Release Notes for COS 2.1.1

OL-31733-01

Last Updated: February 13, 2015

These release notes describe the features and caveats for all releases in the Cisco Cloud Object Store (COS) Release 2.x train.

These release notes are updated with each release in the train. This update adds information for Cisco COS Release 2.1.1. For a list of the caveats that apply to this release, see the "Caveats" section on page 7.

Contents

The following information is in the release notes:

Cisco Systems, Inc.
www.cisco.com

Introduction

The Cisco Cloud Object Store (COS) provides distributed, resilient, high-performance storage and retrieval of binary large object (blob) data. The primary interface for managing COS content is the OpenStack Swift API, with enhancements that improve the quality of service when accessing large media objects.

Object storage is distributed across a cluster of hardware systems, or nodes. The storage cluster is resilient against hard drive failure within a node and against node failure within the cluster. Nodes may be added to or removed from the cluster as needed to provide for changes in cluster capacity.

COS includes COS Service Manager (SM), which provides a web-based GUI as well as related ReST APIs, to simplify setup and management. COS also provides a command-line interface (CLI) for remote or programmatic content management. COS also includes an authentication and authorization service that implements the OpenStack Swauth API.

Through its various management interfaces, COS provides access to large media objects while maintaining high quality of service, supports cluster management, and coordinates the replication of data across sites to improve resiliency and optimize the physical location of stored data.

Related Products

COS 2.1.1 can be implemented as a managed service of Cisco Media Origination System (MOS) 2.3. In this configuration, COS content is managed through the MOS SM GUI.

COS 2.1.1 also interoperates with an upcoming Cisco TV VDS release to provide cloud storage for recorded video programming.

Feature Overview

The table below provides an overview of the COS features. For full descriptions of these features, see the *Cisco Cloud Object Store Release 2.1.1 User Guide*.

Table 1-1 Overview of COS Features

Feature Set	Features
COS Service Manager GUI	• Lets you quickly and easily access many COS deployment and monitoring functions
High Availability (HA)	• COS now supports HA as implemented in MOS
Swauth API	• Simple Auth Service API for authentication of Swift operations • Based on Swauth Open-Source Middleware API • Used to manage accounts, users and account service endpoints

Table 1-1 Overview of COS Features

Feature Set	Features
Swift Object Store API	• An implementation of a subset of the continually evolving OpenStack Swift API • Command executions are authenticated using auth tokens provided by Swauth service • Used to create and manage containers and objects for persistent storage in a COS cluster
Object Store Metadata Resiliency	• Metadata resiliency is provided by a distributed and replicated Cassandra document database • Each COS node participates in the persistence of a subset of the Cassandra database • Manual administrative intervention required upon node failure
Object Store Data Resiliency	• Data is resilient to both hard drive and COS node failures • Local COS node data resiliency provided by local software RAID • COS cluster data resiliency provided by object replication
Service Load Balancing	• COS cluster load balancing is provided by DNS round-robin of a FQDN to multiple physical IPv4 addresses hosted by COS nodes • Optimal load balancing is provided by extensions to the Swift API through the implementation of HTTP redirect

Unsupported Features

The following features are not supported in COS 2.1.1, but are under consideration for future releases:

- Support for multiple-site cluster management
- Support for node failover
- Support for Server RAID
- Support for IPv6

The OpenStack SWIFT and SWAuth APIs continue to evolve. COS does not current implement a full complement of SWIFT or SWAuth API functions. For a list of currently supported functions, see the *Cisco Cloud Object Store Release 2.1.1 User Guide*.

COS 2.1.1 does not support automatic failover of Cassandra working sets in the event of COS node failure. Manual administrative action is required to recover a lost COS node in the event that a COS node cannot be returned to service in a timely manner.

Hardware Support

COS 2.1.1 supports the following hardware as COS storage cluster nodes:

- 460-4R1: CDE-460 with 36 x 3 TB hard drives
- 460-4R3: CDE-460 with 36 x 4 TB hard drives
- 470-4R2: CDE-470 with 72 x 4 TB hard drives

For hardware installation instructions and related details, see the Cisco Content Delivery Engine 205/220/250/420/460/470 Hardware Installation Guide.

Installation

The CDE-460 and CDE-470 appliances used for COS ship with the COS software pre-installed but not configured. The installation software is an .iso file that includes the base (CentOS) distribution of Linux along with all of the additional rpm packages needed by a COS node.

