
 - To modify the replication group name, in the **Name** field, type the new name.
 - To add a VDC to the replication group, click **Add VDC** and select the VDC and storage pool from the list.
 - To delete a VDC from the replication group, click the **Delete** button beside the VDC (and its storage pool).

CAUTION

- Deleting a VDC from one or more replication groups to which it belongs means that you are removing this VDC from the replication group and not from the federation.
- VDC removed from a specific Replication group cannot be added back to the same replication group after deletion.
- Ensure that Geo replication is up-to-date. Stop all writes to the VDC.
- Ensure that the nodes are shut down only for failing (PSO) VDC at the federation level.
- Recovery is initiated only when the VDC is removed from the replication group. Proceed to do that next.
- This VDC will display a status of `Permanently Failed` for failed VDC and not for removed VDC.
- In case of failing VDC, to reconstruct this VDC, it must be added as a new site. Any previous data will be lost, as that data will have failed over to other sites in the federation.

4. Click **Save**.

CHAPTER 4

Authentication Providers

- [Introduction to authentication providers](#)..... 42
- [Working with authentication providers in the ECS Portal](#)..... 42

Introduction to authentication providers

You can add authentication providers to ECS if you want users to be authenticated by systems external to ECS.

An authentication provider is a system that is external to ECS that can authenticate users on behalf of ECS. ECS stores the information that allows it to connect to the authentication provider so that ECS can request authentication of a user.

In ECS, the following types of authentication provider are available:

- **Active Directory (AD) authentication or Lightweight Directory Access Protocol (LDAP) authentication:** Used to authenticate domain users that are assigned to management roles in ECS.
- **Keystone:** Used to authenticate OpenStack Swift object users.

Authentication providers can be created from the ECS Portal or by using the ECS Management REST API or CLI.

Working with authentication providers in the ECS Portal

You can use the **Authentication Provider Management** page available from **Manage > Authentication** to view the details of existing authentication providers, to add AD/LDAP or Keystone authentication providers, to edit existing authentication providers, and to delete authentication providers.

Table 8 Authentication provider properties

Field	Description
Name	The name for the authentication provider.
Type	The type of authentication provider. The authentication provider is an Active Directory (AD), Lightweight Directory Access Protocol (LDAP), or Keystone V3 server.
Domains	The domains that the authentication provider provides access to.
Status	Indicates whether the authentication provider is Enabled or Disabled.
Actions	<p>The actions that can be completed for the authentication provider.</p> <ul style="list-style-type: none"> • Edit: Change the AD or LDAP authentication provider settings that are listed in Table 9 on page 43 or change the Keystone authentication provider settings that are listed in Table 10 on page 47. • Delete: Delete the authentication provider. • New Authentication Provider button: Add an authentication provider.

Considerations when adding Active Directory authentication providers

When you configure ECS to work with Active Directory (AD), you must decide whether to add a single AD authentication provider to manage multiple domains, or to add separate AD authentication providers for each domain.

The decision to add a single AD authentication provider, or multiple, depends on the number of domains in the environment, and the location on the tree from which the manager user can search.

Authentication providers have a single search base from which the search begins, and a single manager account that has read access at the search base level and below.

You can add a single authentication provider for multiple domains in the following conditions:

- You manage an AD forest
- The manager account has privileges to search all user entries in the tree
- The search is conducted throughout the whole forest from a single search base, not just the domains listed in the provider

Otherwise, add separate authentication providers for each domain.

Note: If you manage an AD forest and you have the necessary manager account privileges, there are scenarios in which you might still want to add an authentication provider for each domain. For example, if you want tight control on each domain and more granularity on setting the search base starting point for the search.

The search base must be high enough in the directory structure of the forest for the search to correctly find all the users in the targeted domains. The following search examples describe the best options for adding either single or multiple authentication providers:

- In the scenario where the forest in the configuration contains ten domains but you want to target only three, you would not want to add a single authentication provider to manage multiple domains, because the search would unnecessarily span the whole forest. This might adversely affect performance. In this case, you should add three separate authentication providers for each domain.
- In the scenario where the forest in the configuration contains ten domains and you want to target ten domains, adding a single authentication provider to manage multiple domains is a good choice, because there is less overhead to set up.

AD or LDAP authentication provider settings

You must provide authentication provider information when you add or edit an AD or LDAP authentication provider. You can customize LDAP certificate for ECS authentication.

Table 9 AD or LDAP authentication provider settings

Field	Description and requirements
Name	The name of the authentication provider. You can have multiple providers for different domains.
Description	Free text description of the authentication provider.
Type	The type of authentication provider. Active Directory or LDAP.
Domains	<p>The collection of administratively defined objects that share a common directory database, security policies, and trust relationships. A domain can span multiple physical locations or sites and can contain millions of objects.</p> <p>Example: <code>mycompany.com</code></p> <p>If an alternate UPN suffix is configured in the Active Directory, the Domains field should also contain the alternate UPN configured for the domain. For example, if <code>myco</code> is added as an alternate UPN suffix for <code>mycompany.com</code>, then the Domains field should contain both <code>myco</code> and <code>mycompany.com</code>.</p>
Server URLs	<p>The LDAP or LDAPS (secure LDAP) with the domain controller IP address. The default port for LDAP is 389. The default port for LDAPS is 636.</p> <p>You can specify one or more LDAP or LDAPS authentication provider.</p>


Table 9 AD or LDAP authentication provider settings (continued)

Field	Description and requirements
	<p>Example: <code>ldap://<Domain controller IP>:<port></code> (if not default port) or <code>ldaps://<Domain controller IP>:<port></code>(if not default port)</p> <p>If the authentication provider supports a multidomain forest, use the global catalog server IP and always specify the port number. The default port for LDAP is 3268. The default port for LDAPS is 3269.</p> <p>Example: <code>ldap(s)://<Global catalog server IP>:<port></code></p>
Manager DN	<p>The Active Directory Bind user account that ECS uses to connect to the Active Directory or LDAP server. This account is used to search Active Directory when an ECS administrator specifies a user for role assignment.</p> <p>This user account must have <code>Read all inetOrgPerson</code> information in Active Directory. The <code>InetOrgPerson</code> object class is used in several non-Microsoft, LDAP and X.500 directory services to represent people in an organization.</p> <p>To set this privilege in Active Directory:</p> <ol style="list-style-type: none"> 1. Open Active Directory Users and Computers. 2. Right-click the domain, select Delegate Control, and then click Next. 3. In the Delegation of Control wizard, click Next, and then click Add. 4. In the Select Users, Computers, or Groups dialog box, select the user that you are using for <code>managerdn</code>, and then click Next. 5. In the Tasks to Delegate page, in Delegate the following common tasks, check the <code>Read all inetOrgPerson</code> information task, and then click Next. 6. Click Finish. <p>In this example: <code>CN=Manager,CN=Users,DC=mydomaincontroller,DC=com</code>, the Active Directory Bind user is <code>Manager</code>, in the <code>Users</code> tree of the <code>mydomaincontroller.com</code> domain. Usually <code>managerdn</code> is a user who has fewer privileges than Administrator, but has sufficient privileges to query Active Directory for users attributes and group information.</p> <p>Important: You must update this user account in ECS if the <code>managerdn</code> credentials change in Active Directory.</p>
Manager Password	<p>The password of the <code>managerdn</code> user.</p> <p>Important: You must update this password in ECS if the <code>managerdn</code> credentials change in Active Directory.</p>
Providers	<p>This setting is Enabled by default when adding an authentication provider. ECS validates the connectivity of the enabled authentication provider and that the name and domain of the enabled authentication provider are unique.</p> <p>Select Disabled only if you want to add the authentication provider to ECS, but you do not immediately want to use it for authentication. ECS does not validate the connectivity of a disabled authentication provider, but it does validate that the authentication provider name and domain are unique.</p>
Group Attribute	<p>This attribute applies only to Active Directory; it does not apply to other types of authentication providers.</p> <p>The AD attribute that is used to identify a group. Used for searching the directory by groups.</p> <p>Example: <code>CN</code></p>

Table 9 AD or LDAP authentication provider settings (continued)

Field	Description and requirements
	<p>Note: After you set this attribute for an AD authentication provider, you cannot change it, because the tenants using this provider might already have role assignments and permissions configured with group names in a format that uses this attribute.</p>
Group Whitelist	<p>This setting applies only to Active Directory; it does not apply to other types of authentication providers.</p> <p>Optional. One or more group names as defined by the authentication provider. This setting filters the group membership information that ECS retrieves about a user.</p> <ul style="list-style-type: none"> When a group or groups are included in the whitelist, ECS is aware only of a user's membership in the specified groups. Multiple values (one value on each line in the ECS Portal, and values comma-separated in CLI and API) and wildcards (for example <code>MyGroup*</code>, <code>TopAdminUsers*</code>) are allowed. The default setting is blank. ECS is aware of all groups that a user belongs to. Asterisk (*) is the same as blank. <p>Example: UserA belongs to <code>Group1</code> and <code>Group2</code>.</p> <p>If the whitelist is blank, ECS knows that UserA is a member of <code>Group1</code> and <code>Group2</code>.</p> <p>If the whitelist is <code>Group1</code>, ECS knows that UserA is a member of <code>Group1</code>, but does not know that UserA is a member of <code>Group2</code> (or of any other group).</p> <p>Use care when adding a whitelist value. For example, if you map a user to a namespace that is based on group membership, then ECS must be aware of the user's membership in the group.</p> <p>To restrict access to a namespace to only users of certain groups, complete the following tasks.</p> <ul style="list-style-type: none"> Add the groups to the namespace user mapping. The namespace is configured to accept only users of these groups. Add the groups to the whitelist. ECS is authorized to receive information about them. <p>By default, if no groups are added to the namespace user mapping, users from any groups are accepted, regardless of the whitelist configuration.</p>
Search Scope	<p>The levels to search. Possible values are:</p> <ul style="list-style-type: none"> One Level (search for users one level under the search base) Subtree (search the entire subtree under the search base)
Search Base	<p>The Base Distinguished Name that ECS uses to search for users or AD groups at login time and when assigning roles or setting ACLs.</p> <p>The following example searches for all users in the <code>Users</code> container.</p> <pre>CN=Users,DC=mydomaincontroller,DC=com</pre> <p>The following example searches for all users in the <code>Users</code> container in the <code>myGroup</code> organization unit. Note that the structure of the search base value begins with the leaf level and goes up to the domain controller level, which is the reverse of the structure seen in the Active Directory Users and Computers snap-in.</p> <pre>CN=Users,OU=myGroup,DC=mydomaincontroller,DC=com</pre>
Search Filter	<p>The string used to select subsets of users.</p>

Table 9 AD or LDAP authentication provider settings (continued)

Field	Description and requirements
	<p>Example: <code>userPrincipalName=%u</code></p> <p> Note: ECS does not validate this value when you add the authentication provider.</p> <p>If an alternate UPN suffix is configured in the Active Directory, the Search Filter value must be of the format <code>sAMAccountName=%U</code> where <code>%U</code> is the username, and does not contain the domain name.</p>

Add an AD or LDAP authentication provider

You can add one or more authentication providers to ECS to perform user authentication for ECS domain users.

Before you begin

- This operation requires the System Administrator role in ECS.
- You need access to the authentication provider information listed in [AD/LDAP authentication provider settings](#). Note especially the requirements for the Manager DN user.

Procedure

1. In the ECS Portal, select **Manage > Authentication**.
2. On the **Authentication Provider Management** page, click **New Authentication Provider**.
3. On the **New Authentication Provider** page, type values in the fields. For more information about these fields, see [AD/LDAP authentication provider settings](#).
4. Click **Save**.
5. To verify the configuration, add a user from the authentication provider at **Manage > Users > Management Users**, and then try to log in as the new user.

After you finish

If you want these users to perform ECS object user operations, add (assign) the domain users into a namespace. For more information, see [Add domain users into a namespace](#) on page 72.

Add a Keystone authentication provider

You can add a Keystone authentication provider to authenticate OpenStack Swift users.

Before you begin

- This operation requires the System Administrator role in ECS.
- You can add only one Keystone authentication provider.
- Obtain the authentication provider information listed in [Keystone authentication provider settings](#).

Procedure

1. In the ECS Portal, select **Manage > Authentication**.
2. On the **Authentication Provider Management** page, click **New Authentication Provider**.
3. On the **New Authentication Provider** page, in the **Type** field, select **Keystone V3**.

The required fields are displayed.

4. Type values in the **Name**, **Description**, **Server URL**, **Keystone Administrator**, and **Admin Password** fields. For more information about these fields, see [Keystone authentication provider settings](#).
5. Click **Save**.

Keystone authentication provider settings

You must provide authentication provider information when you add or edit a Keystone authentication provider.

The table lists the Keystone authentication provider settings

Table 10 Keystone authentication provider settings

Field	Description
Name	The name of the Keystone authentication provider. This name is used to identify the provider in ECS.
Description	Free text description of the authentication provider.
Type	Keystone V3.
Server URL	URI of the Keystone system that ECS connects to in order to validate Swift users.
Keystone Administrator	Username for an administrator of the Keystone system. ECS connects to the Keystone system using this username.
Admin Password	Password of the specified Keystone administrator.

CHAPTER 5

Namespaces

- [Introduction to namespaces](#)..... 50
- [Working with namespaces in the ECS Portal](#)..... 51

Introduction to namespaces

You can use namespaces to provide multiple tenants with access to the ECS object store and to ensure that the objects and buckets written by users of each tenant are segregated from the other tenants.

ECS supports access by multiple tenants, where each tenant is defined by a namespace and the namespace has a set of configured users who can store and access objects within the namespace. Users from one namespace cannot access the objects that belong to another namespace.

Namespaces are global resources in ECS. A System Administrator or Namespace Administrator can access ECS from any federated VDC and can configure the namespace settings. The object users that you assign to a namespace are global and can access the object store from any federated VDC.

You configure a namespace with settings that define which users can access the namespace and what characteristics the namespace has. Users with the appropriate privileges can create buckets, and can create objects within buckets, in the namespace.

You can use buckets to create subtenants. The bucket owner is the subtenant administrator and can assign users to the subtenant by using access control lists (ACLs). However, subtenants do not provide the same level of segregation as tenants. Any user assigned to the tenant could be assigned privileges on a subtenant, so care must be taken when assigning users.

An object in one namespace can have the same name as an object in another namespace. ECS can identify objects by the namespace qualifier.

You can configure namespaces to monitor and meter their usage, and you can grant management rights to the tenant so that it can perform configuration, monitoring, and metering operations.

The namespace configuration tasks that you can perform in the ECS Portal can also be performed using the ECS Management REST API.

Namespace tenancy

A System Administrator can set up namespaces in the following tenant scenarios:

Enterprise single tenant

All users access buckets and objects in the same namespace. Buckets can be created for subtenants, to allow a subset of namespace users to access the same set of objects. For example, a subtenant might be a department within the organization.

Enterprise multitenant

Departments within an organization are assigned to different namespaces and department users are assigned to each namespace.

Cloud Service Provider single tenant

A single namespace is configured and the Service Provider provides access to the object store for users within the organization or outside the organization.

Cloud Service Provider multitenant

The Service Provider assigns namespaces to different companies and assigns an administrator for the namespace. The Namespace Administrator for the tenant can then add users and can monitor and meter the use of buckets and objects.

Working with namespaces in the ECS Portal

You can use the **Namespace Management** page available from **Manage > Namespace** to view the details of existing namespaces, to create new namespaces, to edit existing namespaces, and to delete namespaces.

Table 11 Namespace properties

Field	Description
Name	The name of the namespace.
Default Replication Group	The default replication group for the namespace.
Notification Quota	The quota limit at which notification is generated.
Max Quota	The quota limit at which writes to the namespace are blocked.
Encryption	Specifies if D@RE server-side encryption is enabled for the namespace.
Actions	<p>The actions that can be completed for the namespace.</p> <ul style="list-style-type: none"> Edit: Change the namespace name, the Namespace Administrator, the default replication group, namespace quota, bucket quota, server-side encryption, access during outage, and compliance settings for the namespace. Delete: Delete the namespace.

Namespace settings

The following table describes the settings that you can specify when you create or edit an ECS namespace.

How namespace and bucket names are used when addressing objects in ECS is described in [Object base URL](#) on page 140.

Table 12 Namespace settings

Field	Description	Can be edited
Name	The name of the namespace, in lowercase characters.	No
Namespace Admin	The user ID of one or more users who are assigned to the Namespace Administrator role; a list of users is comma that is separated. Namespace Administrators can be local or domain users. If the Namespace Administrator is a domain user, ensure that an authentication provider is added to ECS. See Introduction to users and roles on page 60 for details.	Yes
Domain Group Admin	The domain group that is assigned to the Namespace Administrator role. Any member, when authenticated, is assigned the Namespace Administrator role for the namespace. The domain group must be assigned to the namespace by setting the Domain User Mappings for the namespace. To use this feature, you must ensure that an authentication provider is added to ECS. See Introduction to users and roles on page 60 for details.	Yes
Replication Group	The default replication group for the namespace.	Yes

Table 12 Namespace settings (continued)

Field	Description	Can be edited
Namespace Quota	<p>The storage space limit that is specified for the namespace. You can specify a storage limit for the namespace and define notification and access behavior when the quota is reached. The quota setting for a namespace cannot be less than 1 GiB. You can specify namespace quota settings in increments of GiB. You can select one of the following quota behavior options:</p> <ul style="list-style-type: none"> • Notification Only at <quota_limit_in_GiB> Soft quota setting at which you are notified. • Block Access Only at <quota_limit_in_GiB> Hard quota setting which, when reached, prevents write/update access to buckets in the namespace. • Block Access at <quota_limit_in_GiB> and Send Notification at <quota_limit_in_GiB> Hard quota setting which, when reached, prevents write/update access to the buckets in the namespace and the quota setting at which you are notified. 	Yes
Default Bucket Quota	<p>The default storage limit that is specified for buckets that are created in this namespace. This is a hard quota which, when reached, prevents write/update access to the bucket. Changing the default bucket quota does not change the bucket quota for buckets that are already created.</p>	Yes
Server-side Encryption	<p>The default value for server-side encryption for buckets created in this namespace.</p> <ul style="list-style-type: none"> • Server-side encryption, also known as Data At Rest Encryption or D@RE, encrypts data inline before storing it on ECS disks or drives. This encryption helps prevent sensitive data from being acquired from discarded or stolen media. • If you turn this setting on for the namespace, and then all its buckets are encrypted and this setting cannot be changed when a bucket is created. If you want the buckets in the namespace to be unencrypted, and then you must leave this setting off. If you leave this setting off for the namespace, individual buckets can be set as encrypted when created. • For a complete description of the feature, see the <i>ECS Security Configuration Guide</i>, available from the ECS Product Documentation page. 	No
Access During Outage	<p>The default behavior when accessing data in the buckets created in this namespace during a temporary site outage in a geo-federated setup.</p> <ul style="list-style-type: none"> • If you turn this setting on for the namespace and a temporary site outage occurs, if you cannot access a bucket at the failed site where the bucket was created (owner site), you can access a copy of the bucket at another site. Objects that you access in the buckets in the namespace might have been updated at the failed site, but changes might not have been propagated to the site from which you are accessing the object. • If you leave this setting off for the namespace, data in the site which has the temporary outage is not available for access from other sites, and object reads for data that is owned by the failed site will fail. 	Yes

Table 12 Namespace settings (continued)

Field	Description	Can be edited
	<ul style="list-style-type: none"> For more information, see TSO behavior with the ADO bucket setting turned on on page 176. 	
Compliance	<ul style="list-style-type: none"> The rules that limit changes that can be made to retention settings on objects under retention. ECS has object retention features enabled or defined at the object level, bucket level, and namespace level. Compliance strengthens these features by limiting changes that can be made to retention settings on objects under retention. You can turn this setting on only at the time the namespace is created; you cannot change it after the namespace is created. Compliance is supported by S3 and CAS systems. For details about the rules enforced by compliance, see the <i>ECS Data Access Guide</i>, available from the ECS Product Documentation page. 	No
Retention Policies	<p>Enables one or more retention policies to be added and configured.</p> <ul style="list-style-type: none"> A namespace can have one or more associated retention policies, where each policy defines a retention period. When you apply a retention policy to several objects, rather than to an individual object, a change to the retention policy changes the retention period for all the objects to which the policy is applied. A request to modify an object before the expiration of the retention period is disallowed. In addition to specifying a retention policy for several objects, you can specify retention policies and a quota for the entire namespace. For more information about retention, see Retention periods and policies on page 53. 	Yes
Domain	<p>Enables Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domains to be specified and the rules for including users from the domain to be configured.</p> <ul style="list-style-type: none"> Domain users can be assigned to ECS management roles and can use the ECS self-service capability to register as object users. The mapping of domain users into a namespace is described in Domain users require an assigned namespace to perform object user operations on page 62. 	Yes

You can set the following attribute using the ECS Management REST API, but not from the ECS Portal.

Allowed (and Disallowed) Replication Groups

Enables a client to specify the replication groups that the namespace can use.

Retention periods and policies

ECS provides the ability to prevent data from being modified or deleted within a specified retention period.

You can specify retention by using retention periods and retention policies that are defined in the metadata that is associated with objects and buckets. The retention periods and retention policies

are checked each time a request to modify an object is made. Retention periods are supported on all ECS object protocols (S3, Swift, Atmos, and CAS).

Note: For detailed information about setting retention on object interfaces, including CAS retention and CAS advanced retention, see the *ECS Data Access Guide*, available from the [ECS Product Documentation page](#).

Retention Periods

You can assign retention periods at the object level or the bucket level. Each time a user requests to modify or delete an object, an expiration time is calculated. The object expiration time equals the object creation time plus the retention period. When you assign a retention period for a bucket, the object expiration time is calculated based on the retention period set on the object and the retention period set on the bucket, whichever is the longest.

When you apply a retention period to a bucket, the retention period for all objects in a bucket can be changed at any time, and can override the value written to the object by an object client by setting it to a longer period.

You can specify that an object is retained indefinitely.

Auto-Commit Period

Auto-commit period is the time interval in which the updates through NFS are allowed for objects under retention. This attribute enables NFS files that are written to ECS to be WORM compliant. The interval is calculated from the last modification time.

The auto-commit value must be less than or equal to the retention value with a maximum of 1 day. A value of 0 indicates no auto-commit period.

Retention Policies

Retention policies are associated with a namespace. Any policy that is associated with the namespace can be assigned to an object belonging to the namespace. A retention policy has an associated retention period.

When you change the retention period that is associated with a policy, the retention period automatically changes for objects that have that policy that is assigned.

You can apply a retention policy to an object. When a user attempts to modify or delete an object, the retention policy is retrieved. The retention period in the retention policy is used with object retention period and bucket retention period to verify whether the request is allowed.

For example, you could define a retention policy for each of the following document types, and each policy could have an appropriate retention period. When a user requests to modify or delete the legal document four years after it was created, the larger of the bucket retention period or the object retention period is used to verify whether the operation can be performed. In this case, the request is not allowed, and the document cannot be modified or deleted for one more year.

- Email - six months
- Financial - three years
- Legal - five years

ECS Management REST API retention policy methods

The retention policy creation and configuration tasks that can be performed in the ECS Portal can also be performed using the ECS Management REST API. The following table describes the ECS Management REST API methods that relate to retention policies:

ECS Management REST API method	Description
PUT /object/bucket/{ <i>bucketName</i> }/retention	The retention value for a bucket that defines a mandatory retention period which is applied to every object within a bucket. If the retention value is one year, an object from the bucket cannot be modified or deleted for one year.
GET /object/bucket/{ <i>bucketName</i> }/retention	Returns the retention period that is set for a specified bucket.
POST /object/namespaces/namespace/{ <i>namespace</i> }/retention	The retention setting for namespaces that acts like a policy, where each policy is a < <i>name</i> >: < <i>retention period</i> > pair. You can define several retention policies for a namespace and you can assign a policy, by name, to an object within the namespace. This allows you to change the retention period for a set of objects that have the same policy assigned, by changing the corresponding policy.
PUT /object/namespaces/namespace/{ <i>namespace</i> }/retention/{ <i>class</i> }	Updates the period for a retention class that is associated with a namespace.
GET /object/namespaces/namespace/{ <i>namespace</i> }/retention	Returns the retention classes that are defined for a namespace.

For information about how to access the ECS Management REST API, see the *ECS Data Access Guide*, available from the [ECS Product Documentation page](#).

Create a namespace

You can create a namespace.

Before you begin

- This operation requires the System Administrator role in ECS.
- A replication group must exist. The replication group provides access to storage pools in which object data is stored.
- If you want to enable domain users to access the namespace, an authentication provider must be added to ECS. To configure domain object users or a domain group, you must plan how you want to map users into the namespace. For more information about mapping users, see [Domain users require an assigned namespace to perform object user operations](#) on page 62.

About this task

For more information about namespaces, see [Namespace settings](#) on page 51.

Procedure

1. In the ECS Portal, select **Manage > Namespace**.
2. On the **Namespace Management** page, click **New Namespace**.
3. On the **New Namespace** page, in the **Name** field, type the name of the namespace.
The name cannot be changed once created.
4. In the **Namespace Admin** field, specify the user ID of one or more domain or local users to whom you want to assign the Namespace Administrator role.
You can add multiple users or groups as comma-separated lists.
5. In the **Domain Group Admin** field, you can also add one or more domain groups to whom you want to assign the Namespace Administrator role.
6. In the **Replication Group** field, select the default replication group for this namespace.

7. In the **Namespace Quota** field, click **On** to specify a storage space limit for this namespace. If you enable a namespace quota, select one of the following quota behavior options:
 - a. **Notification Only at <quota_limit_in_GiB>**
 Select this option if you want to be notified when the namespace quota setting is reached.
 - b. **Block Access Only at <quota_limit_in_GiB>**
 Select this option if you want write/update access to the buckets in this namespace that is blocked when the quota is reached.
 - c. **Block Access at <quota_limit_in_GiB> and Send Notification at <quota_limit_in_GiB>**
 Select this option if you want write/update access to the buckets in this namespace that is blocked when the quota is reached and you want to be notified when the quota reaches a specified storage limit.
8. In the **Default Bucket Quota** field, click **On** to specify a default storage space limit that is automatically set on all buckets that are created in this namespace.
9. In the **Server-side Encryption** field, click **On** to enable server-side encryption on all buckets that are created in the namespace and to encrypt all objects in the buckets. If you leave this setting **Off**, you can apply server-side encryption to individual buckets in the namespace at the time of creation.
10. In the **Access During Outage** field, click **On** or **Off** to specify the default behavior when accessing data in the buckets created in this namespace during a temporary site outage in a geo-federated setup.

 If you turn this setting on, if a temporary site outage occurs in a geo-federated system and you cannot access a bucket at the failed site where it was created (owner site), you can access a copy of the bucket at another site.

 If you leave this setting off, data in the site which has the temporary outage is not available for access from other sites, and object reads for data that is owned by the failed site will fail.
11. In the **Compliance** field, click **On** to enable compliance features for objects in this namespace.

 Once you turn this setting on, you cannot turn it off.

 You can only turn this setting on during namespace creation.

 Once you turn this setting on, you can add a retention policy by completing the following steps:
 - a. In the **Retention Policies** area, in the **Name** field, type the name of the policy.
 - b. In the **Value** fields, select a numerical value and then select the unit of measure (seconds, minutes, hours, days, months, years, infinite) to set the retention period for this retention policy.

 Instead of specifying a specific retention period, you can select **Infinite** as a unit of measure to ensure that buckets that are assigned to this retention policy are never deleted.
 - c. Click **Add** to add the new policy.
12. To specify an Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) domain that contains the users who can log in to ECS and perform administration tasks for the namespace, click **Domain**.

- a. In the **Domain** field, type the name of the domain.
- b. Specify the groups and attributes for the domain users that are allowed to access ECS in this namespace by typing the values in the **Groups**, **Attribute**, and **Values** fields.

For information about how to perform complex mappings using groups and attributes, see [Domain users require an assigned namespace to perform object user operations](#) on page 62.

13. Click **Save**.

Edit a namespace

You can change the configuration of an existing namespace.

Before you begin

This operation requires the System Administrator role in ECS.

The Namespace Administrator role can modify the AD or LDAP domain that contains the users in the namespace that are object users or management users that can be assigned the Namespace Administrator role for the namespace.

About this task

You cannot edit the **Name**, **Server-side Encryption**, or **Compliance** fields after the namespace has been created.

Procedure

1. In the ECS Portal, select **Manage > Namespace**.
2. On the **Namespace Management** page, locate the namespace that you want to edit in the table. Click **Edit** in the **Actions** column beside the namespace you want to edit.
3. On the **Edit Namespace** page:
 - To modify the domain or local users to whom you want to assign the Namespace Administrator role, in the **Namespace Admin** or **Domain Group Admin** fields, change the user IDs.
 - To modify the default replication group for this namespace, in the **Replication Group** field, select a different replication group.
 - To modify which of the following settings are enabled, click the appropriate **On** or **Off** options.
 - **Namespace Quota**
 - **Default Bucket Quota**
 - **Access During Outage**
4. To modify an existing retention policy, in the **Retention Policies** area:
 - a. Click **Edit** in the **Actions** column beside the retention policy you want to edit.
 - b. To modify the policy name, in the **Name** field, type the new retention policy name.
 - c. To modify the retention period, in the **Value** field, type the new retention period for this retention policy.
5. To modify the AD or LDAP domain that contains the object users in the namespace and management users that can be assigned the Namespace Administrator role for the namespace, click **Domain**.
 - a. To modify the domain name, in the **Domain** field, type the new domain name.

- b. To modify the groups and attributes for the domain users that are allowed to access ECS in this namespace, type the new values in the **Groups**, **Attribute**, and **Values** fields.
6. Click **Save**.

Delete a namespace

You can delete a namespace, but you must delete the buckets in the namespace first.

Before you begin

This operation requires the System Administrator role in ECS.

Procedure

1. In the ECS Portal, select **Manage > Namespace**.
2. On the **Namespace Management** page, locate the namespace that you want to delete in the table. Click **Delete** in the **Actions** column beside the namespace you want to delete.

An alert displays informing you of the number of buckets in the namespace and instructs you to delete the buckets in the namespace before removing the namespace. Click **OK**.
3. Delete the buckets in the namespace.
 - a. Select **Manage > Buckets**.
 - b. On the **Bucket Management** page, locate the bucket that you want to delete in the table. Click **Delete** in the **Actions** column beside the bucket you want to delete.
 - c. Repeat step 4b. for all the buckets in the namespace.
4. On the **Namespace Management** page, locate the namespace that you want to delete in the table. Click **Delete** in the **Actions** column beside the namespace you want to delete.

Since there are no longer any buckets in this namespace, a message displays to confirm that you want to delete this namespace. Click **OK**.
5. Click **Save**.

CHAPTER 6

Users and Roles

- [Introduction to users and roles](#)..... 60
- [Users in ECS](#)..... 60
- [Management roles in ECS](#)..... 64
- [Working with users in the ECS Portal](#)..... 68

Introduction to users and roles

In ECS you can configure users and roles to control access to the ECS management tasks and to the object store. Management users can perform administration tasks in the ECS Portal. Object users cannot access the ECS Portal but can access the object store using clients that support the ECS data access protocols.

Roles in ECS determine the operations that a management user can perform in the ECS Portal or by using the ECS Management REST API.

Management users and object users are stored in different tables and their credentials are different. Management users require a local username and password, or a link to a domain user account. Object users require a username and a secret key. You can create a management user and an object user with the same name, but they are effectively different users as their credentials are different.

Management user and object user names can be unique across the ECS system or can be unique within a namespace, which is referred to as user scope.

Domain and local users can be assigned as management users or object users. Local user credentials are stored by ECS. Domain users are users defined in an Active Directory AD/LDAP database and ECS must talk to the AD or LDAP server to authenticate user login request.

Users in ECS

ECS requires two types of user: management users, who can perform administration of ECS, and object users, who access the object store to read and write objects and buckets.

Management users

Management users can perform the configuration and administration of the ECS system and of namespaces (tenants) configured in ECS.

The roles that can be assigned to management users are System Administrator, System Monitor, Namespace Administrator, and Lock Administrator as described in [Management roles in ECS](#) on page 64.

Management users can be local users or domain users. Management users that are local users are authenticated by ECS against the locally held credentials. Management users that are domain users are authenticated in Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) systems. For more information about domain and local users, see [Domain and local users](#) on page 62.

Management users are not replicated across geo-federated VDCs.

Default management users

On installation, ECS creates two default local management users, root and emcsecurity, to enable for the initial and ongoing configuration of ECS. The root and emcsecurity management users can access the ECS system by using the ECS Portal or the ECS Management REST API. These default users cannot be removed from the ECS system and they are not replicated across sites in a geo-federation. The following table describes the default management users:

Table 13 Default management users

Default user	Default password	User description	Role assigned to user	Role permissions	Can more users be created?
root	ChangeMe	This user performs the initial configuration of the ECS system, and creates users with System Administrator roles. The first time the root user accesses ECS, the user is prompted to change the password and immediately log in again with the new password. From an audit perspective, it is important to know which user carried out changes to the system, so the root user should not be used after system initialization. After system initialization, each System Administrator user should log in to the system using their own credentials, not the root user credentials.	System Administrator	<ul style="list-style-type: none"> • Create and delete management and object users • Change user passwords • Grant permissions to object users • Create, delete, modify storage pools, namespaces, buckets, and replication groups • View monitoring metrics 	Yes
emcsecurity	ChangeMe	This user can prevent remote SSH access to nodes by locking them. The password for this user should be changed after system installation and securely recorded.	Lock Administrator	<ul style="list-style-type: none"> • Lock and unlock nodes • Change its own password 	No

Object users

Object users are users of the ECS object store. They access ECS through object clients that are using the object protocols that ECS supports (S3, EMC Atmos, OpenStack Swift, and CAS). Object users can be assigned Unix-style permissions to access buckets exported as file systems for HDFS.

A management user (System or Namespace Administrator) can create an object user. The management user defines a username and assigns a secret key to the object user when the user is created or at any time thereafter. A username can be a local name or a domain-style username that includes @ in the name. The object user uses the secret key to access the ECS object store. The secret key of object user is distributed by email or other means.

Users that are added to ECS as domain users can later add themselves as object users by creating their own secret key using the ECS self-service capability through a client that communicates with the ECS Management REST API. The object username that they are given is the same as their domain name. Object users do not have access to the ECS Portal. For more information about domain users, see the [Domain and local users](#) on page 62. For information about creating a secret key, see the *ECS Data Access Guide*, available from the [ECS Product Documentation page](#).

Object users are global resources. An object user can have privileges to read and write buckets, and objects within the namespace to which they are assigned, from any VDC.

Domain and local users

ECS supports for local user and domain users. Local and domain users can be assigned as management users or object users.

The ECS self-service capability authenticates domain users and enables domain users to create a secret key for themselves. When a domain user creates their own secret key, they become an object user in the ECS system. You can use AD and LDAP to give many users from an existing user database access to the ECS object store (as object users). Without creating each user individually.

Note: Domain users that are object users must be added (mapped) into a namespace. For more information, see [Add domain users into a namespace](#) on page 72

ECS stores credentials of local users. The credentials for object users are global resources and are available from all VDCs in ECS.

Domain users are defined in an Active Directory AD or LDAP database. Domain usernames are defined by using the `user@domain.com` format. Usernames without `@` are authenticated against the local user database. ECS uses an authentication provider to supply the credentials to communicate with the AD or LDAP server to authenticate a domain user login request. Domain users assigned to management roles can be authenticated against their AD or LDAP credentials to enable them to access ECS and perform ECS administration operations.

Domain users require an assigned namespace to perform object user operations

You must add (assign) domain users into a namespace if you want these users to perform ECS object user operations. To access the ECS object store, object users and Namespace Administrators must be assigned to a namespace. You can add an entire domain of users into a namespace, or you can add a subset of the domain users into a namespace by specifying a particular group or attribute associated with the domain.

A domain can provide users for multiple namespaces. For example, you might decide to add a set of users such as the Accounts department in the `yourco.com` domain into Namespace1, and a set of users such as the Finance department in the `yourco.com` domain into Namespace2. In this case, the `yourco.com` domain is providing users for two namespaces.

An entire domain, a particular set of users, or a particular user cannot be added into more than one namespace. For example, the `yourco.com` domain can be added into Namespace1, but the domain cannot also be added into Namespace2.

The following example shows that a System or Namespace Administrator has added into a namespace a subset of users in the `yourco.com` domain; the users that have their Department attribute = Accounts in Active Directory. The System or Namespace Administrator has added the users in the Accounts department from this domain into a namespace by using the **Edit Namespace** page in the ECS Portal.

Figure 6 Adding a subset of domain users into a namespace using one AD attribute

Domain *	Groups	Attribute *	Values *
yourco.com X	Comma separated groups	department X	Accounts

ATTRIBUTE

DOMAIN

The following example shows a different example where the System or Namespace Administrator is using more granularity in adding users into a namespace. In this case, the System or Namespace

Administrator has added the members in the `yourco.com` domain who belong to the Storage Admins group with the Department attribute = Accounts AND Region attribute = Pacific, OR belong to the Storage Admins group with the Department attribute = Finance.

Figure 7 Adding a subset of domain users into a namespace using multiple AD attributes

For more information about adding domain users into namespaces using the ECS Portal, see [Add domain users into a namespace](#) on page 72.

User scope

The user scope setting affects all object users, in all namespaces across all federated VDCs.

The user scope can be `GLOBAL` or `NAMESPACE`. If the scope is set to `GLOBAL`, object user names are unique across all VDCs in the ECS system. If the scope is set to `NAMESPACE`, object user names are unique within a namespace, so the same object user names can exist in different namespaces.

The default setting is `GLOBAL`. If you intend to use ECS in a multitenant configuration and you want to ensure that namespaces can use names that are in use in another namespace, you must change this setting to `NAMESPACE`.

Note: Set the user scope before you create the first object user.

Set the user scope

You can set the user scope using the ECS Management REST API.

Before you begin

This operation requires the System Administrator role in ECS.

If you are going to change the default user scope setting from `GLOBAL` to `NAMESPACE`, you must do so before you create the first object user in ECS.

