Cisco Elastic Services Controller 6.0 Release Notes

First Published: 2023-10-26

Introduction

Cisco Elastic Services Controller (ESC) is a Virtual Network Functions Manager (VNFM), which performs lifecycle management of Virtual Network Functions (VNFs).

The Cisco Elastic Services Controller (ESC) promotes agility, flexibility, and programmability in Network Function Virtualization (NFV) environments, and offers comprehensive automated lifecycle management capabilities. By design, Cisco ESC is built as an open and a modular system. It provides a single point of control to manage all aspects of VNF lifecycle for generic virtual network functions (VNFs) in a dynamic environment. Drawing on industry standards and open APIs, you can control the full lifecycle of all of your virtualized resources, whether using Cisco or third-party VNFs, allowing you to choose best-of-breed industry solutions.

- As part of the Cisco Orchestration Suite, ESC is packaged with Cisco Network Services Orchestrator (NSO) and Cisco NFV Orchestrator (NFVO) bundle. This is available within Cisco Solutions such as Cisco Managed Services Accelerator (MSX).
- As a Specialized Virtual Network Function Manager (SVNFM), ESC tightly integrates with the Cisco Mobility VNFs.
- ESC can also be utilized as a Generic Virtual Network Function Manager (GVNFM) to provide lifecycle management for both Cisco and third-party VNFs.

Supported Virtual Infrastructure Managers (VIM)

ESC supports lifecycle management of VNFs on OpenStack, VMware vCenter, vCloud Director, and so on. For more details, see the Cisco Elastic Services Controller Install and Upgrade Guide.

New Features and Enhancements in 6.0

ESC 6.0 release focuses on fixing security vulnerabilities and upgrading the 3rd party libraries to their recent version. As part of the exercise, the following are the upgrades done in this release:

- **Base Operating System Change: From CentOS to Cisco Secure Linux based on Alma Linux** –

  Till ESC 5.10, the core operating system was CentOS 7.9 bundled with ESC rpm, since CentOS is nearing the end of life or support, from ESC 6.0 release, the base operating system has been changed to Cisco Secure Linux based on Alma Linux version 8.8.

- **3rd Party Component Upgrades:**
  - **PostgreSQL upgrade:** ESC 6.0 uses PostgreSQL version 15.2, an upgrade from PostgreSQL 9.4 version used in previous releases.

- **ConfD upgrade:** ESC 6.0 uses ConfD version 7.2.6, an upgrade from ConfD 6.6.1 version used in previous releases.
- **Spring Boot Framework upgrade:** ESC 6.0 uses Spring Boot Framework 2.5.15, an upgrade from Spring Boot Framework 1.x version used in previous releases. Also, ESC 6.0 uses Java 17, an upgrade from Java 8 used in previous releases.

- **UEFI:** ESC 6.0 image mandates UEFI based image booting, it does not support BIOS mode of booting.

Cisco Elastic Services Controller 6.0 Pre-Requisites:

To boot ESC 6.0 image on OpenStack or VMware, the respective Virtual Infrastructure platform must support UEFI. On a UEFI supported virtual infrastructure, perform the following additional steps to boot ESC 6.0 image:

Pre-Requisites for OpenStack:

While glancing the ESC 6.0 image on OpenStack, make sure that the following property is configured for that image, only then the ESC 6.0 image will boot.

```
--property hw_firmware_type=uefi
```

If Cisco Virtual Infrastructure Manager (CVIM) is being used as Virtual Infrastructure platform, then UEFI is NOT SUPPORTED by CVIM 3.x versions. For more details on UEFI support on CVIM platform, please refer to the respective product user guide.

While glancing the ESC 6.0 image on CVIM 4.x platform, ensure that the following properties are configured for that image, only then the ESC 6.0 image will boot.

```
--property hw_firmware_type=uefi--property hw_machine_type=q35
```

Pre-Requisites for VMware vCenter:

While booting ESC 6.0 OVA using vCenter GUI set the Firmware as EFI as shown in the picture:

Cisco Elastic Services Controller 6.0 Upgrade Limitations:

- Users cannot upgrade from earlier versions of ESC such as 5.10 or 5.9 to ESC 6.0 using the RPM upgrade procedure. In general RPM upgrade is supported only when the major and minor release numbers are the same. Example: 5.10.0.95 to 5.10.0.97
- Users cannot use InService Upgrade to upgrade from earlier versions of ESC for example 5.10 or 5.9 versions to ESC 6.0 version. Since ESC 6.0 comes with a newer version of 3rd party libraries and base operating systems, InService upgrade is not supported to upgrade from earlier versions to ESC 6.0 release.

Note The only option to upgrade from ESC 5.x to 6.0 is backup-restore mode of upgrade.

Cisco Elastic Services Controller Bugs

For a complete list of resolved bugs for this release, use the Cisco Bug Search tool.

Resolved Bugs

The following table lists the resolved issues in the Cisco Elastic Services Controller 6.0 release.

Table 1: Resolved Bugs in Cisco Elastic Services Controller 6.0

Bug ID	Description
CSCwf34829	Filter used in vnf_package API is not as per ETSI standard.
CSCwh85430	Could not login to ESC portal
CSCwh81575	Unable to disable port_security of an interface when it has allowed_address_pairs configured.
CSCwh50973	Default security group is not assigned if no security group is mentioned with port security enabled.

Cisco Bug Search Tool

Bug Search Tool (BST), the online successor to Bug Toolkit, is designed to improve our customers' effectiveness in network risk management and device troubleshooting.

BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The service has provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To use the BST to search for a specific bug or to search for all bugs in a release:

Procedure

Step 1 Go to http://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 Return.

Step 4 To search for bugs in the current release:

a. In the Search For field, enter a keyword and press Return. (Leave the other fields empty).

b. When the search results are displayed, use the filter tools to find the types of bugs you are looking for. You can search for bugs by modified date, status, severity, and so forth.

Tip To export the results to a spreadsheet, click the Export All to Spreadsheet link.

See Bug Search Tools & Resources on Cisco.com. For more details on the tool overview and functionalities, check out the help page, located at http://www.cisco.com/web/applicat/cbsshelp/help.html

Accessibility Features in Cisco ESC

For a list of accessibility features in Cisco ESC 6.0, see Voluntary Product Accessibility Template (VPAT) on the Cisco website, or contact accessibility@cisco.com.

All product documents are accessible except for images, graphics, and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.

Related Documentation

The following documents are available for Cisco Elastic Services Controller:

- *Cisco Elastic Services Controller User Guide*
- *Cisco Elastic Services Controller Install and Upgrade Guide*
- *Cisco Elastic Services Controller ETSI NFV MANO Guide*
- *Cisco Elastic Services Controller Administration Guide*
- *Cisco Elastic Services Controller Troubleshooting Guide*
- *Cisco Elastic Services Controller NETCONF API Guide*
- *Cisco Elastic Services Controller REST API Guide*
- *Cisco Elastic Services Controller ETSI API Guide*
- *Cisco Elastic Services Controller Deployment Attributes*

You can access the documents at:

http://www.cisco.com/c/en/us/support/cloud-systems-management/elastic-services-controller-esc/tsd-products-support-series-home.html.

© 2023 Cisco Systems, Inc. All rights reserved.