Cisco Application Services Engine Release Notes, Release 1.1(3)

Cisco Application Services Engine provides a common platform for deploying Cisco Data Center applications. These applications provide real time analytics, visibility, and assurance for policy and infrastructure.

This document describes the features, issues, and limitations for Cisco Application Services Engine for the fabric external mode.

For more information, see Related Content.

Date	Description
January 28, 2022	Release 1.1(3f) became available. Additional open issue CSCwa47299 for prior releases.
December 22, 2020	Release 1.1(3e) became available. Additional open issues for 1.1(3d) release.
July 2, 2020	Release 1.1(3d) became available.
May 18, 2020	Release 1.1(3c) became available.

Content

New Software Features

Note: Beginning from Cisco Application Services Engine Release 1.1(3), only the fabric external mode is supported.

Feature	Description

GUI support for fabric external mode	Added GUI support for all the operations of the Cisco Applications Services Engine.
Multifabric support	Service nodes can be spanned across the fabrics based on the latency and bandwidth requirements of apps.
Horizontal Scaling	Added “worker nodes” in addition to master nodes. Upto 4 worker nodes can be added to a cluster. Worker nodes can be spanned across the fabrics.
Basic RBAC support	An administrator can grant access to several users.
Cluster upgrade and downgrade	Firmware Management is used to perform cluster or firmware upgrade or downgrade.
Tech support	An administrator can perform technical support collections, faults and events, to process core files and debug data from the fabric to any external host.
Backup & Restore	An administrator can backup the configuration and restore the same configuration from the backup.
Audit logs	Audit Logs are user triggered configuration changes.

Changes in Behavior

If you are deploying or upgrading to this release:

- Downgrading from Release 1.1.3d or later to Release 1.1.3c is not supported.
- If your cluster is running Network Assurance Engine, Release 5.0.1 or 5.0.1a, upgrading from Release 1.1.3d to Release 1.1.3e is not supported. In this case, we recommend that you upgrade to Nexus Dashboard, Release 2.0.1 instead.
- Nexus Insights deployment with Management and Data network in same subnet are not supported.

Open Issues

This section lists the open issues. Click the bug ID to access the Bug Search tool and see additional information about the issue. The "Exists In" column of the table specifies the releases in which the issue exists.

Bug ID	Description	Exists in
CSCvu28666	Intersight device connector should connect to Cisco APIC using the Cisco APIC Inband IP.	1.1(3c)
CSCvu29151	Intersight device connector upgrade does not happen on all the pods.	1.1(3c)
CSCvu21661	When logging into the Nexus Dashboard GUI, you may get intermittent "Middleware error" responses.	1.1(3d)
CSCvv76180	API server will return 500 errors when a node is down for long periods of time.	1.1(3d)

CSCvv78541	On one node shutdown, MSO mongodb will fail because of loss of quorum resulting in MSO app unusable.	1.1(3d)
CSCvv86087	The /logs/kms/ directory may become full due to excess bin logging.	1.1(3d)
CSCvv82660	When Management and Data network are in same subnet, traffic is not routed properly.	1.1(3d)
CSCvw20211	With ASE 1.1.3d, SSH to OOB interface from external server on the same network with data, does not produce response. SSH to data interface does respond.	1.1(3d)
CSCvw23388	Upgrade of MSO app fails with an error to execute the pre-upgrade hooks for the application.	1.1(3d)
CSCvq72219	NTP, DNS, Firmware, DC proxy over inband management is not supported.	1.1(3c) and later
CSCvt78295	API shows active status for all the nodes, even though one node is down.	1.1(3c) and later
CSCvu25186	After Cisco Application Services Engine session timeout, the app page shows "Authorization field missing" error upon refreshing the page.	1.1(3c) and later
CSCvu13175	Upgrade GUI shows error when nodes are upgrading and upgrade status is not visible.	1.1(3c) and later
CSCvu18725	DNS search domains are not updated until the Cisco Application Service Engine nodes are rebooted.	1.1(3c) and later
CSCvu21304	Intersight device connector connects to the intersight over the Cisco Application Services Engine Out-Of-Band Management.	1.1(3c) and later
CSCvt72554	Audit logs are not generated for Cisco Application Services Engine upgrade or downgrade.	1.1(3c) and later
CSCvu28529	IP address of the NTP server is required during the first-boot setup.	1.1(3c) and later
CSCvu81594	Intersight DeviceConnector in Cisco ASE 1.1.3 allows read-only user to view and configure its settings.	1.1(3c) and later