About this task

The user scope setting affects all object users in ECS.

Procedure

1. In the ECS Management REST API, use the `PUT /config/object/properties` API call and pass the user scope in the payload.

The following example shows a payload that sets the `user_scope` to `NAMESPACE`.

```
PUT /config/object/properties/
<property_update>
  <properties>
    <properties>
      <entry>
        <key>user_scope</key>
        <value>NAMESPACE</value>
      </entry>
    </properties>
  </property_update>
```

User tags

A tag in the form of name=value pairs can be associated with the user ID for an object user, and retrieved by an application. For example, an object user can be associated with a project or cost-center. Tags cannot be associated with management users.

This functionality is not available from the ECS Portal. Tags can be set on an object user, and the tags that are associated with the object user can be retrieved by using the ECS Management REST API. You can add a maximum of 20 tags.

Management roles in ECS

ECS defines roles to determine the operations that a user can perform in the ECS Portal or when accessing ECS using the ECS Management REST API. Management users and groups can be assigned to administration roles in ECS and can be either local users or domain users. Roles can also be assigned to Active Directory group names.

The following list provides the four possible management roles that exist in ECS:

- System Administrator
- System Monitor
- Namespace Administrator
- Lock Administrator

System Administrator

The System Administrator role allows a user to configure ECS and during initial configuration, specify the storage used for the object store, how the store is replicated, how tenant access to the object store is configured (by defining namespaces), and which users have permissions within an assigned namespace. The System Administrator can also configure namespaces and perform namespace administration, or can assign a user who belongs to the namespace as the Namespace Administrator.

The System Administrator has access to the ECS Portal and system administration operations can also be performed from programmatic clients using the ECS Management REST API.

After initial installation of ECS, the System Administrator is a pre-provisioned local management user called `root`. The default root user is described in [Default management users](#) on page 60.

Because management users are not replicated across sites, a System Administrator must be created at each VDC that requires one.

System Monitor


The System Monitor role enables a user to have read-only access to the ECS Portal. The System Monitor can view all ECS Portal pages and all information on the pages, except user detail information such as passwords and secret key data. The System Monitor cannot provision or configure the ECS system. For example, the monitor cannot create or update storage pools, replication groups, namespaces, buckets, users through the portal or ECS Management REST API. Monitors cannot modify any other portal setting except their own passwords.

Because management users are not replicated across sites, a System Monitor must be created at each VDC that requires one.

Namespace Administrator

The Namespace Administrator is a management user who can access the ECS Portal. The Namespace Administrator can assign local users as object users for the namespace and create and manage buckets within the namespace. Namespace Administrator operations can also be performed using the ECS REST API. A Namespace Administrator can only be the administrator of a single namespace.

Because authentication providers and namespaces are replicated across sites (they are ECS global resources), a domain user who is a Namespace Administrator can log in at any site and perform namespace administration from that site.

 **Note:** If a domain user is to be assigned to the Namespace Administrator role, the user must be mapped into the namespace if the user is not a namespace administrator.

Local management users are not replicated across sites, so a local user who is a Namespace Administrator can only log in at the VDC at which the management user was created. If you want the same username to exist at another VDC, the user must be created at the other VDC. As they are different users, changes to a same-named user at one VDC, such as a password change, is not propagated to the user with the same name at the other VDC.

For more details see the *ECS Administration Guide* which is available on the [ECS Product Documentation page](#).

Lock Administrator

The Lock Administrator is the only management user who can lock and unlock nodes from the ECS Portal or the ECS Management REST API. *Locking* a node is the ability to disable remote SSH access to the node. The Lock Administrator is a default local user called `emcsecurity`. The `emcsecurity` user is described in [Default management users](#) on page 60.

The Lock Administrator can only change their passwords and lock and unlock nodes. The Lock Administrator role cannot be assigned to another user. System Administrators and System Monitors can view the lock status of nodes. For instructions on locking and unlocking nodes, see [Lock and unlock nodes using the ECS Portal](#) on page 166.

Tasks performed by role

The tasks that can be performed in the ECS Portal or ECS Management REST API by each role are described in the following table:

Table 14 Tasks performed by ECS management user role

Task	System Admin	System Monitor	Namespace Admin	Lock Admin
Tenancy				
Create namespaces (tenants)	Yes	No	No	No
Delete namespaces	Yes	No	No	No
User management (management and object users unless otherwise noted)				
Create local object users and assign them to namespaces	Yes (in all namespaces)	No	Yes (in one namespace)	No
Create local management users and assign them to namespaces	Yes (in all namespaces)	No	No	No
Delete local object users	Yes (in all namespaces)	No	Yes (in one namespace)	No
Delete/unlock local management users	Yes	No	No	No
Edit/change password of local management users	Yes	No	No	No
Set user scope (global or namespace) for all object users	Yes	No	No	No
Add an AD, LDAP, or Keystone authentication provider	Yes (in all namespaces)	No	No	No
Delete an AD, LDAP, or Keystone authentication provider	Yes (in all namespaces)	No	No	No
Add AD and LDAP domain users or AD groups into a namespace	Yes (in all namespaces)	No	Yes (in one namespace)	No
Create an AD group (LDAP and Keystone groups are not supported)	Yes (in all namespaces)	No	No	No
Delete domain users or AD groups	Yes (in all namespaces)	No	No	No
Role management				
Assign administration roles to local and domain management users and AD groups	Yes (in all namespaces)	No	No	No
Revoke roles from local and domain users and AD groups	Yes (in all namespaces)	No	No	No
Storage configuration				
Create, modify, storage pools	Yes (in the VDC where the System Admin was created)	No	No	No

Table 14 Tasks performed by ECS management user role (continued)

Task	System Admin	System Monitor	Namespace Admin	Lock Admin
Create, modify, delete VDCs	Yes (in the VDC where the System Admin was created)	No	No	No
Create, modify replication groups	Yes (in the VDC where the System Admin was created)	No	No	No
Create, modify, delete buckets	Yes (in all namespaces)	No	Yes (in one namespace)	No
Set the bucket ACL permissions for a user	Yes (buckets in all namespaces)	No	Yes (buckets in one namespace)	No
Create, modify, delete NFS exports	Yes (buckets in all namespaces)	No	Yes (buckets in one namespace)	No
Create, modify, delete mapping of users and groups to files and objects in buckets	Yes (buckets in all namespaces)	No	Yes (buckets in one namespace)	No
Add, modify, delete the object Base URL to use ECS object storage for Amazon S3 applications	Yes (in all namespaces)	No	No	No
Monitoring and reports				
Get metering information for each namespace and bucket	Yes (in all namespaces)	Yes (in all namespaces)	Yes (in one namespace)	No
Get audit information (list of all activity of users using the ECS Portal and ECS Management REST API)	Yes (in all namespaces)	Yes (in all namespaces)	No	No
View alerts and perform alert actions (such as acknowledging or assigning alerts)	Yes (in all namespaces)	Yes (in all namespaces)	No	No
Configure alerts	Yes (in all namespaces)	No	No	No
Monitor capacity utilization of storage pools, nodes, disks, and the entire VDC	Yes (in all namespaces)	Yes (in all namespaces)	No	No
Monitor the health and utilization of the infrastructure environment (nodes, disks, NIC bandwidth, CPU, and memory utilization)	Yes (in all namespaces)	Yes (in all namespaces)	No	No
Monitor requests and network performance for VDCs and nodes	Yes (in all namespaces)	Yes (in all namespaces)	No	No

Table 14 Tasks performed by ECS management user role (continued)

Task	System Admin	System Monitor	Namespace Admin	Lock Admin
Monitor status of data erasure encoding for each storage pool	Yes (in all namespaces)	Yes (in all namespaces)	No	No
Monitor recovery status of storage pools after an outage or failure (data rebuilding process)	Yes (in all namespaces)	Yes (in all namespaces)	No	No
Monitor disk use metrics at the VDC or individual node level	Yes (in all namespaces)	Yes (in all namespaces)	No	No
Monitor geo-replication metrics including network traffic, data pending replication and XOR, failover and bootstrapping processing status	Yes (in all namespaces)	Yes (in all namespaces)	No	No
Monitor information on cloud-hosted VDCs and cloud replication traffic	Yes (in all namespaces)	Yes (in all namespaces)	No	No
Licensing, ESRS, security, and event configuration				
View license and subscription information for all components	Yes	Yes	No	No
Procure and apply new licenses	Yes	No	No	No
Add, modify, delete EMC Secure Remote Services (ESRS) server	Yes	No	No	No
Change password	Yes	Yes	Yes	Yes
Lock nodes to prevent remote access through SSH	No	No	No	Yes
Add or delete an SNMP trap recipient to forward ECS events	Yes	No	No	No
Add or delete a syslog server to remotely store ECS logging messages	Yes	No	No	No

Working with users in the ECS Portal

You can use the **User Management** page available from **Manage > Users** to create local users who are assigned as object users for a namespace. You can also create management users, which can

be new local users to whom you assign management roles, or domain users to whom you assign management roles.

The **User Management** page has two tabs: the **Object Users** tab and the **Management Users** tab.

Object Users tab

You can use the **Object Users** tab to view the details of object users, to edit object users, and to delete object users. The object users who are listed on this page include:

- The local object users who are created by a System or Namespace Administrator in the ECS Portal.
- The domain users that have become object users by way of obtaining a secret key using a client that communicates with the ECS Management REST API.

A System Administrator sees the object users for all namespaces. A Namespace Administrator sees only the object users in their namespace.

Table 15 Object user properties

Field	Description
Name	The name of the object user.
Namespace	The namespace to which the object user is assigned.
Actions	<p>The actions that can be completed for the object user.</p> <ul style="list-style-type: none"> • Edit: Change the object user's name, the namespace to which the user is assigned, or the S3, Swift, or CAS object access passwords for the user. • Delete: Delete the object user. • New Object User button: Adds a new object user.

Management Users tab

You can use the **Management Users** tab to view the details of local and domain management users, to edit management users, and to delete management users. This tab is only visible to System Administrators.

Table 16 Management user properties

Field	Description
Name	The name of the management user.
Actions	<p>The actions that can be completed for the management user.</p> <ul style="list-style-type: none"> • Edit: For a local management user: Change the user's name, password, and System Administrator or System Monitor role assignment. For a domain management user: Change the AD or LDAP username or AD group name, and System Administrator or System Monitor role assignment. • Delete: Delete the management user. • New Management User button: Add a new management user that can be assigned the System Administrator role or the System Monitor role. • Unlock: A system administrator can unlock a management user who is locked out.

Add an object user

You can create object users and configure them to use the supported object access protocols. You can edit an object user configuration by adding or removing access to an object protocol, or by creating a new secret key for the object user.

Before you begin

- This operation requires the System Administrator or Namespace Administrator role in ECS.
- A System Administrator can assign new object users into any namespace.
- A Namespace Administrator can assign new object users into the namespace in which they are the administrator.
- If you create an object user who will access the ECS object store through the OpenStack Swift object protocol, the Swift user must belong to an OpenStack group. A group is a collection of Swift users that have been assigned a role by an OpenStack administrator. Swift users that belong to the `admin` group can perform all operations on Swift buckets (containers) in the namespace to which they belong. Do not add ordinary Swift users to the `admin` group. For Swift users that belong to any group other than the `admin` group, authorization depends on the permissions that are set on the Swift bucket. You can assign permissions on the bucket from the OpenStack Dashboard UI or in the ECS Portal using the Custom Group ACL for the bucket. For more information, see [Set custom group bucket ACLs](#) on page 84.

Procedure

1. In the ECS Portal, select **Manage > Users**.
2. On the **User Management** page, click **New Object User**.
3. On the **New Object User** page, in the **Name** field, type a name for the local object user.

You can type domain-style names that include `@` (for example, `user@domain.com`). You might want to do this to keep names unique and consistent with AD names. However, local object users are authenticated using a secret key that is assigned to the username, not through AD or LDAP.

Note: User names can include uppercase letters, lowercase letters, numbers, and any of the following characters: `! # $ & ' () * + , - . / : ; = ? @ _ ~`

4. In the **Namespace** field, select the namespace that you want to assign the object user to, and then complete one of the following steps:
 - To add the object user, and return later to specify passwords or secret keys to access the ECS object protocols, click **Save**.
 - To specify passwords or secret keys to access the ECS object protocols, click **Next to Add Passwords**.
5. On the **Update Passwords for User <username>** page, in the **Object Access** area, for each of the protocols that you want the user to use to access the ECS object store, type or generate a key for use in accessing the S3/Atmos, Swift, or CAS interfaces.
 - a. For S3 access, in the **S3/Atmos** box, click **Generate & Add Secret Key**.

The secret key (password) is generated.

To view the secret key in plain text, select the **Show Secret Key** checkbox.

To create a second secret key to replace first secret key for security reasons, click **Generate & Add Secret Key**.

The **Add S3/Atmos Secret Key/Set Expiration on Existing Secret Key** dialog is displayed. When adding a second secret key, you can specify for how long to retain the first password. Once this time has expired, the first secret key expires.

In the **Minutes** field, type the number of minutes for which you want to retain the first password before it expires. For example, if you typed 3 minutes, you would see *This password will expire in 3 minute(s)*.

After 3 minutes, you would see that the first password displays as expired and you could then delete it.


b. For Swift access:

- In the **Swift Groups** field, type the OpenStack group to which the user belongs.
- In the **Swift password** field, type the OpenStack Swift password for the user.
- Click **Set Groups & Password**.

If you want an S3 user to be able to access Swift buckets, you must add a Swift password and group for the user. The S3 user is authenticated by using the S3 secret key, and the Swift group membership enables access to Swift buckets.

c. For CAS access:

- In the **CAS** field, type the password and click **Set Password** or click **Generate** to automatically generate the password and click **Set Password**.
- Click **Generate PEA file** to generate a Pool Entry Authorization (PEA) file. The file output displays in the **PEA file** box and the output is similar to the following example. The PEA file provides authentication information to CAS before CAS grants access to ECS; this information includes the username and secret. The secret is the base64-encoded password that is used to authenticate the ECS application.

 **Note:** **Generate PEA file** button is displayed after the password is set.

```
<pea version="1.0.0">
<defaultkey name="s3user4">
<credential id="csp1.secret" enc="base64">WlFOOTlTZUFsaU13Mlg3VnZaQ0k=</credential>
</defaultkey>
<key type="cluster" id="93b8729a-3610-33e2-9a38-8206a58f6514" name="s3user4">
<credential id="csp1.secret" enc="base64">WlFOOTlTZUFsaU13Mlg3VnZaQ0k=</credential>
</key>
</pea>
```

- In the **Default Bucket** field, select a bucket, and click **Set Bucket**.
- Optional. Click **Add Attribute** and type values in the **Attribute** and **Group** fields.
- Click **Save Metadata**.

6. Click **Close**.

The passwords/secret keys are saved automatically.

Add a domain user as an object user

You can configure domain users so that they can access the ECS object store and generate secret keys for themselves. By doing so, they add themselves as object users to ECS.

Before you begin

- AD or LDAP domain users must have been added to ECS through an AD or LDAP authentication provider. Adding an authentication provider must be performed by a System Administrator and is described in [Add an AD or LDAP authentication provider](#) on page 46.

- Domain users must have been added into a namespace by a System or Namespace Administrator as described in [Add domain users into a namespace](#) on page 72.

Procedure

1. Domain users can create secret keys for themselves by using the instructions in the *ECS Data Access Guide*, available from the [ECS Product Documentation page](#).

When a domain user creates their own secret key, they become an object user in the ECS system.

Add domain users into a namespace

In the ECS Portal, you can add domain users into a namespace based on the AD or LDAP domain, groups, and attributes associated with the users. Domain users must be added (mapped) into a namespace to perform ECS object user operations.

Before you begin

- This operation requires the System Administrator or Namespace Administrator role in ECS.
- An authentication provider must exist in the ECS system that provides access to the domain that includes the users you want to add into the namespace.

Procedure

1. In the ECS Portal, select **Manage > Namespace**.
2. On the **Namespace Management** page, beside the namespace, click **Edit**.
3. On the **Edit Namespace** page, click **Domain** and type the name of the domain in the **Domain** field.
4. In the **Groups** field, type the names of the groups that you want to use to add users into the namespace.

The groups that you specify must exist in AD.

5. In the **Attribute** and **Values** fields, type the name of the attribute and the values for the attribute.

The specified attribute values for the users must match the attribute values specified in AD or LDAP.

If you do not want to use attributes to add users into the namespace, click the **Attribute** button with the trash can icon to remove the attribute fields.

6. Click **Save**.

Create a local management user or assign a domain user or AD group to a management role

You can create a local management user, and you can assign a management role to a local user, a domain user, or an AD group. Management users can perform system-level administration (VDC administration) and namespace administration. You can also remove the management role assignment.


Before you begin

- This operation requires the System Administrator or Namespace Administrator role in ECS.
- By default, the ECS root user is assigned the System Administrator role and can perform the initial assignment of a user to the System Administrator role.
- To assign a domain user or an AD group to a management role, the domain users or AD group must have been added to ECS through an authentication provider. Adding an authentication

provider must be performed by a System Administrator and is described in [Add an AD or LDAP authentication provider](#) on page 46.

- To assign the Namespace Administrator role to a management user, you must create a management user using the following procedure and perform the role assignment on the **Edit Namespace** page in the ECS Portal (see [Assign the Namespace Administrator role to a user or AD group](#) on page 73). The user cannot log in until the Namespace Administrator role is assigned.

Procedure

1. In the ECS Portal, select **Manage > Users**.
 2. On the **User Management** page, click the **Management Users** tab.
 3. Click **New Management User**.
 4. Click **AD/LDAP User or AD Group** or **Local User**.
 - For a domain user, in the **Username** field, type the name of the user. The username and password that ECS uses to authenticate a user are held in AD or LDAP, so you do not need to define a password.
 - For an AD group, in the **Group Name** field, type the name of the group. The username and password that ECS uses to authenticate the AD group are held in AD, so you do not need to define a password.
 - For a local user, in the **Name** field, type the name of the user and in the **Password** field, type the password for the user.
-  **Note:** User names can include uppercase letters, lowercase letters, numbers and any of the following characters: ! # \$ & ' () * + , - . / : ; = ? @ _ ~
5. To assign the System Administrator role to the user or AD group, in the **System Administrator** box, click **Yes**.

If you select **Yes**, but later you want to remove System Administrator privileges from the user, you can edit this setting and select **No**.
 6. To assign the System Monitor role to the user or AD group, in the **System Monitor** box, click **Yes**.
 7. Click **Save**.

Assign the Namespace Administrator role to a user or AD group

You can assign the Namespace Administrator role to a local management user, a domain user, or AD group that exists in the ECS system.

Before you begin

- This operation requires the System Administrator role in ECS.

Procedure

1. In the ECS Portal, select **Manage > Namespace**.
2. On the **Namespace Management** page, beside the namespace into which you want to assign the Namespace Administrator, click **Edit**.
3. On the **Edit Namespace** page:
 - a. For a local management user or a domain user, in the **Namespace Admin** field, type the name of the user to whom you want to assign the Namespace Administrator role.

To add more than one Namespace Administrator, separate the names with commas.

A user can be assigned as the Namespace Administrator only for a single namespace.

- b. For an AD group, in the **Domain Group Admin** field, type the name of the AD group to which you want to assign the Namespace Administrator role.

When the AD group is assigned the Namespace Administrator role, all users in the group are assigned this role.

An AD group can be the Namespace Administrator only for one namespace.

4. Click **Save**.

CHAPTER 7

Buckets

- [Introduction to buckets](#)..... 76
- [Working with buckets in the ECS Portal](#)..... 76
- [Create a bucket using the S3 API \(with s3curl\)](#)..... 89
- [Bucket, object, and namespace naming conventions](#)..... 92
- [Disable unused services](#)..... 94

Introduction to buckets

Buckets are object containers that are used to control access to objects and to set [properties](#) that define attributes for all contained objects, such as [retention periods](#) and quotas.

In S3, object containers are called *buckets* and this term has been adopted as a general term in ECS. In Atmos, the equivalent of a bucket is a *subtenant*. In Swift, the equivalent of a bucket is a *container*. In CAS, a bucket is a *CAS pool*.

In ECS, buckets are assigned a type, which can be S3, Swift, Atmos, or CAS. S3, Atmos, or Swift buckets can be configured to support file system access (for NFS and HDFS). A bucket that is configured for file system access can be read and written by using its object protocol and by using the NFS or HDFS protocol. S3 and Swift buckets can also be accessed using each other's protocol. Accessing a bucket using more than one protocol is often referred to as *cross-head support*.

You can create buckets for each object protocol using its API, usually using a client that supports the appropriate protocol. You can also create S3, file system-enabled (NFS or HDFS), and CAS buckets using the ECS Portal and the ECS Management REST API.

Bucket ownership

A bucket is assigned to a namespace and object users are also assigned to a namespace. An object user can create buckets only in the namespace to which the object user is assigned. An ECS System or Namespace Administrator can assign the object user as the owner of a bucket, or a grantee in a bucket ACL, even if the user does not belong to the same namespace as the bucket, so that buckets can be shared between users in different namespaces. For example, in an organization where a namespace is a department, a bucket can be shared between users in different departments.

Bucket access

Objects in a bucket that belong to a replication group spanning multiple VDCs can be accessed from all of the VDCs in the replication group. Objects in a bucket that belongs to a replication group that is associated with only one VDC can be accessed from only that VDC. Buckets cannot be accessed or listed from other VDCs that are not in the replication group. However, because the identity of a bucket and its metadata, such as its ACL, are global management information in ECS, and the global management information is replicated across the system storage pools, the existence of the bucket can be seen from all VDCs in the federation.

For information about how objects in buckets can be accessed during site outages, see [TSO behavior with the ADO bucket setting turned on](#) on page 176.

Working with buckets in the ECS Portal

You can use the **Bucket Management** page available from **Manage > Buckets** to view the details of existing buckets in a selected namespace, to modify the Access Control List (ACL) for buckets, to modify the policy for buckets, and to delete buckets.

To ensure that the system works correctly, always have life cycle policies that are configured with versioned buckets.

Bucket settings

The following table describes the settings that you can specify when you create or edit a bucket:

Table 17 Bucket settings



Attribute	Description	Can be Edited
Name	Name of the bucket. For information about bucket naming, see Bucket, object, and namespace naming conventions on page 92.	No
Namespace	Namespace with which the bucket is associated.	No
Replication Group	Replication group in which the bucket is created.	No
Bucket Owner	Bucket owner.	Yes
File System	Indicates whether the bucket can be used as a file system (NFS export or HDFS). To simplify access to the file system, a default group, and default permissions that are associated with the group, can be defined. For more information, see Default group on page 79.  Note: File system-enabled buckets only support the / delimiter when listing objects.	No
CAS	Indicates whether the bucket can be used for CAS data.	No
Metadata Search	Indicates that metadata search indexes are created for the bucket based on specified key values. <ul style="list-style-type: none"> If turned on, metadata keys that are used as the basis for indexing objects in the bucket can be defined. These keys must be specified at bucket creation time. After the bucket is created, search can be turned off altogether, but the configured index keys cannot be changed. The way the attribute is defined is described in Metadata search fields on page 79.  Note: Metadata that is used for indexing is not encrypted, so metadata search can still be used on a bucket when Server-side Encryption (D@RE) is turned on.	No
Access During Outage (ADO)	<ul style="list-style-type: none"> The ECS system behavior when accessing data in the bucket during a temporary site outage in a geo-federated setup. If you turn this setting on, and a temporary site outage occurs, if you cannot access a bucket at the failed site where the bucket was created (owner site), you can access a copy of the bucket at another site. Note that objects that you access in the buckets in the namespace might have been updated at the failed site, but changes might not have been propagated to the site from which you are accessing the object. If you turn this setting off, data in the site which has the temporary outage is not available for access from other sites, and object reads for data that is owned by the failed site will fail. This is the default ECS system behavior to maintain strong consistency by continuing to allow access to data owned by accessible sites and preventing access to data owned by a failed site. Read-Only option: Specifies whether a bucket with the ADO setting that is turned on is accessible as read-only or read/write during a temporary site outage. If you select the Read-Only option, the bucket is only accessible in read-only mode during the outage. 	Yes

Table 17 Bucket settings (continued)


Attribute	Description	Can be Edited
	<ul style="list-style-type: none"> For more information, see TSO behavior with the ADO bucket setting turned on on page 176. 	
Server-side Encryption	<p>Indicates whether server-side encryption is turned on or off.</p> <ul style="list-style-type: none"> Server-side encryption, also known as Data At Rest Encryption or D@RE, encrypts data inline before storing it on ECS disks or drives. This encryption helps prevent sensitive data from being acquired from discarded or stolen media. If you turn encryption on when the bucket is created, this feature cannot be turned off later. If the bucket's namespace is encrypted, then every bucket is encrypted. If the namespace is not encrypted, you can select encryption for individual buckets. For a complete description of the feature, see the <i>ECS Security Configuration Guide</i>, available from the ECS Product Documentation page. 	No
Quota	<p>The storage space limit that is specified for the bucket. You can specify a storage limit for the bucket and define notification and access behavior when the quota is reached. The quota setting for a bucket cannot be less than 1 GiB. You can specify bucket quota settings in increments of GiB. You can select one of the following quota behavior options:</p> <ul style="list-style-type: none"> Notification Only at <quota_limit_in_GiB> Soft quota setting at which you are notified. Block Access Only at <quota_limit_in_GiB> Hard quota setting which, when reached, prevents write/update access to the bucket. Block Access at <quota_limit_in_GiB> and Send Notification at <quota_limit_in_GiB> Hard quota setting which, when reached, prevents write/update access to the bucket and the quota setting at which you are notified. <p> Note: Quota enforcement depends on the usage reported by ECS metering. Metering is a background process that is designed so that it does not impact foreground traffic and so the metered value can lag the actual usage. Because of the metering lag, there can be a delay in the enforcement of quotas.</p>	Yes
Bucket Tagging	<p>Name-value pairs that are defined for a bucket and enable buckets to be classified. For more information about bucket tagging, see Bucket tagging on page 79.</p>	Yes
Bucket Retention	<p>Retention period for a bucket.</p> <ul style="list-style-type: none"> The expiration of a retention period on an object within a bucket is calculated when a request to modify an object is made and is based on the value set on the bucket and the objects themselves. The retention period can be changed during the lifetime of the bucket. You can find more information about retention and applying retention periods and policies in Retention periods and policies on page 53. 	Yes

Table 17 Bucket settings (continued)

Attribute	Description	Can be Edited
Auto-Commit Period	Auto-commit period is the time interval in which the updates through NFS are allowed for objects under retention. This attribute enables NFS files that are written to ECS to be WORM compliant. The interval is calculated from the last modification time. The auto-commit value must be less than or equal to the retention value with a maximum of 1 day. A value of 0 indicates no auto-commit period.	Yes

Default group

When you turn the **File System** setting on for a bucket to enable file system access, you can assign a default group for the bucket. The default group is a Unix group, the members of which have permissions on the bucket when it is accessed as a file system. Without this assignment, only the bucket owner can access the file system.

You can also specify Unix permissions that are applied to files and directories created using object protocols so that they are accessible when the bucket is accessed as a file system.

Metadata search fields

When you set the **Metadata Search** option to **On** for a bucket, objects in the bucket can be indexed based on their metadata fields. S3 object clients can search for objects based on the indexed metadata using a rich query language.

Each object has a set of system metadata that is automatically assigned, and can also have user assigned metadata. Both system and user metadata can be included in the index and used as the subject of metadata searches.

When metadata search is enabled on a bucket, you can select **System** or **User** as the metadata search **Type**. When you select a metadata search **Type** as **System**, metadata that is automatically assigned to objects in a bucket is listed for selection in the **Name** drop-down menu.

When you select a metadata search **Type** of **User**, you must specify the name of the user metadata to create an index for. You must also specify its data type so that ECS knows how to interpret the metadata values provided in search queries.

You can read more about the metadata search feature in the *ECS Data Access Guide*, available from the [ECS Product Documentation page](#).

Bucket tagging

Bucket tags are key-value pairs that you can associate with a bucket so that the object data in the bucket can be categorized. For example, you could define keys like `Project` or `Cost Center` on each bucket and assign values to them. You can add up to ten tags to a bucket.

You can assign bucket tags and values using the ECS Portal or using a custom client through the ECS Management REST API. Bucket tags are included in the metering data reports displayed in the ECS Portal or retrieved using the ECS Management REST API.

Create a bucket

You can create and configure S3, S3+FS, or CAS buckets in the ECS Portal.

Before you begin

- This operation requires the System Administrator or Namespace Administrator role in ECS.

- A System Administrator can create buckets in any namespace.
- A Namespace Administrator can create buckets in the namespace in which they are the administrator.

About this task

For CAS-specific instructions on setting up a CAS bucket for a CAS object user, see *ECS Data Access Guide*, available from the [ECS Product Documentation page](#).

Procedure

1. In the ECS Portal, select **Manage > Buckets**.
2. On the **Bucket Management** page, click **New Bucket**.
3. On the **New Bucket** page, on the **Basic** tab, do the following:
 - a. In the **Name** field, type the bucket name.
 - b. In the **Namespace** field, select the namespace that you want the bucket and its objects to belong to.
 - c. In the **Replication Group** field, select the replication group that you want to associate the bucket with.
 - d. In the **Bucket Owner** field, type the bucket owner, or select the **Set current user as Bucket Owner** checkbox.

The bucket owner must be an ECS object user for the namespace. If you do not specify a user, you are assigned as the owner. However, you cannot access the bucket unless your username is also assigned as an object user.

The user that you specify is given Full Control.

- e. Click **Next**.
4. On the **New Bucket** page, on the **Required** tab, do the following:
 - a. In the **File System** field, click **On** to specify that the bucket supports operation as a file system (for NFS or HDFS access).

The bucket is an S3 bucket that supports file systems.

You can set a default UNIX group for access to the bucket and for objects that are created in the bucket. For more information, see [Default group](#) on page 79.

- b. In the **CAS** field, click **On** to set the bucket as a CAS bucket.

By default, CAS is disabled and the bucket is marked as an S3 bucket.

In the **Reflection Expiration** field, click **On** to configure an expiration time for reflections in the bucket.

In the **Reflection Age** field, select the appropriate expiration time. (The minimum expiration time is 1 day and the maximum is 99 years.)

If there is no configured expiration time for a reflection, the reflection is never deleted.

- c. In the **Metadata Search** field, click **On** to specify that the bucket supports searches based on object metadata.

If the **Metadata Search** setting is turned on, you can add user and system metadata keys that are used to create object indexes. For more information about entering metadata search keys, see [Metadata search fields](#) on page 79.

Note: If the bucket supports CAS, metadata search is automatically enabled and a `CreateTime` key is automatically created. The metadata can be searched using the S3 metadata search capability or using the Centera API.

- d. In the **Access During Outage** field, click **On** if you want the bucket to be available during a temporary site outage. For more information about this option, see [TSO behavior with the ADO bucket setting turned on](#) on page 176.
 - If the **Access During Outage** setting is turned on, you have the option of selecting the **Read-Only** checkbox to restrict create, update, or delete operations on the objects in the bucket during a temporary site outage. Once you turn the **Read-Only** option on for the bucket, you cannot change it after the bucket is created. For more information about this option, see [TSO behavior with the ADO bucket setting turned on](#) on page 176.
 - e. In the **Server-side Encryption** field, click **On** to specify that the bucket is encrypted.
 - f. Click **Next**.
5. On the **New Bucket** page, on the **Optional** tab, do the following:
 - a. In the **Quota** field, click **On** to specify a quota for the bucket and select the quota setting you require.

The settings that you can specify are described in [Bucket settings](#) on page 76.
 - b. In the **Bucket Tagging** field, click **Add** to add tags, and type name-value pairs.

For more information, see [Bucket tagging](#) on page 79.
 - c. In the **Bucket Retention Period** field, type a time period to set a bucket retention period for the bucket, or click **Infinite** if you want objects in the bucket to be retained forever.

For more information about retention periods, see [Retention periods and policies](#) on page 53.
 - d. In the **Auto-Commit Period** field, type a time period to enable updates to the files that are under retention. The interval applies only to file enabled buckets.

The auto-commit value must be less than or equal to the retention value with a maximum of 1 day. A value of 0 indicates no auto-commit period.
 - e. Click **Save** to create the bucket.

Results

To assign permissions on the bucket for users or groups, see the tasks later in this section.

Edit a bucket

You can edit some bucket settings after the bucket has been created and after it has had objects that are written to it.

Before you begin

- This operation requires the System Administrator or Namespace Administrator role in ECS.
- A System Administrator can edit the settings for a bucket in any namespace.
- A Namespace Administrator can edit the settings for a bucket in the namespace in which they are the administrator.

To edit a bucket, you must be assigned to the Namespace Administrator or System Administrator role.

About this task

You can edit the following bucket settings:

- Quota
- Bucket Owner
- Bucket Tagging
- Access During Outage
- Bucket Retention
- Reflection Expiration and Reflection Age (for CAS buckets)

You cannot change the following bucket settings:

- Replication Group
- Server-side Encryption
- File System
- CAS
- Metadata Search

Known issue with changing NFS bucket owners

If you change the bucket owner and try to revert the changes, reverting the bucket ownership does not work. You cannot access the NFS mount over the previous bucket owner until you reset the bucket ownership using the API mentioned in the support KB article [KB 534080](#).

Procedure

1. In the ECS Portal, select **Manage > Buckets**.
2. On the **Bucket Management** page, in the Buckets table, select the **Edit** action for the bucket for which you want to change the settings.
3. Edit the settings that you want to change.

You can find out more information about the bucket settings in [Bucket settings](#) on page 76.

4. Click **Save**.


Set ACLs

The privileges a user has when accessing a bucket are set using an Access Control List (ACL). You can assign ACLs for a user, for a set of pre-defined groups, such as all users, and for a custom group.

When you create a bucket and assign an owner to it, an ACL is created that assigns a default set of permissions to the bucket owner - the owner is, by default, assigned full control.

You can modify the permissions assigned to the owner or you can add new permissions for a user by selecting the Edit ACL operation for the bucket.


In the ECS Portal, the **Bucket ACLs Management** page has **User ACLs**, **Group ACLs**, and **Custom Group ACLs** tabs to manage the ACLs associated with individual users and pre-defined groups, and to allow groups to be defined that can be used when accessing the bucket as a file system.

 **Note:** For information about ACLs with CAS buckets, see the *ECS Data Access Guide*, available from the [ECS Product Documentation page](#).

Bucket ACL permissions reference

The ACL permissions that can be assigned are provided in the following table. The permissions that are applicable depend on the type of bucket.

Table 18 Bucket ACLs

ACL	Permission
Read	Allows user to list the objects in the bucket.
Read ACL	Allows user to read the bucket ACL.
Write	Allows user to create or update any object in the bucket.
Write ACL	Allows user to write the ACL for the bucket.
Execute	Sets the execute permission when accessed as a file system. This permission has no effect when the object is accessed using the ECS object protocols.
Full Control	Allows user to Read, Write, Read ACL, and Write ACL.  Note: Non-owners can Read, Write, Read ACL, and Write ACL if the permission has been granted or can only list the objects.
Privileged Write	Allows user to perform writes to a bucket or object when the user does not have normal write permission. Required for CAS buckets.
Delete	Allows user to delete buckets and objects. Required for CAS buckets.
None	User has no privileges on the bucket.

Set the bucket ACL permissions for a user

The ECS Portal enables you to set the bucket ACL for a user or for a pre-defined group.


Before you begin

- This operation requires the System Administrator or Namespace Administrator role in ECS.
- A System Administrator can edit the ACL settings for a bucket in any namespace.
- A Namespace Administrator can edit the ACL settings for a bucket in the namespace in which they are the administrator.

Procedure

1. In the ECS Portal, select **Manage > Buckets**.
2. On the **Bucket Management** page, locate the bucket that you want to edit in the table and select the **Edit ACL** action.
3. On the **Bucket ACLs Management** page, the **User ACLs** tab displays by default and shows the ACLs that have been applied to the users who have access to the bucket.

The bucket owner has default permissions that are assigned.

 **Note:** Because the ECS Portal supports S3, S3 + File system (HDFS or NFS), and CAS buckets, the range of permissions that can be set are not applicable to all bucket types.

4. To set (or remove) the ACL permissions for a user that already has permissions that are assigned, in the ACL table, in the **Action** column, click **Edit** or **Remove**.
5. To add a user and assign ACL permissions to the bucket, click **Add**.

- a. Enter the username of the user that the permissions apply to.
- b. Select the permissions for the user.

For more information about ACL permissions, see [Bucket ACL permissions reference](#) on page 83.

6. Click **Save**.

Set the bucket ACL permissions for a pre-defined group

You can set the ACL for a bucket for a pre-defined group from the ECS Portal.

Before you begin

- This operation requires the System Administrator or Namespace Administrator role in ECS.
- A System Administrator can edit the group ACL settings for a bucket in any namespace.
- A Namespace Administrator can edit the group ACL settings for a bucket in the namespace in which they are the administrator.

Procedure

1. In the ECS Portal, select **Manage > Buckets**.
2. On the **Bucket Management** page, locate the bucket that you want to edit in the table and select the **Edit ACL** action.
3. Click the **Group ACLs** tab to set the ACL permissions for a pre-defined group.
4. Click **Add**.
5. The **Edit Group** page is displayed.

The group names are described in the following table:

Group	Description
public	All users, authenticated or not.
all users	All authenticated users.
other	Authenticated users but not the bucket owner.
log delivery	Not supported.

6. Select the permissions for the group.
7. Click **Save**.

Set custom group bucket ACLs

You can set a group ACL for a bucket in the ECS Portal and you can set bucket ACLs for a group of users (Custom Group ACL), for individual users, or a combination of both. For example, you can grant full bucket access to a group of users, but you can also restrict (or even deny) bucket access to individual users in that group.

Before you begin

- This operation requires the System Administrator or Namespace Administrator role in ECS.
- A System Administrator can edit the group ACL settings for a bucket in any namespace.
- A Namespace Administrator can edit the group ACL settings for a bucket in the namespace in which they are the administrator.

About this task

Custom group ACLs enable groups to be defined and for permissions to be assigned to the group. The main use case for assigning groups to a bucket is to support access to the bucket as a file system. For example, when making the bucket available for NFS or HDFS.