The same .iso file can be used to reinstall or upgrade the software on an existing COS node. For additional details, see the *Cisco Cloud Object Store Release 2.1.1 User Guide*.

Installing COS Swauth and COS Swift Utilities

The cos-swauth and cos-swift utilities are included in the COS software ISO image, and are packaged as an RPM contained within a YUM repository on the ISO. To install the utilities, you first copy the ISO to the target client machine, and then mount it to the /mnt/cdrom location on the client.

Note The cos-swauth and cos-swift commands are intended to be executed on a CentOS 6.4 installation on a client machine, not on the COS nodes directly, and communicate with the COS cluster over the network using the Swift and Swauth protocols.

These utilities are intended only to exercise the service protocols. They are not intended to be tools for managing the COS nodes or COS cluster, and do not in any way replace the Service Manager.

After copying the ISO to the client machine, install the utilities as follows:

Step 1 Copy the ISO to the client machine.

Step 2 Mount the ISO as shown in the following example:

```
[root@utah96 ~]# ll cos_repo-2.1.1.iso
-rw-r--r-- 1 root root 250613760 Dec 12 20:39 cos_repo-2.1.1.iso
[root@utah96 ~]# mount -oloop cos_repo-2.1.1.iso /mnt/cdrom
```

Step 3 Configure the YUM repository as shown in the following example:

```
[root@utah96 ~]# cd /mnt/cdrom
[root@utah96 cdrom]# ./local_repo_setup
Loaded plugins: fastestmirror
Determining fastest mirrors
cos-2.1.1-0b8                 | 3.6 kB     00:00 ...
cos-2.1.1-0b8/group_gz        |  536 B     00:00 ...
cos-2.1.1-0b8/filelists_db    |  66 kB     00:00 ...
cos-2.1.1-0b8/primary_db      |  43 kB     00:00 ...
```

```
cos-2.1.1-0b8/other_db     |  20 kB     00:00 ...
Metadata Cache Created
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
repo id           repo name                          status
cos-2.1.1-0b8     Cisco Cloud Object Store 2.1.1     57
repolist: 57
```

Step 4 Install the package as shown in the following example:

```
[root@utah96 ~]# yum install cos-cli
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package cos-cli.x86_64 0:2.1.1-cos0.1 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
Package        Arch       Version        Repository         Size
================================================================================
Installing:
cos-cli        x86_64     2.1.1-cos0.1   cos-2.1.1-0b8      142 k

Transaction Summary
================================================================================
Install       1 Package(s)

Total download size: 142 k
Installed size: 635 k
Is this ok [y/N]: y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : cos-cli-2.1.1-cos0.1.x86_64              1/1
  Verifying  : cos-cli-2.1.1-cos0.1.x86_64              1/1

Installed:
  cos-cli.x86_64 0:2.1.1-cos0.1

Complete!
```

You can now display help for the utilities by entering the commands shown below.

For cos-swauth:

```
[root@utah96 ~]# cos-swauth

Usage:  The 'cos-swauth' command-line utility is used to manage
    authentication accounts and users in a COS cluster using
    the Swauth API. The command options are given below:

cos-swauth [-a <auth-ip>] [-u <admin-user>] [-k <admin-key>]
    [-h/--help <sub-command>] [-v/--verbose] <sub-command [options]>

    -a <auth-ip>
        The IP address of the COS authentication service. May alternatively
    be specified by setting the COS_AUTH_IP environment variable.

-u <admin-user>
```

```
    Name of the user authorizing the command. Defaults to
'.super_admin'. Other admin user names are specified as
<account>:<user>. The admin user name may alternatively be
specified by setting the COS_ADMIN_USER environment variable.

-k <admin-key>
    The authentication key (password) of the admin user.
The admin key may alternatively be specified by setting
the COS_ADMIN_KEY environment variable.

-h/--help [sub-command]
    Subcommands include 'l/list', 'sa/set-account', 'su/set-user',
    'g/get', 'i/info', 'd/delete'

-v/--verbose
    Prints extra information

sub-command [options]
    Subcommands include '-l/list', '-sa/set-account',
'-su/set-user', '-g/get', '-i/info', '-d/delete'
```

For cos-swift:

```
[root@utah96 ~]# cos-swift

cos-swift [-t <auth-token>] [-a <storage-url>] [-v/--verbose]
        [-h/--help <sub-command>] <sub-command [options]>

    -t <auth-token>
        Authentication token returned by 'cos-swauth get', also be
    specified by setting environment variables 'COS_AUTH_TOKEN'.

    -a <storage-url>
        Storage URL returned by 'cos-swauth get',also be specified
    by setting environment variables 'COS_STORAGE_URL'.

    -v/--verbose
        Prints extra information

    -h/--help [sub-command]
        Subcommands include 'i/info','l/list','s/set','g/get','u/update','d/delete'.

    sub-command [options]
        Subcommands include '-i/info','-l/list','-s/set','-g/get','-u/update','-d/delete'.
```

Supported Environments

COS 2.1.1 supports a Swift/Swauth API environment, and also supports an HTTP-based API for cluster management.