CSCvu86665	In certain conditions, pods are running ready but this is not reported at service level. This creates two issues: 1) Breaks the health check where we expect all the instances of a service running and ready and can eventually lead to upgrade failure. 2) As one of the endpoint is missing from service, it impacts API load balancing across all endpoints for a given service.	1.1(3c) and later
CSCvw86325	This is socket leak in docker daemon hence it's possible that over the period of time docker gets to socket limit and kubelet fails to communicate with docker at all. In specific situation, impacted node will be moved to ?not-ready? state and will not recover automatically. As the node is marked as not-ready, usual pod eviction will be triggered. UI will show node status into error as well set of services into failed state.	1.1(3d) and later
CSCwa47299	Evaluation of nd-appliance for Log4j RCE (Log4Shell) Vulnerability vulnerability.	1.1(3c)-1.1(3e)
CSCvv75573	in 1.1.3 version, SE upgrade fails with workers trying to upgrade before all primary nodes are upgraded.	1.1(3e) and later

Resolved Issues

This section lists the resolved issues. Click the bug ID to access the Bug Search tool and see additional information about the issue. The "Fixed In" column of the table specifies whether the bug was resolved in the base release or a patch release.

Bug ID	Description	Fixed in
CSCvu28666	Intersight device connector should connect to Cisco APIC using the Cisco APIC Inband IP.	1.1(3d)
CSCvu29151	Intersight device connector upgrade does not happen on all the pods.	1.1(3d)
CSCvu21661	When logging into the Nexus Dashboard GUI, you may get intermittent "Middleware error" responses.	1.1(3e)
CSCvv76180	API server will return 500 errors when a node is down for long periods of time.	1.1(3e)
CSCvv78541	On one node shutdown, MSO mongodb will fail because of loss of quorum resulting in MSO app unusable.	1.1(3e)
CSCvv86087	The /logs/kms/ directory may become full due to excess bin logging.	1.1(3e)
CSCvv82660	In Application Services Engine 1.1.3, upgrade fails with workers trying to upgrade before all primary nodes are upgraded.	1.1(3e)
CSCvw20211	With ASE 1.1.3d, SSH to OOB interface from external server on the same network with data, does not produce response. SSH to data interface does respond.	1.1(3e)

CSCvw23388	Upgrade of MSO app fails with an error to execute the pre-upgrade hooks for the application.	1.1(3e)
CSCwa47299	Evaluation of nd-appliance for Log4j RCE (Log4Shell) Vulnerability vulnerability.	1.1(3f)

Compatibility Information

For Cisco Applications Service Engine compatibility with Day-2 Operations and ACI Multi-Site Orchestrator apps, see the Cisco Day-2 Operations Apps Support Matrix.

Related Content

See the Cisco Application Services Engine page for the documentation.

The documentation includes installation, upgrade, configuration, programming, and troubleshooting guides, technical references, and release notes, as well as other documentation.

Document	Description
Cisco Application Services Engine Release Notes	This document.
Cisco Application Services Engine Deployment Guide	Describes how to download, install, and set up Cisco Application Services Engine cluster.
Cisco Application Services Engine User Guide	Describes how to use Cisco Application Services Engine cluster and GUI.
Cisco Application Services Engine Hardware Installation Guide	Describes how to install and set up Cisco Application Services Engine hardware.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to ciscodcnapps-docfeedback@cisco.com.

Legal Information