Members of the UNIX group can access the bucket when it is accessed as a file system (using NFS or HDFS).

Procedure

1. In the ECS Portal, select **Manage > Buckets**.
2. On the **Bucket Management** page, locate the bucket that you want to edit in the table and select the **Edit ACL** action.
3. Click the **Custom Group User ACLs** tab to set the ACL for a custom group.
4. Click **Add**.

The **Edit Custom Group** page displays.

5. On the **Edit Custom Group** page, in the **Custom Group Name** field, type the name for the group.

This name can be a Unix/Linux group, or an Active Directory group.

6. Select the permissions for the group.

At a minimum you should assign **Read, Write, Execute, and Read ACL**.

7. Click **Save**.

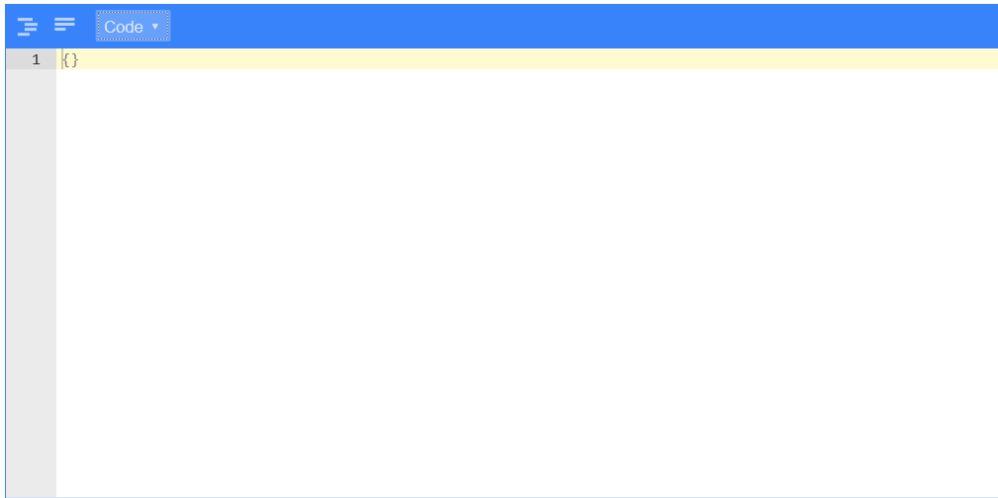
Set bucket policies

The ECS Portal provides a Bucket Policy Editor to enable you to create a bucket policy for an existing bucket.

For each bucket, you can define ACLs for an object user. Bucket policies provide greater flexibility than ACLs and allow fine grained control over permissions for bucket operations and for operations on objects within the bucket. Policy conditions are used to assign permissions for a range of objects that match the condition and are used to automatically assign permissions to newly uploaded objects.

Policies are defined in JSON format and the syntax used for policies is the same as that used for Amazon AWS. The operations for which permissions can be assigned are limited to those operations supported by ECS. For more information, see the *ECS Data Access Guide*, available from the [ECS Product Documentation page](#).

The bucket policy editor has a code view and a tree view. The code view, shown in the following screenshot, enables you to enter JSON policies from scratch or to paste existing policies into the editor and modified. For example, if you have existing policies in JSON format, you can paste them into the code view and modify them.

Figure 8 Bucket Policy Editor code view

The tree view, shown in the following screenshot, provides a mechanism for navigating a policy and is useful where you have a large number of statements in a policy. You can expand and contract the statements and search them.

Figure 9 Bucket Policy Editor tree view

Bucket policy scenarios

In general, the bucket owner has full control on a bucket and can grant permissions to other users and can set S3 bucket policies using an S3 client. In ECS, it is also possible for an ECS System or Namespace Administrator to set bucket policies using the Bucket Policy Editor from the ECS Portal.

You can use bucket policies in the following typical scenarios:

- Grant bucket permissions to a user
- Grant bucket permissions to all users
- Automatically assign permissions to created objects

Grant bucket permissions to a user

To grant permission on a bucket to a user apart from the bucket owner, specify the resource that you want to change the permissions for. Set the principal attribute to the name of the user, and specify one or more actions that you want to enable.

The following example shows a policy that grants a user who is named `user1` the permission to update and read objects in the bucket that is named `mybucket`:

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "Grant permission to user1",
      "Effect": "Allow",
      "Principal": ["user1"],
      "Action": [ "s3:PutObject", "s3:GetObject" ],
      "Resource": [ "mybucket/*" ]
    }
  ]
}
```

You can also add conditions. For example, if you only want the user to read and write object when accessing the bucket from a specific IP address, add a `IpAddress` condition as shown in the following policy:

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "Grant permission ",
      "Effect": "Allow",
      "Principal": ["user1"],
      "Action": [ "s3:PutObject", "s3:GetObject" ],
      "Resource": [ "mybucket/*" ]
      "Condition": { "IpAddress": { "aws:SourceIp": "<Ip address>" }
    }
  ]
}
```

Grant bucket permissions to all users

To grant permission on a bucket to a user apart from the bucket owner, specify the resource that you want to change the permissions for. Set the principal attribute as anybody (*), and specify one or more actions that you want to enable.

The following example shows a policy that grants anyone permission to read objects in the bucket that is named `mybucket`:

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId2",
  "Statement": [
    {
      "Sid": "statement2",
      "Effect": "Allow",
      "Principal": ["*"],
      "Action": [ "s3:GetObject" ],
      "Resource": [ "mybucket/*" ]
    }
  ]
}
```

```
]
}
```

Automatically assign permissions to created objects

You can use bucket policies to automatically enable access to ingested object data. In the following example bucket policy, `user1` and `user2` can create subresources (that is, objects) in the bucket that is named `mybucket` and can set object ACLs. With the ability to set ACLs, the users can then set permissions for other users. If you set the ACL in the same operation, a condition can be set. Such that a canned ACL `public-read` must be specified when the object is created. This ensures anybody can read all the created objects.

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId3",
  "Statement": [
    {
      "Sid": "statement3",
      "Effect": "Allow",
      "Principal": ["user1", "user2"],
      "Action": [ "s3:PutObject", "s3:PutObjectAcl" ],
      "Resource": [ "mybucket/*" ]
      "Condition": {"StringEquals": {"s3:x-amz-acl": ["public-read"]}}
    }
  ]
}
```

Create a bucket policy

You can create a bucket policy for a selected bucket using the Bucket Policy Editor in the ECS Portal.

Before you begin

This operation requires the System Administrator or Namespace Administrator role (for the namespace to which the bucket belongs).

About this task

You can also create a bucket policy in a text editor and deploy it using the ECS Management REST API or the S3 API.

Procedure

1. In the ECS Portal, select **Manage > Buckets**
2. From the **Namespace** drop-down, select the namespace to which the bucket belongs.
3. In the **Actions** column for the bucket, select **Edit Policy** from the drop-down menu.
4. Provided your policy is valid, you can switch to the tree view of the Bucket Policy Editor. The tree view makes it easier to view your policy and to expand and contract statements.
5. In the Bucket Policy Editor, type the policy or copy and paste a policy that you have previously created.

Some examples are provided in [Bucket policy scenarios](#) on page 86 and full details of the supported operations and conditions are provided in *ECS Data Access Guide*, available from the [ECS Product Documentation page](#).

6. **Save.**

The policy is validated and, if valid, the Bucket Policy Editor exits and the portal displays the **Bucket Management** page. If the policy is invalid, the error message provides information on the reason the policy is invalid.

Create a bucket using the S3 API (with s3curl)

You can use the S3 API to create a bucket in a replication group. Because ECS uses custom headers (`x-emc`), the string to sign must be constructed to include these headers. In this procedure the `s3curl` tool is used. There are also several programmatic clients you can use, for example, the S3 Java client.

Before you begin

- To create a bucket, ECS must have at least one replication group configured.
- Ensure that Perl is installed on the Linux machine on which you run `s3curl`.
- Ensure that `curl` tool and the `s3curl` tool are installed. The `s3curl` tool acts as a wrapper around `curl`.
- To use `s3curl` with `x-emc` headers, minor modifications must be made to the `s3curl` script. You can obtain the modified, ECS-specific version of `s3curl` from the [EMCECS Git Repository](#).
- Ensure that you have obtained a secret key for the user who will create the bucket. For more information, see *ECS Data Access Guide*, available from the [ECS Product Documentation page](#).

About this task

The EMC headers that can be used with buckets are described in [Bucket HTTP headers](#) on page 91.

Procedure

1. Obtain the identity of the replication group in which you want the bucket to be created, by typing the following command:

```
GET https://<ECS IP Address>:4443/vdc/data-service/vpools
```

The response provides the name and identity of all data services virtual pools. In the following example, the ID is `urn:storageos:ReplicationGroupInfo:8fc8e19b-edf0-4e81-bee8-79acc867f64:global`.

```
<data_service_vpools>
<data_service_vpool>
  <creation_time>1403519186936</creation_time>
  <id>urn:storageos:ReplicationGroupInfo:8fc8e19b-edf0-4e81-bee8-79acc867f64:global</
id>
  <inactive>false</inactive>
  <tags/>
  <description>IsilonVPool1</description>
  <name>IsilonVPool1</name>
  <varrayMappings>
    <name>urn:storageos:VirtualDataCenter:1de0bbc2-907c-4ede-b133-f5331e03e6fa:vdc1</
name>
    <value>urn:storageos:VirtualArray:793757ab-ad51-4038-b80a-682e124eb25e:vdc1</
value>
  </varrayMappings>
</data_service_vpool>
</data_service_vpools>
```

2. Set up `s3curl` by creating a `.s3curl` file in which to enter the user credentials.

The `.s3curl` file must have permissions `0600 (rw-/-/-)` when `s3curl.pl` is run.

In the following example, the profile `my_profile` references the user credentials for the `user@yourco.com` account, and `root_profile` references the credentials for the root account.

```
%awsSecretAccessKeys = (
  my_profile => {
    id => 'user@yourco.com',
    key => 'sZRCTZyk93IWukHEGQ3evPJEvPUq4ASL8Nre0awN'
  },
  root_profile => {
    id => 'root',
    key => 'sZRCTZyk93IWukHEGQ3evPJEvPUq4ASL8Nre0awN'
  },
);
```

3. Add the endpoint that you want to use `s3curl` against to the `.s3curl` file.

The endpoint is the address of your data node or the load balancer that sits in front of your data nodes.

```
push @endpoints , (
  '203.0.113.10', 'lg1w3183.lss.dell.com',
);
```

4. Create the bucket using `s3curl.pl` and specify the following parameters:
 - Profile of the user
 - Identity of the replication group in which to create the bucket (`<vpool_id>`, which is set using the `x-emc-dataservice-vpool` header
 - Any custom `x-emc` headers
 - Name of the bucket (`<BucketName>`).

The following example shows a fully specified command:

```
./s3curl.pl --debug --id=my_profile --acl public-read-write
--createBucket -- -H 'x-emc-file-system-access-enabled:true'
-H 'x-emc-dataservice-vpool:<vpool_id>' http://<DataNodeIP>:9020/<BucketName>
```

The example uses the `x-emc-dataservice-vpool` header to specify the replication group in which the bucket is created and the `x-emc-file-system-access-enabled` header to enable the bucket for file system access, such as for NFS or HDFS.

Note: The `-acl public-read-write` argument is optional, but can be used to set permissions to enable access to the bucket. For example, if you intend to access to bucket as NFS from an environment that is not secured using Kerberos.

If successful, (with --debug on) output similar to the following is displayed:

```
s3curl: Found the url: host=203.0.113.10; port=9020; uri=/S3B4; query=;
s3curl: ordinary endpoint signing case
s3curl: StringToSign='PUT\n\n\nThu, 12 Dec 2013 07:58:39 +0000\nx-amz-acl:public-read-
write
\nx-emc-file-system-access-enabled:true\nx-emc-dataservice-vpool:
urn:storageos:ReplicationGroupInfo:8fc8e19b-edf0-4e81-bee8-79accc867f64:global:\n/S3B4'
s3curl: exec curl -H Date: Thu, 12 Dec 2013 07:58:39 +0000 -H Authorization: AWS
root:AiTcfMDhsi6iSq2rIbHEZon0WN0= -H x-amz-acl: public-read-write -L -H content-type:
--data-binary -X PUT -H x-emc-file-system-access-enabled:true
-H x-emc-dataservice-vpool:urn:storageos:ObjectStore:e0506a04-340b-4e78-
a694-4c389ce14dc8: http://203.0.113.10:9020/S3B4
```

After you finish

You can list the buckets using the S3 interface, using:

```
./s3curl.pl --debug --id=my_profile http://<DataNodeIP>:9020/
```

Bucket HTTP headers

There are various headers that determine the behavior of ECS when creating buckets using the objects APIs.

The following `x-emc` headers are provided:

Table 19 Bucket headers

Header	Description
<code>x-emc-dataservice-vpool</code>	Determines the replication group is used to store the objects associated with this bucket. If you do not specify a replication group using the <code>x-emc-dataservice-vpool</code> header, ECS selects the default replication group that is associated with the namespace.
<code>x-emc-file-system-access-enabled</code>	Configures the bucket for NFS or HDFS access. The header must not conflict with the interface that is used. That is, a create bucket request from NFS or HDFS cannot specify <code>x-emc-file-system-access-enabled=false</code> .
<code>x-emc-namespace</code>	Specifies the namespace that is used for this bucket. If the namespace is not specified using the S3 convention of host-style or path-style request, and then it is specified using the <code>x-emc-namespace</code> header. If the namespace is not specified in this header, the namespace that is associated with the user is used.
<code>x-emc-retention-period</code>	Specifies the retention period that is applied to objects in a bucket. Each time a request is made to modify an object in a bucket, the expiration of the retention period for the object is calculated based on the retention period that is associated with the bucket.
<code>x-emc-is-stale-allowed</code>	Specifies whether the bucket is accessible during a temporary VDC outage in a federated configuration.
<code>x-emc-server-side-encryption-enabled</code>	Specifies whether objects that are written to a bucket are encrypted.

Table 19 Bucket headers (continued)

Header	Description
x-emc-metadata-search	Specifies one or more user or system metadata values that are used to create indexes of objects for the bucket. The indexes are used to perform object searches that are filtered based on the indexed metadata.

Bucket, object, and namespace naming conventions

Bucket and object (also referred to as key) names for the S3, OpenStack Swift, Atmos, and CAS protocols must conform to the ECS specifications described in this section.

Note: To use a bucket for HDFS, you must not use underscores in the bucket name as they are not supported by the URI Java class. For example, `viprfs://my_bucket.ns.site/` is an invalid URI and is thus not understood by Hadoop.

Namespace name

The following rules apply to the naming of ECS namespaces:

- Cannot be null or an empty string
- Length range is 1..255 (Unicode char)
- Valid characters are defined by regex `/[a-zA-Z0-9-_]+/`. That is, alphanumeric characters and hyphen (-) and underscore (_) special characters.

S3 bucket and object naming in ECS

Bucket and object names must conform to the ECS naming specification when using the ECS S3 Object API.

Bucket name

The following rules apply to the naming of S3 buckets in ECS:

- Must be between one and 255 characters in length. (S3 requires bucket names to be 1–255 characters long)
- Can include dot (.), hyphen (-), and underscore (_) characters and alphanumeric characters ([a-zA-Z0-9])
- Can start with a hyphen (-) or alphanumeric character.
- Cannot start with a dot (.)
- Cannot contain a double dot (..)
- Cannot end with a dot (.)
- Must not be formatted as IPv4 address.

You can compare this with naming restriction that is specified by the S3 specification: <http://docs.aws.amazon.com/AmazonS3/latest/dev/BucketRestrictions.html>.

Object name

The following rules apply to the naming of S3 objects in ECS:

- Cannot be null or an empty string
- Length range is 1..255 (Unicode char)

- No validation on characters

OpenStack Swift container and object naming in ECS

Container and object names must conform to the ECS naming specification when using the ECS OpenStack Swift Object API.

Container name

The following rules apply to the naming of Swift containers:

- Cannot be null or an empty string
- Length range is 1..255 (Unicode char)
- Can include dot (.), hyphen (-), and underscore (_) characters and alphanumeric characters ([a-zA-Z0-9])
- Can include the at symbol (@) with the assistance of your customer support representative.

Object name

The following rules apply to the naming of Swift objects:

- Cannot be null or an empty string
- Length range is 1..255 (Unicode char)
- No validation on characters

Atmos bucket and object naming in ECS

Subtenant and object names must conform to the ECS naming specification when using the ECS Atmos Object API.

Subtenant (bucket)

The subtenant is created by the server, so the client does not need to know the naming scheme.

Object name

The following rules apply to the naming of Atmos objects:

- Cannot be null or an empty string
- Length range is 1..255 (Unicode characters)
- No validation on characters
- Name should be percent-encoded UTF-8.

CAS pool and object naming in ECS

CAS pools and objects (*clips* in CAS terminology) names must conform to the ECS naming specification when using the CAS API.

CAS pool naming

The following rules apply to the naming of CAS pools in ECS:

- Can contain a maximum of 255 characters
- Cannot contain: ' " / & ? * < > <tab> <newline> or <space>

Clip naming

The CAS API does not support user-defined keys. When an application using CAS API creates a clip, it opens a pool, creates a clip, and adds tags, attributes, streams and so on. After a clip is complete, it is written to a device.

A corresponding clip ID is returned by the CAS engine and can be referred to using <pool name>/<clip id>.

Disable unused services

This section provides you information about the ECS supported services and the available connection options.

About this task

ECS supports the following services and the connection options to connect to those services:

- S3 - http/https/https,http/disabled
- Atmos - http/https/https,http/disabled
- Swift - http/https/https,http/disabled
- HDFS - enabled/disabled
- NFS - enabled/disabled
- CAS - enabled/disabled

The service waits on the key for changes and takes appropriate action. For example, S3 waits for changes to the S3 key. When it realizes that HTTP is no longer requested, then you cannot connect to the service using the HTTP protocol.

- To update a single service, run:

```
PUT /service/{service_name}
{
  "name": "{service_name}",
  "settings": ["setting1", "setting2", "settingN"]
}
```

For example,

```
PUT /service/atmos
{
  "name": "atmos",
  "settings": ["disabled"]
}
```

- To update multiple services, run:

```
PUT /service
{
  "service": [{
    "name": "{service_name}",
    "settings": ["setting1", "setting2", "settingN"]
  },
  {
    "name": "{service_name}",
    "settings": ["setting1", "setting2", "settingN"]
  }
]
```

For example,

```
PUT /service
{ "service": [{
```

```
    "name": "s3",  
    "settings": ["http", "https"]  
  },  
  {  
    "name": "swift",  
    "settings": ["http"]  
  },  
  {  
    "name": "cas",  
    "settings": ["enabled"]  
  }  
]
```


CHAPTER 8

File Access

- [Introduction to file access](#)..... 98
- [ECS multi-protocol access](#)..... 98
- [Working with NFS exports in the ECS Portal](#)..... 101
- [Working with user/group mappings in the ECS Portal](#)..... 101
- [ECS NFS configuration tasks](#)..... 102
- [Mount an NFS export example](#)..... 112
- [NFS access using the ECS Management REST API](#)..... 114
- [NFS WORM \(Write Once, Read Many\)](#)..... 115
- [S3A support](#)..... 118
- [Geo-replication status](#)..... 119

Introduction to file access

ECS allows you to configure object buckets for access as NFS file systems using NFSv3.

In the ECS Portal, you can make ECS buckets and the directories within them accessible as file systems to Unix users by:

- creating NFS exports of ECS buckets and specifying the hosts that you want to be able to access the export.
- mapping ECS object users/groups to Unix users/groups so that the Unix users can access the NFS export.

Mapping the ECS bucket owner to a Unix ID gives that Unix user permissions on the file system. In addition, ECS allows you to assign a default custom group to the bucket so that members of a Unix group mapped to the ECS default custom group can access the bucket.

ECS NFS supports:

- multi-protocol access, so that files written using NFS can also be accessed using object protocols, and vice versa.
- Kerberos security
- advisory locking and locking over multiple sites as well as shared and exclusive locks.

The ECS NFS configuration tasks that you can perform in the ECS Portal can also be performed using the ECS Management REST API or CLI.

ECS multi-protocol access

ECS supports multi-protocol access, so that files written using NFS can also be accessed using Amazon Simple Storage Service (Amazon S3), OpenStack Swift, and EMC Atmos object protocols. Similarly, objects written using S3 and OpenStack Swift object protocols can be made available through NFS. For Atmos, objects created using the namespace interface can be listed using NFS, however, objects created using an object ID cannot. Objects and directories created using object protocols can be accessed by Unix users and by Unix group members by mapping the object users and groups.

S3/NFS multi-protocol access to directories and files

ECS supports writing objects using the S3 protocol and accessing them as files using NFS and, conversely, writing files using NFS and accessing the files as objects using the S3 protocol. You must understand how directories are managed when you use multi-protocol access.

The S3 protocol does not make provision for the creation of folders or directories.

To enable multi-protocol operation, ECS support for the S3 protocol formalizes the use of `/` and creates *directory* objects for all intermediate paths in an object name. An object named `/a/b/c.txt` results in the creation of a file object named `c.txt` and directory objects for `a` and `b`. The directory objects are not exposed to users through the S3 protocol, and are maintained only to provide multi-protocol access and compatibility with file system-based APIs. This means that ECS can display files within a directory structure when the bucket is viewed as an NFS or HDFS file system.

Limitations

- An issue can arise where both a directory object and a file object are created with the same name. This can occur in the following ways:

- A file `path1/path2` is created from NFS, then an object `path1/path2/path3` is created from S3. Because S3 allows creation of objects that have another object's name as the prefix, this operation is valid and is supported. A file and a directory called `path2` will exist.
- A directory `path1/path2` is created from NFS, then an object `path1/path2` is created from S3. This operation is a valid operation from S3 because directory `path1/path2` is not visible through the S3 API. A file and a directory called `path2` will exist.

To resolve this issue, requests from S3 always return the file, and requests from NFS always return the directory. However, this means that in the first case the file created by NFS is hidden by the object created by S3.

- NFS does not support filenames with a trailing `/` in them, but the S3 protocol does. NFS does not show these files.

Multi-protocol access permissions

Objects can be accessed using NFS and using the object service. Each access method has a way of storing permissions: Object Access Control List (ACL) permissions and File System permissions.

When an object is created or modified using the object protocol, the permissions associated with the object owner are mapped to NFS permissions and the corresponding permissions are stored. Similarly, when an object is created or modified using NFS, ECS maps the NFS permissions of the owner to object permissions and stores them.

The S3 object protocol does not have the concept of groups. Changes to group ownership or permissions from NFS do not need to be mapped to corresponding object permissions. When you create a bucket or an object within a bucket (the equivalent of a directory and a file), ECS can assign Unix group permissions, and they can be accessed by NFS users.

For NFS, the following ACL attributes are stored:

- Owner
- Group
- Other

For object access, the following ACLs are stored:

- Users
- Custom Groups
- Groups (Pre-defined)
- Owner (a specific user from Users)
- Primary Group (a specific group from Custom Groups)

For more information on ACLs, see [Set ACLs](#) on page 82.

The following table shows the mapping between NFS ACL attributes and object ACL attributes.

NFS ACL attribute	Object ACL attribute
Owner	User who is also Owner
Group	Custom Group that is also Primary Group
Others	Pre-Defined Group

Examples of this mapping are discussed later in this topic.

The following Access Control Entries (ACE) can be assigned to each ACL attribute.

NFS ACEs:

- Read (R)
- Write (W)
- Execute (X)

Object ACEs:

- Read (R)
- Write (W)
- Execute (X)
- ReadAcl (RA)
- WriteAcl (WA)
- Full Control (FC)

Creating and modifying an object using NFS and accessing using the object service

When an NFS user creates an object using the NFS protocol, the owner permissions are mirrored to the ACL of the object user who is designated as the owner of the bucket. If the NFS user has RWX permissions, Full Control is assigned to the object owner through the object ACL.

The permissions that are assigned to the group that the NFS file or directory belongs to are reflected onto a custom group of the same name, if it exists. ECS reflects the permissions associated with Others onto pre-defined groups permissions.

The following example illustrates the mapping of NFS permissions to object permissions.

NFS ACL	Setting	Object ACL	Setting
Owner	John : RWX	Users	John : Full Control
Group	ecsgroup : R-X --->	Custom Groups	ecsgroup : R-X
Other	RWX	Groups	All_Users : R, RA
		Owner	John
		Primary Group	ecsgroup

When a user accesses ECS using NFS and changes the ownership of an object, the new owner inherits the owner ACL permissions and is given Read_ACL and Write_ACL. The previous owner permissions are kept in the object user's ACL.

When a `chmod` operation is performed, the ECS reflects the permissions in the same way as when creating an object. Write_ACL is preserved in Group and Other permissions if it already exists in the object user's ACL.

Creating and modifying objects using the object service and accessing using NFS

When an object user creates an object using the object service, the user is the object owner and is automatically granted Full Control of the object. The file owner is granted RWX permissions. If the owner permissions are set to other than Full Control, ECS reflects the object RWX permissions onto the file RWX permissions. An object owner with RX permissions results in an NFS file owner with RX permissions. The object primary group, which is set using the Default Group on the bucket, becomes the Custom Group that the object belongs to and the object permissions are set based on the default permissions that have been set. These permissions are reflected onto the NFS.group permissions. If the object Custom Group has Full Control, these permissions become the RWX permissions for the NFS group. If pre-defined groups are specified on the bucket, these are applied to the object and are reflected as Others permissions for the NFS ACLs.

The following example illustrates the mapping of object permissions onto NFS permissions.

Object ACL	Setting	NFS ACL
------------	---------	---------

```

Setting
Users          John : Full Control      Owner   John : RWX
Custom Groups  ecsgroup : R-X         ----> Group  ecsgroup : R-X
Groups        All_Users : R, RA      Other   RWX
Owner         John
Primary Group ecsgroup

```

If the object owner is changed, the permissions associated with the new owner applied to the object and reflected onto the file RWX permissions .

Working with NFS exports in the ECS Portal

You can use the **Exports** tab on the **File** page available from **Manage > File** to view the details of existing NFS exports, to create new NFS exports, and to edit existing exports.

The **Exports** tab has a **Namespace** field that allows you to select the namespace for which you want to see the currently defined exports.

Table 20 NFS export properties

Field	Description
Namespace	The namespace that the underlying storage belongs to.
Bucket	The bucket that provides the underlying storage for the NFS export.
Export Path	The mount point associated with the export, in the form: / <namespace_name>/<bucket_name>/<export_name> . The export name is only be specified if you are exporting a directory that exists within the bucket.
Actions	The actions that can be completed on the NFS export. <ul style="list-style-type: none"> Edit: Edit the bucket quota and export host options. Delete: Delete the NFS export.

Working with user/group mappings in the ECS Portal

You can use the **User/Group Mapping** tab on the **File** page available from **Manage > File** to view the existing mappings between ECS object users/groups and Unix users, to create new user/group mappings, and to edit mappings.

The **User/Group Mapping** tab has a **Namespace** field that allows you to select the namespace for which you want to see the configured user/group mappings.

ECS stores the owner and group for the bucket, and the owner and group for files and directories within the bucket, as ECS object username and custom group names, respectively. The names must be mapped to Unix IDs in order that NFS users can be given access with the appropriate privileges.

The mapping enables ECS to treat an ECS object user and an NFS user as the same user but with two sets of credentials, one to access ECS using NFS, and one to access the ECS using the object protocols. Because the accounts are mapped, files written by an NFS user will be accessible as objects by the mapped object user and objects written by the object users will be accessible as files by the NFS user.

The permissions associated with the file or object will be based on a mapping between POSIX and object protocol ACL privileges. For more information, see [Multi-protocol access permissions](#) on page 99.

Field	Description
User/Group Name	The object username of the user.
ID	The Unix User ID or Group ID that has been mapped to the object user.
Type	Indicates whether the ID is for a User or Group.
Actions	The actions that can be completed on the user or group mapping. They are: View and Delete

ECS NFS configuration tasks

You must perform the following tasks to configure ECS NFS.

Procedure

1. [Create a bucket for NFS using the ECS Portal](#) on page 102
2. [Add an NFS export using the ECS Portal](#) on page 104
3. [Add a user or group mapping using the ECS Portal](#) on page 105
4. [Configure ECS NFS with Kerberos security](#) on page 106

After you finish

After you perform the above steps, you can [mount the NFS export on the export host](#).

Create a bucket for NFS using the ECS Portal

You can use the ECS Portal to create a bucket configured for use with NFS.

Before you begin

- This operation requires the Namespace Administrator or System Administrator role in ECS.
- If you are a Namespace Administrator, you can create buckets in your namespace.
- If you are System Administrator, you can create a bucket belonging to any namespace.

About this task

The steps provided here focus on the configuration you need to perform to make a bucket suitable for use by NFS. The bucket that you create is an S3 bucket that is enabled for file system use.

Procedure

1. In the ECS Portal, select **Manage > Buckets > New Bucket**.
2. On the **New Bucket** page, in the **Name** field, type a name for the bucket.
3. In the **Namespace** field, select the namespace that the bucket belongs to.
4. In the **Replication Group** field, select a replication group or leave blank to use the default replication group for the namespace.
5. In the **Bucket Owner** field, type the name of the bucket owner.
6. On the **Required** page, in the **File System** field, click **On**.

Once file system access is enabled, the fields for setting a default group for the file system/ bucket and for assigning group permissions for files and directories that are created in the bucket are available.

7. In the **Default Bucket Group** field, type a name for the default bucket group.

This group is the group that is associated with the NFS root file system and with any files or directories that are created in the NFS export. It enables users who are members of the group to access the NFS export and to access files and directories.

This group must be specified at bucket creation. If it is not, the group would have to be assigned later from the NFS client.

8. Set the default permissions for files and directories that are created in the bucket using the object protocol.

These settings are used to apply UNIX group permissions to objects created using object protocols.

The S3 protocol does not have the concept of groups. Thus there is no opportunity for setting group permissions in S3 and mapping them to UNIX permissions. Hence, this provides a one-off opportunity for a file or directory created using the S3 protocol to be assigned to the specified default group with the permissions specified here.


- a. Set the **Group File Permissions** by clicking the appropriate permission buttons.

You normally set Read and Execute permissions.

- b. Set the **Group Directory Permissions** by clicking the appropriate permission buttons.

You normally set Read and Execute permissions.

9. In the **CAS** field, do not enable CAS.


 **Note:** A bucket that is intended for use as NFS cannot be used for CAS. The **CAS** field is disabled when the **File System** field is enabled.

10. Enable any other bucket features that you require.

You can enable any of the following features on an NFS bucket:

- Quota
- Server-side Encryption
- Metadata Search
- Access During Outage
- Read-Only Access During Outage
- Bucket Retention Period

For information about these settings, see [Bucket settings](#) on page 76.

 **Note:** A bucket that is compliance-enabled cannot be written to using the NFS protocol. However, data that are written using object protocols can be read from NFS.

11. Click **Save** to create the bucket.

Add an NFS export using the ECS Portal

You can use the ECS Portal to create an NFS export and set the options that control access to the export.

Before you begin

- This operation requires the Namespace Administrator or System Administrator role in ECS.
- If you are a Namespace Administrator, you can add NFS exports into your namespace.
- If you are System Administrator, you can add NFS exports into any namespace.
- You must have created a bucket to provide the underlying storage for the export. For more information, see [Create a bucket for NFS using the ECS Portal](#) on page 102.

Procedure

1. In the ECS Portal, select **File > Exports > New Export**.

The **New File Export** page is displayed.

2. On the **New File Export** page, in the **Namespace** field, select the namespace that owns the bucket that you want to export.
3. In the **Bucket** field, select the bucket.
4. In the **Export Path** field, specify the path.

ECS automatically generates the export path that is based on the namespace and bucket. You only have to enter a name if you are exporting a directory that exists within the bucket. So if you enter `/namespace1/bucket1/dir1`, for example, you should ensure that `dir1` exists. If it does not, mounting the export fails.

5. Set the **Show Bucket Quota** option to **No** or **Yes** depending on how you want the export size to be reported.

Option	Description
No	The export size is reported as the storage pool size.
Yes	The export size is reported as the hard quota on the bucket, if set.

6. To add the hosts that you want to be able to access the export, complete the following steps:



- a. In the **Export Host Options** area, click **Add**.


The **Add Export Host** dialog is displayed.

- b. In the **Add Export Host** dialog, specify one or more hosts that you want to be able to access the export and configure the access options.

You must choose an **Authentication** option. This is normally `sys` unless you are intending to configure Kerberos. Default values for Permissions (`ro`) and Write Transfer Policy (`async`) are already set in the **Add Export Host** dialog and are passed to the NFS server. The remaining options are the same as the NFS server defaults and so are only passed by ECS if you change them.

The following table describes the parameters that you can specify when you add a host:

Setting	Description
Export Host	Sets the IP address of the host or hosts that can access the export. Use a comma-separated list to specify more than one host.
Permissions	Enables access to the export to be set as Read/Write or Read only. This is the same as setting <code>rw</code> or <code>ro</code> in <code>/etc/exports</code> .
Write Transfer Policy	Sets the write transfer policy as synchronous or asynchronous. The default is asynchronous. This parameter is the same as setting <code>sync</code> or <code>async</code> for an export in <code>/etc/exports</code> .
Authentication	Sets the authentication types that are supported by the export.
Mounting Directories Inside Export	Specifies whether subdirectories of the export path are allowed as mount points. This parameter is the same as the <code>alldir</code> setting in <code>/etc/exports</code> . With the <code>alldir</code> option, if you exported <code>/namespace1/bucket1</code> , for example, you can also mount subdirectories, such as <code>/namespace1/bucket1/dir1</code> , provided the directory exists.
AnonUser	An object user name (must have an entry in user/group mapping) to which all unknown (not mapped using the user/group mapping) user IDs will be mapped when accessing the export.  Note: For performance reasons, user mapping must be predefined and can be selected here.
AnonGroup	An object group name (must have an entry in user/group mapping) to which all unknown (not mapped using the user/group mapping) group IDs will be mapped when accessing the export.  Note: For performance reasons, group mapping must be predefined and can be selected here.
RootSquash	An object user name to which the root user ID (0) will be mapped when accessing the export.

 **Note:** The AnonUser/AnonGroup is the object user/group name that is used to map any incoming user id. This overrides user mapping provided at the Namespace level.

- c. Click **Add** to finish defining the host options.
7. If you want to add more hosts that can access the export, but with different options, repeat the previous step.
8. Click **Save** to save the NFS export definition.

After you finish

[Add a user or group mapping using the ECS Portal](#) on page 105.

Add a user or group mapping using the ECS Portal

To provide NFS access to the file system (the bucket), you must map an object user who has permissions on the bucket to a UNIX User ID (UID) so that the UNIX user acquires the same permissions as the object user. Alternatively, you can map an ECS custom group that has permissions on the bucket to a UNIX Group ID (GID) to provide access for members of the UNIX group.

Before you begin

- This operation requires the Namespace Administrator or System Administrator role in ECS.
- If you are a Namespace Administrator, you can add user or group mappings into your namespace.
- If you are System Administrator, you can add user or group mappings into any namespace.
- For mapping a single ECS object user to a UNIX user:

- ■ Ensure that the UID exists on the NFS client and the username is an ECS object username.
- For mapping a group of ECS object users to a group of UNIX users:
 - ■ Ensure that a default custom group has been assigned to the bucket (either a [default group](#) that was assigned at bucket creation, or a [custom group ACL](#) that was set after bucket creation). In order for UNIX group members to have access to the file system, a default custom group must be assigned to the bucket and the UID for each member of the group must be known to ECS. In other words, there must be a UNIX UID mapping for each member of the group in ECS.
 - ■ Ensure that default object and directory permissions have been assigned to the bucket in order that group members have access to objects and directories created using object protocols.

Procedure

1. In the ECS Portal, select **Manage > File** and click the **User/Group Mapping** tab.
2. Click **New User/Group Mapping**.
The **New User/Group Mapping** page is displayed.
3. In the **User/Group Name** field, type the name of the ECS object user or ECS custom group that you want to map to a UNIX UID or GID.
4. In the **Namespace** field, select the namespace that the ECS object user or custom group belongs to.
5. In the **ID** field, enter the UNIX UID or GID that you want the ECS user or group to map to.
6. In the **Type** field, click the type of mapping: **User** or **Group** so that ECS knows that the ID you have entered is a UID or a GID.
7. Click **Save**.

Configure ECS NFS with Kerberos security

To configure Kerberos authentication with ECS NFS, you must configure both the ECS nodes and the NFS client, and create keytabs for the NFS server principal and for the NFS client principal.

Before you begin

Depending on your internal IT setup, you can use a Key Distribution Center (KDC) or you can use Active Directory (AD) as your KDC.

To use AD, follow the steps in these tasks:

- [Register an ECS node with Active Directory](#) on page 110
- [Register a Linux NFS client with Active Directory](#) on page 111

About this task

The following scenarios are supported:

- ECS client to single ECS node. The keytab on each ECS that you want to use as the NFS server must be specific to that node.
- ECS client to load balancer. The keytab on all ECS nodes is the same, and uses the hostname of the load balancer.

Procedure

1. Ensure that the hostname of the ECS node can be resolved.

You can use the `hostname` command to ensure that the FQDN of the ECS node is added to `/etc/HOSTNAME`.

```
dataservice-10-247-142-112:~ # hostname ecsnode1.yourco.com
dataservice-10-247-142-112:~ # hostname -i
10.247.142.112
dataservice-10-247-142-112:~ # hostname -f
ecsnode1.yourco.com
dataservice-10-247-142-112:~ #
```

2. Create the Kerberos configuration file (`krb5.conf`) on the ECS node as `/opt/emc/caspian/fabric/agent/services/object/data/hdfs/krb5.conf`. Unless HDFS has already been configured, you must create the `hdfs` directory with 755 (`drwxr-xr-x`) permissions (`chmod 755 hdfs`) and make user with uid 444 and group with gid 444 as the owner (`chown 444:444 hdfs`).

Change the file permissions to 644 and make the user with id 444(`storageos`) the owner of the file.