System Requirements

COS 2.1.1 can operate as a managed service of MOS 2.3, in which case it uses certain MOS HTTP interface components as well as the MOS Document Store for system management. See the MOS 2.3 documentation for MOS system requirements.

Caveats

Caveats describe unexpected behavior in COS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only selected severity 3 caveats are included in the caveats document.

Caveat numbers and brief descriptions for Cisco COS Release 2.1.1 releases are listed in this section.

Open Caveats

Open Caveats for Cisco COS Release 2.1.1

Table 2 lists the open issues in the COS 2.1.1 release.

Bug details are displayed in the Bug Search.

Table 2 Open Caveats in COS 2.1.1 Release

Bug ID	Description
CSCus08986	211B6: cosd dead after post-initial-setup reboot. An issue was found in which the cosd daemon crashed after an initial COS node configuration and reboot. The issue can be verified by executing the “service cosd status” command on the node console. This issue is more likely to occur after the initial node configuration and the first reboot. The Cassandra daemon takes longer to initialize, and this precipitates the cosd crash. To resolve this issue, no operator action is required. The cosd daemon will automatically be restarted within 60 seconds after the crash.
CSCus09019	One node http 500 error after cassandra restart in both nodes. An issue was found in which all requests directed to a malfunctioning COS node may fail with a 500 "Service Unavailable" status. To duplicate this issue while all nodes are in a correctly running state, manually stop only the Cassandra service on all nodes. Wait 20 seconds, then manually restart the Cassandra service on all nodes. This may result in the cosd daemon on one or more nodes being unable to reconnect to the Cassandra service after it has been restarted. To resolve this issue, restart the cosd daemon on the affected nodes by executing "service cosd restart" on the node console.

Table 2 Open Caveats in COS 2.1.1 Release (continued)

Bug ID	Description

CSCus11580	Decommission skipped when node removed from 2-node cluster.
	
	An issue was found in which a node is removed from a two-node Cassandra cluster using the COS SM GUI, but after removal, sometimes appears listed as "DN" (down) in the output when running the "nodetool status" command on the remaining node in the cluster.
	
	The root cause of this issue is that the COS AIC client receives notifications at different times about the nodes in a cluster changing and about their removal. At the time a node is removed, if the COS AIC client finds only one node in the cluster, it skips decommission as there is apparently no other node to which it can stream data.
	
	To avoid this issue:
	
	• Before removing a node from a two-node cluster, first ensure the replication factor is 2, and then run "nodetool repair" manually on both nodes.
	
	This ensures that the system will not be adversely affected even if the decommission gets skipped when the node is removed from cluster.
	
	• After removing the node from cluster, if decommission gets skipped, run the commands **nodetool status** and **nodetool removenode <hostid>** on the other (up, "UN") node to locate its host ID and remove it from the Cassandra cluster:
	
	For example:
	
	`# nodetool status cos`
	`...`
	`-- Address Load Tokens Owns (effective) Host ID`
	`Rack`
	`UN 172.22.99.127 55.77 KB 256 52.9%`
	`15235785-a7fb-43ae-9efa-73083c30d7db RAC1`
	`DN 10.74.116.216 63.57 KB 256 47.1%`
	`bc28aa44-85d2-4b43-bf71-b92561f8fe81 RAC1`
	
	`# nodetool removenode bc28aa44-85d2-4b43-bf71-b92561f8fe81`

CSCus18144	COS-AIC: After changing ippool, the preivous IPs added to DNS. After changing the IP Pool reference for a C/F interface, the external DNS may reference both the old and the new C/F interface IPs. This condition is only met when the C/F interface(s) are not currently "enabled," and the user changes the IP Pool reference from pool "X" to pool "Y" using the PAM GUI or SM API. Prior to switching the IP Pool reference, ensure that the individual C/F interfaces are set to "enabled" in the PAM GUI (or via SM API). Put the node into "Maintenance" mode, then change the IP Pool reference(s) for the C/F interfaces. Once the process is complete, you may again set the interfaces to "disabled" and then reboot the node so cServer can pickup the new addresses. If the above procedure is not followed and the external DNS shows both old and new IP addresses, the external DNS will have to be edited to correct the problem.