In the example below, the following values are used and must be replaced with your own settings.

Kerberos REALM

Set to `NFS-REALM` in this example.

KDC

Set to `kdcname.yourco.com` in this example.

KDC Admin Server

In this example, the KDC acts as the admin server.

```
[libdefaults]
    default_realm = NFS-REALM.LOCAL
[realms]
    NFS-REALM.LOCAL = {
        kdc = kdcname.yourco.com
        admin_server = kdcname.yourco.com
    }
[logging]
    kdc = FILE:/var/log/krb5/krb5kdc.log
    admin_server = FILE:/var/log/krb5/kadmind.log
    default = SYSLOG:NOTICE:DAEMON
```



Note:

If HDFS for Kerberos is already configured, instead of replacing `/opt/emc/caspian/fabric/agent/services/object/data/hdfs/krb5.conf`, merge the REALM information, if it is different, into the existing `krb5.conf` file. Usually there is no change to this file as REALM has been configured by HDFS. In addition, the default permissions and owner should have already been configured by HDFS and should not require any change.

3. Add a host principal for the ECS node and create a keytab for the principal.

In this example, the FQDN of the ECS node is `ecsnodel.yourco.com`

```
$ kadmin
kadmin> addprinc -randkey nfs/ecsnodel.yourco.com
kadmin> ktadd -k /datanode.keytab nfs/ecsnodel.yourco.com
kadmin> exit
```

4. Copy the keytab (`datanode.keytab`) to `/opt/emc/caspian/fabric/agent/services/object/data/hdfs/krb5.keytab`. Unless HDFS has already been configured, you need to create the `hdfs` directory with 755 (`drwxr-xr-x`) permissions (`chmod 755 hdfs`) and make user with uid 444 and group with gid 444 as the owner (`chown 444:444 hdfs`).

Change its file permissions to 644 and make the user with id 444 (`storageos`) the owner of the file.

If HDFS is already configured, instead of replacing `/opt/emc/caspian/fabric/agent/services/object/data/hdfs/krb5.keytab`, merge the `datanode.keytab` file into the existing keytab file using `ktutil`. Default permissions and owner should already be configured by HDFS and should not require any change.

5. Download the *unlimited* JCE policy archive from `oracle.com` and extract it to the `/opt/emc/caspian/fabric/agent/services/object/data/jce/unlimited` directory.

Kerberos may be configured to use a strong encryption type, such as AES-256. In that situation, the JRE within the ECS nodes must be reconfigured to use the 'unlimited' policy.

 **Note:** This step should be performed only if you are using a strong encryption type.

If HDFS is already configured, this step would have been completed by HDFS Kerberos configuration.

6. Run the following command from inside the object container.

```
service storageos-dataservice restarthdfs
```

7. To set up the client, begin by making sure that the hostname of the client can be resolved.

You can use the `hostname` command to ensure that the FQDN of the ECS node is added to `/etc/HOSTNAME`.

```
dataservice-10-247-142-112:~ # hostname ecsnodel.yourco.com
dataservice-10-247-142-112:~ # hostname -i
10.247.142.112
dataservice-10-247-142-112:~ # hostname -f
ecsnodel.yourco.com
dataservice-10-247-142-112:~ #
```

8. If your client is running SUSE Linux make sure that line `NFS_SECURITY_GSS="yes"` is uncommented in `/etc/sysconfig/nfs`.
9. If you are on Ubuntu make sure to have line `NEED_GSSD=yes` in `/etc/default/nfs-common`.

10. Install `rpcbind` and `nfs-common`.

Use `apt-get` or `zypper`. On SUSE Linux, for `nfs-common`, use:

```
zypper install yast2-nfs-common
```

By default these are turned off in Ubuntu client.

11. Set up your Kerberos configuration file.

In the example below, the following values are used and you must replace them with your own settings.

Kerberos REALM

Set to `NFS-REALM` in this example.

KDC

Set to `kdcname.yourco.com` in this example.

KDC Admin Server

In this example, the KDC acts as the admin server.

```
[libdefaults]
    default_realm = NFS-REALM.LOCAL
[realms]
    NFS-REALM.LOCAL = {
        kdc = kdcname.yourco.com
        admin_server = kdcname.yourco.com
    }
[logging]
    kdc = FILE:/var/log/krb5/krb5kdc.log
    admin_server = FILE:/var/log/krb5/kadmind.log
    default = SYSLOG:NOTICE:DAEMON
```

12. Add a host principal for the NFS client and create a keytab for the principal.

In this example, the FQDN of the NFS client is `nfsclient.yourco.com`

```
$kadmin
kadmin> addprinc -randkey host/nfsclient.yourco.com
kadmin> ktadd -k /nkclient.keytab host/nfsclient.yourco.com
kadmin> exit
```

13. Copy the keytab file (`nfsclient.keytab`) from the KDC machine to `/etc/krb5.keytab` on the NFS client machine.

```
scp /nkclient.keytab root@nfsclient.yourco.com:/etc/krb5.keytab
ssh root@nfsclient.yourco.com 'chmod 644 /etc/krb5.keytab'
```

14. Create a principal for a user to access the NFS export.

```
$kadmin
kadmin> addprinc yourusername@NFS-REALM.LOCAL
kadmin> exit
```

15. Log in as root and add the following entry to your `/etc/fstab` file.

```
HOSTNAME:MOUNTPOINT    LOCALMOUNTPOINT      nfs
rw,user,nolock,noauto,vers=3,sec=krb5 0    0
```

For example:

```
ecsnode1.yourco.com:/s3/b1    /home/kothan3/lb1    nfs
rw,user,nolock,noauto,vers=3,sec=krb5 0 0
```

16. Log in as non root user and `kinit` as the non-root user that you created.

```
kinit yourusername@NFS-REALM.LOCAL
```

17. You can now mount the NFS export. For more information, see [Mount an NFS export example](#) on page 112 and [Best practices for mounting ECS NFS exports](#) on page 114.



Note:

Mounting as the root user does not require you to use `kinit`. However, when using root, authentication is done using the client machine's host principal rather than your Kerberos principal. Depending upon your operating system, you can configure the authentication module to fetch the Kerberos ticket when you login, so that there is no need to fetch the ticket manually using `kinit` and you can mount the NFS share directly.

Register an ECS node with Active Directory

To use Active Directory (AD) as the KDC for your NFS Kerberos configuration, you must create accounts for the client and server in AD and map the account to a principal. For the NFS server, the principal represents the NFS service accounts, for the NFS client, the principal represents the client host machine.

Before you begin

You must have administrator credentials for the AD domain controller.

Procedure

1. Log in to AD.
2. In Server Manager, go to **Tools > Active Directory Users and Computers**.
3. Create a user account for the NFS principal using the format "nfs-<host>" , for example, "nfs-ecsnode1". Set a password and set the password to never expire.
4. Create an account for yourself (optional and one time).

- Execute the following command to create a keytab file for the NFS service account.

```
ktpass -princ nfs/<fqdn>REALM.LOCAL +rndPass -mapUser nfs-
<host>@REALM.LOCAL -mapOp set -crypto All -ptype KRB5_NT_PRINCIPAL -out
filename.keytab
```

For example, to associate the `nfs-ecsnode1` account with the principle `nfs/ecsnode1.yourco.com@NFS-REALM.LOCAL`, you can generate a keytab using:

```
ktpass -princ nfs/ecsnode1.yourco.com@NFS-REALM.LOCAL +rndPass -mapUser
nfs-ecsnode1@NFS-REALM.LOCAL -mapOp set -crypto All -ptype
KRB5_NT_PRINCIPAL -out nfs-ecsnode1.keytab
```

- Import the keytab to the ECS node.

```
ktutil
ktutil> rkt <keytab to import>
ktutil> wkt /etc/krb5.keytab
```

- Test registration by running.

```
kinit -k nfs/<fqdn>@NFS-REALM.LOCAL
```

- See the cached credentials by running the `klist` command.
- Delete the cached credentials by running the `kdestroy` command.
- View the entries in the keytab file by running the `klist` command.

Example:

```
klist -kte /etc/krb5.keytab
```

- Follow steps 2 on page 107, 4 on page 108, and 5 on page 108 from [Configure ECS NFS with Kerberos security](#) on page 106 to place the Kerberos configuration files (`krb5.conf`, `krb5.keytab` and `jce/unlimited`) on the ECS node.

Register a Linux NFS client with Active Directory

To use Active Directory (AD) as the KDC for your NFS Kerberos configuration, you must create accounts for the client and server in AD and map the account to a principal. For the NFS server, the principal represents the NFS service accounts, for the NFS client, the principal represents the client host machine.

Before you begin

You must have administrator credentials for the AD domain controller.

Procedure

- Log in to AD.
- In Server Manager, go to **Tools > Active Directory Users and Computers**.
- Create a computer account for the client machine (for example, "nfsclient"). Set the password to never expire.

4. Create an account for a user (optional and one time)
5. Execute the following command to create a keytab file for the NFS service account.

```
ktpass -princ host/<fqdn>@REALM.LOCAL +rndPass -mapUser
<host>@REALM.LOCAL -mapOp set -crypto All -ptype KRB5_NT_PRINCIPAL -out
filename.keytab
```

For example, to associate the `nfs-ecsnode1` account with the principle `host/nfsclient.yourco.com@NFS-REALM.LOCAL`, you can generate a keytab using:

```
ktpass -princ host/nfsclient.yourco.com@NFS-REALM.LOCAL +rndPass -
mapUser nfsclient$@NFS-REALM.LOCAL -mapOp set -crypto All -ptype
KRB5_NT_PRINCIPAL -out nfsclient.keytab
```

6. Import the keytab to the client node.

```
ktutil
ktutil> rkt <keytab to import>
ktutil> wkt /etc/krb5.keytab
```

7. Test registration by running.

```
kinit -k host/<fqdn>@NFS-REALM.LOCAL
```

8. See the cached credentials by running the `klist` command.
9. Delete the cached credentials by running the `kdestroy` command.
10. View the entries in the keytab file by running the `klist` command.

```
klist -kte /etc/krb5.keytab
```

11. Follow steps 2 on page 107, 4 on page 108, and 5 on page 108 from [Configure ECS NFS with Kerberos security](#) on page 106 to place the Kerberos configuration files (`krb5.conf`, `krb5.keytab` and `jce/unlimited`) on the ECS node.

Mount an NFS export example

When you mount an export, you must ensure that the following prerequisites steps are carried out:

- The bucket owner name is mapped to a Unix UID.
- A default group is assigned to the bucket and the name of the default group is mapped to a Linux GID. This ensures that the default group shows as the associated Linux group when the export is mounted.
- You review the [Best practices for mounting ECS NFS exports](#) on page 114.

The following steps provide an example of how to mount an ECS NFS export file system.

1. Create a directory on which to mount the export. The directory should belong to the same owner as the bucket.

In this example, the user `fred` creates a directory `/home/fred/nfsdir` on which to mount an export.

```
su - fred
mkdir /home/fred/nfsdir
```

2. As the root user, mount the export in the directory mount point that you created.

```
mount -t nfs -o "vers=3,noexec" 10.247.179.162:/s3/tc-nfs6 /home/fred/nfsdir
```

When mounting an NFS export, you can specify the name or IP address of any of the nodes in the VDC or the address of the load balancer.

It is important that you specify `-o "vers=3"`.

3. Check that you can access the file system as user `fred`.

a. Change to user `fred`.

```
$ su - fred
```

b. Check you are in the directory in which you created the mount point directory.

```
$ pwd
/home/fred
```

c. List the directory.

```
fred@lrmh229:~$ ls -al
total
drwxr-xr-x  7 fred  fredsgroup   4096 May 31 05:38 .
drwxr-xr-x 18 root   root         4096 May 30 04:03 ..
-rw-----  1 fred  fred          16 May 31 05:31 .bash_history
drwxrwxrwx  3 fred  anothergroup 96 Nov 24 2015 nfsdir
```

In this example, the bucket owner is `fred` and a default group, `anothergroup`, was associated with the bucket.

If no group mapping had been created, or no default group has been associated with the bucket, you will not see a group name but a large numeric value, as shown below.

```
fred@lrmh229:~$ ls -al
total
drwxr-xr-x  7 fred  fredssgroup 4096 May 31 05:38 .
drwxr-xr-x 18 root   root         4096 May 30 04:03 ..
-rw-----  1 fred  fred          16 May 31 05:31 .bash_history
drwxrwxrwx  3 fred  2147483647   96 Nov 24 2015 nfsdir
```

If you have forgotten the group mapping, you can create appropriate mapping in the ECS Portal.

You can find the group ID by looking in `/etc/group`.

```
fred@lrmh229:~$ cat /etc/group | grep anothergroup
anothergroup:x:1005:
```

And adding a mapping between the name and GID (in this case: `anothergroup => GID 1005`).

If you try and access the mounted file system as the root user, or another user that does not have permissions on the file system, you will see `?`, as below.

```
root@lrnh229:~# cd /home/fred
root@lrnh229:/home/fred# ls -al
total
drwxr-xr-x  8 fred  fredsgroup 4096 May 31 07:00 .
drwxr-xr-x 18 root   root       4096 May 30 04:03 ..
-rw-----  1 fred   fred       1388 May 31 07:31 .bash_history
d????????? ? ?    ?           ?         ?   nfsdir
```

Best practices for mounting ECS NFS exports

The following best practices apply when you mount ECS NFS exports.

Use `async`

Whenever possible, use the `async` mount option. This option dramatically reduces latency, improves throughput, and reduces the number of connections from the client.

Set `wsize` and `rsize` to reduce round trips from the client

Where you expect to read and/or write large files, ensure that the read or write size of files is set appropriately using the `rsize` and `wsize` mount options. Usually, you set the `wsize` and `rsize` options to the highest possible value to reduce the number of round trips from the client. This is typically 512 KB (524288 B).

For example, to write a 10 MB file, if the `wsize` option is set to 524288 (512 KB), the client makes 20 separate calls. If the write size is set as 32 KB this results in 16 times as many calls.

When using the mount command, you can supply the read and write size using the options (`-o`) switch. For example:

```
# mount 10.247.97.129:/home /home -o "vers=3,nolock,rsize=524288,wsize=524288"
```

NFS access using the ECS Management REST API

You can use the following APIs to configure and manage NFS access.

Table 21 ECS Management REST API calls for managing NFS access

Method	Description
POST /object/nfs/exports	Creates an export. The payload specifies the export path, the hosts that can access the export, and a string that defines the security settings for the export.
PUT/GET/DELETE /object/nfs/exports/{id}	Performs the selected operation on the specified export.
GET /object/nfs/exports	Retrieves all user exports that are defined for the current namespace.
POST /object/nfs/users	Creates a mapping between an ECS object user name or group name and a Unix user or group ID.
PUT/GET/DELETE /object/nfs/users/{mappingid}	Performs the selected operation on the specified user or group mapping.

Table 21 ECS Management REST API calls for managing NFS access (continued)

Method	Description
GET /object/nfs/users	Retrieves all user mappings that are defined for the current namespace.

The ECS Management REST API documentation provides full details of the API and the documentation for the NFS export methods can be accessed in the [ECS API Reference](#).

NFS WORM (Write Once, Read Many)

NFS data become Write Once Read Many (WORM) compliant when autocommit is implemented on it.

In detail, creating files through NFS is a multi step process. To write to a new file, NFS client first sends the CREATE request with no payload to NFS server. After receiving a response, the server issues a WRITE request. It is a problem for FS enabled buckets under retention as the file created with 0 bytes blocks any writes to it. Due to this reason, until ECS 3.3, retention on FS enabled bucket makes the whole mounted file-system read-only. There is no End of File (EOF) concept in NFS. Thus, setting a retention for files, on the FS enabled buckets, after writing to them does not work as expected.


To remove the constraints that are placed on NFS files in a retention enabled bucket, the autocommit period is implemented on NFS data. For this reason, it is decided to introduce the autocommit period during which certain types of updates (for now identified as writes, Acl updates and deletes that are required for rsync, and rename that is required for Vim editor) are allowed, which removes the retention constraints for that period alone.

Note:

- The autocommit and the Atmos retention start delay are the same.
- Autocommit period is a bucket property like retention period.
- Autocommit period is,
 - Applicable only for the file system enabled buckets with retention period
 - Applicable to the buckets in noncompliant namespace
 - Applies to only requests from NFS and Atmos

Seal file

The seal file functionality helps to commit the file to WORM state when the file is written, ignoring the remaining autocommit period. The seal function is performed through the command: `chmod ugo-w <file>` on the file.

 **Note:** The seal functionality does not have any effect outside the retention period.

High level overview

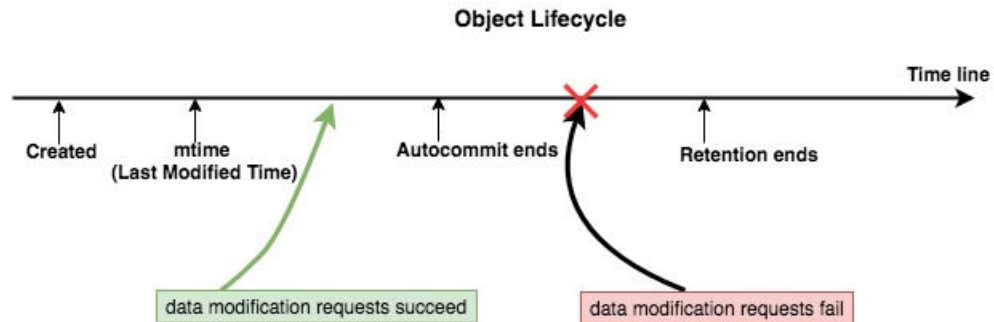
Table 22 Autocommit terms

Term	Description
Autocommit period	Time interval relative to the object's last modified time during which certain retention constraints (example: file modifications, file deletions, and so on) are not applied. This does not have any effect outside of the retention period.

Table 22 Autocommit terms (continued)

Term	Description
Retention Start Delay	Atmos head uses the start delay to indicate the autocommit period.

The following diagram provides an overview of the autocommit period behavior:



Autocommit configuration

The autocommit period can be set from the user interface or bucket REST API or S3 head or Atmos subtenant API.

User Interface

The user interface has the following support during bucket create and edit:

- When the File System is not enabled, no autocommit option is displayed.
- When the File System is enabled /no retention value is specified, autocommit is displayed but disabled.
- When the File System is enabled/retention value selected/autocommit is displayed and enabled for selection.

Note: Maximum autocommit period is limited to the smaller of the Bucket Retention period or the default maximum period of one day.

REST API

Create bucket REST API is modified with the new header, `x-emc-autocommit-period`.

```
lglou063:~ # curl -i -k -T /tmp/bucket -X POST https://10.247.99.11:4443/object/bucket -H "$token" -H "Content-Type: application/xml" -v
```

```
The contents of /tmp/bucket
<object_bucket_create>
  <name>bucket2</name>
  <namespace>s3</namespace>
  <filesystem_enabled>>true</filesystem_enabled>
  <autocommit_period>300</autocommit_period>
  <retention>1500</retention>
</object_bucket_create>
```

S3 head

Bucket creation

Bucket creation flow through s3 head can make use of optional request header, `x-emc-autocommit-period:seconds` to set the autocommit period. The following checks are made in this flow:

- Allow only positive integers
- Settable only for file system buckets
- Settable only when the retention value is present

```
./s3curl.pl --ord --id=naveen --key=+1Zh4YC2r2puuUaj3Lbnj3u0G9qgPRj0RIWJhPxH
--createbucket -- -H 'x-emc-autocommit-period:600' -H 'x-emc-file-system-
access-enabled:true' -H 'x-emc-namespace:ns1' http://10.249.245.187:9020/
bucket5 -v
```

Atmos

Atmos creates a subtenant request header, `x-emc-retention-start-delay`, captures the autocommit interval.

```
./atmoscurl.pl -user USER1 -action PUT -pmode TID -path / -header "x-emc-
retention-period:300" -header "x-emc-retention-start-delay:120" -include
```

Behavior of file operations

File Operation	Expected within autocommit period	Expected within retention period (after autocommit period)
Change permission of file	Allowed	Denied
Change ownership of file	Allowed	Denied
Write to existing file	Allowed	Denied
Create empty file	Allowed	Allowed
Create non empty file	Allowed	Denied
Remove file	Allowed	Denied
Move file	Allowed	Denied
Rename file	Allowed	Denied
Make dir	Allowed	Allowed
Remove directory	Denied	Denied
Move directory	Denied	Denied
Rename directory	Denied	Denied
Change permission on directory	Denied	Denied
list	Allowed	Allowed
Read file	Allowed	Allowed
Truncate file	Allowed	Denied
Copy of local read-only files to NFS share	Allowed	Allowed
Copy of read-only files from NFS share to NFS share	Allowed	Allowed

File Operation	Expected within autocommit period	Expected within retention period (after autocommit period)
Change atime/mtime of file/ directory	Allowed	Denied

S3A support

The AWS S3A client is a connector for HDFS (Hadoop Distributed File System), which enables you to run MapReduce jobs with ECS S3.

Note: S3A support is available on Hadoop 2.7 or later version.

Configuration at ECS

About this task

To use S3A on Hadoop, do the following:

Procedure

1. Create an object user having S3 credentials.
2. Create a normal object bucket at ECS UI.
ECS does not enable you to run S3A client on FS enabled buckets.
3. Make the object user as the owner of the bucket.
4. Copy the S3 secret key that has to be put at HDP Ambari node.

Configuration at Ambari Node

About this task

Following are some of the basic configurations which should be added to make S3A work at Ambari UI > HDFS > core-site.xml. There are other parameters that can be added to the Ambari node. All these parameters are listed [here](#).

Note: Putting S3A credentials to Ambari UI leads to security vulnerability. Follow a secured way of passing credentials as shown in #c. The following list of configuration should be added in core-site.xml on Ambari UI:

```
fs.s3a.endpoint= <ECS IP address (only one node address) or LoadBalancer IP>:9020
#Comment //s3a does not support multiple IP addresses so better to have a
loadbalancer
fs.s3a.access.key= <S3 Object User as created on ECS>
fs.s3a.secret.key=<S3 Object User Secret Key as on ECS>
fs.s3a.connection.maximum=15
fs.s3a.connection.ssl.enabled=false
fs.s3a.path.style.access=false
fs.s3a.connection.establish.timeout=5000
fs.s3a.connection.timeout=200000
fs.s3a.paging.maximum=1000
fs.s3a.threads.max=10
fs.s3a.socket.send.buffer=8192
fs.s3a.socket.recv.buffer=8192
fs.s3a.threads.keepalivetime=60
fs.s3a.max.total.tasks=5
fs.s3a.multipart.size=100M
fs.s3a.multipart.threshold=2147483647
fs.s3a.multiobjectdelete.enable=true
fs.s3a.acl.default=PublicReadWrite
```

```
fs.s3a.multipart.purge=false
fs.s3a.multipart.purge.age=86400
fs.s3a.block.size=32M
fs.s3a.readahead.range=64K
fs.s3a.buffer.dir=${hadoop.tmp.dir}/s3a
```

Significance of each parameter:

```
fs.s3a.access.key - Your AWS access key ID
fs.s3a.secret.key - Your AWS secret key
fs.s3a.connection.maximum - Controls how many parallel connections HttpClient
spawns (default: 15)
fs.s3a.connection.ssl.enabled - Enables or disables SSL connections to S3
(default: true)
fs.s3a.attempts.maximum - How many times we should retry commands on
transient errors (default: 10)
fs.s3a.connection.timeout - Socket connect timeout (default: 5000)
fs.s3a.paging.maximum - How many keys to request from S3 when doing directory
listings at a time (default: 5000)
fs.s3a.multipart.size - How big (in bytes) to split a upload or copy
operation up into (default: 100 MB)
fs.s3a.multipart.threshold - Until a file is this large (in bytes), use non-
parallel upload (default: 2 GB)
fs.s3a.acl.default - Set a canned ACL on newly created/copied objects
(PublicRead | PublicReadWrite | AuthenticatedRead |
LogDeliveryWrite | BucketOwnerRead | BucketOwnerFullControl)
fs.s3a.multipart.purge - True if you want to purge existing multipart uploads
that may not have been completed/aborted correctly (default: false)
fs.s3a.multipart.purge.age - Minimum age in seconds of multipart uploads to
purge (default: 86400)
fs.s3a.buffer.dir - Comma separated list of directories that will be used to
buffer file writes out of (default: uses fs.s3.buffer.dir)
fs.s3a.server-side-encryption-algorithm - Name of server side encryption
algorithm to use for writing files (e.g. AES256) (default: null)
```

For details, see [here](#).

Add this parameter in your command line while copying a large file: `-D`

`fs.s3a.fast.upload=true`. For details, see [here](#).

Geo-replication status

The ECS S3 head supports Geo replication status of an object with `replicationInfo`. It API retrieves Geo replication status of an object using `replicationInfo`. This automates their capacity management operations, enable site reliability operations and ensures that the critical date is not deleted accidentally.

Retrieves Geo replication status of an object by API to confirm that the object has been successfully replicated.

```
Request:
GET /bucket/key?replicationInfo

Response:
<ObjectReplicationInfo xmlns="http://s3.amazonaws.com/doc/
2006-03001/"
  <IndexReplicated>false</IndexReplicated>
```

```
<ReplicatedDataPercentage>64.0</ReplicatedDataPercentage>  
</ObjectReplicationInfo>
```


CHAPTER 9

Certificates

- [Introduction to certificates](#)..... 122
- [Generate certificates](#)..... 122
- [Upload a certificate](#)..... 130
- [Verify installed certificates](#)..... 136

Introduction to certificates

ECS ships with an SSL certificate installed in the keystore for each node. This certificate is not trusted by applications that talk to ECS, or by the browser when users access ECS through the ECS Portal.

To prevent users from seeing an untrusted certificate error, or to allow applications to communicate with ECS, you should install a certificate signed by a trusted Certificate Authority (CA). You can generate a self-signed certificate to use until you have a CA signed certificate. The self-signed certificate is installed into the certificate store of any machines that will access ECS.

ECS uses the following types of SSL certificates:

Management certificates

Used for management requests using the ECS Management REST API. These HTTPS requests use port 4443.

Object certificates

Used for requests using the supported object protocols. These HTTPS requests use ports 9021 (S3), 9023 (Atmos), 9025 (Swift).

You can upload a self-signed certificate, a certificate signed by a CA authority, or, for an object certificate, you can request ECS to generate a certificate or you. The key/certificate pairs can be uploaded to ECS by using the ECS Management REST API on port 4443.

Generate certificates

You can generate a self-signed certificate, or you can purchase a certificate from a certificate authority (CA). The CA-signed certificate is strongly recommended for production purposes because it can be validated by any client machine without any extra steps.

Certificates must be in PEM-encoded x509 format.

When you generate a certificate, you typically specify the hostname where the certificate is used. Because ECS has multiple nodes, and each node has its own hostname, installing a certificate created for a specific hostname could cause a common name mismatch error on the nodes that do not have that hostname. You can create certificates with alternative IPs or hostnames called Subject Alternative Names (SANs).

For maximum compatibility with object protocols, the Common Name (CN) on your certificate must point to the wildcard DNS entry used by S3, because S3 is the only protocol that utilizes virtually-hosted buckets (and injects the bucket name into the hostname). You can specify only one wildcard entry on an SSL certificate and it must be under the CN. The other DNS entries for your load balancer for the Atmos and Swift protocols must be registered as a Subject Alternative Names (SANs) on the certificate.

The topics in this section show how to generate a certificate or certificate request using `openssl`, however, your IT organization may have different requirements or procedures for generating certificates.

Create a private key

You must create a private key to sign self-signed certificates and to create signing requests.

About this task

SSL uses public-key cryptography which requires a private and a public key. The first step in configuring it is to create a private key. The public key is created automatically, using the private key, when you create a certificate signing request or a certificate.

The following steps describe how to use the `openssl` tool to create a private key.

Procedure

1. Log in to an ECS node or to a node that you can connect to the ECS cluster.
2. Use the `openssl` tool to generate a private key.

For example, to create a key called `server.key`, use:

```
openssl genrsa -des3 -out server.key 2048
```

3. When prompted, enter a passphrase for the private key and reenter it to verify. You will need to provide this passphrase when creating a self-signed certificate or a certificate signing request using the key.

You must create a copy of the key with the passphrase removed before uploading the key to ECS. For more information, see [Upload a certificate](#) on page 130.

4. Set the permissions on the key file.

```
chmod 0400 server.key
```

Generate a SAN configuration

If you want your certificates to support Subject Alternative Names (SANs), you must define the alternative names in a configuration file.

About this task

OpenSSL does not allow you to pass Subject Alternative Names (SANs) through the command line, so you must add them to a configuration file first. To do this, you must locate your default OpenSSL configuration file. On Ubuntu, it is located at `/usr/lib/ssl/openssl.cnf`.

Procedure


1. Create the configuration file.

```
cp /usr/lib/ssl/openssl.cnf request.conf
```

2. Edit the configuration file with a text editor and make the following changes.
 - a. Add the `[alternate_names]`.

For example:

```
[ alternate_names ]
DNS.1 = os.example.com
DNS.2 = atmos.example.com
DNS.3 = swift.example.com
```

 **Note:** There is a space between the bracket and the name of the section.

If you are uploading the certificates to ECS nodes rather than to a load balancer, the format is:

```
[ alternate_names ]
IP.1 = <IP node 1>
IP.2 = <IP node 2>
IP.3 = <IP node 3>
...
```

b. In the section [v3_ca], add the following lines:

```
subjectAltName      = @alternate_names
basicConstraints    = CA:FALSE
keyUsage            = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage    = serverAuth
```

The following line is likely to already exist in this [v3_ca] section. If you create a certificate signing request, you must comment it out as shown:

```
#authorityKeyIdentifier=keyid:always,issuer
```

c. In the [req] section, add the following lines:

```
x509_extensions = v3_ca      #for self signed cert
req_extensions   = v3_ca     #for cert signing req
```

d. In the section [CA_default], uncomment or add the line:

```
copy_extension=copy
```

Create a self-signed certificate

You can create a self-signed certificate.

Before you begin

- Create a private key using the procedure in [Create a private key](#) on page 123.
- To create certificates that use SAN, you must create a SAN configuration file using the procedure in [Generate a SAN configuration](#) on page 123.
- Create a self-signed certificate for management and one for data (object).

About this task

Procedure

1. Use the private key to create a self-signed certificate.

Two ways of creating the signing request are shown. One for use if you have already prepared a SAN configuration file to specify the alternative server name, another if you have not.

If you are using SAN:

```
openssl req -x509 -new -key server.key -config request.conf -out server.crt
```

If you are not, use:

```
openssl req -x509 -new -key server.key -out server.crt
```

Example output.

```
Signature ok
subject=/C=US/ST=GA/
```

2. Enter the pass phrase for your private key.
3. At the prompts, enter the fields for the DN for the certificate.

Most fields are optional. Enter a Common Name (CN).

Note: The CN should be an FQDN. Even if you install the certificate on the ECS nodes, you must use an FQDN and all the IP addresses must be in the alternate names section.

You see the following prompts:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Acme
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:*.acme.com
Email Address []:
```

4. Enter the Distinguished Name (DN) details when prompted. More information about DN fields is provided in [Distinguished Name \(DN\) fields](#) on page 125.
5. View the certificate.

```
openssl x509 -in server.crt -noout -text
```

Distinguished Name (DN) fields

The following table describes the fields that comprise the Distinguished Name (DN).

Name	Description	Example
Common Name (CN)	The fully qualified domain name (FQDN) of your server. This is the name that you specified when you installed the ECS appliance.	*.yourco.com ecs1.yourco.com

Name	Description	Example
Organization	The legal name of your organization. This must not be abbreviated and should include suffixes such as Inc, Corp, or LLC.	Yourco Inc.
Organizational Unit	The division of your organization handling the certificate.	IT Department
Locality/City	The state/region where your organization is located. This must not be abbreviated.	Mountain View
State/Province	The city where your organization is located.	California
Country	The two-letter ISO code for the country where your organization is location.	US
Email address	An email address to contact your organization.	contact@yourco.com

Create a certificate signing request

You can create a certificate signing request to submit to a CA to obtain a signed certificate.

Before you begin

- You must create a private key using the procedure in [Create a private key](#) on page 123.
- To create certificates that use SAN, you must create a SAN configuration file using the procedure in [Generate a SAN configuration](#) on page 123.

Procedure

1. Use the private key to create a certificate signing request.

Two ways of creating the signing request are shown. One for if you have already prepared a SAN configuration file to specify the alternative server name, another if you have not.

If you are using SAN:

```
openssl req -new -key server.key -config request.conf -out server.csr
```

If you are not, use:

```
openssl req -new -key server.key -out server.csr
```

When creating a signing request, you are asked to supply the Distinguished Name (DN) which comprises a number of fields. Only the Common Name is required and you can accept the defaults for the other parameters.

2. Enter the pass phrase for your private key.
3. At the prompts, enter the fields for the DN for the certificate.

Most fields are optional. However, you must enter a Common Name (CN).

Note: The CN should be a FQDN. Even if you install the certificate on the ECS nodes, you must use an FQDN and all of the IP addresses must be in the alternate names section.

You will see the following prompts:

```

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Acme
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:*.acme.com
Email Address []:

```

More information on the DN fields are provided in [Distinguished Name \(DN\) fields](#) on page 125.

4. You are prompted to enter an optional challenge password and a company name.

```

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

```

5. View the certificate request.

```
openssl req -in server.csr -text -noout
```

Results


You can submit the certificate signing request to your CA who will return a signed certificate file.

After you finish

Once you receive the CA-signed certificate file, make sure it is in the correct format as described in [CA-signed certificate file format](#).

CA-signed certificate file format

If you received a signed certificate from a corporate CA, the format is *host certificate* > *intermediate certificate* > *root certificate*, as shown below. The root certificate file should be included so that clients can import it.

 **Note:** There is no text between the end of each certificate and the beginning of the next certificate.

```

-----BEGIN CERTIFICATE-----
host certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
intermediate certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
root certificate
-----END CERTIFICATE-----

```

If you received a signed certificate from a public CA, including the root certificate file is not required because it is installed on the client. The certificate file format is *host certificate* > *intermediate certificate*, as shown below. (Note there is no text between the end of the host certificate and the beginning of the intermediate certificate.)

```
—BEGIN CERTIFICATE—
host certificate
—END CERTIFICATE—
—BEGIN CERTIFICATE—
intermediate certificate
—END CERTIFICATE—
```

Certificate check steps

If the data format is wrong and `sha256sum` is incorrect, certificate installation fails. Perform the certification steps as described below:

Issue Received 400 error when uploading a SSL certificate.

Command:

```
# curl -svk -H "$TOKEN" -H "Content-type: application/xml" -H "X-EMC-REST-CLIENT: TRUE" -X PUT -d "`cat /home/admin/vcssl/server_nopass.key`cat /home/admin/vcssl/cert.cer`" https://xxx.xxx.xxx.xxx:4443/vdc/keystore
```

Example:

```
< HTTP/1.1 400 Bad Request
< Date: Wed, 27 Sep 2017 12:21:57 GMT
< Content-Type: application/xml
< Content-Length: 337
< Connection: keep-alive
* HTTP error before end of send, stop sending
<
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><error><code>1013</code><description>Bad request body</description><details>javax.xml.bind.UnmarshalException
- with linked exception:
* Closing connection 0
* SSLv3, TLS alert, Client hello (1):
[org.apache.xerces.impl.io.MalformedByteSequenceException: Invalid byte 1 of
1-byte UTF-8 sequence.]</details><retryable>false</retryable></error>
```

Cause:

- The certificate that is named `cert.cer` in this case is binary format not PEM causing the issue.

Command:

```
# file <PATH_TO_SERVER_KEY> <PATH_TO_CERTIFICATE>
```

Example:


```
/home/admin/vcssl # file server_nopass.key cert.cer
server_nopass.key: PEM RSA private key
cert.cer:          data
```

- Validate the certificate is matching the server key generated format.

Commands:

```
# openssl x509 -in <PATH_TO_CERTIFICATE> -noout -modulus | openssl sha256
# openssl rsa -in <PATH_TO_SERVER_KEY> -noout -modulus | openssl sha256
```

Example:

 **Note:** The two values must match to be a valid pair.

```
admin@node1:~> openssl x509 -in server.crt -noout -modulus | openssl sha256
(stdin)= a7263a89f0d8aa48cc4de0c76e3ccfe0c2e4fb585ab1f39bf8c82e3c39459bb3
admin@node1:~> openssl rsa -in server_nopass.key -noout -modulus | openssl
sha256 (stdin)=
a7263a89f0d8aa48cc4de0c76e3ccfe0c2e4fb585ab1f39bf8c82e3c39459bb3
```

Resolution

- Change certificate from DER format to PEM format then retry upload command to resolve.

Command: (No output expected)

```
# openssl x509 -in cert.cer -inform der -outform pem -out cert.pem
```

- Upload the newly reformatted certificate.

Management Certificate Command:

```
# curl -svk -H "$TOKEN" -H "Content-type: application/xml" -H "X-EMC-REST-
CLIENT: TRUE" -X PUT -d
"<rotate_keycertchain><key_and_certificate><private_key>`cat /home/admin/
vcssl/server_nopass.key`</private_key><certificate_chain>`cat /home/admin/
vcssl/cert.pem`</certificate_chain></key_and_certificate></
rotate_keycertchain>" https://`hostname -i`:4443/vdc/keystore
```

Data Access Certificate Command:

```
# curl -svk -H "$TOKEN" -H "Content-type: application/xml" -H "X-EMC-REST-
CLIENT: TRUE" -X PUT -d
"<rotate_keycertchain><key_and_certificate><private_key>`cat key.pem`</
private_key><certificate_chain>`cat cert.cert`</certificate_chain></
key_and_certificate></rotate_keycertchain>" https://`hostname -i`:4443/object-
cert/keystore
```

Example:

```
* Hostname was NOT found in DNS cache
* Trying x.x.x.x...
* Connected to x.x.x.x (x.x.x.x) port 4443 (#0)
* successfully set certificate verify locations:
* CAfile: none
  CApath: /etc/ssl/certs/
* SSLv3, TLS handshake, Client hello (1):
* SSLv3, TLS handshake, Server hello (2):
* SSLv3, TLS handshake, CERT (11):
* SSLv3, TLS handshake, Server key exchange (12):
* SSLv3, TLS handshake, Server finished (14):
* SSLv3, TLS handshake, Client key exchange (16):
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
```

```
* SSLv3, TLS change cipher, Client hello (1):
* SSLv3, TLS handshake, Finished (20):
* SSL connection using TLSv1.0 / ECDHE-RSA-AES256-SHA
* Server certificate:
*   subject: CN=localhost
*   start date: 2017-06-14 19:58:44 GMT
*   expire date: 2027-06-12 19:58:44 GMT
*   issuer: CN=localhost
*   SSL certificate verify result: self signed certificate (18),
continuing anyway.
> PUT /vdc/keystore HTTP/1.1
> User-Agent: curl/7.37.0
> Host: x.x.x.x:4443
> Accept: */*

< HTTP/1.1 200 OK
< Date: Sat, 30 Sep 2017 00:59:15 GMT
< Content-Type: application/xml
< Content-Length: 1308
< Connection: keep-alive
```

Upload a certificate

You can upload management or data certificates to ECS. Whichever type of certificate you upload, you must authenticate with the API.

Authenticate with the ECS Management REST API

To run ECS Management REST API commands, you must first authenticate with the API service and obtain an authentication token.

Procedure

1. Authenticate with the ECS Management REST API and obtain an authentication token that can be used when using the API to upload or verify certificates.
 - a. Run the following command:

```
export TOKEN=`curl -s -k -v -u <root user>:<root user password>
https://<management IP>:4443/login 2>&1 | grep X-SDS-AUTH-TOKEN | awk
'{print $2, $3}'`
```

The username and password are those used to access the ECS Portal. The `public_ip` is the public IP address of the node.

- b. Verify the token exported correctly.

```
echo $TOKEN
```

Example output:

```
X-SDS-AUTH-TOKEN:
BAAcTGZjUjJ2Zml1YURSUfZzKzhBSVVPQVFDRUuWPQMAjAQASHVybJpzdG9yYWdlb3M6VmlydHVhbERhdGFkZDZw
50ZXJEYXRhOjcxYjAlZTgwLTNkNzktND
dmMC04OThhLWI2OTU4NDk1YmVmYgIADTE0NjQ3NTM2MjgzMTIDAC51cm46VG9rZW46YWMwN2Y0NGYtMjE5OS00
ZjA4LTgyM2EtZTAwNTc3ZWl0NDAYAgAC
0A8=
```

Upload a management certificate

You can upload a management certificate which is used to authenticate access to management endpoints, such as the ECS Portal and the ECS Management REST API.

Before you begin

- Ensure that you have authenticated with the ECS Management REST API and stored the token in a variable (`$TOKEN`) as described in [Authenticate with the ECS Management REST API](#) on page 130.
- Ensure that the machine that you use has a suitable REST client (such as curl) and can access the ECS nodes using the ECS Management REST API.
- Ensure your private key and certificate are available on the machine from which you intend to perform the upload.

Procedure

1. Ensure that your private key does not have a passphrase.

If it does, you can create a copy with the passphrase stripped, by typing the following command:

```
openssl rsa -in server.key -out server_nopass.key
```

2. Upload the keystore for the data path using your private key and signed certificate.

Using curl:

```
curl -svk -H "$TOKEN" -H "Content-type: application/xml" -H "X-EMC-REST-CLIENT: TRUE" -X PUT -d
"<rotate_keycertchain><key_and_certificate><private_key>`cat
privateKeyFile`</private_key><certificate_chain>`cat certificateFile`</
certificate_chain></key_and_certificate></rotate_keycertchain>"https://
<Management IP>:4443/vdc/keystore
```

Using the ECS command line interface (`ecscli.py`):

```
python ecscli.py vdc_keystore update -hostname <Management IP> -port
4443 -cf <cookiefile> -privateKey privateKeyFile -certificateChain
certificateFile
```

The `privateKeyFile`, for example `<path>/server_nopass.key`, and `certificateFile`, for example `<path>/server.crt`, must be replaced with the path to the key and certificate files.

3. Log in to one of the ECS nodes as the admin user.
4. Verify that the `MACHINES` file has all nodes in it.

The `MACHINES` file is used by ECS wrapper scripts that execute commands on all nodes, such as `viprexec`.

The `MACHINES` file is in `/home/admin`.

- a. Display the contents of the `MACHINES` file.

```
cat /home/admin/MACHINES
```

- b. If the `MACHINES` file does not contain all nodes, recreate it.

```
getrackinfo -c MACHINES
```

Verify that the `MACHINES` file now contains all nodes.

5. Restart the `objcontrolsvd` and `nginx` services once the management certificates are applied.
 - a. Restart the object service.

```
viprexec -f ~/MACHINES -i 'pidof objcontrolsvd;
kill `pidof objcontrolsvd`; sleep 60; pidof objcontrolsvd'
```

- b. Restart the `nginx` service.

```
sudo -i viprexec -i -c "/etc/init.d/nginx restart;sleep 60;/etc/init.d/nginx status"
```

After you finish

You can verify the certificate has uploaded correctly using the following procedure: [Verify the management certificate](#) on page 136.

Upload a data certificate for data access endpoints

You can upload a data certificate which is used to authenticate access for the S3, EMC Atmos, or OpenStack Swift protocols.

Before you begin

- Ensure that you have authenticated with the ECS Management REST API and stored the token in a variable (`$TOKEN`). See [Authenticate with the ECS Management REST API](#) on page 130.
- Ensure that the machine that you use has a suitable REST client (such as `curl`) and can access the ECS nodes using the ECS Management REST API.
- Ensure your private key and certificate are available on the machine from which you intend to perform the upload.

Procedure

1. Ensure that your private key does not have a pass phrase.

If it does, you can create a copy with the pass phrase stripped, using:

```
openssl rsa -in server.key -out server_nopass.key
```

2. Upload the keystore for the data path using your private key and signed certificate.

```
curl -svk -H "$TOKEN" -H "Content-type: application/xml" -H "X-EMC-REST-CLIENT: TRUE" -X PUT -d
"<rotate_keycertchain><key_and_certificate><private_key>`cat
privateKeyFile`</private_key><certificate_chain>`cat certificateFile`</
certificate_chain></key_and_certificate></rotate_keycertchain>"https://
<Management IP>:4443/vdc/keystore
```

Using the ECS command line interface (`ecscli.py`):

```
python ecscli.py vdc_keystore update -hostname <Management IP> -port
4443 -cf <cookiefile> -privateKey privateKeyFile -certificateChain
certificateFile
```

The `privateKeyFile`, for example `<path>/server_nopass.key`, and `certificateFile`, for example `<path>/server.crt`, must be replaced with the path to the key and certificate files.

- The certificate is distributed when the `dataheadsvc` service is restarted. You can do this with the commands below.

Note: You do not need to restart the services when changing data certificate, `dataheadsvc` is restarted automatically on each node two hours from certificate update.

```
ssh admin@<ecs_ip_where_cert_uploaded>
```

```
sudo kill `pidof dataheadsvc`
```

After you finish

You can verify that the certificate has correctly uploaded using the following procedure: [Verify the object certificate](#) on page 137.

The ECS CLI Reference is provided [here](#).

Add custom LDAP certificate

You can add the customize LDAP certificate for ECS authentication.

Before you begin

- This operation requires the System Administrator role in ECS.
- Ensure that you have authenticated with the ECS Management REST API and stored the token in a variable (`$TOKEN`) as described in [Authenticate with the ECS Management REST API](#) on page 130.
- Ensure that the machine that you use has a suitable REST client (such as `curl`) and can access the ECS nodes using the ECS Management REST API.
- Ensure your private key and certificate are available on the machine from which you intend to perform the upload.

Procedure

- To add certificate to TrustStore, use:

```
curl -s -k -X PUT -H Content-Type:application/json -H "X-SDS-AUTHTOKEN:
BAAcNThsbWVXbGFLUGhZQ0pXOTZ4azNOeFNsZkhBPQMAjAQASHVybypzdG9yYWdlb3M6Vmly
dHVhbERhdGFDZW50ZXJEYXRhOjU1NDEyZjdmLWQyNGItNGU1Ni05MGM1LWRmZWVmZGUwMTNi
ZgIADTE1NjM4OTM1NjE2NzIDAC51cm46VG9rZW46ZmE3NzIyNzktODg0Yi00NjAxLTg1MWUt
YjkyYjQ4YjAwOGMwAgAC0A8=" -H ACCEPT:application/json https://
10.243.83.105 :4443/vdc/truststore -d @file1.json
```

Request Payload JSON example:

```
{
  "add": [
    "-----BEGIN CERTIFICATE-----\nMI7FS8J...DF=r\n-----END
    CERTIFICATE-----"
  ]
}
```

Response Payload JSON example:

```
{"certificate":["-----BEGIN CERTIFICATE-----\nMIIDdzCCAl+gAwIBAgIQU
+WFap1wZplFATLD4CWbnTANBqkqhkiG9w0BAQUFADBO\r
\nMRUwEwYKcZImiZPyLQBGryFbG9jYWwxFjAUBgoJkiaJk/IsZAEZFgZoYWRvb3Ax\r
\nHTAbBgNVBAMTFGhhZG9vcC1OSUxFMylWTTQzLUNBMB4XDTE1MDkwNzEzMDA0MfoX\r
\nDTIwMDkwNzEzMTAzOVowTjEVMBMGCSJomT8ixkARKWBWxvY2FsMRywFAYKcZIm\r
\niZPyLQBGryGaGFkb29wMR0wGwYDVQQDExRoYWRvb3AtTk1MRTMtVk00My1DQTCC\r
\nASlWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOqoxHBtrND7CiHQvHXSDdKy\r
\nxyZv6qK0Bj1QK1QR2qiCjfoC3By9b8cSvzVf06mdDiQurxPj1z5JLALfbIMxcs1N\r
\nBvDkzn9tzzspbYSLyRqOyMxe4F+Bo9Hm8nGLtZU61liLBglPgrSt77Qvi6pAU0EjN\r
\nNZ3ZqBYZcmx/rD3iCeHojcl/P4UDy41bCb317w6GbrzczGRimitkFiriD3kUtkXyw\r
\nMM4L+ZY1j8o6WXSfcmhX0nX8OCrSiukMyZKcreeUQg4xykSp6GhIB74I6R6gIAh0\r
\nFOqQLsRNjMRjEhWpVXB7tTW74E3DgVwe2PF/3aL1i9sx90UekZREhA3L1sKKm10C\r
\nAwEAAANRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYE\r
\nFDRcvMyr1H52IuQtDpsfnj4PbBNwMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3\r
\nDQEBBQUAA4IBAQAAXPE0Agbjuhi02Yufz0UtUBQYcAHsRCwrxLkRvzn1UBqA3wU87\r
\nnbUQDppQ7e3Iz5SJ9PZ/3nUVQyMgnI5NS1UP6Hn/j9jVlaAB4MKXzgxDBCIDUotzh\r
\nBZuvlZ6FDjBbBSyrAk3LVnqSC2DNYVPbyRrUBHQxWnYT2FuIMQeGDb/rjtwALkvb\r
\n7sTsLKiGhkwmeYyrsiUpzoyarw21EWxLRRmfnX1/CrGg883k0mYuEyG0aFmoi0\r
\nRWZBz2NE10V5yorVniuiql/Tvbi3gPYLhy3DFMO4mjh9eSgcakYCNsQfc5msmu4Y\r
\nG6ab3ChgU6kVF5sIEv/wXvyId8X2uLoa8Wcj\r\n-----END CERTIFICATE-----"]}
```

2. To get certificate from TrustStore, use:

```
curl -s -k -X GET -H Content-Type:application/json -H "X-SDS-AUTHTOKEN:
BAACNThsbWVXbGFLUGhZQ0pXOTZ4azNOeFNsZkhBPQMAjAQASHVyb3pzdG9yYWdlb3M6Vmly
dHVhberhdGFDZw50ZXJEYXRhOjU1NDEyZjdmLWQyNGItNGU1Ni05MGM1LWRmZWVmZGUwMTNi
ZgIADTE1NjM4OTM1NjE2NzIDAC51cm46VG9rZW46ZmE3NzIyNzktODg0Yi00NjAxLTglMWUt
YjkyYjQ4YjAwOGMwAgAC0A8=" -H ACCEPT:application/json https://
10.243.83.105:4443/vdc/truststore
```

Response Payload JSON example:

```
{"certificate":["-----BEGIN CERTIFICATE-----\nMIIDdzCCAl+gAwIBAgIQU
+WFap1wZplFATLD4CWbnTANBqkqhkiG9w0BAQUFADBO\r
\nMRUwEwYKcZImiZPyLQBGryFbG9jYWwxFjAUBgoJkiaJk/IsZAEZFgZoYWRvb3Ax\r
\nHTAbBgNVBAMTFGhhZG9vcC1OSUxFMylWTTQzLUNBMB4XDTE1MDkwNzEzMDA0MfoX\r
\nDTIwMDkwNzEzMTAzOVowTjEVMBMGCSJomT8ixkARKWBWxvY2FsMRywFAYKcZIm\r
\niZPyLQBGryGaGFkb29wMR0wGwYDVQQDExRoYWRvb3AtTk1MRTMtVk00My1DQTCC\r
\nASlWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOqoxHBtrND7CiHQvHXSDdKy\r
\nxyZv6qK0Bj1QK1QR2qiCjfoC3By9b8cSvzVf06mdDiQurxPj1z5JLALfbIMxcs1N\r
\nBvDkzn9tzzspbYSLyRqOyMxe4F+Bo9Hm8nGLtZU61liLBglPgrSt77Qvi6pAU0EjN\r
\nNZ3ZqBYZcmx/rD3iCeHojcl/P4UDy41bCb317w6GbrzczGRimitkFiriD3kUtkXyw\r
\nMM4L+ZY1j8o6WXSfcmhX0nX8OCrSiukMyZKcreeUQg4xykSp6GhIB74I6R6gIAh0\r
\nFOqQLsRNjMRjEhWpVXB7tTW74E3DgVwe2PF/3aL1i9sx90UekZREhA3L1sKKm10C\r
\nAwEAAANRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYE\r
\nFDRcvMyr1H52IuQtDpsfnj4PbBNwMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3\r
\nDQEBBQUAA4IBAQAAXPE0Agbjuhi02Yufz0UtUBQYcAHsRCwrxLkRvzn1UBqA3wU87\r
\nnbUQDppQ7e3Iz5SJ9PZ/3nUVQyMgnI5NS1UP6Hn/j9jVlaAB4MKXzgxDBCIDUotzh\r
```

```
\nBZuvlz6FDjBbBSyrAk3LVnqSC2DNYVPbyRrUBHQxWnYT2FuIMQeGDb/rjtWALkvb\r
\n7sTsLKIGHwkmeYrsiUpzoyarw21EWxLRRrMfNX1/CrGg883k0mYuEYgOaFmoi0\r
\nRWZBz2NE10V5yorVniuiql/Tvbi3gPYLhy3DFMO4mjh9eSgcakYCNsQFc5msmu4Y\r
\nG6ab3ChgU6kVF5sIEv/wXvyId8X2uLoa8Wcj\r\n-----END CERTIFICATE-----"}]
```

3. To delete certificate from TrustStore, use:

```
curl -s -k -X PUT -H Content-Type:application/json -H "X-SDS-AUTHTOKEN:
BAACNThsbWVXbGFLUGhZQ0pXOTZ4azNOeFNsZkhBPQMAjAQASHVybjpgzdg9yYWdlb3M6Vmly
dHVhbERhdGFDZw50ZXJEYXRhOjU1NDEyZjdmLWQyNGItNGU1Ni05MGM1LWRmZWVmZGUwMTNi
ZgIADTE1NjM4OTM1NjE2NzIDAC5lcm46VG9rZW46ZmE3NzIyNzktODg0Yi00NjAxLTg1MWUt
YjkyYjQ4YjAwOGMwAgAC0A8=" -H ACCEPT:application/json https://
10.243.83.105:4443/vdc/truststore -d @file1.json
```

Request Payload JSON example:

```
{
  "remove": [
    "-----BEGIN CERTIFICATE-----\nMIIGWT...PvCr\n-----END
    CERTIFICATE-----",
  ]
}
```

Response Payload JSON example:

```
{"certificate": []}
```

4. To set TrustStore settings, use:

```
curl -s -k -X PUT -H Content-Type:application/json -H "X-SDS-AUTHTOKEN:
BAACNThsbWVXbGFLUGhZQ0pXOTZ4azNOeFNsZkhBPQMAjAQASHVybjpgzdg9yYWdlb3M6Vmly
dHVhbERhdGFDZw50ZXJEYXRhOjU1NDEyZjdmLWQyNGItNGU1Ni05MGM1LWRmZWVmZGUwMTNi
ZgIADTE1NjM4OTM1NjE2NzIDAC5lcm46VG9rZW46ZmE3NzIyNzktODg0Yi00NjAxLTg1MWUt
YjkyYjQ4YjAwOGMwAgAC0A8=" -H ACCEPT:application/json https://
10.243.83.105:4443/vdc/truststore/settings -d @truststoresettings.json
```

Request Payload JSON example:

```
{
  "accept_all_certificates": ""
}
```

Response Payload JSON example:

```
{"accept_all_certificates":true}
```

5. To get TrustStore settings, use:

```
curl -s -k -X GET -H Content-Type:application/json -H "X-SDS-AUTHTOKEN:
BAACNThsbWVXbGFLUGhZQ0pXOTZ4azNOeFNsZkhBPQMAjAQASHVybjpgzdg9yYWdlb3M6Vmly
```

```
dHVhbERhdGFDZW50ZXJEYXRhOjU1NDEyZjdmLWQyNGItNGU1Ni05MGM1LWRmZWVmZGUwMTNi
ZgIADTE1NjM4OTM1NjE2NzIDAC51cm46VG9rZW46ZmE3NzIyNzktODg0Yi00NjAxLTg1MWUt
YjkyYjQ4YjAwOGMwAgAC0A8=" -H ACCEPT:application/json https://
10.243.83.105:4443/vdc/truststore/settings
```

Response Payload JSON example:

```
{"accept_all_certificates":true}
```

Verify installed certificates

The object certificate and management certificate each has an ECS Management REST API GET request to retrieve the installed certificate.

Verify the management certificate

You can retrieve the installed management certificate using the ECS Management REST API.

Before you begin

- Ensure that you have authenticated with the ECS Management REST API and stored the token in a variable (`$TOKEN`). See [Authenticate with the ECS Management REST API](#) on page 130.
- If you have restarted services, the certificate is available immediately. Otherwise, you must wait two hours to be sure that the certificate is propagated to all nodes.

About this task

Procedure

1. Use the `GET /vdc/keystore` method to return the certificate.

Using the curl tool, the method can be run by typing the following:

```
curl -svk -H "$TOKEN" https://x.x.x.x:4443/vdc/keystore
```

Using the ECS command line interface (`ecscli.py`):

```
python ecscli.py vdc_keystore get -hostname <ecs_host_ip> -port 4443 -cf <cookiefile>
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><certificate_chain><chain>
-----BEGIN CERTIFICATE-----
MIIDgjCCAmoCCQCEDeNwcGsttTANBgkqhkiG9w0BAQUFADCBgjELMAkGA1UEBhMC&#xD;
VVMxCzAJBgNVBAGMAkdBMQwwCgYDVQQHDANBVEwxDDAKBgNVBAoMA0VNQzEMMAoG&#xD;
A1UECwwDRU5HMQ4wDAYDVQQDDAVjaHJpczEsMCoGCSqGSIb3DQEJARYdY2hyaXN0&#xD;
b3BoZXIuZ2hva2FzaWFuQGVTYy5jb20wHhcNMTYwNjAxMTg0MTIyWhcNMTcwNjAy&#xD;
MTg0MTIyWjCBgjELMAkGA1UEBhMCVVMxCzAJBgNVBAGMAkdBMQwwCgYDVQQHDANB&#xD;
VEwxDDAKBgNVBAoMA0VNQzEMMAoGA1UECwwDRU5HMQ4wDAYDVQQDDAVjaHJpczEs&#xD;
MCoGCSqGSIb3DQEJARYdY2hyaXN0b3BoZXIuZ2hva2FzaWFuQGVTYy5jb20wggEi&#xD;
MA0GCSqGSIb3DQEBQUAA4IBDwAwggEKAoIBAQBDb9WtdcW5HJpIDOuTB7o7ic0RK&#xD;
dwA4dY/nJXrk6Ikae5zDWO8XH4noQNhAu8FnEwS5kjtBKlhGI2GEFBtLkIH49AUp&#xD;
c4KrMmotDmbCeHvOhNcqBLZ5JM6DACfO/elHpb2hgBENTd6zyp7mz/7MUf52s9Lb&#xD;
x5pRRcpl1LDw3s15iodZ5GL8pRT62puJVk1do9mPfmOL22woR3YB2++AkSdAgEFH&#xD;
```



```
1XLI sFGkBsEJObbDBoEMEjEIivnTRPiyocyWki6gfLh50u9Y9B2GRzLAzIlgNiEs&#xD;
L/vyyrHcwOs4up9QqhAlvMn3Al01VF+OH0omQECSchBdsc/R/Bc35FAEVdmTAgMB&#xD;
AAEwDQYJKoZIhvcNAQEFBQADggEBAAyYcvJtEhOq+n87wukjPMgC719n7rgvaTmo&#xD;
tZpQhtt6kFoSB07p//76DNzXRXhBDADwpUGG9S4tgHChAFu9DpHFzvnjNGGw83ht&#xD;
qcJ6JYgB2M3lOQAssgW4fU6VD2bfQbGRWKy9G1rPYGVsmKQ59Xeuvf/cWvplkwW2&#xD;
bKnZmAbWEfE1cEOqt+5m20qGPcf45B7DPp2J+wVdDD7N8198Jj5HJBjt3T3aUEwj&#xD;
kvnPx1PtFM9YORKXFX2InF3UOdMs0zJUkhBZT9cJ0gASi1w0vEnx850secu1CPLf&#xD;
WB9G7R5qHWOXlkbAVPuFN01Tav+yrr8RgTawAcsv9LhkTTOUcqI=&#xD;
-----END CERTIFICATE-----</chain></certificate_chain>
```

2. You can verify the certificate using `openssl` on all nodes.

```
openssl s_client -showcerts -connect <node_ip>:<port>
```

 **Note:** The management port is 4443.

For example:

```
openssl s_client -showcerts -connect 10.1.2.3:4443
```

Verify the object certificate

You can retrieve the installed object certificate using the ECS Management REST API.

Before you begin

- Ensure that you have authenticated with the ECS Management REST API and stored the token in a variable (`$TOKEN`). See [Authenticate with the ECS Management REST API](#) on page 130.
- If you have restarted services, the certificate will be available immediately. Otherwise, you need to wait two hours to be sure that the certificate has propagated to all nodes.

Procedure

1. Use the `GET /object-cert/keystore` method to return the certificate.

Using the `curl` tool, the method can be run by typing the following:


```
curl -svk -H "$TOKEN" https://x.x.x.x:4443/object-cert/keystore
```

Using the ECS command line interface (`ecscli.py`):

```
python ecscli.py keystore show -hostname <ecs_host_ip> -port 4443 -cf <cookiefile>
```

2. You can verify the certificate using `openssl` on all nodes.

```
openssl s_client -showcerts -connect <node_ip>:<port>
```

 **Note:** Ports are: s3: 9021, Atmos: 9023, Swift: 9025

Example:

```
openssl s_client -showcerts -connect 10.1.2.3:9021
```

CHAPTER 10

ECS Settings

- [Introduction to ECS settings](#).....140
- [Object base URL](#)..... 140
- [Key Management](#)..... 143
- [EMC Secure Remote Services](#)..... 152
- [Alert policy](#).....156
- [Event notification servers](#)..... 157
- [Platform locking](#).....165
- [Licensing](#)..... 167
- [Security](#)..... 168
- [About this VDC](#).....172

Introduction to ECS settings

This section describes the settings that the System Administrator can view and configure in the **Settings** section of the ECS Portal. These settings include:

- [Object base URL](#)
- [Key Management](#)
- [ESRS](#)
- [Alert policy](#)
- [Event notification](#)
- [Platform locking](#)
- [Licensing](#)
- [Security](#)
- [About this VDC](#)

Object base URL

ECS supports Amazon S3 compatible applications that use virtual host style and path style addressing schemes. In multitenant configurations, ECS enables the namespace to be provided in the URL.

The base URL is used as part of the object address where virtual host style addressing is used and enables ECS to know which part of the address refers to the bucket and, optionally, namespace.

For example, if you are using an addressing scheme that includes the namespace so that you have addresses of the form `mybucket.mynamespace.mydomain.com`, you must tell ECS that `mydomain.com` is the base URL so that ECS identifies `mybucket.mynamespace` as the bucket and namespace.

By default, the base URL is set to `s3.amazonaws.com`.

An ECS System Administrator can add a base URL by using the ECS Portal or by using the ECS Management REST API.

Bucket and namespace addressing

When an S3 compatible application makes an API request to perform an operation on an ECS bucket, ECS can identify the bucket in several ways.

For authenticated API requests, ECS infers the namespace by using the namespace that the authenticated user is a member of. To support anonymous, unauthenticated requests that require CORS support or anonymous access to objects, you must include the namespace in the address so that ECS can identify the namespace for the request.

When the user scope is `NAMESPACE`, the same user ID can exist in multiple namespaces (for example, `namespace1/user1` and `namespace2/user1`). Therefore, you must include the namespace in the address. ECS cannot infer the namespace from the user ID.

Namespace addresses require wildcard DNS entries (for example, `*.ecs1.yourco.com`) and also wildcard SSL certificates to match if you want to use HTTPS. Non-namespace addresses and path style addresses do not require wildcards since there is only one hostname for all traffic. If you use non-namespace addresses with virtual host style buckets, you will still need wildcard DNS entries and wildcard SSL certificates.

You can specify the namespace in the `x-emc-namespace` header of an HTTP request. ECS also supports extraction of the location from the host header.

Virtual host style addressing

In the virtual host style addressing scheme, the bucket name is in the hostname. For example, you can access the bucket named `mybucket` on host `ecs1.yourco.com` using the following address:

```
http://mybucket.ecs1.yourco.com
```

You can also include a namespace in the address.

Example: `mybucket.mynamespace.ecs1.yourco.com`

To use virtual host style addressing, you must configure the base URL in ECS so that ECS can identify which part of the URL is the bucket name. You must also ensure that the DNS system is configured to resolve the address. For more information on DNS configuration, see [DNS configuration](#) on page 142

Path style addressing

In the path style addressing scheme, the bucket name is added to the end of the path.

Example: `ecs1.yourco.com/mybucket`

You can specify a namespace by using the `x-emc-namespace` header or by including the namespace in the path style address.

Example: `mynamespace.ecs1.yourco.com/mybucket`

ECS address processing

When ECS processes a request from an S3 compatible application to access ECS storage, ECS performs the following actions:

1. Try to extract the namespace from the `x-emc-namespace` header. If found, skip the following steps and process the request.
2. Get the hostname of the URL from the host header and check if the last part of the address matches any of the configured base URLs.
3. Where there is a BaseURL match, use the prefix part of the hostname (the part that is left when the base URL is removed), to obtain the bucket location.

The following examples demonstrate how ECS handles incoming HTTP requests with different structures:

Note: When you add a base URL to ECS, you can specify if your URLs contain a namespace in the **Use base URL with Namespace** field on the **New Base URL** page in the ECS Portal. This tells ECS how to treat the bucket location prefix. For more information, see [Add a Base URL](#) on page 142

Example 1: Virtual Host Style Addressing, Use base URL with Namespace is enabled

```
Host:          baseball.image.yourco.finance.com
BaseURL:       finance.com
Use BaseURL with namespace enabled

Namespace:     yourco
Bucket Name:   baseball.image
```

Example 2: Virtual Host Style Addressing, Use base URL with Namespace is disabled

```
Host:          baseball.image.yourco.finance.com
BaseURL:      finance.com
Use BaseURL without namespace enabled

Namespace:    null (Use other methods to determine namespace)
Bucket Name:  baseball.image.yourco
```

Example 3: ECS treats this request as a path style request

```
Host:          baseball.image.yourco.finance.com
BaseURL:      not configured