Table 2 Open Caveats in COS 2.1.1 Release (continued)

Bug ID	Description
CSCur84487	Mackenzie: Get token failed while COS is rebooting and recovering An issue was found in which some COS Swift and Swauth API requests fail with a "500 (Service Unavailable)" response. During COS node shutdown and during COS node start-up, there is a window of time during which requests may execute more slowly if they require metadata stored on that node. In some cases, the metadata access or modification portion of the request may exceed 60 seconds in duration. In this case, COS will respond to the affected request with a "500 (Service Unavailable)" status. To help avoid this issue, schedule node shutdown and restart for time periods when there is less activity in the system. This reduces, but does not eliminate, the possibility of "500 (Service Unavailable)" responses.

CSCur92063	Cassandra db-remove mechanism issue.
	
	When a node is added to a cluster using the COS SM GUI, the COS AIC client tries to initialize the Cassandra database on the node being added. If the initialization fails, the db-init flag that marks successful initialization of the database is not set.
	
	Later, if an attempt is made to remove the node from the cluster using the COS SM GUI, the Cassandra initialization script (cassandra-init) my still launch due to the db-init flag not being set.
	
	The COS AIC client log (/arroyo/log/cos-aic-client.log) may contain the following messages:
	
	`DB running`
	`Done initializing DB`
	`[2014-11-27 21:13:24.478] [INFO] aicc - db-init exited normally`
	`[2014-11-27 21:13:24.478] [INFO] aicc - Done writing dbinitflag`
	
	These messages indicate that db-init was attempted and dbiniflag was written.
	
	If the cassandra-init script succeeds this time, it may leave the COS node in a state where the Cassandra database is initialized and started on the node, and the node is still part of the database cluster even though it is not part of COS cluster.
	
	If the COS node ends up in this state, run the following script on the node that was supposed to be decommissioned from the Cassandra database cluster:
	
	`sh /opt/cisco/cos-aic-client/cassandra/cassandra-remove.sh`
	
	Or, if this is the only node remaining in the cluster, run:
	
	`sh /opt/cisco/cos-aic-client/cassandra/cassandra-remove.sh solitary`
	
	This script will decommission the node (if not the only remaining node), shut down the Cassandra service, remove the Cassandra service from the list of services to be started at boot, and delete any stored Cassandra data.

CSCur95716	Gossip issue when COS node is added to cluster. When a COS node is added to a cluster and then removed using the COS SM GUI, the COS node may still appear in the Cassandra cluster, but the Cassandra service may fail to start. This issue is intermittent, and is most likely to occur with clusters containing more than three nodes.

Table 2 Open Caveats in COS 2.1.1 Release (continued)

Bug ID	Description
CSCur99109	Bootstrapping issue when starting up the Cassandra service. When two or more nodes are added to a cluster in quick succession, an issue may arise in which the Cassandra service fails to initialize on the new node, preventing it from being added to the Cassandra cluster. This failure is indicated by the following error message in the Cassandra event log (/var/log/cassandra/cassandra.log): `Exception encountered during startup: Other bootstrapping/leaving/moving nodes detected, cannot bootstrap while cassandra.consistent.rangemovement is true.` The root cause of this issue is that the node is being added while the Cassandra cluster topology is still in flux, so that initialization of the new node cannot proceed. To avoid this possible issue, be sure to provide (or have a script provide) a time delay of at least two minutes between adding two nodes to the cluster in sequence.

Table 2 Open Caveats in COS 2.1.1 Release (continued)

Bug ID	Description

CSCur99122	Replication factor should not be 3 when a third node fails to be added.
	
	When trying to add a third node to a two-node cluster, the Cassandra database sometimes fails to initialize on the third node, and the following error message appears in the COS AIC client log (/arroyo/log/cos-aic-client.log):
	
	`Starting-up DB seems to be taking too long, aborting`
	`[2014-12-03 05:39:31.451] [ERROR] aicc - db-init exited with code: 245`
	
	This message suggests that the Cassandra database did not successfully initialize on the new node. Despite this failure, the existing nodes in the cluster still may have an updated replication factor.
	
	In lab testing, it was found that the replication factor got updated even when a new node failed to be added to a cluster or when an existing node failed to be removed from a cluster.
	
	Ideally, the replication factor should be 1 for one node, 2 for two nodes, or 3 for three or more nodes in the cluster. If the replication factor is too high or too low, use the following script on any one node in the cluster to adjust it:
	
	`sh /opt/cisco/cos-aic-client/cassandra/cassandra-adjust-replication.sh {1 | 2 | 3}`
	
	For the final argument, use 1 for one node, 2 for two nodes, or 3 for three or more nodes in the cluster.
	
	To determine which replication factor is currently set in a cluster, run the **cqlsh** command on an existing node in a cluster with Cassandra running.
	
	For example:
	
	`[root@cos460-1 tmp]# cqlsh 172.22.97.207`
	`...`
	`cqlsh> SELECT * from system.schema_keyspaces;`
	
	`keyspace_name | durable_writes | strategy_class | strategy_options`
	`---------------+----------------+--------------------------------------`
	`---------------+----------------------------`
	`...`
	`cos | True | org.apache.cassandra.locator.NetworkTopologyStrategy |`
	`{"DC1":"3"}`
	
	where `{"DC1":"3"}` in this example indicates a replication factor of 3.

Accessing Bug Search Tool

This section explains how to use the Bug Search tool to search for a specific bug or to search for all bugs in a release.

Step 1 Go to https://tools.cisco.com/bugsearch/.

Step 2 At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, enter the bug ID in the Search For field, and press **Enter**.

Step 4 To search for bugs in the current release, specify the following criteria:

- Select the **Model/SW Family** Product Category drop-down list box, then enter **Cisco Videoscape Distribution Suite for Television** or select the name from the **Select from list** option.
- Select **Cisco Videoscape Distribution Suite for Television** from the list that displays.
- The **Cloud Object Store** type displays in the Software Type drop-down list box.
- Releases: 2.0.1.
- Advanced Filter Options—Define custom criteria for an advanced search by selecting an appropriate value from the drop-down lists by choosing either one Filter or multiple filters from the available categories. After each selection, the results page will automatically load below the filters pane. If you select multiple filters, it behaves like an AND condition.
  - Modified Date—Select one of these options to filter bugs: **Last Week**, **Last 30 days**, **Last 6 months**, **Last year**, or **All**.
  - Status—Select **Fixed**, **Open**, **Other**, or **Terminated**.

    Select **Fixed** to view fixed bugs. To filter fixed bugs, uncheck the Fixed check box and select the appropriate suboption (Resolved or Verified) that appears below the Fixed check box.

    Select **Open** to view all open bugs. To filter the open bugs, uncheck the Open check box and select the appropriate suboptions that appear below the Open check box.

    Select **Other** to view any bugs that are duplicates of another bug.

    Select **Terminated** to view terminated bugs. To filter terminated bugs, uncheck the Terminated check box and select the appropriate suboption (Closed, Junked, or Unreproducible) that appears below the Terminated check box. Select multiple options as required.
  - Severity—Select the severity level:

    1: Catastrophic.

    2: Severe

    3: Moderate

    4: Minor

    5: Cosmetic

    6: Enhancement
  - Rating—Select the bug's quality rating: **5 Stars** (excellent), **4 or more Stars** (good), **3 or more Stars** (medium), **2 or more Stars** (moderate), **1 or more Stars** (poor), or **No Stars**.
  - Support Cases—Select whether the bug **Has Support Cases** or **No Support Cases**.
  - Bug Type—Select whether the bug is **Employee Visible & Customer Visible** or **Customer Visible Only**.

Step 5 The Bug Toolkit displays the list of bugs based on the specified search criteria.

Step 6 You can save or email the current search by clicking their respective option.

If you have any problems using the Bug Search tool, log into the Technical Support website at http://www.cisco.com/cisco/web/support/index.html or contact the Cisco Technical Assistance Center (TAC).

Related Documentation

Refer to the following documents for additional information about the Cisco COS 2.0.1:

- *Cisco Cloud Object Store Release 2.1.1 User Guide*
- *Cisco Content Delivery Engine 205/220/250/420/460/470 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for Cisco Content Delivery Engines*
- *Open Source Used in Cisco COS 2.1.1*

  http://www.cisco.com/en/US/products/ps12653/products_licensing_information_listing.html

The entire VDS-TV software documentation suite is available on Cisco.com at:

http://www.cisco.com/en/US/products/ps12653/tsd_products_support_series_home.html

The entire VDS hardware documentation suite is available on Cisco.com at:

http://www.cisco.com/en/US/products/ps7126/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.