Namespace:    null (Use other methods to determine namespace.)
Bucket Name:  null (Use other methods to determine the bucket name.)
```

DNS configuration

In order for an S3 compatible application to access ECS storage, you must ensure that the URL resolves to the address of the ECS data node, or the data node load balancer.

If your application uses path style addressing, you must ensure that your DNS system can resolve the address. For example, if your application issues requests in the form `ecs1.yourco.com/bucket`, you must have a DNS entry that resolves `ecs1.yourco.com` to the IP address of the load balancer that is used for access to the ECS nodes. If your application is configured to talk to Amazon S3, the URI is in the form `s3-eu-west-1.amazonaws.com`.

If your application uses virtual host style addressing, the URL includes the bucket name and can include a namespace. Under these circumstances, you must have a DNS entry that resolves the virtual host style address by using a wildcard in the DNS entry. This also applies where you are using path style addresses that include the namespace in the URL.

For example, if the application issues requests in the form `mybucket.s3.yourco.com`, you must have the following DNS entries:

- `ecs1.yourco.com`
- `*.ecs1.yourco.com`

If the application is previously connected to the Amazon S3 service using `mybucket.s3.amazonaws.com`, you must have the following DNS entries:

- `s3.amazonaws.com`
- `*.s3.amazonaws.com`

These entries resolve the virtual host style bucket address and the base name when you issue service-level commands (for example, list buckets).

If you create an SSL certificate for the ECS S3 service, it must have the wildcard entry on the name of the certificate and the non wildcard version as a Subject Alternate Name.

Add a Base URL

You must add a base URL if you use object clients that encode the location of an object, its namespace (optional), and bucket in a URL.

Before you begin

This operation requires the System Administrator role in ECS.

About this task

Ensure that the domain specified in a request that uses a URL to specify an object location resolves to the location of the ECS data node or a load balancer that sits in front of the data nodes.

Procedure

1. In the ECS Portal, select **Settings > Object Base URL**.

The **Base URL Management** page is displayed with a list of base URLs. The **Use with Namespace** property indicates whether your URLs include a namespace.

2. On the **Base URL Management** page, click **New Base URL**.
3. On the **New Base URL** page, in the **Name** field, type the name of the base URL.

The name provides a label for this base URL in the list of base URLs on the **Base URL Management** page.

4. In the **Base URL** field, type the base URL.

If your object URLs are in the form `https://mybucket.mynamespace.acme.com` (that is, `bucket.namespace.baseurl`) or `https://mybucket.acme.com` (that is, `bucket.baseurl`), the base URL would be `acme.com`.

5. In the **Use base URL with Namespace** field, click **Yes** if your URLs include a namespace.
6. Click **Save**.

Key Management

Key Management enhances enterprise grade security by supporting centralized external key management (KMIP protocol compliant).

Key Management uses centralized key servers to store top level Key Encrypting Keys (KEKs). Key management servers provide HSM based key protection and latest encryption technology.

Key Management protects against the loss of an entire appliance. The top level key information is stored outside the appliance. If an appliance is compromised, data remains inaccessible.


 **Note:** Key Management in Settings is visible only when an encryption license is installed.

There are two types of keys:

- User-supplied keys with the S3 API headers
- Randomly generated, hierarchically structured system keys
- External key management, externally managed

With the S3 API, encryption keys can be specified in the header. If the encryption header has the key that is provided, then encryption of the object is done with the user-supplied key. ECS validates that the key provided for update, appends, and reads is the same as the key used for object creation. If the encryption header does not provide a key and the object still requires encryption, ECS then uses a system-generated key to encrypt the data.

System-generated keys at each level are auto-generated and encrypted using the key of its immediate parent. The master key is encrypted by using asymmetric public-private encryption. In asymmetric public-private encryption both the public and private keys are used to encrypt and decrypt the master key.

 **Note:** D@RE does not restrict caching of unencrypted encryption keys in memory, but ensures that plain text keys are never persisted on disk.

Keys are generated and encrypted in a hierarchical order:

- Public-Private Key pair – a pair of public-private keys generated for each ECS system. The private key is stored in the system root disk of the node. The public key is stored with the master key on the ECS commodity disks.
- Master Key – randomly generated key encrypted using the public key.
- Namespace Key – randomly generated namespace key encrypted using the master key.
- Bucket Key – randomly generated bucket key encrypted using the namespace key.
- Object Key – randomly generated object key encrypted using the bucket key and object id.
- Rotation Key - modified per rotation request. It is used to alter the object key encryption hierarchy to protect new data. When external key management is in use, the Rotation Key is maintained (and protected) by the external key manager. When native key management is in use, the rotation key has a protection hierarchy (consider each "->" as representing the statement "is protected by"): Rotation Key -> Rotation Master Key -> Public-Private Key.
- Virtual Key - represents the combination of a rotation key and a parent key. The two types of virtual keys are:
 - Virtual Master Key = Rotation Key + Master Key
 - Virtual Bucket Key = Rotation Key + Bucket Key

The hierarchy looks similar to 3.2 and earlier versions of ECS, with some modifications to use these new virtual keys.

When native key management is being used (consider each "->" as representing the statement "is protected by"):

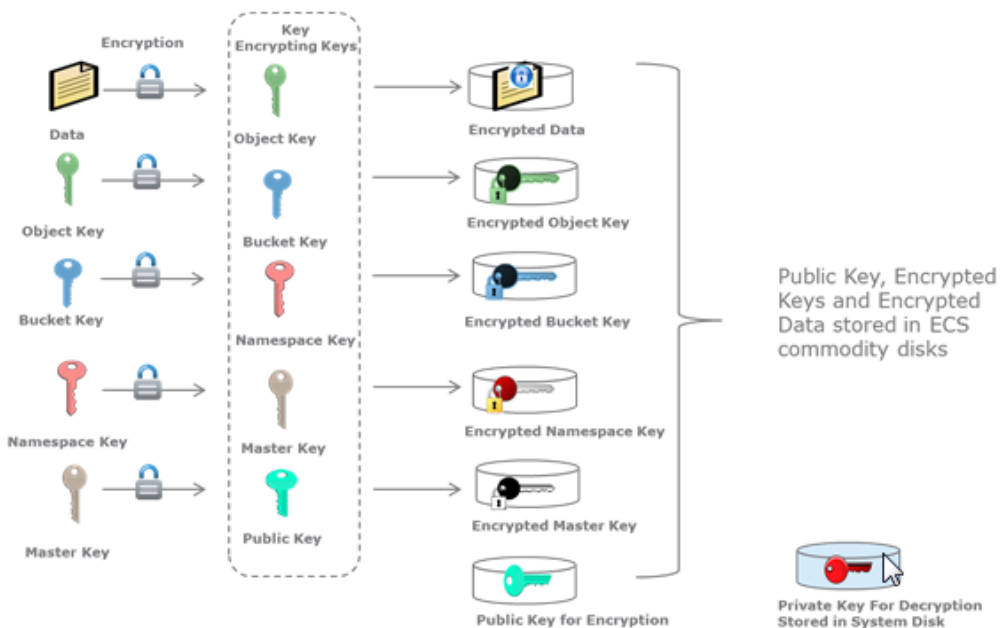
- Object key -> Virtual Bucket Key
- Bucket key -> Namespace Key -> Virtual Master Key
- Rotation Key -> Rotation Master Key -> Public-Private Key

When external key management is being used (consider each "->" as representing the statement "is protected by"):

- Object key -> Virtual Bucket Key
- Bucket key -> Namespace Key -> Virtual Master Key
- Rotation Key maintained and protected by external key manager
- Master Key maintained and protected by external key manager

The private key for decryption of master key is stored on system disks (managed by vNest). The other encrypted keys are stored in logical tables and in chunks, similar to data. They are also triple-mirrored, like data. When an object read or write request comes in, the node servicing the request traverses the key hierarchy to encrypt or decrypt the object. It uses the private key that is common to all nodes to decrypt the master key. Figure 24 provides a pictorial view of the key hierarchy.

Figure 10 Data encryption using system-generated keys

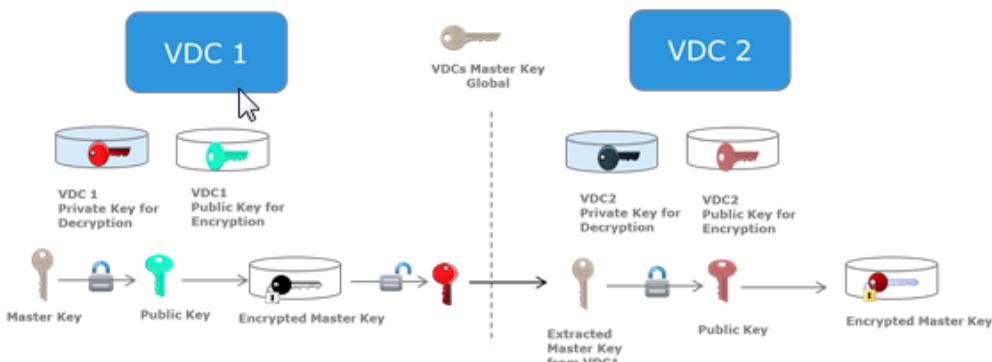


In a geo-replicated environment:

- A system being added to form or extend a federation generates public/private keys. These keys are used for encryption/decryption of federation's master key.
- Upon federation, ECS extracts the master key on the original system using the private key of that system.
- ECS encrypts the master key using the public key that the new system generates and shares it with the new system.
- The master key is now global and known to both systems within the federation.

In a geo-replicated environment, when a new ECS system joins an existing system (referred as federation), the master key is extracted using the public-private key of the existing system. The master key is also encrypted using the new public-private key pair generated from the new system that joined the federation. From this point on, the master key is global and known to both systems within the federation. In Figure 25, the ECS system that is labeled VDC 2 joins the federation. The master key of VDC 1 (the existing system) is extracted and passed to VDC 2 for encryption with the public-private key randomly which VDC 2 generates.

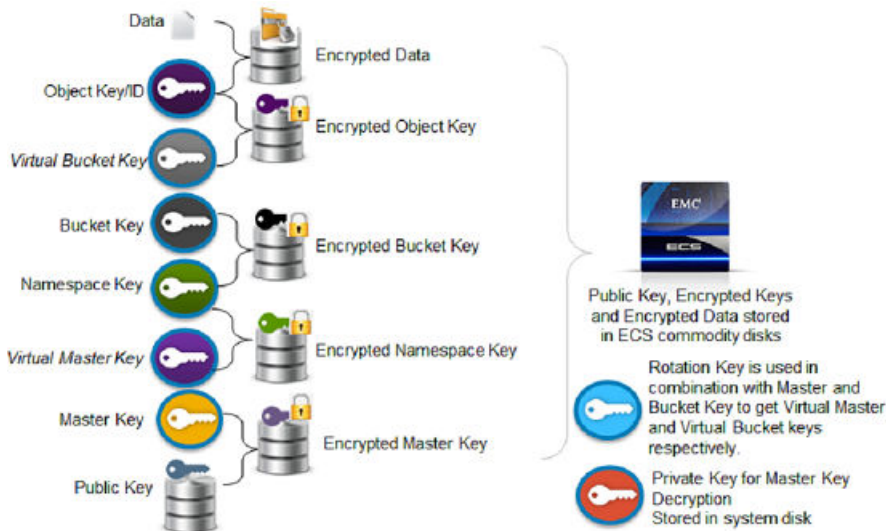
Figure 11 Encryption of the master key in a geo-replicated environment



Native Key Management

Native encryption key management uses a hierarchy as shown in the following illustration. Each VDC has associated with it a **Public-Private Key** pair that is used to protect natively generated **Master Keys** and **Rotation Master Keys** (not shown in illustration). Rotation master key is used to protect all natively generated **Rotation Keys**. Rotation key in turn is used to derive **Virtual Keys**. Each namespace in ECS has an associated **Namespace Key**, which is protected by a **Virtual Master Key**. Virtual master key is a key that is derived from master key and rotation key, but unlike these keys, it is never persisted to disks. All buckets in a namespace have an associated **Bucket Key** which is protected by its corresponding namespace key. Data for each object is encrypted using a unique object key, which is protected using a **Virtual Bucket Key**. Virtual bucket key is derived from bucket and rotation key and is not saved to disks.

Figure 12 Native key management



External Key Management

As a part of Data at Rest Encryption (D@RE), ECS supports centralized external key managers. The centralized external key managers are compliant with the Key Management Interoperability Protocol (KMIP) which enhance the enterprise grade security in the system. Also, it enables the customers to use the centralized key servers to store top-level Key Encrypting Keys (KEKs) to provide the following benefits:

- Helps in obtaining benefits from the Hardware Security Module (HSM) based key production and the latest encryption technology that is provided by the specialized key management servers.
- Provides production against loss of the entire appliance by storing top-level key information outside of the appliance.

ECS incorporates the KMIP standard for integration with external key managers and serves as a KMIP client, and supports the following:

- Supports the Gemalto Safenet and IBM SKLM (Security Key Lifecycle Manager) key managers.

Note: The key manager supported versions are determined by Dell EMC's Key-Trust-Platform (KTP) client.

- Supports the use of top-level KEK (master key) supplied by an external key manager.

- Supports rotation of top-level KEK (master key) supplied by an external key manager.

Activating external key management

Before you begin

- Ensure that you are the security administrator or have the credentials to log in as an administrator.
- Ensure that you complete the following steps before the activation.

Procedure

1. Create an EKM Cluster representing the key management cluster. For more information, see [New cluster](#)
2. Create EKM Servers, each representing a member of the external key management cluster. For more information, see [External key servers](#)
3. Map a set of the EKMServers to each VDC. For more information, see [VDC EKM Mapping](#)
 - By default, ECS requires that there are at least two EKM Servers that are mapped per VDC.
 - When mapping, the first EKMServer in the list is considered the primary, which is the server that is expected to handle key creations and retrieval.
 - The other EKMServers are considered secondaries and are used as a backup for key retrieval in case the primary is unreachable or unavailable.

Once the EKMServers have been mapped, a background process is run to validate connectivity from each VDC. If all mapped primary EKMServers are reachable, activate the EKMCluster, either through the UI or the API.

Results

Invoking the EKMCluster activation operation, triggers a background task to run the activation steps. These steps can be observed through the UI. Upon completion of the activation steps, you complete the following:

- Master key created on external key manager
- Master key retrieval validated against all external key members
- Internal reference to the new Master Key is updated
- Rotation key created on external key manager
- Rotation key retrieval validated against all external key members.
- Internal reference to the new Rotation key is updated
- All namespace keys are re-protected using the virtual master key, which would now reference the new rotation key)

External Key Manager Configuration

This section provides you information about External Key Management properties.

System Administrators can add a cluster, view VDC EKM mapping information, and rotate keys on the **Settings > Key Management** page in the ECS Portal.

Table 23 Key Management properties

Field	Description
Cluster Name	Name of the cluster
Cluster Type	Vendor Type
Server Count	Total number of servers that have been created for the cluster
Status	Indicates the status of the cluster. When first created, it is in the 'UNACTIVATED' status. When activation is performed, the status changes to match the step in the activation process.
FQDN/IP	FQDN or IP address of the EKM Server
Server Host	Server host is provided in the certificate that is used to identify the client associated with the identity store.
Port	Port number that is associated with the KMIP server. The port number is used for communicating between ECS and the external key server. Default is 5696.
Import Server Certificate	Import Server Certificate is associated with the key server that is presented to ECS for validation.
Import Revocation Certificate	Compromised certificate that is not accepted (can be an empty file).
Import Identity Store	Client certificate, signed by server and encrypted into .p12 file.
Identity Store Password	Identity store certificate password.
Username	User name must match that is defined on the Gemalto key server. Optional field for Gemalto.
Password	Password for the client that is defined on the Gemalto key server. Optional field for Gemalto.
Device Serial Number	Provide the device serial number. Optional field for SKLM.
Device ID	Provide the device ID. Optional field for SKLM.

Create cluster

From the Key Management **External Key Servers** you can create a cluster and then create external key servers.

About this task

Table 24 Create cluster

Field	Description
Cluster	Name of the cluster
Type	Vendor Type
Server Count	Total number of servers that have been created for the cluster
Status	Indicates the status of the cluster. When first created, it is in the 'UNACTIVATED' status. When activation is


Table 24 Create cluster (continued)

Field	Description
	performed, the status changes to match the step in the activation process.
FQDN/IP	FQDN or IP address of the EKM Server
Server Host	Server host is provided in the certificate that is used to identify the client associated with the identity store.
Port	Port number that is associated with the KMIP server. The port number is used for communicating between ECS and the external key server. Default is 5696.
Actions	<ul style="list-style-type: none"> • Edit - Edit the cluster name • Delete - Delete inactive cluster • Add Server - Add External Key Server to the cluster • Activate - Activate the cluster

Procedure

1. Select **Settings > Key Management > External Key Servers > New Cluster**.
2. In the **Cluster Name** field, type a unique name for the cluster.
3. In the **External Key Management Type** field, select the vendor type from the drop-down menu.
4. Click **Save**.

After creating a cluster and before VDC EKM-Mapping, add key servers.

 **Note:** Only one cluster can be created and used per ECS federation.

Add External Key Management Servers to Cluster

An external key management cluster identifies a set of external key servers that are configured as part of the cluster. External key servers are the entities that ECS nodes contact to create/retrieve cryptographic keys. After a cluster has been created, servers must be added, and then mapped to a VDC before activating the cluster.

New External Key Servers**About this task****Table 25** New external key servers

Field	Description
Cluster Name	Name of the cluster
Hostname/IP of EKM Server	The Hostname/IP of EKM Server
Server Host Name	Server Host Name is the server name that is provided in the certificate that is used to identify the client associated with the identity store.

Table 25 New external key servers (continued)

Field	Description
Port	Port number that is associated with the KMIP server. The port number is used for communicating between ECS and the external key server. Default is 5696.
Import Server Certificate	Import Server Certificate is associated with the key server that is presented to ECS for validation.
Import Revocation Certificate	Compromised certificate that is not accepted (can be an empty file).
Import Identity Store	Client certificate, signed by server and encrypted into .p12 file.
Identity Store Password	Identity store certificate password.
EKM Type	Gemalto or SKLM.
Username	User name must match that is defined on the Gemalto key server.
Password	Password for the client that is defined on the Gemalto key server.

Procedure

1. Select **Settings > Key Management > External Key Servers > New External Key Server**.
2. In the New External Key Server form, enter the Hostname/IP of the EKM Server.
3. Enter the Server Host Name.
This is the server name that is provided in the certificate that is used to identify the client associated with the identity store.
4. Enter the Port.
If different from the default 5696.
5. To import the server certificate that is associated with the key server and presented for ECS validation, click **Browse**.
6. To import the revocation certificate that is not accepted, click **Browse**.
It can be an empty file.
7. To import the Identity store, which is the client certificate that is signed by server and encrypted into the .p12 file, click **Browse**.
8. Enter the identity store password.
9. Confirm the identity store password.
10. Enter the username for the Gemalto key server.
The user name must match the client that is defined on the Gemalto key server.
i Note: Username and password are optional for Gemalto. These fields are only available when cluster type is Gemalto.
Device Serial Number and Device ID are optional for SKLM. These fields are only available when cluster type is SKLM.
11. Enter the password for the Gemalto key server.
12. Confirm the password.
13. Click **Save**.

Note: At least two key servers should be added before proceeding to VDC EKM Mapping. Activation is not enabled without a minimum of two key servers. Once a key server is mapped, delete option is disabled. You must remove EKM Mapping to delete the key server.

Add VDC to EKM Server Mapping

VDC EKM mapping assigns a subset of a cluster member server to a VDC so that nodes in the VDC can use them to access cryptographic keys.

Add VDC to EKM Server Mapping

VDC EKM mapping assigns a subset of a cluster member server to a VDC so that nodes in the VDC can use them to access cryptographic keys.

About this task

Table 26 Key Management properties

Field	Description
VDC	All VDCs in the system
Number of Servers	Number of servers currently mapped
External Key Manager FQDNIP	FQDN or IP address of the EKM Server
Port	Port number that is associated with the KMIP server. The port number is used for communicating between ECS and the external key server. Default is 5696.
Status	When not expanded, the Status indicates the overall status of the mapping. When expanded, each server displays its individual status.
Actions	Edit the VDC Mapping to add, remove, and prioritize key servers.

Procedure

1. Select **Settings > Key Management > VDC EKM Mapping**.
 - a. To expand the vdc, and to see details of the server click > .
2. Click **Edit** button for the VDC.
3. Select servers from the available table and add to the selected table.

Minimum of two servers are required. The first server in the selected list is the primary EKM Server for the VDC.

After servers are mapped to a VDC, the EKM Cluster has to be activated.

Note: After the VDC mappings are created, a background process will validate connectivity to all mapped servers per VDC. The result of this server check will be attached to each server per VDC.

Activate EKM Cluster

Procedure

1. To activate the EKM cluster, **External Key Servers > Edit > Activate**.

As part of cluster activation, key rotation will automatically be initiated. You can check its status in the Key Rotation tab as described in **Key Rotation** section.

Note: Activation can be initiated successfully only after the server check (noted in the **Add VDC to EKM Server Mapping** section) marks all the primary servers with a status of **Good**.

Key Rotation

This section provides information about ECS Key rotation and the limitations.

ECS supports rotation of keys, a practice of changing keys to limit the amount of data that is protected by any given key, to support industry standard practices. It can be performed on demand both through API and user interface, and is designed to minimize the risk from compromised keys.

During key rotation, the system does the following:

- Create rotation key natively or on EKM (if activated).
- Activate new rotation key across all sites in the federation.
- Once activated, the new rotation key is used to generate new virtual bucket and master keys.
- The new virtual master key is used to rewrap all namespace keys.
- The new virtual bucket key is used to protect all new object keys and associated new data.
- Rewrapped namespace keys are instrumental in protecting existing data.
- Data is not reencrypted as a result of key rotation.

To initiate key rotation, select **Settings > Key Management > Key Rotation > Rotate Keys**.

Note: Rotation is an asynchronous operation, and the latest status of current operation can be seen in the table. The Rotate Keys table also lists the status of previous rotation operations.

Limitations

- Key rotation does not rotate master, namespace, and bucket keys.
- Only one key rotation request can be active anytime and any other new request fails.
- Scope of the key rotation is at cluster level so all the new system encrypted objects are affected.
- Master, namespace, or bucket level rotation is not supported.

EMC Secure Remote Services

EMC Secure Remote Services (ESRS) is the recommended way for your customer support representative to receive notification of potential system issues. ESRS enables your customer support representative to troubleshoot system errors remotely by analyzing logs.

System Administrators can view ESRS information, add an ESRS server, disable ESRS call home alerts, test the ESRS dial home feature, and delete an ESRS server on the **Settings > ESRS > EMC Secure Remote Services Management** page in the ECS Portal. The **EMC Secure Remote Services Management** page contains the following information:

Table 27 ESRS properties

Field	Description
FQDN/IP	ESRS Gateway FQDN or IP address
Port	ESRS Gateway port (9443 by default)
VDC Serial Number	The software ID of the VDC.

Table 27 ESRS properties (continued)

Field	Description
Status	<p>Can be one of the following:</p> <ul style="list-style-type: none"> • Connected - ESRS server has been successfully added to the VDC, ECS is registered with ESRS, and heartbeat between ESRS server and VDC succeeds. • Disconnected - After the ESRS server connection with the VDC is established, ESRS and the VDC are not able to communicate with each other, and the heartbeat fails. The mouse-over error message for the Disconnected status reads: <code>KeepAlive failed: reason: INVALID_CREDENTIALS</code> • Failed - During the process of adding an ESRS server to the VDC, a connection cannot be established between the ESRS server and the VDC due to invalid ESRS FQDN/IP, port, or user credential information. <ul style="list-style-type: none"> ▪ When invalid ESRS Gateway FQDN/IP or port information is entered in the ECS Portal when adding an ESRS server, the mouse-over error message for the Failed status reads: <code>Failed to configure the esrs server, reason: ESRS_CONNECTION_REFUSED</code> ▪ When invalid https://support.emc.com/myservice360/ username or password credentials are entered in the ECS Portal when adding an ESRS server, the mouse-over error message for the Failed status reads: <code>Failed to add device <VDC serial number> to esrs gw <esrs gateway IP>, reason: INVALID_CREDENTIALS</code> • Disabled - The System Administrator has disabled the ESRS connection with the VDC. A System Administrator might choose to do this temporarily during a planned maintenance activity to prevent flooding ESRS with alerts.
Test Dial Home Status	<p>Can be one of the following:</p> <ul style="list-style-type: none"> • Never Run • Passed (with timestamp) • Failed (with timestamp)

ESRS prerequisites

ECS requires ESRS Virtual Edition (VE) version 3.12 and later.

Before you add an ESRS server to ECS using the ECS Portal, you must:

- **Activate** the ECS license and **upload** it the ECS Portal.
- Configure the ESRS Gateway server at the physical site where the VDC is located. The ESRS Gateway server facilitates communication between ECS and the back-end ESRS server at Dell EMC. For more information on configuring ESRS Gateway servers, see the [ESRS VE documentation](#).
- Verify that the Activated Site ID defined in the ECS license is supported on the ESRS Gateway server that will be used by ECS.
The Activated Site ID is the license site number for the physical site where ECS is installed. You can obtain the Activated Site ID in the **Activated Site** column in the ECS Portal on the **Settings > Licensing** page. To verify the Activated Site ID is supported on the ESRS Gateway server:

1. Log in to the ESRS Gateway web UI.
2. In the top menu bar, click **Devices > Manage Device**.
A list of ECS managed devices, such as VDCs and racks, displays. At the top of the list there is a row with the heading **Site ID:** followed by a comma-separated list of Site ID numbers. For example: **Site ID:** 67520, 89645, 111489
3. If the Activated Site ID you obtained from the ECS Portal is:
 - listed in the Site ID row at the top of the Managed Device list in the ESRS Gateway web UI, it is supported on the ESRS Gateway server.
 - not listed in the Site ID row at the top of the Managed Device list in the ESRS Gateway web UI, you must add it by clicking the **Add SiteID** button at the bottom of the page.
- Verify that you have full access (administrator) rights to the Activated Site ID and that the VDC Serial Number is associated with the Activated Site ID.
You can obtain the VDC Serial Number on the **Settings > Licensing** in the ECS Portal.
 1. Go to <https://support.emc.com/myservice360/>.
 2. Log in and validate that you have full access rights.
If you can access this page, then you can use your user account credentials to configure ESRS.
 3. To verify that the VDC Serial number is associated with the Activated Site ID, click the **Install Base** link near the center of the page.
If you have access to multiple sites, select the appropriate site in the **My Sites** drop-down list.
 4. In the search box, type the VDC Serial Number.
The VDC Serial Number is verified when it displays in the **Product ID** column in the table below the search box.

Add an ESRS Server

You can use the ECS Portal to add an ESRS server to an existing VDC.

Before you begin

- In an ECS geo-federated system, you must add an ESRS server for each VDC in the system.
- If you already have an ESRS server enabled, you must delete it, then add the new server. You cannot edit an ESRS server in this release.
- You must review the [ESRS prerequisites](#) before performing this procedure in the ECS Portal.
- This operation requires the System Administrator role in ECS.

Procedure

1. In the ECS Portal, select **Settings > ESRS > New Server**.
2. On the **New ESRS Server** page:
 - a. In the **FQDN/IP** field, type the ESRS Gateway FQDN or IP address.
 - b. In the **PORT** field, type the ESRS Gateway port (9443 by default).
 - c. In the **Username** field, type the login user name used to interface with ECS support. This is the same login user name used to log in to <https://support.emc.com/myservice360/>.
 - d. In the **Password** field, type the password set up with the login user name.
3. Click **Save**.

Server connectivity may take a few minutes to complete. To monitor the process, click the refresh button. Possible states of transition are **Processing**, **Connected**, or **Failed**.

Note: If you receive an `INVALID_CREDENTIALS` error message, email support@emc.com with a description of the issue, your account email, VDC serial number, and Activated Site ID.

- If ESRS is configured with more than one gateway for high availability, repeat steps 1 to 3 to add additional ESRS gateway servers.

Verify that ESRS call home works

You can verify ESRS connectivity by testing the ESRS call home functionality. In the ECS Portal, you can generate a test call home alert, and then verify that the alert is received. This is an optional procedure.

Before you begin

This operation requires the System Administrator role in ECS.

The VDC must be connected to the ESRS gateway.

Procedure

- In the ECS Portal, select **Settings > ESRS**.
- On the **EMC Secure Remote Services Management** page, click **Test Dial Home** in the **Actions** column.

If the ESRS notification is successfully received, the status displays as `Passed` with a timestamp in the **Test Dial Home Status** column.

- You can also verify that the latest test alert is present on the ESRS server.
 - SSH into the ESRS server.
 - Go to the location of the `RSC` file.

```
# cd /opt/connectemc/archive/
```

- Check for the latest `RSC` file:

```
# ls -lrt RSC_<VDC SERIAL NUMBER>*
```

- Open the `RSC` file, and check if the latest test alert shows in the description.

Disable call home

Before you begin

This operation requires the System Administrator role in ECS.

The VDC must be connected to the ESRS gateway.

About this task

System Administrators can use this feature to temporarily disable ESRS call home alerts. System Administrators should use this feature during planned maintenance activities or during troubleshooting scenarios that require taking nodes offline to prevent flooding ESRS with unnecessary alerts.

Procedure

- In the ECS Portal, select **Settings > ESRS**.
- On the **EMC Secure Remote Services Management** page, click **Disable** in the **Actions** column beside the ESRS server that you want to temporarily disable call home alerts.

The ESRS server status displays as `Disabled` in the **Status** column.

Alert policy

Alert policies are created to alert about metrics, and are triggered when the specified conditions are met. Alert policies are created per VDC.

You can use the **Settings > Alerts Policy** page to view alert policies.

There are two types of alert policy:

System alert policies

- System alert policies are precreated and exist in ECS during deployment.
- All the metrics have an associated system alert policy.
- System alert policies cannot be updated or deleted.
- System alert policies can be enabled/disabled.
- Alert is sent to the UI and all channels (SNMP, SYSLOG, and Secure Remote Services).

User-defined alert policies

- You can create User-defined alert policies for the required metrics.
- Alert is sent to the UI and customer channels (SNMP and SYSLOG).

New alert policy

You can use the **Settings > Alerts Policy > New Alert Policy** tab to create user-defined alert policies.

Procedure

1. Select **New Alert Policy**.
2. Give a unique policy name.
3. Use the metric type drop-down menu to select a metric type.

Metric Type is a grouping of statistics. It consists of:

- Btree Statistics
- CAS GC Statistics
- Geo Replication Statistics
- Metering Statistics
- Garbage Collection Statistics
- EKM

4. Use the metric name drop-down menu to select a metric name.
5. Select level.
 - a. To inspect metrics at the node level, select **Node**.
 - b. To inspect metrics at the VDC level, select **VDC**.
6. Select polling interval.

Polling Interval determines how frequently data should be checked. Each polling interval gives one data point which is compared against the specified condition and when the condition is met, alert is triggered.

7. Select instances.

Instances describe how many data points to check and how many should match the specified conditions to trigger an alert.

For metrics where historical data is not available only the latest data is used.

8. Select conditions.

You can set the threshold values and alert type with Conditions.

The alerts can be either a Warning Alert, Error Alert, or Critical Alert.

9. To add more conditions with multiple thresholds and with different alert levels, select **Add Condition**.

10. Click **Save**.

Event notification servers

You can add SNMPv2 servers, SNMPv3 servers, and Syslog servers to ECS to route SNMP and Syslog event notifications to external systems.

In ECS, you can add the following types of event notification servers:

- Simple Network Management Protocol (SNMP) servers, also known as SNMP agents, provide data about network-managed device status and statistics to SNMP Network Management Station clients. For more information, see [SNMP servers](#).
- Syslog servers provide a method for centralized storage and retrieval of system log messages. ECS supports forwarding of alerts and audit messages to remote syslog servers, and supports operations using the BSD Syslog and Structured Syslog application protocols. For more information, see [Syslog servers](#).

You can add event notification servers from the ECS Portal or by using the ECS Management REST API or CLI.

SNMP servers

Simple Network Management Protocol (SNMP) servers, also known as SNMP agents, provide data about network managed device status and statistics to SNMP Network Management Station clients.


To allow communication between SNMP agents and SNMP Network Management Station clients, you must configure both sides to use the same credentials. For SNMPv2, both sides must use the same Community name. For SNMPv3, both sides must use the same Engine ID, username, authentication protocol and authentication passphrase, and privacy protocol and privacy passphrase.

To authenticate traffic between SNMPv3 servers and SNMP Network Management Station clients, and to verify message integrity between hosts, ECS supports the SNMPv3 standard use of the following cryptographic hash functions:

- Message Digest 5 (MD5)
- Secure Hash Algorithm 1 (SHA-1)

To encrypt all traffic between SNMPv3 servers and SNMP Network Management Station clients, ECS supports encryption of SNMPv3 traffic by using the following cryptographic protocols:

- Digital Encryption Standard (using 56-bit keys)
- Advanced Encryption Standard (using 128-bit, 192-bit or 256-bit keys)

 **Note:** Support for advanced security modes (AES192/256) provided by the ECS SNMP trap feature might be incompatible with certain SNMP targets (for example, iReasoning).

Add an SNMPv2 trap recipient

You can configure Network Management Station clients as SNMPv2 trap recipients for the SNMP traps that are generated by the ECS fabric using SNMPv2 standard messaging.

Before you begin

This operation requires the System Administrator role in ECS.

Procedure

1. In the ECS Portal, select **Settings > Event Notification**.
On the **Event Notification** page, the **SNMP** tab displays by default and lists the SNMP servers that have been added to ECS.
2. To add an SNMP server target, click **New Target**.
The **New SNMP Target** page is displayed.
3. On the **New SNMP Target** page, complete the following steps:
 - a. In the **FQDN/IP** field, type the Fully Qualified Domain Name or IP address for the SNMP v2c trap recipient node that runs the `snmptrapd` server.
 - b. In the **Port** field, type the port number of the SNMP v2c `snmptrapd` running on the Network Management Station clients.
The default port number is 162.
 - c. In the **Version** field, select **SNMPv2**.
 - d. In the **Community Name** field, type the SNMP community name.
Both the SNMP server and any Network Management Station clients that access it must use the same community name to ensure authentic SNMP message traffic, as defined by the standards in RFC 1157 and RFC 3584.
The default community name is `public`.
4. Click **Save**.

Add an SNMPv3 trap recipient

You can configure Network Management Station clients as SNMPv3 trap recipients for the SNMP traps that are generated by the ECS fabric using SNMPv3 standard messaging.

Before you begin

This operation requires the System Administrator role in ECS.

Procedure

1. In the ECS Portal, select **Settings > Event Notification**.
On the **Event Notification** page, the **SNMP** tab displays by default and lists the SNMP servers that have been added to ECS.
2. To add an SNMP server target, click **New Target**.
The **New SNMP Target** page is displayed.
3. On the **New SNMP Target** page, complete the following steps:
 - a. In the **FQDN/IP** field, type the Fully Qualified Domain Name or IP address for the SNMPv3 trap recipient node that runs the `snmptrapd` server.

- b. In the **Port** field, type the port number of the SNMP 3c `snmptrapd` running on the Network Management Station client.

The default port number is 162.

- c. In the **Version** field, select **SNMPv3**.
- d. In the **Username** field, type in the username that will be used in authentication and message traffic as per the User-based Security Model (USM) defined by RFC 3414.
- Both the SNMP server and any Network Management Station clients that access it must specify the same username to ensure communication. This is an octet string of up to 32 characters in length.
- e. In the **Authentication** box, click **Enabled** if you want to enable Message Digest 5 (MD5) (128-bit) or Secure Hash Algorithm 1 (SHA-1) (160-bit) authentication for all SNMPv3 data transmissions, and do the following:
- In the **Authentication Protocol** field, select **MD5** or **SHA**.
This is the cryptographic hash function to use to verify message integrity between hosts. The default is **MD5**.
 - In the **Authentication Passphrase** field, type the string to use as a secret key for authentication between SNMPv3 USM standard hosts, when calculating a message digest.
The passphrase can be 16 octets long for MD5 and 20 octets long for SHA-1.
- f. In the **Privacy** box, click **Enabled** if you want to enable Digital Encryption Standard (DES) (56-bit) or Advanced Encryption Standard (AES) (128-bit, 192-bit or 256-bit) encryption for all SNMPv3 data transmissions, and do the following:
- In the **Privacy Protocol** field, select **DES**, **AES128**, **AES192**, or **AES256**.
This is the cryptographic protocol to use in encrypting all traffic between SNMP servers and SNMP Network Management Station clients. The default is **DES**.
 - In the **Privacy Passphrase** field, type the string to use in the encryption algorithm as a secret key for encryption between SNMPv3 USM standard hosts.
The length of this key must be 16 octets for DES and longer for the AES protocols.

4. Click **Save**.

Results

When you create the first SNMPv3 configuration, the ECS system creates an SNMP Engine ID to use for SNMPv3 traffic. The **Event Notification** page displays that SNMP Engine ID in the **Engine ID** field. You could instead obtain an Engine ID from a Network Monitoring tool and specify that Engine ID in the **Engine ID** field. The important issue is that the SNMP server and any SNMP Network Management Station clients that have to communicate with it using SNMPv3 traffic must use the same SNMP Engine ID in that traffic.

Send a test SNMP trap

You can send a test SNMP trap to validate configuration, and test traps without having to do a real failure.

Before you begin

This operation requires the System Administrator role in ECS.

Procedure

1. In the ECS Portal, select **Settings > Event Notification**.

On the **Event Notification** page, the **SNMP** tab displays by default and lists the SNMP servers that have been added to ECS.

2. To send a test SNMP trap, click the drop-down under Actions, and select **Send Test Trap**. A success message is displayed for a successful SNMP trap.
3. Confirm that the test trap has reached the SNMP Target Host.
Current test functionality is to ensure that ECS can send out a trap, but there is no verification that it was reached.

Support for SNMP data collection, queries, and MIBs in ECS

ECS provides support for Simple Network Management Protocol (SNMP) data collection, queries, and MIBs in the following ways:

- During the ECS installation process, your customer support representative can configure and start an `snmpd` server to support specific monitoring of ECS node-level metrics. A Network Management Station client can query these kernel-level `snmpd` servers to gather information about memory and CPU usage from the ECS nodes, as defined by standard Management Information Bases (MIBs). For the list of MIBs for which ECS supports SNMP queries, see [SNMP MIBs supported for querying in ECS](#) on page 160.
- The ECS fabric life cycle layer includes an `snmp4j` library which acts as an SNMP server to generate SNMPv2 traps and SNMPv3 traps and send them to as many as ten SNMP trap recipient Network Management Station clients. For details of the MIBs for which ECS supports as SNMP traps, see [ECS-MIB SNMP Object ID hierarchy and MIB definition](#) on page 160. You can add the SNMP trap recipient servers by using the **Event Notification** page in the ECS Portal. For more information, see [Add an SNMPv2 trap recipient](#) on page 158 and [Add an SNMPv3 trap recipient](#) on page 158.

SNMP MIBs supported for querying in ECS

You can query the `snmpd` servers that can run on each ECS node from Network Management Station clients for the following SNMP MIBs:

- MIB-2
- DISMAN-EVENT-MIB
- HOST-RESOURCES-MIB
- UCD-SNMP-MIB

You can query ECS nodes for the following basic information by using an SNMP Management Station or equivalent software:

- CPU usage
- Memory usage
- Number of processes running

ECS-MIB SNMP Object ID hierarchy and MIB definition

This topic describes the SNMP OID hierarchy and provides the full SNMP MIB-II definition for the enterprise MIB known as ECS-MIB.

The SNMP enterprise MIB named ECS-MIB defines the objects `trapAlarmNotification`, `notifyTimestamp`, `notifySeverity`, `notifyType`, and `notifyDescription`. The SNMP enterprise includes supported SNMP traps that are associated with managing ECS appliance hardware. ECS sends traps from the Fabric lifecycle container, using services provided by the `snmp4j` Java library. The objects contained in the ECS-MIB have the following hierarchy:

```
emc.....1.3.6.1.4.1.1139
ecs.....1.3.6.1.4.1.1139.102
```



```

trapAlarmNotification...1.3.6.1.4.1.1139.102.1.1
  notifyTimestamp.....1.3.6.1.4.1.1139.102.0.1.1
  notifySeverity.....1.3.6.1.4.1.1139.102.0.1.2
  notifyType.....1.3.6.1.4.1.1139.102.0.1.3
  notifyDescription...1.3.6.1.4.1.1139.102.0.1.4

```

You can download the ECS-MIB definition (as the file `ECS-MIB-v2.mib`) from the Support Site in the Downloads section under Add-Ons. The following Management Information Base syntax defines the SNMP enterprise MIB named ECS-MIB:

```

ECS-MIB DEFINITIONS ::= BEGIN
  IMPORTS enterprises, Counter32, OBJECT-TYPE,
  MODULE-IDENTITY, NOTIFICATION-TYPE
  FROM SNMPv2-SMI;

  ecs MODULE-IDENTITY
    LAST-UPDATED "201605161234Z"
    ORGANIZATION "EMC ECS"
    CONTACT-INFO "EMC Corporation 176 South Street Hopkinton, MA 01748"
    DESCRIPTION "The EMC ECS Manager MIB module"
    ::= { emc 102 }

  emc OBJECT IDENTIFIER ::= { enterprises 1139 }

  -- Top level groups

  notificationData OBJECT IDENTIFIER ::= { ecs 0 }
  notificationTrap OBJECT IDENTIFIER ::= { ecs 1 }

  -- The notificationData group
  -- The members of this group are the OIDs for VarBinds
  -- that contain notification data.

  genericNotify OBJECT IDENTIFIER ::= { notificationData 1 }

  notifyTimestamp OBJECT-TYPE
    SYNTAX OCTET STRING
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "The timestamp of the notification"
    ::= { genericNotify 1 }

  notifySeverity OBJECT-TYPE
    SYNTAX OCTET STRING
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "The severity level of the event"
    ::= { genericNotify 2 }

  notifyType OBJECT-TYPE
    SYNTAX OCTET STRING
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "A type of the event"
    ::= { genericNotify 3 }

  notifyDescription OBJECT-TYPE
    SYNTAX OCTET STRING
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION "A complete description of the event"
    ::= { genericNotify 4 }

  -- The SNMP trap
  -- The definition of these objects mimics the SNMPv2 convention for

```

```

-- sending traps. The enterprise OID gets appended with a 0
-- and then with the specific trap code.

trapAlarmNotification NOTIFICATION-TYPE
  OBJECTS {
    notifyTimestamp,
    notifySeverity,
    notifyType,
    notifyDescription,
  }
  STATUS current
  DESCRIPTION "This trap identifies a problem on the ECS. The description can be used
to describe the nature of the change"
  ::= { notificationTrap 1 }
END

```

Trap messages that are formulated in response to a Disk Failure alert are sent to the ECS Portal Monitor > Events > Alerts page in the format Disk {diskSerialNumber} on node {fqdn} has failed:

```

2016-08-12 01:33:22 lviprbig248141.lss.dell.com [UDP: [10.249.248.141]:39116-
>[10.249.238.216]]:
iso.3.6.1.6.3.18.1.3.0 = IPAddress: 10.249.238.216      iso.3.6.1.6.3.1.1.4.1.0 = OID:
iso.3.6.1.4.1.1139.102.1.1      iso.3.6.1.4.1.1139.102.0.1.1 = STRING: "Fri Aug 12 13:48:03
GMT 2016"      iso.3.6.1.4.1.1139.102.0.1.2 = STRING: "Critical"
iso.3.6.1.4.1.1139.102.0.1.3 = STRING: "2002"      iso.3.6.1.4.1.1139.102.0.1.4 = STRING: "Disk
1EGAGMRB on node provo-mustard.ecs.lab.dell.com has failed"

```

Trap messages that are formulated in response to a Disk Back Up alert are sent to the ECS Portal Monitor > Events > Alerts page in the format Disk {diskSerialNumber} on node {fqdn} was revived:

```

2016-08-12 04:08:42 lviprbig249231.lss.dell.com [UDP: [10.249.249.231]:52469-
>[10.249.238.216]]:
iso.3.6.1.6.3.18.1.3.0 = IPAddress: 10.249.238.216      iso.3.6.1.6.3.1.1.4.1.0 = OID:
iso.3.6.1.4.1.1139.102.1.1      iso.3.6.1.4.1.1139.102.0.1.1 = STRING: "Fri Aug 12 16:23:23
GMT 2016"      iso.3.6.1.4.1.1139.102.0.1.2 = STRING: "Info"      iso.3.6.1.4.1.1139.102.0.1.3 =
STRING: "2025"      iso.3.6.1.4.1.1139.102.0.1.4 = STRING: "Disk 1EV1H2WB on node provo-
copper.ecs.lab.dell.com was revived"

```

Syslog servers

Syslog servers provide a method for centralized storage and retrieval of system log messages. ECS supports forwarding of alerts and audit messages to remote syslog servers, and supports operations using the following application protocols:

- BSD Syslog
- Structured Syslog

Alerts and audit messages that are sent to Syslog servers are also displayed on the ECS Portal, with the exception of OS level Syslog messages (such as node SSH login messages), which are sent only to Syslog servers and not displayed in the ECS Portal.

Once you add a Syslog server, ECS initiates a syslog container on each node. The message traffic occurs over either TCP or the default UDP.

ECS sends Audit log messages to Syslog servers, including the severity level, using the following format:

```

${serviceType} ${eventType} ${namespace} ${userId} ${message}

```

ECS sends Alert logs to Syslog servers using the same severity as appears in the ECS Portal, using the following format:

```
`${alertType} ${symptomCode} ${namespace} ${message}
```

ECS sends Fabric alerts using the following format:

```
Fabric {symptomCode} "{description}"
```

Starting with ECS 3.1, ECS forwards only the following OS logs to Syslog servers:

- External SSH messages
- All `sudo` messages with Info severity and higher
- All messages from the auth facility with Warning severity and higher, which are security-related and authorization-related messages

Add a Syslog server

You can configure a Syslog server to remotely store ECS logging messages.

Before you begin

- This operation requires the System Administrator role in ECS.

Procedure

1. In the ECS Portal, select **Settings > Event Notification**.
2. On the **Event Notification** page, click the **Syslog** tab.
This page lists the Syslog servers that have been added to ECS and allows you to configure new Syslog servers.
3. To add a Syslog server, click **New Server**.
The **New Syslog Server** page is displayed.
4. On the **New Syslog Server** page, complete the following steps:
 - a. In the **Protocol** field, select **UDP** or **TCP**.
UDP is the default protocol.
 - b. In the **FQDN/IP** field, type the Fully Qualified Domain Name or IP address for the node that runs the Syslog server.
 - c. In the **Port** field, type the port number for the Syslog server on which you want to store log messages.
The default port number is 514.
 - d. In the **Severity** field, select the severity of threshold for messages to send to the log.
The drop-down options are **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Informational**, or **Debug**.
5. Click **Save**.

Server-side filtering of Syslog messages

This topic describes how an ECS Syslog message can be further filtered with server-side configuration.

You can configure Syslog servers in the ECS Portal (or by using the ECS Management REST API) to specify the messages that are delivered to the servers. You can then use server-side filtering techniques to reduce the number of messages that are saved to the logs. Filtering is done at the facility level. A facility segments messages by type. ECS directs messages to facilities as described in the following table.

Table 28 Syslog facilities used by ECS

Facility	Keyword	Defined use	ECS use
1	user	User-level messages	Fabric alerts
3	daemon	System daemons	OS messages
4	auth	Security and authorization messages	ssh and sudo success and failure messages
16	local0	Local use 0	Object alerts, object audits
All facilities	*		

For each facility, you can filter by severity level by using the following format:

facility-keyword.severity-keyword

Severity keywords are described in the following table.

Table 29 Syslog severity keywords

Severity level number	Severity level	Keyword
0	Emergency	emerg
1	Alert	alert
2	Critical	crit
3	Error	err
4	Warning	warn
5	Notice	notice
6	Informational	info
7	Debug	debug
All severities	All severities	*

Modify the Syslog server configuration using the `/etc/rsyslog.conf` file

You can modify your existing configuration by editing the `/etc/rsyslog.conf` file on the Syslog server.

Procedure

1. You might configure the `/etc/rsyslog.conf` file in the following ways:
 - a. To receive incoming ECS messages from all facilities and all severity levels, use this configuration and specify the complete path and name of your target log file:

```
*.* /var/log/ecs-messages.all
```

- b. To receive all fabric alerts, object alerts and object audits, use this configuration with the full path and name of your target log file:

```
user.*,local0.* /var/log/ecs-fabric-object.all
```

- c. To receive all fabric alerts, object alerts and object audits, and limit auth facility messages to warning severity and above, use this configuration with the full path and name of your target log file:

```
user.*,local0.* /var/log/ecs-fabric-object.allauth.warn /var/log/ecs-auth-messages.warn
```

- d. To segment the traffic to a facility into multiple files log files:

```
auth.info /var/log/ecs-auth-info.log
auth.warn /var/log/ecs-auth-warn.log
auth.err /var/log/ecs-auth-error.log
```

2. After any modification of the configuration file, restart the Syslog service on the Syslog server:

```
# service syslog restart
```

Output:

```
Shutting down syslog services done
Starting syslog services done
```

Platform locking

You can use the ECS Portal to lock remote access to nodes.

ECS can be accessed through the ECS Portal or the ECS Management REST API by management users assigned administration roles. ECS can also be accessed at the node level by a privileged default node user named `admin` that is created during the initial ECS install. This default node user can perform service procedures on the nodes and have access:

- By directly connecting to a node through the management switch with a service laptop and using SSH or the CLI to directly access the node's operating system.
- By remotely connecting to a node over the network using SSH or the CLI to directly access the node's operating system.

For more information about the default `admin` node-level user, see the *ECS Security Configuration Guide*, available from the [ECS Product Documentation page](#).

Node locking provides a layer of security against remote node access. Without node locking, the `admin` node-level user can remotely access nodes at any time to collect data, configure hardware, and run Linux commands. If all the nodes in a cluster are locked, then remote access can be planned and scheduled for a defined window to minimize the opportunity for unauthorized activity.

You can lock selected nodes in a cluster or all the nodes in the cluster by using the [ECS Portal](#) or the [ECS Management REST API](#). Locking affects only the ability to remotely access (SSH to) the locked nodes. Locking does not change the way the ECS Portal and the ECS Management REST APIs access nodes, and it does not affect the ability to directly connect to a node through the management switch.

For node maintenance using remote access, you can unlock a single node to allow remote access to the entire cluster by using SSH as the `admin` user. After the `admin` user successfully logs in to

the unlocked node using SSH, the `admin` user can SSH from that node to any other node in the cluster through the private network.

You can unlock nodes to remotely use commands that provide OS-level read-only diagnostics.

Node lock and unlock events appear in audit logs and Syslog. Failed attempts to lock or unlock nodes also appear in the logs.

Lock and unlock nodes using the ECS Portal

You can use the ECS Portal to lock and unlock remote SSH access to ECS nodes.

Before you begin

This operation requires the Lock Administrator role assigned to the `emcsecurity` user in ECS.

About this task

Locking affects only the ability to remotely access (SSH to) the locked nodes. Locking does not change the way the ECS Portal and the ECS Management REST APIs access nodes, and it does not affect the ability to directly connect to a node through the management switch.

Procedure

1. Log in as the `emcsecurity` user.

For the initial login for this user, you are prompted to change the password and log back in.

2. In the ECS Portal, select **Settings > Platform Locking**.

The **Platform Locking** page lists the nodes in the cluster and displays the lock status.

The node states are:

- Unlocked: Displays an open green lock icon and the **Lock** action button.
- Locked: Displays a closed red lock icon and the **Unlock** action button.
- Offline: Displays a circle-with-slash icon but no action button because the node is unreachable and the lock state cannot be determined.

3. Perform any of the following steps.

- a. Click **Lock** in the **Actions** column beside the node you want to lock.

Any user who is remotely logged in by SSH or CLI has approximately five minutes to exit before their session is terminated. An impending shutdown message appears on the user's terminal screen.

- b. Click **Unlock** in the **Actions** column beside the node you want to unlock.

The `admin` default node user can remotely log in to the node after a few minutes.

- c. Click **Lock the VDC** if you want to lock all unlocked, online nodes in the VDC.

It does not set a state where a new or offline node is automatically locked once detected.

Lock and unlock nodes using the ECS Management REST API

You can use the following APIs to manage node locks.

Table 30 ECS Management REST API calls for managing node locking

Resource	Description
GET /vdc/nodes	Gets the data nodes that are currently configured in the cluster
GET /vdc/lockdown	Gets the locked/unlocked status of a VDC
PUT /vdc/lockdown	Sets the locked/unlocked status of a VDC
PUT /vdc/nodes/{nodeName}/lockdown	Sets the Lock/unlock status of a node
GET /vdc/nodes/{nodeName}/lockdown	Gets the Lock/unlock status of a node

Licensing

ECS licensing is capacity-based. The ECS license file is a single file that contains base and add-on software features. A license applies to a single VDC. In geo-federated systems, each VDC requires a license. In a VDC configuration with multiple racks, the license file includes the total capacity for all racks in the VDC.

The ECS license file contains the following information:

- **Feature:** ViPR Unstructured (base feature) and may include ECS Server Side Encryption (free software add-on feature)
- **Type:** Permanent or Temporary
- **Status:** Licensed or Expired
- **Entitlement:** Describes the maximum storage that is licensed for the ViPR Unstructured feature in TB.
- **VDC Serial Number:** The software ID of the VDC
- **PSNT:** The quantity of PSNTs (racks) in the VDC. Each rack in a VDC has a product serial number tag (PSNT). In a VDC with multiple racks, multiple PSNTs maps to the serial number of the VDC. Click the right-facing arrow > next to the Feature name in the licensing table to expand and display the PSNT values.
- **Activated Site:** The license site number for the physical site where ECS will be installed
- **Expiration:** If the license is temporary, the license expiration date displays. If the license is permanent, the date the license was issued displays.

Once the license is activated, the information that is contained in the license file displays on the **Settings > Licensing** page in the ECS Portal.

There is a single ECS license file for the following scenarios:

- New ECS 3.3 installation
- Adding racks to an existing VDC
- Adding nodes to an existing rack
- Adding disks to existing nodes

In each of these scenarios, you can obtain the license as described in [Obtain the Dell EMC ECS license file](#) on page 168.

If you are upgrading from ECS 3.2.0.x to 3.3, you must contact your ECS customer support representative to perform internal license configuration. In ECS 3.3, the licensing scheme changed so that racks in a single VDC all have the same VDC serial number. Prior to 3.3, racks in a single

VDC had different VDC serial numbers. This change impacts how licensed capacity entitlements are reported and therefore require Dell EMC support.

Obtain the Dell EMC ECS license file

You can obtain a license file (.lic) from the Dell EMC license management website.

Before you begin

To obtain the license file, you must have the License Authorization Code (LAC), which was emailed from Dell EMC. If you have not received the LAC, contact your customer support representative.

Procedure

1. Go to the license page at: <https://support.emc.com/servicecenter/license/>
2. From the list of products, select **ECS Appliance**.
3. Click **Activate My Software**.
4. On the **Activate** page, enter the LAC code, and then click **Activate**.
5. Select the feature to activate, and then click **Start Activation Process**.
6. Select **Add a Machine** to specify any meaningful string for grouping licenses.
For the machine name, enter any string that helps you to keep track of your licenses. (It does not have to be a machine name.)
7. Enter the quantities for each feature, or select **Activate All**, and then click **Next**.
8. Optionally, specify an addressee to receive an email summary of the activation transaction.
9. Click **Finish**.
10. Click **Save to File** to save the license file (.lic) to a folder on your computer.

Upload the ECS license file

You can upload the ECS license file from the ECS Portal.

Before you begin

- This operation requires the System Administrator role in ECS.
- Ensure that you have a valid license file. You can follow the instructions that are provided in [Obtain the Dell EMC ECS license file](#) on page 168 to obtain a license.

About this task

Where you are installing more than one VDC in a geo-federated system, ensure that the licensing scheme across VDCs is the same. For example, if the existing VDC has a server side encryption-enabled license, any new VDC added to it should have the same.

Procedure

1. In the ECS Portal, select **Settings > Licensing**.
2. On the **Licensing** page, in the **Upload a New License File** field, click **Browse** to go to your local copy of the license file.
3. Click **Upload** to add the license.

The license features and associated information be displayed in the list of licensed features.

Security

You can use the ECS Portal to change your password, set password rules, manage user sessions, and set user agreement text. ECS logs an audit log event when the password change fails for

reasons such as connection disruption, forgetting the password. You can see and audit log for failed password changes.

- [Password](#) on page 169
- [Password Rules](#)
- [Sessions](#)
- [User Agreement](#)


Password

You can use the ECS Portal to change your password.

About this task

The **Change Password** operation changes the password for the logged in user.

 **WARNING** All user sessions are terminated on successful password change.

 **Note:** Management user and password allow special characters.

Procedure

1. In the ECS Portal, select **Settings > Security > Password**.
The **Password** page opens.
2. On the **Password** page, in the **Old Password** field, enter the old password.
3. Enter the new password, in the **Password** field, and then enter it again in the **Confirm Password**.
4. Click **Save**.

Password Rules

You can use the ECS Portal to set password rules.

Before you begin

This operation requires the System Administrator role in ECS.

About this task



 **Note:** The Password Rules take effect only when the **Password Rules Switch** is **Enabled**. The **Password Rules Switch** is **Disabled** by default.

Table 31 Password rules

Field	Description
Password Rules Switch	The Password Rules Switch controls the compliance checks for the rules on this page. <ul style="list-style-type: none"> • Enabled: All rules apply when creating/ updating passwords • Disabled: No rules apply when creating/ updating passwords
Minimum number of characters	The minimum number of characters that are required for a password must be greater than or equal to 8, and not to exceed 256.

Table 31 Password rules (continued)

Field	Description
Minimum number of upper case characters	The minimum number of upper case characters that are required for a password must be greater than or equal to 1.
Minimum number of lower case characters	The minimum number of lower case characters that are required for a password must be greater than or equal to 1.
Minimum number of numeric characters	The minimum number of numeric characters that are required for a password must be greater than or equal to 1.
Minimum number of special characters	The minimum number of special characters that are required for a password must be greater than or equal to 1.
Minimum character change	The minimum number of characters that must change from previous password must be greater than or equal to 3.
Password expiration(days)	The maximum lifetime of a password until it expires must be greater than or equal to 1.
Max login attempts	<p>The maximum number of attempts to log in with invalid password before the user is locked.</p> <ul style="list-style-type: none"> • Must be greater than or equal to 3. • System admin can unlock users through the management user interface. <p>If a user is locked due to password expiration or failed login attempts, System Administrator can unlock the user. Go to Manage> Users> Management Users> Unlock Action.</p>
Max lock day	If the password is not changed, the number of days to lock a user must be greater than or equal to 1.
Min Password duration(hours)	The minimum lifetime for a password. Must be greater than or equal to 1.
Passwords repeat	The minimum number of previous passwords that cannot be reused. Must be greater than or equal to 1.

 **Note:** When a user is locked out due to password expiration or failed login attempts, *System Administrator* can unlock the user from **Manage>Users>Management Users Unlock Action**.

Procedure

1. In the ECS Portal, select **Settings > Security > Password Rules**.
2. Enter the values for all the fields in the **Password Rules** page.
3. Click **Save**.

Sessions

You can use the ECS Portal to manage user sessions.

Before you begin

This operation requires the System Administrator role in ECS.

About this task

Table 32 Sessions

Field	Description
Management sessions per user	The maximum number of sessions per user. Must be greater than or equal to 2.
Inactive session timeout(mins)	The maximum number of minutes before an inactive session is terminated. <ul style="list-style-type: none"> • Must be greater than or equal to 15. • Inactive session timeout applies to any logged in session. • Use the Inactive UI Session timeout setting to limit ECS UI session inactivity.
Inactive UI session timeout(mins)	The maximum number of minutes before an inactive ECS UI session is terminated. <ul style="list-style-type: none"> • Must be greater than or equal to 10. Inactive UI session timeout value may not exceed the Inactive session timeout value. • Inactive UI session timeout applies to any session where user logged in through ECS UI.

Procedure

1. In the ECS Portal, select **Settings > Security > Sessions**.
2. Enter the values for all the fields in the **Sessions** page.
3. Click **Save**.

User Agreement

You can use the ECS Portal to define the user agreement text.

Before you begin

This operation requires the System Administrator role in ECS.

About this task

Table 33 User agreement

Field	Description
Agreement text	Enter the appropriate agreement text or upload from a .txt file. This content is

Table 33 User agreement

Field	Description
	displayed from the User Agreement link on the login page. Maximum character limit is 5000.

Procedure

1. In the ECS Portal, choose **Settings > Security > User Agreement**.
2. Enter the agreement text in the **Agreement text** field or click **UPLOAD.TXT FILE** to upload text from a text file.
You can review and modify the agreement text before you proceed.
3. Click **Save**.

About this VDC

You can view information about software version numbers for the current node or other nodes in the VDC on the **About this VDC** page.

About this task

You can view information that is related to the node you are currently connected to on the **About** tab. You can view the names, IP addresses, rack IDs, and software versions of the nodes available in the VDC on the **Nodes** tab. You can identify any nodes that are not at the same software version as the node you are connected to on the **Nodes** tab.

Procedure

1. In the ECS Portal, select **Settings > About this VDC**.
On the **About this VDC** page, the **About** tab displays by default and shows the ECS software version and ECS Object service version for the current node.
2. On the **About this VDC** page, to view the software version for the reachable nodes in the cluster, click the **Nodes** tab.
The green checkmark indicates the current node. A star indicates the nodes that have a different software version.

CHAPTER 11

ECS Outage and Recovery

- [Introduction to ECS site outage and recovery](#) 174
- [TSO behavior](#) 174
- [PSO behavior](#) 182
- [Recovery on disk and node failures](#) 183
- [Data rebalancing after adding new nodes](#) 184

Introduction to ECS site outage and recovery

ECS is designed to provide protection when a site outage occurs due to a disaster or other problem that causes a site to go offline or become disconnected from the other sites in a geo-federated deployment.

Site outages can be classified as a temporary site outage (TSO) or a permanent site outage (PSO). A TSO is a failure of the WAN connection between two sites, or a temporary failure of an entire site (for example, a power failure). A site can be brought back online after a TSO. ECS can detect and automatically handle these types of temporary site failures.

A PSO is when an entire site becomes permanently unrecoverable, such as when a disaster occurs. In this case, the System Administrator must permanently fail over the site from the federation to initiate failover processing.

Note: For more information about TSO and PSO behavior, see the *ECS High Availability Design* white paper.

Note: Do not delete buckets during rejoin after TSO.

TSO behavior

VDCs in a geo-replicated environment have a heartbeat mechanism. Sustained loss of heartbeats for a configurable duration (by default, 15 minutes) indicates a network or site outage and the system transitions to identify the TSO.

ECS marks the unreachable site as TSO and the site status displays as `Temporarily unavailable` on the **Replication Group Management** page in the ECS Portal.

There are two important concepts that determine how the ECS system behaves during a TSO.

- *Owner site.* If a bucket or object is created within a namespace in Site A, and then Site A is the owner site of that bucket or object. When a TSO occurs, the behavior for read/write requests differs depending on whether the request is made from the site that owns the bucket or object, or from a nonowner site that does not own the primary copy of the object.
- *Access During Outage (ADO) bucket setting.* Access to buckets and the objects within them during a TSO differs depending on whether the ADO setting is turned on for buckets. The ADO setting can be set at the bucket level; meaning you can turn this setting on for some buckets and off for others.
 - If the **ADO setting is turned off** for a bucket, strong consistency is maintained during a TSO by continuing to enable access to data owned by accessible sites and preventing access to data owned by a failed site.
 - If the **ADO setting is turned on** for a bucket, read and optionally write access to all geo-replicated data is enabled, including the data that is owned by the failed site. During a TSO, the data in the ADO-enabled bucket temporarily switches to eventual consistency. Once all sites are back online it reverts back to strong consistency.

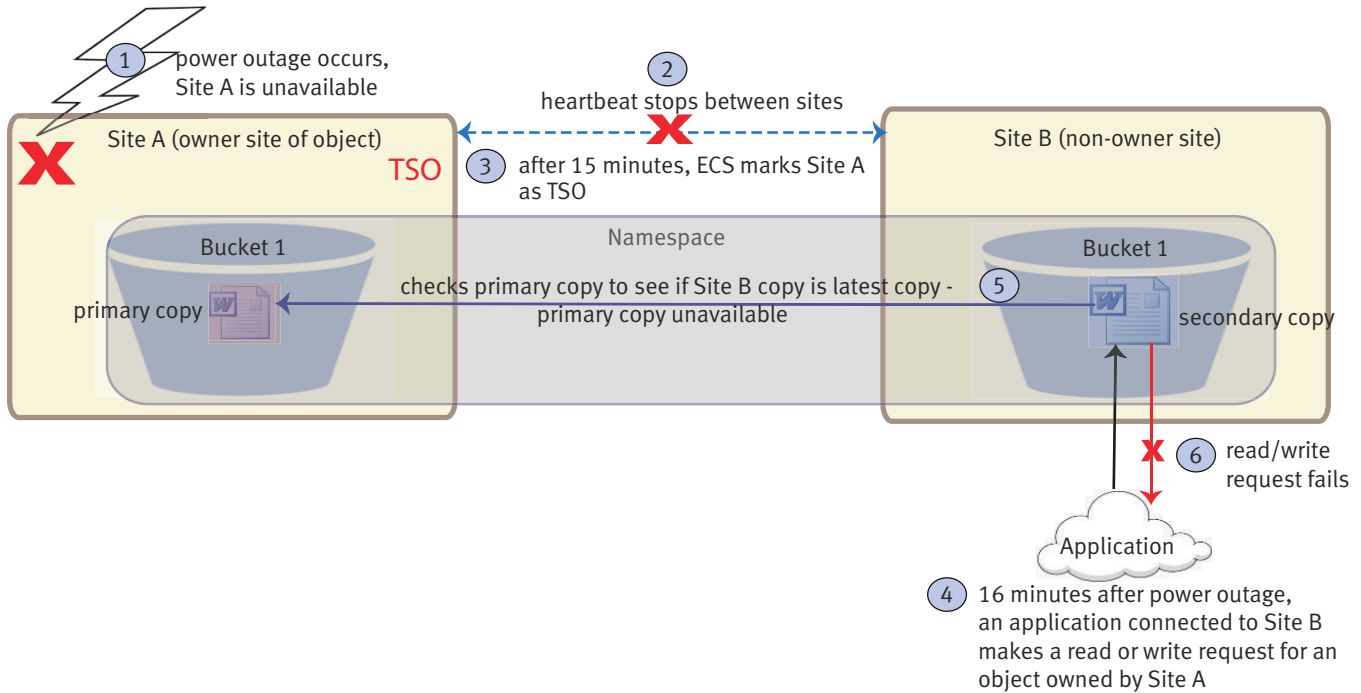
TSO behavior with the ADO bucket setting turned off

If the Access During Outage (ADO) setting is turned off for a bucket, during a TSO you will only be able to access the data in that bucket if it is owned by an available site. You will not be able to access data in a bucket that is owned by a failed site. By default, the ADO setting is turned off because there is a risk that object data retrieved during a TSO is not the most recent.

In the ECS system example shown in the following figure, Site A is marked as TSO and is unavailable. Site A is the owner of Bucket 1, because that is where the bucket (and the objects

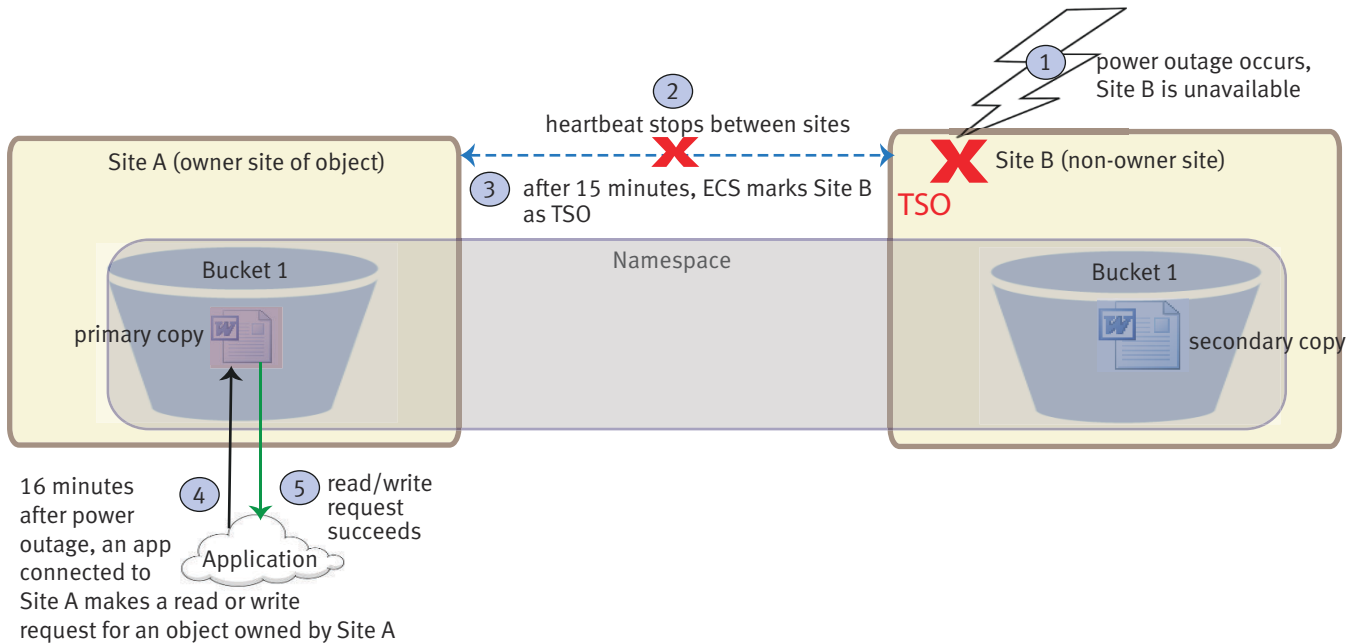
within it) was created. At the time Bucket 1 was created, the ADO setting was turned off. The read/write requests for objects in that bucket made by applications connected to Site A will fail. When an application tries to access an object in that bucket from a non-owner site (Site B), the read/write request will also fail. Note that the scenario would be the same if the request was made before the site was officially marked as TSO by the system (which occurs after the heartbeat is lost for a sustained period of time, which is set at 15 minutes by default). In other words, if a read/write request was made from an application connected to Site B within 15 minutes of the power outage, the request would still fail.

Figure 13 Read/write request fails during TSO when data is accessed from non-owner site and owner site is unavailable



The following figure shows a non-owner site that is marked as TSO with the ADO setting turned off for the bucket. When an application tries to access the primary copy at the owner site, the read/write request made to the owner site will be successful. A read/write request made from an application connected to the non-owner site will fail.

Figure 14 Read/write request succeeds during TSO when data is accessed from owner site and non-owner site is unavailable



TSO behavior with the ADO bucket setting turned on

Turning the ADO setting on for a bucket marks the bucket, and all of the objects in the bucket, as available during an outage. You can turn the ADO setting on for a bucket so that the primary copies of the objects in that bucket are available, even when the site that owns the bucket fails. If the ADO setting is turned off for a bucket, the read/write requests for the objects in the bucket that is owned by a failed site cannot be made from the other sites.

When you turn the ADO setting on, the following occurs during a TSO:

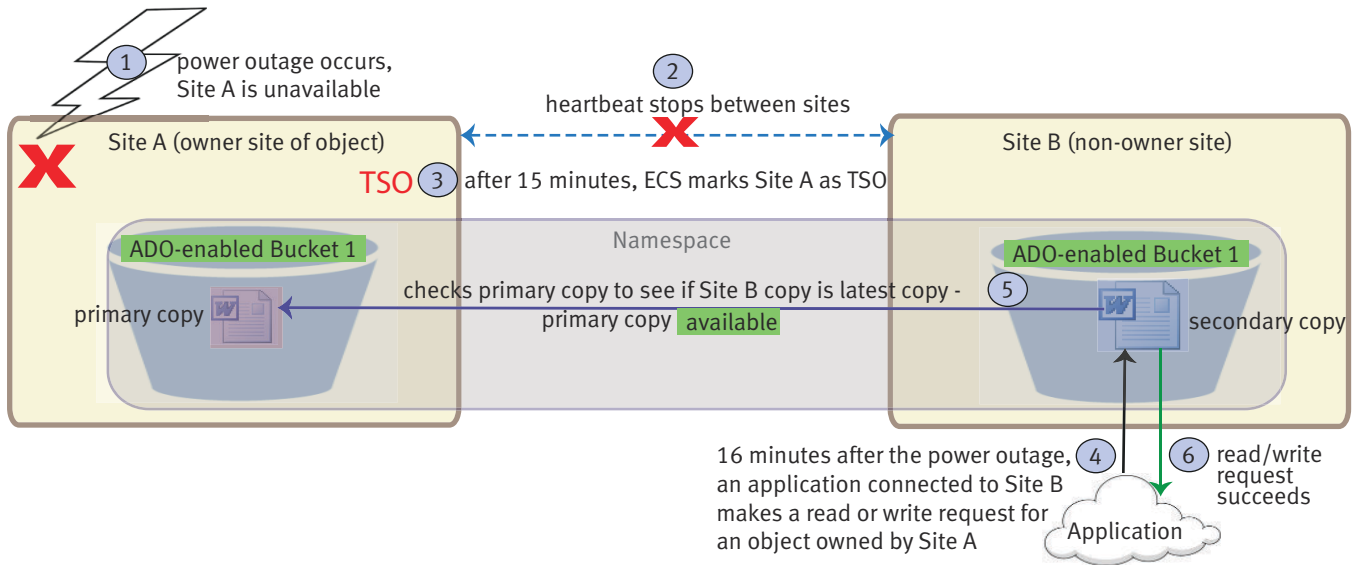
- Object data is accessible for both read and write operations during the outage.
- File systems within file system-enabled (HDFS/NFS) buckets that are owned by the unavailable site are read-only during an outage.

You can turn the ADO setting on when you create a bucket, and you can change this setting after the bucket is created (as long as all sites are online.) You can turn the ADO setting on when creating a bucket from the following interfaces:

- ECS Portal (see [Create a bucket](#) on page 79)
- ECS Management REST API
- ECS CLI
- Object API REST interfaces such as S3, Swift, and Atmos

With the ADO setting turned on for a bucket and upon detecting a temporary outage, read/write requests from applications that are connected to a nonowner site are accepted and honored, as shown in the following illustration.

Figure 15 Read/write request succeeds during TSO when ADO-enabled data is accessed from non-owner site and owner site is unavailable



The ECS system operates under the eventual consistency model during a TSO with ADO turned on for buckets. When a change is made to an object at one site, it will be *eventually* consistent across all copies of that object at other sites. Until enough time elapses to replicate the change to other sites, the value might be inconsistent across multiple copies of the data at a particular point in time.

An important factor to consider is that turning the ADO setting on for buckets has performance consequences; ADO-enabled buckets have slower read/write performance than buckets with the ADO turned off. The performance difference is because when ADO is turned on for a bucket, ECS must first resolve object ownership to provide strong consistency when all sites become available after a TSO. When ADO is turned off for a bucket, ECS does not have to resolve object ownership because the bucket does not enable change of object ownership during a TSO.

The benefit of the ADO setting is that it enables you to access data during temporary site outages. The disadvantage is that the data returned may be outdated and read/write performance on ADO buckets will be slower.


By default, the ADO setting is turned off because there is a risk that object data retrieved during a TSO is not the most recent.

TSO behavior with the ADO bucket setting that is turned on is described for the following ECS system configurations:

- [Two-site geo-federated deployment with ADO-enabled buckets](#) on page 178
- [Three-site active federated deployment with ADO-enabled buckets](#) on page 179
- [Three-site passive federated deployment with ADO-enabled buckets](#) on page 180

ADO Read-Only option

When you create a bucket and turn the ADO setting on, you also have the additional option of selecting Read-Only. You can only set the Read-Only option while creating the bucket; you cannot change this option after the bucket has been created. When you select the Read-Only option for the ADO-enabled bucket, the bucket is only accessible in read-only mode during the outage. You cannot edit or delete the bucket and its contents, and you cannot create objects in the bucket during the outage. Access to file systems is not impacted because they are automatically in read-only mode when ADO is turned on for file system buckets.

 **Note:** ADO-enabled buckets (with or without the Read-Only option selected) will have slower read/write performance than buckets with the ADO setting turned off.

Two-site geo-federated deployment with ADO-enabled buckets

When an application is connected to a non-owner site, and it modifies an object within an ADO-enabled bucket during a network outage, ECS transfers ownership of the object to the site where the object was modified.

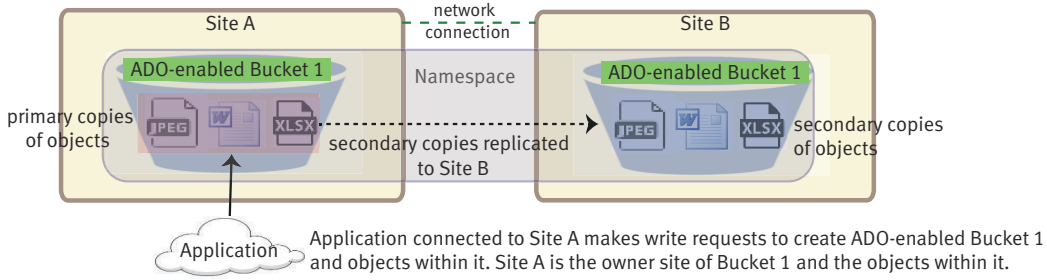
The following figure shows how a write to a non-owner site causes the non-owner site to take ownership of the object during a TSO in a two-site geo-federated deployment. This functionality allows applications connected to each site to continue to read and write objects from buckets in a shared namespace.

When the same object is modified in *both* Site A and Site B during a TSO, the copy on the non-owner site is the authoritative copy. When an object that is owned by Site B is modified in both Site A and Site B during a network outage, the copy on Site A is the authoritative copy that is kept, and the other copy is overwritten.

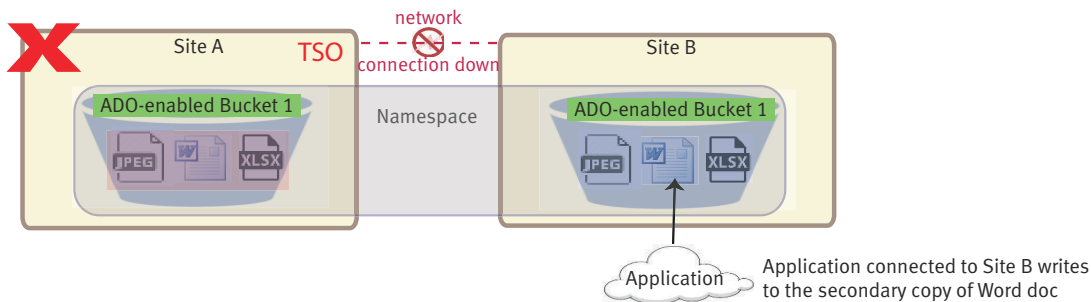
When network connectivity between two sites is restored, the heartbeat mechanism automatically detects connectivity, restores service, and reconciles objects from the two sites. This synchronization operation is done in the background and can be monitored on the **Monitor > Recovery Status** page in the ECS Portal.

Figure 16 Object ownership example for a write during a TSO in a two-site federation

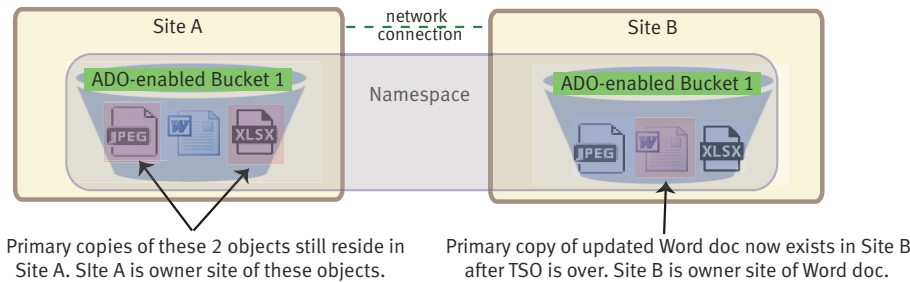
Before TSO - normal state



During TSO - Site A is temporarily unavailable



After TSO - Site A rejoins federation and object versions are reconciled



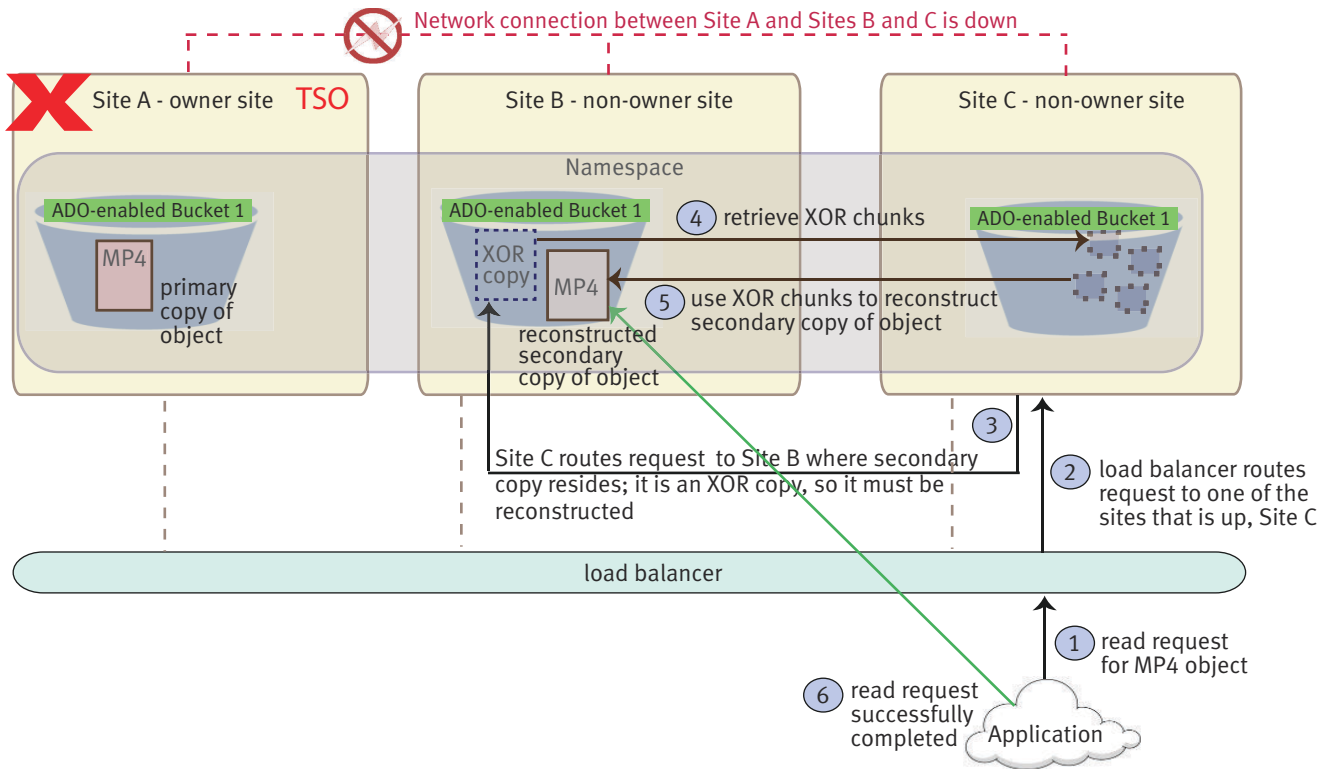
Three-site active federated deployment with ADO-enabled buckets

Note: Do not delete buckets during rejoin after TSO. Delete operation will not be performed during rejoin execution.

When more than two sites are part of a replication group, and if network connectivity is interrupted between one site and the other two, and then write/update/ownership operations continue as they would with two sites, but the process for responding to read requests is more complex.

If an application requests an object that is owned by a site that is not reachable, ECS sends the request to the site with the secondary copy of the object. The secondary copy might have been subject to a data contraction operation, which is an XOR between two different datasets that produces a new dataset. The site with the secondary copy must retrieve the chunks of the object that is included in the original XOR operation, and it must XOR those chunks with the recovery copy. This operation returns the contents of the chunk that is originally stored on the owner site. Then the chunks from the recovered object can be reassembled and returned. When the chunks are reconstructed, they are also cached so that the site can respond more quickly to subsequent requests. Reconstruction is time consuming. More sites in a replication group imply more chunks that must be retrieved from other sites, and hence reconstructing the object takes longer. The following illustration shows the process for responding to read requests in a three-site federation.

Figure 17 Read request workflow example during a TSO in a three-site federation



Three-site passive federated deployment with ADO-enabled buckets

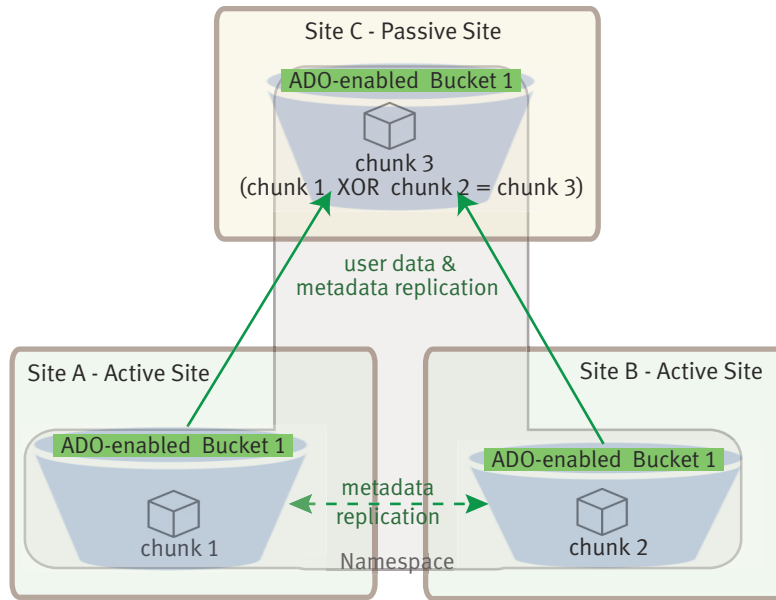
When ECS is deployed in a three-site passive configuration, the TSO behavior is the same as described in [Three-site active federated deployment with ADO-enabled buckets](#) on page 179, with one difference. If a network connection fails between an active site and the passive site, ECS always marks the passive site as TSO (not the active site).

When the network connection fails between the two active sites, the following normal TSO behavior occurs:

1. ECS marks one of the active sites as TSO (unavailable), for example, owner Site B.
2. Read/write/update requests are rendered from the site that is up (Site A).
3. For a read request, Site A requests the object from the passive site (Site C).
4. Site C decodes (undo XOR) the XOR chunks and sends to Site A.
5. Site A reconstructs a copy of the object to honor the read request.
6. In the case of a write/update request, Site A becomes the owner of the object and keeps the ownership after the outage.

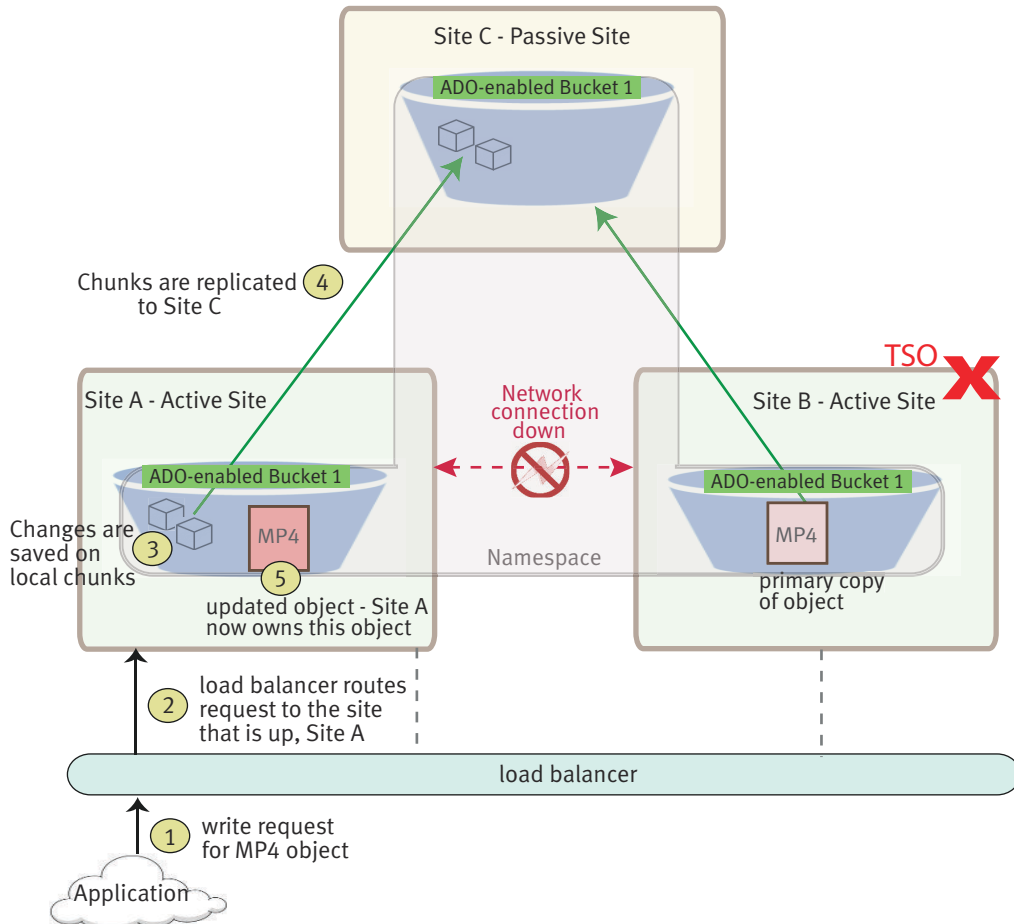
The following illustration shows a passive configuration in a normal state; users can read and write to active Sites A and B and the data and metadata is replicated one way to the passive Site C. Site C XORs the data from the active sites.

Figure 18 Passive replication in normal state



The following illustration shows the workflow for a write request that is made during a TSO in a three-site passive configuration.

Figure 19 TSO for passive replication



TSO considerations

You can perform many object operations during a TSO. You cannot perform create, delete, or update operations on the following entities at any site in the geo-federation until the temporary failure is resolved, regardless of the ADO bucket setting:

- Namespaces
- Buckets
- Object users
- Authentication providers
- Replication groups (you can remove a VDC from a replication group for a site failover)
- NFS user and group mappings

The following limitations apply to buckets during a TSO:

- File systems within file system-enabled (HDFS/NFS) buckets that are owned by the unavailable site are read-only.
- When you copy an object from a bucket owned by the unavailable site, the copy is a full copy of the source object. This means that the same object's data is stored more than once. Under normal non-TSO circumstances, the object copy consists of the data indices of the object, not a full duplicate of the object's data.

NFS file system access during a TSO

NFS provides a single namespace across all ECS nodes and can continue to operate in the event of a TSO. When you mount an NFS export, you can specify any of the ECS nodes as the NFS server or you can specify the address of a load balancer. Whichever node you point at, the ECS system can resolve the file system path.

In the event of a TSO, if your load balancer can redirect traffic to a different site, your NFS export remains available. Otherwise, you must remount the export from another, nonfailed site.

When the owner site fails, and ECS is required to reconfigure to point at a nonowner site, data can be lost due to NFS asynchronous writes and also due to unfinished ECS data replication operations.

For more information about how to access NFS-enabled buckets, see [Introduction to file access](#) on page 98.

PSO behavior

If a disaster occurs, an entire site can become unrecoverable; it is referred in ECS as a permanent site outage (PSO). ECS treats the unrecoverable site as a temporary site failure, but only if the entire site is down or unreachable over the WAN. If the failure is permanent, the System Administrator must permanently fail over the site from the federation to initiate failover processing. This initiates resynchronization and reprotection of the objects that are stored on the failed site. The recovery tasks that are run as a background process. For more information about how to perform the failover procedure in the ECS Portal, see [Fail a VDC \(PSO\)](#) on page 36.

Note:

- Before triggering PSO (planned or unplanned), ensure that the site is off (all nodes are shut down). Make sure you fail the site from the federation and remove the site from all the replication groups.

- If you want to reuse the same racks from the PSOed site, disconnect the racks physically and the nodes should be reimaged before you bring them online.

Before you initiate a PSO in the ECS Portal, it is advised to contact your customer support representative, so that the representative can validate the cluster health. Data is not accessible until the failover processing is completed. You can monitor the progress of the failover processing on the **Monitor > Geo Replication > Failover Processing** tab in the ECS Portal. While the recovery background tasks are running, but after failover processing has completed, some data from the removed site might not be read back until the recovery tasks fully complete.

Recovery on disk and node failures

ECS continuously monitors the health of the nodes, their disks, and objects stored in the cluster. ECS disperses data protection responsibilities across the cluster and automatically re-protects at-risk objects when nodes or disks fail.

Disk health

ECS reports disk health as Good, Suspect, or Bad.

- Good: The disk's partitions can be read from and written to.
- Suspect: The disk has not yet met the threshold to be considered bad.
- Bad: A certain threshold of declining hardware performance has been met. When met, no data can be read or written.

ECS writes only to disks in good health. ECS does not write to disks in suspect or bad health. ECS reads from good disks and suspect disks. When two of an object's chunks are located on suspect disks, ECS writes the chunks to other nodes.

Node health

ECS reports node health as Good, Suspect, or Bad.

- Good: The node is available and responding to I/O requests in a timely manner.
- Suspect: The node has been unavailable for more than 30 minutes.
- Bad: The node has been unavailable for more than an hour.

ECS writes to reachable nodes regardless of the node health state. When two of an object's chunks are located on suspect nodes, ECS writes two new chunks of it to other nodes.

Data recovery

When there is a failure of a node or drive in the site, the storage engine:

1. Identifies the chunks or erasure coded fragments affected by the failure.
2. Writes copies of the affected chunks or erasure coded fragments to good nodes and disks that do not currently have copies.

NFS file system access during a node failure

NFS provides a single namespace across all ECS nodes and can continue to operate in the event of node failure. When you mount an NFS export, you can specify any of the ECS nodes as the NFS server or you can specify the address of a load balancer. Whichever node you point at, the ECS system resolves the file system path.

In the event of a node failure, ECS recovers data using its data fragments. If your NFS export is configured for asynchronous writes, you run the risk of losing data that is related to any transactions that have not yet been written to disk. This is the same with any NFS implementation.

If you mounted the file system by pointing at an ECS node and that node fails, you must remount the export by specifying a different node as the NFS server. If you mounted the export by using

the load balancer address, failure of the node is handled by the load balancer which automatically directs requests to a different node.

Data rebalancing after adding new nodes

When the number of nodes at a site is expanded due to the addition of new racks or storage nodes, new erasure coded chunks are allocated to the new storage and existing data chunks are redistributed (rebalanced) across the new nodes. Four or more nodes must exist for erasure coding of chunks to take place. Addition of new nodes over and above the required four nodes results in erasure coding rebalancing.

The redistribution of erasure coded fragments is performed as a background task so that the chunk data is accessible during the redistribution process. In addition, the new fragment data is distributed as a low priority to minimize network bandwidth consumption.

Fragments are redistributed according to the same erasure coding scheme with which they were originally encoded. If a chunk was written using the cold storage erasure coding scheme, ECS uses the cold storage scheme when creating the new fragments for redistribution.

CHAPTER 12

Advanced Monitoring

- [Advanced Monitoring](#)..... 186
- [Flux API](#)..... 192
- [Dashboard API's to be deprecated or changed in the next release](#)..... 198

Advanced Monitoring

Advanced Monitoring dashboards provide critical information about the ECS processes on the VDC you are logged in to. The advanced monitoring dashboards are based on time series database, and are provided by Grafana, which is well known open-source time series analytics platform.

Refer [Grafana](#) for basic details of navigation in Grafana dashboards.

View Advanced Monitoring Dashboards

To view the advanced monitoring dashboards in the ECS Portal, select **Advanced Monitoring**. **Data Access Performance - Overview** dashboard is the default.

Table 34 Advanced monitoring dashboards

Dashboard	Description
Data Access Performance - Overview	You can use the Data Access Performance - Overview dashboard to monitor VDC data.
Data Access Performance - by Namespaces	You can use the Data Access Performance - by Namespaces dashboard to monitor performance data for individual namespace or group of Namespaces.
Data Access Performance - by Nodes	You can use the Data Access Performance - by Nodes dashboard to see performance data for individual node or group of nodes in a VDC.
Data Access Performance - by Protocols	You can use the Data Access Performance - by Protocols dashboard to see performance data for each supported protocol (S3, ATMOS, SWIFT, etc.) or set of protocols.

Table 35 Advanced monitoring dashboard fields

Dashboard	Field	Description
All	Related dashboards	Allows you to switch to other dashboards in access performance group, with the selected time.
All	Transaction Summary	Lists the total Successful requests, System Failures, User Failures, and Failure % Rate for the selected VDCs, namespaces, nodes, or protocols.
All	Successful requests	The number of data requests that were successfully completed.
All	System Failures	The number of data requests that failed due to hardware or service errors. System failures are failed requests that are associated with hardware or service errors (typically an HTTP error code of 5xx).
All	User Failures	The number of data requests from all object heads are classified as user failures. User failures are known error types originating from the object heads (typically an HTTP error code of 4xx).

Table 35 Advanced monitoring dashboard fields (continued)

Dashboard	Field	Description
All	Failure % Rate	The percentage of failures for the VDC, namespace, nodes, or protocols.
All	TPS (success/ failure)	Rate of successful requests and failures per second.
<ul style="list-style-type: none"> Data Access Performance - Overview Data Access Performance - by Nodes Data Access Performance - by Protocols 	Bandwidth (read/ write)	Data access bandwidth of successful requests per second.
All	Failed Requests/s by error type (user/ system)	Rate of failed requests per second, split by error type (user/system).
<ul style="list-style-type: none"> Data Access Performance - Overview Data Access Performance - by Nodes Data Access Performance - by Protocols 	Latency	Latency of read/write requests.
<ul style="list-style-type: none"> Data Access Performance - Overview Data Access Performance - by Nodes 	Successful request drill down	Displays the rate of successful requests per second, by method, node, and protocol.
<ul style="list-style-type: none"> Data Access Performance - Overview Data Access Performance - by Nodes 	Successful Requests/s by Method	Rate of successful requests per second, by method.
All	Successful Requests/s by Node	Rate of successful requests per second, by node.

Table 35 Advanced monitoring dashboard fields (continued)

Dashboard	Field	Description
<ul style="list-style-type: none"> Data Access Performance - Overview Data Access Performance - by Nodes 	Successful Requests/s by Protocol	Rate of successful requests per second, by protocol.
<ul style="list-style-type: none"> Data Access Performance - Overview Data Access Performance - by Nodes 	Failures drill down	Displays the rate of failed requests per second, by method, node, and protocol.
<ul style="list-style-type: none"> Data Access Performance - Overview Data Access Performance - by Nodes 	Failed Requests/s by Method	Rate of failed requests per second, by method.
All	Failed Requests/s by Node	Rate of failed requests per second, by node.
<ul style="list-style-type: none"> Data Access Performance - Overview Data Access Performance - by Nodes 	Failed Requests/s by Protocol	Rate of failed requests per second, by protocol.
<ul style="list-style-type: none"> Data Access Performance - Overview Data Access Performance - by Nodes 	Failed Requests/s by error code	Rate of failed requests per second, by error code.
<ul style="list-style-type: none"> Data Access Performance - by Nodes Data Access Performance - by Namespaces Data Access Performance - by Protocols 	Compare TPS of successful requests	Select multiple nodes and compare rates of successful requests per second.

Table 35 Advanced monitoring dashboard fields (continued)

Dashboard	Field	Description
Data Access Performance - by Namespaces	Compare TPS of failed requests	Select multiple nodes and compare rates of failed requests per second, by error type (user/system).
<ul style="list-style-type: none"> Data Access Performance - by Nodes Data Access Performance - by Protocols 	Compare read bandwidth	Select multiple nodes and compare data access bandwidth (read) of successful requests per second.
<ul style="list-style-type: none"> Data Access Performance - by Nodes Data Access Performance - by Protocols 	Compare write bandwidth	Select multiple nodes and compare data access bandwidth (write) of successful requests per second.
<ul style="list-style-type: none"> Data Access Performance - by Nodes Data Access Performance - by Protocols 	Compare read latency	Select multiple nodes and compare latency of read requests.
<ul style="list-style-type: none"> Data Access Performance - by Nodes Data Access Performance - by Protocols 	Compare write latency	Select multiple nodes and compare latency of write requests.
<ul style="list-style-type: none"> Data Access Performance - by Nodes Data Access Performance - by Protocols 	Compare rate of failed requests/s	Select multiple nodes and compare rates of failed requests per second, split by error type (user/system).
Data Access Performance - by Namespaces	Request drill down by nodes	Rate of requests per second, split by node.

View mode

Procedure

1. To view a dashboard in the view mode, click the title of a dashboard, for example **(TPS (success/failure) > View**.

The dashboard opens in the view mode or in the full-screen mode.

2. Click **Back to dashboard** icon to return back to the dashboards view.

Export CSV

Procedure

1. To export the dashboard data to .csv format click the title of a dashboard, for example (**TPS (success/failure)**) > **More** > **Export CSV**.

The Export CSV window pops-up.

You can customize the csv output by modifying the **Mode**, **Date Time Format**, and check/uncheck the **Excel CSV Dialect** attributes.

2. Click **Export** > **Save** to export the dashboard data to .csv format to your local storage.

View Advanced Monitoring Dashboards- Overview

Data Access Performance - Overview dashboard is the default.

In the **Data Access Performance - Overview** dashboard, you can monitor for all nodes in the VDC:

- TPS (success/failure)
- Bandwidth (read/write)
- Failed Requests/s by error type (user/system)
- Latency
- Successful Requests/s by Method
- Successful Requests/s by Node
- Successful Requests/s by Protocol
- Failed Requests/s by Method
- Failed Requests/s by Node
- Failed Requests/s by Protocol
- Failed Requests/s by error code

To view the **Data Access Performance - Overview** dashboard in the ECS Portal, select **Advanced Monitoring**.

Click **Successful requests drill down** to see the successful requests by all the methods, nodes, and protocols.

Click **Failures drill down** to see the failed requests by all the methods, nodes, protocols, and error code.

Click **Related dashboards** to view the other dashboards, with the selected time.

View Advanced Monitoring Dashboards- by Namespaces

In the **Data Access Performance - by Namespaces** dashboard, you can monitor for namespaces:

- TPS (success/failure)
- Failed Requests/s by error type (user/system)
- Successful Requests/s by Node
- Failed Requests/s by Node
- Compare TPS of successful requests

- Compare TPS of failed requests

To view the **Data Access Performance - by Namespaces** dashboard in the ECS Portal, select **Advanced Monitoring > Related dashboards > Data Access Performance - by Namespaces**.

All the namespace data are visible in the default view. To select a namespace, click the legend parameter for the namespace below the graph.

Requests drill down by nodes shows the successful and failed requests by node.

Compare: select multiple namespaces compares TPS of successful and failed requests.

View Advanced Monitoring Dashboards- by Nodes

In the **Data Access Performance - by Nodes** dashboard, you can monitor for nodes in a VDC:

- TPS (success/failure)
- Bandwidth (read/write)
- Failed Requests/s by error type (user/system)
- Latency
- Successful Requests/s by Method
- Successful Requests/s by Node
- Successful Requests/s by Protocol
- Failed Requests/s by Method
- Failed Requests/s by Node
- Failed Requests/s by Protocol
- Failed Requests/s by error code
- Compare TPS of successful requests
- Compare TPS of failed requests
- Compare read bandwidth
- Compare write bandwidth
- Compare read latency
- Compare write latency

To view the **Data Access Performance - by Nodes** dashboard in the ECS Portal, select **Advanced Monitoring > Related dashboards > Data Access Performance - by Nodes**.

Data for all the nodes are visible in the default view. To select data for a node, click the legend parameter for the node below the graph.

Successful requests drill down shows the successful requests by method, node, and protocol.

Failures drill down shows the failed requests by method, node, protocol, and error code.

Compare: select multiple namespaces compares TPS of successful and failed requests, compare read/write bandwidth, compare read/write latency.

View Advanced Monitoring Dashboards- by Protocols

In the **Data Access Performance - by Protocols** dashboard, based on the protocol, you can monitor:

- TPS (success/failure)
- Bandwidth (read/write)
- Failed Requests/s by error type (user/system)

- Latency
- Successful Requests/s by Node
- Failed Requests/s by Node
- Compare TPS of successful requests
- Compare TPS of failed requests
- Compare read bandwidth
- Compare write bandwidth
- Compare read latency
- Compare write latency

To view the **Data Access Performance - by Nodes** dashboard in the ECS Portal, select **Advanced Monitoring > Related dashboards > Data Access Performance - by Protocols**.

Data for all the protocols are visible in the default view. To select data for a protocol, click the legend parameter for the protocol below the graph.

Requests drill down by nodes shows the successful and failed requests by node.

Compare: select multiple namespaces compares TPS of successful and failed requests, compare read/write bandwidth, compare read/write latency.

Share Advanced Monitoring Dashboards

Share dashboard icon enables you to create a direct link to the dashboard or panel, share a snapshot of an interactive dashboard publicly, and export the dashboard to a JSON file.

For procedures on sharing the dashboard link, dashboard snapshot, and dashboard as a JSON file, refer to [Grafana documentation](#).

Flux API

Flux API enables you to retrieve time series database data by sending REST queries using curl. You can get raw data from `fluxd` service in a way similar to using the Dashboard API. You have to get a token, and provide the token in the requests.

Procedure

1. Use `curl https://<ip>:4443/login -k -u "user:passwd" -v` to get the security token.
2. Enter the token in the request header.
 - Query is displayed in the request body.
 - Nginx validates token in `authsvc`, and sends proxy request to `fluxd` on local host.
 - Fluxd handles query, and return results in JSON or .CSV format.

Example of Flux API output:

```
curl -k -H "X-SDS-AUTH-TOKEN: xxxx" -XPOST --data-urlencode
'query=from(bucket: "monitoring_main") |> filter(fn: (r) =>
r._measurement ==
"statDataHead_performance_internal_transactions") |> range(start:
-30m) ' 'https://10.249.230.55:4443/dashboard/v2/query'
```


Example of Dashboard API output:

```
{
  "_links": {
    "self": { "href": "/dashboard/zones/localzone"},
    "storagepools": { "href": "/dashboard/zones/localzone/storagepools" },
    "nodes": { "href": "/dashboard/zones/localzone/nodes" },
    "replicationgroups": { "href": "/dashboard/zones/localzone/replicationgroups" },
    "rglinksFailed": { "href": "/dashboard/zones/localzone/rglinksFailed" },
    "rglinksBootstrap": { "href": "/dashboard/zones/localzone/rglinksBootstrap" }
  },
  "apiChange": "1",
  "name": "vdcl",
  "numNodes": 16,
  ...
  "nodeCpuUtilizationAvg": [ {"t": "12345678", "Percent": 10}, {"t": "23435455", "Percent": 43}, {"t": "55433455", "Percent": 39}],
  ...
  "diskSpaceAllocatedCurrent": [ {"t": "12345678", "Bytes": 10000}, {"t": "23456789", "Bytes": 12000} ]
}
```

Example of Flux API JSON output:

```
{
  [
    {
      "table": "0",
      "_start": "2019-03-06T10:30:00Z",
      "_stop": "2019-03-07T11:15:00Z",
      "time": "2019-03-06T10:30:00Z",
      "_value": 95.30918181366027,
      "field": "usage_idle",
      "measurement": "cpu",
      "cpu": "cpu-total",
      "host": "layton-ivory.ecs.lab.emc.com",
      "node_id": "1f2815b3-b340-45ce-b863-de8f46e8b691",
      "tag": "system"
    },
    {
      "table": "0",
      "_start": "2019-03-06T10:30:00Z",
      "_stop": "2019-03-07T11:15:00Z",
      "time": "2019-03-06T10:35:00Z",
      "_value": 95.52097124715358,
      "field": "usage_idle",
      "measurement": "cpu",
      "cpu": "cpu-total",
      "host": "layton-ivory.ecs.lab.emc.com",
      "node_id": "1f2815b3-b340-45ce-b863-de8f46e8b691",
      "tag": "system"
    },
    {
      "table": "1",
      "_start": "2019-03-06T10:30:00Z",
      "_stop": "2019-03-07T11:15:00Z",
      "time": "2019-03-06T10:30:00Z",
      "_value": 85.41386518615308,
      "field": "usage_idle",
      "measurement": "cpu",
      "cpu": "cpu-total",
      "host": "lehi-ivory.ecs.lab.emc.com",
      "node_id": "48e607ef-2e81-4f8b-b9e2-b61b45ef2240",
      "tag": "system"
    },
    {
      "table": "1",
      "_start": "2019-03-06T10:30:00Z",
      "_stop": "2019-03-07T11:15:00Z",
      "time": "2019-03-06T10:35:00Z",
      "_value": 67.13489651306735,
      "field": "usage_idle",
      "measurement": "cpu",
      "cpu": "cpu-total",
      "host": "lehi-ivory.ecs.lab.emc.com",
      "node_id": "48e607ef-2e81-4f8b-b9e2-b61b45ef2240",
      "tag": "system"
    }
  ]
}
```

Example of Flux API CSV output:

```
#datatype,string,long,dateTime:RFC3339,dateTime:RFC3339,dateTime:RFC3339,double,string,string,string,string,string,string
#group,false,false,true,true,false,false,true,true,true,true,true,true
#default,_result,,,,,,,,,
,result,table,_start,_stop,_time,_value,_field,_measurement,cpu,host,node_id,tag
,,0,2019-03-06T10:30:00Z,2019-03-07T11:15:00Z,2019-03-06T10:30:00Z,95.30918181366027,usage_idle,cpu,cpu-total,dallas-straw,1f2815b3-b340-45ce-b863-de8f46e8b691,system
,,0,2019-03-06T10:30:00Z,2019-03-07T11:15:00Z,2019-03-06T10:35:00Z,95.52097124715358,usage_idle,cpu,cpu-total,dallas-straw,1f2815b3-b340-45ce-b863-de8f46e8b691,system
,,0,2019-03-06T10:30:00Z,2019-03-07T11:15:00Z,2019-03-06T10:40:00Z,85.41386518615308,usage_idle,cpu,cpu-total,dallas-straw,48e607ef-2e81-4f8b-b9e2-b61b45ef2240,system
,,0,2019-03-06T10:30:00Z,2019-03-07T11:15:00Z,2019-03-06T10:45:00Z,67.13489651306735,usage_idle,cpu,cpu-total,dallas-straw,48e607ef-2e81-4f8b-b9e2-b61b45ef2240,system
```

Note: Flux query language that is supported for flux API is a subset of operations that are supported by Influxdb Flux language v0.12. Refer [Get started with Flux](#) for more details.

Query enabled to run by Flux API:

- from <https://docs.influxdata.com/flux/v0.12/functions/inputs/from/>
- filter <https://docs.influxdata.com/flux/v0.12/functions/transformations/filter/>
- range <https://docs.influxdata.com/flux/v0.12/functions/transformations/range/>
- last <https://docs.influxdata.com/flux/v0.12/functions/transformations/selectors/last/>
- first <https://docs.influxdata.com/flux/v0.12/functions/transformations/selectors/first/>
- limit <https://docs.influxdata.com/flux/v0.12/functions/transformations/limit/>
- drop <https://docs.influxdata.com/flux/v0.12/functions/transformations/drop/>
- keep <https://docs.influxdata.com/flux/v0.12/functions/transformations/keep/>

Example of Flux API query:

```
from(bucket: "monitoring_main")
|> filter(fn: (r) => r._measurement ==
"statDataHead_performance_internal_transactions")
|> range(start: -30m)
|> keep(columns: ["_time", "_value", "host"])
```

List of metrics for performance-related data

Table 36 Metrics for performance-related data

Tag	Field reference
host	Name of data node
node_id	ID of data node
tag	Internal, set to dashboard
process	Internal, set to statDataHead
head	Type of protocol
namespace	Name of namespace
method	Protocol-specific request method (GET, POST, READ, WRITE)

Note: When measurement has tags, it is possible to query TSDB for a subset of data. For example, measurements with tag `head` provide information for each protocol independently.

Database `monitoring_main`

Performance metrics in this database are `raw`, each split by data node, all have `node` and `node_id` tags.

Most of integer fields are increasing counters, values that increase over time. Increasing counters restart from zero after data head service restart.

```
Measurement: statDataHead_performance_internal_error
Tags: host, node_id, process, tag
Fields: system_errors (integer)
        user_errors (integer)

Measurement: statDataHead_performance_internal_error_code
Tags: code, host, node_id, process, tag
Fields: error_counter (integer)

Measurement: statDataHead_performance_internal_error_head
Tags: head, host, node_id, process, tag
Fields: system_errors (integer)
        user_errors (integer)

Measurement: statDataHead_performance_internal_error_head_namespace
Tags: head, host, namespace, node_id, process, tag
Fields: system_errors (integer)
        user_errors (integer)

Measurement: statDataHead_performance_internal_latency
Tags: host, id, node_id, process, tag
Fields: +Inf (integer)
        0.0 (integer)
        1.0 (integer)
        111.6295328521717 (integer)
        12461.15260479408 (integer)
        23.183877401213103 (integer)
        2588.0054039994393 (integer)
        4.814963904455889 (integer)
        537.4921713544796 (integer)
        59999.999999999985 (integer)
```

```

Measurement: statDataHead_performance_internal_latency_head
Tags: head, host, id, node_id, process, tag
Fields: +Inf (integer)
        0.0 (integer)
        1.0 (integer)
        111.6295328521717 (integer)
        12461.15260479408 (integer)
        23.183877401213103 (integer)
        2588.0054039994393 (integer)
        4.814963904455889 (integer)
        537.4921713544796 (integer)
        59999.999999999985 (integer)

Measurement: statDataHead_performance_internal_throughput
Tags: host, node_id, process, tag
Fields: total_read_requests_size (integer)
        total_write_requests_size (integer)

Measurement: statDataHead_performance_internal_throughput_head
Tags: head, host, node_id, process, tag
Fields: total_read_requests_size (integer)
        total_write_requests_size (integer)

Measurement: statDataHead_performance_internal_transactions
Tags: host, node_id, process, tag
Fields: failed_request_counter (integer)
        succeed_request_counter (integer)

Measurement: statDataHead_performance_internal_transactions_head
Tags: head, host, node_id, process, tag
Fields: failed_request_counter (integer)
        succeed_request_counter (integer)

Measurement: statDataHead_performance_internal_transactions_head_namespace
Tags: head, host, namespace, node_id, process, tag
Fields: failed_request_counter (integer)
        succeed_request_counter (integer)

Measurement: statDataHead_performance_internal_transactions_method
Tags: host, method, node_id, process, tag
Fields: failed_request_counter (integer)
        succeed_request_counter (integer)

```

Database monitoring_vdc

Performance metrics in this database are calculated values over whole VDC without reference to particular data node.

Most of values are:

- Rates (number of requests per second)- for all measurements not ending by `_delta`
- Delta values (increase of a counter from previous timestamp)- for all measurements ending by `_delta`

```

Measurement: cq_performance_error
Tags: none
Fields: system_errors (float)
        user_errors (float)

Measurement: cq_performance_error_code
Tags: code
Fields: error_counter (float)

Measurement: cq_performance_error_delta

```

```

Tags: none
Fields: system_errors_i (integer)
       user_errors_i (integer)

Measurement: cq_performance_error_head
Tags: head
Fields: system_errors (float)
       user_errors (float)

Measurement: cq_performance_error_head_delta
Tags: head
Fields: system_errors_i (integer)
       user_errors_i (integer)

Measurement: cq_performance_error_ns
Tags: namespace
Fields: system_errors (float)
       user_errors (float)

Measurement: cq_performance_error_ns_delta
Tags: namespace
Fields: system_errors_i (integer)
       user_errors_i (integer)

Measurement: cq_performance_latency
Tags: id
Fields: p50 (float)
       p99 (float)

Measurement: cq_performance_latency_head
Tags: head, id
Fields: p50 (float)
       p99 (float)

Measurement: cq_performance_throughput
Tags: none
Fields: total_read_requests_size (float)
       total_write_requests_size (float)

Measurement: cq_performance_throughput_head
Tags: head
Fields: total_read_requests_size (float)
       total_write_requests_size (float)

Measurement: cq_performance_transaction
Tags: none
Fields: failed_request_counter (float)
       succeed_request_counter (float)

Measurement: cq_performance_transaction_delta
Tags: none
Fields: failed_request_counter_i (integer)
       succeed_request_counter_i (integer)

Measurement: cq_performance_transaction_head
Tags: head
Fields: failed_request_counter (float)
       succeed_request_counter (float)

Measurement: cq_performance_transaction_head_delta
Tags: head
Fields: failed_request_counter_i (integer)
       succeed_request_counter_i (integer)

Measurement: cq_performance_transaction_method
Tags: method
Fields: failed_request_counter (float)
       succeed_request_counter (float)

```

```

Measurement: cq_performance_transaction_ns
Tags: namespace
Fields: failed_request_counter (float)
        succeed_request_counter (float)

Measurement: cq_performance_transaction_ns_delta
Tags: namespace
Fields: failed_request_counter_i (integer)
        succeed_request_counter_i (integer)

```

Dashboard API's to be deprecated or changed in the next release

The dashboard APIs listed below will be deprecated or changed in the next major release of ECS. New or replacement API's are listed for reference. You are advised to make any needed adjustments to the use of these API's in anticipation of the next release.

API to be removed

The following table lists the APIs which will be removed in the future release:

Table 37 API - Remove

API Name	Syntax	Description
Get Process	GET /dashboard/processes/{id}	Gets the process instance details.
Get Node Processes	GET /dashboard/nodes/{id}/processes	Gets the details of processes in the node.
Get Hosted Zone	GET /dashboard/zones/hostedzone	Gets the hosted VDC details.
Get Zone	GET /dashboard/zones/{id}	Gets the hosted VDC details.
Get Hosted Zone Replication Groups	GET /dashboard/zones/hostedzone/replicationgroups	Gets the hosted VDC replication groups details.

API to be changed

The following table lists the APIs which will be changed in the future release:

Table 38 API - Change

API Name	Syntax	Description
Get Local Zone	GET /dashboard/zones/localzone	Gets the local VDC details.
Get Local Zone Nodes	GET /dashboard/zones/localzone/nodes	Gets the local VDC node details.
Get Node	GET /dashboard/nodes/{id}	Gets the node instance details.
Get Storage Pool Nodes	GET /dashboard/storagepools/{id}/nodes	Gets the details of nodes in the storage pool.

The following data will be removed from the APIs:

- - nodeCpuUtilization*, nodeMemoryUtilizationBytes*, nodeMemoryUtilization*,
 - nodeNicBandwidth*, nodeNicReceivedBandwidth*, nodeNicTransmittedBandwidth*
 - nodeNicUtilization*, nodeNicReceivedUtilization*, nodeNicTransmittedUtilization*
 - capacityRebalanceEnabled, capacityRebalanced, capacityPendingRebalancing
 - capacityRebalancedAvg, capacityRebalanceRate, capacityPendingRebalancingAvg
 - transactionReadLatency, transactionWriteLatency, transactionReadBandwidth, transactionWriteBandwidth
 - transactionReadTransactionsPerSec, transactionWriteTransactionsPerSec, transactionErrors.*
 - diskReadBandwidthTotal, diskWriteBandwidthTotal, diskReadBandwidthEc, diskWriteBandwidthEc
 - diskReadBandwidthCc, diskWriteBandwidthCc, diskReadBandwidthRecovery, diskWriteBandwidthRecovery
 - diskReadBandwidthGeo, diskWriteBandwidthGeo, diskReadBandwidthUser
 - diskWriteBandwidthUser, diskReadBandwidthXor, diskWriteBandwidthXor

API to stay without change

The following table lists the APIs, which will not be changed:

Table 39 API - No change

API Name	Syntax	Description
Get Local Zone Storage Pools	GET /dashboard/zones/localzone/storagepools	Gets the local VDC storage pool details.
Get Local Zone Replication Groups	GET /dashboard/zones/localzone/replicationgroups	Gets the local VDC replication groups details.
Get Local Zone Replication Group Failed Links	GET /dashboard/zones/localzone/rglinksFailed	Gets the local VDC replication group failed links details.
Get Local Zone Disks	GET /dashboard/zones/localzone/disks	Gets the local VDC disks details.
Get Storage Pool	GET /dashboard/storagepools/{id}	Gets the storage pool details.
Get Disk	GET /dashboard/disks/{id}	Gets the disk instance details.
Get Node Disks	GET /dashboard/nodes/{id}/disks	Gets the details of disks in the node.
Get Local Zone Replication Group Bootstrap Links	GET /dashboard/zones/localzone/rglinksBootstrap	Gets the local VDC replication group bootstrap links details.
Get Replication Group	GET /dashboard/replicationgroups/{id}	Gets the replication group instance details.
Get RG Link	GET /dashboard/rglinks/{id}	Gets the replication group link instance details.

Table 39 API - No change (continued)

API Name	Syntax	Description
Get Replication Group Links	GET /dashboard/replicationgroups/{id}/rlinks	Gets the replication group instance associated link details.
Get Replication Group Data Table	GET /dashboard/datatables/{id}	Gets the datatable details.
Get Replication Group Data Tables	GET /dashboard/replicationgroups/{id}/datatables	Gets the details of the datatables in the replication group.
Get Cas Gc Buckets	GET /dashboard/zones/localzone/cas	Gets the local VDC CAS GC buckets details
Get Cas Gc Bucket	GET /dashboard/cas/{id}	Gets the CAS GC bucket instance details.

Flux API for deprecated dashboard API

You can retrieve analogues of metrics currently available through dashboard API, which will be deprecated in the future release. Flux API will provide API for metrics used to build new Advanced Monitoring dashboards. Node or process level metrics will be available as raw metrics. In ECS 3.4 not all the metrics which are planned to be deprecated in a future version are available through Flux API. The metrics that are available in ECS 3.4 is listed here:

Processes statistics

- Dashboard API
GET /dashboard/nodes/{id}/processes
- Flux API
Database: monitoring_op
Measurement: procstat
Fields: memory_rss, cpu_usage, and num_threads
Tags: host - hostname (fqdn), node_id - host id and process_name. The valid process names are:
 - blobsvc
 - cm
 - coordinatorsvc
 - dataheadsvc
 - dtquery
 - ecsportalsvc
 - eventsvc
 - georeceiver
 - metering
 - metering
 - objcontrolsvc
 - resourcesvc
 - transformsvc
 - vnest

- fluxd
- influxd
- throttler
- grafana-server
- dockerd
- fabric-agent
- fabric-lifecycle
- fabric-registry
- fabric-zookeeper

Nodes statistics

- Dashboard API
GET /dashboard/nodes/{id}
- Flux API
Database: monitoring_op
Measurement : cpu
Fields: usage_idle
Tags:
 - host - hostname (fqdn)
 - node_id - host id
 Measurement : mem
Fields: free - free memory on host (bytes)
Tags:
 - host - hostname (fqdn)
 - node_id - host id

Performance statistics

- Dashboard API
 - GET /dashboard/nodes/{id}
 - GET /dashboard/zones/localzone
 - GET /dashboard/zones/localzone/nodes
- Flux API: See *List of metrics for performance-related data* section for details.

