Cisco Elastic Services Controller 5.10 Release Notes

First Published: 2023-07-05

Last Modified: 2023-09-05

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, Amazon Web Services (AWS) and so on. For more details, see the Cisco Elastic Services Controller Install and Upgrade Guide.

New Features and Enhancements in 5.10

- Starting ESC 5.10, when a user deploys a VNF with port-security enabled on an interface, user must explicitly set the security-group for it, otherwise no security group is assigned to that VNF.

  Example for deployment through NetConf interface:

  By default port-security is enabled, so one has to set the security-group explicitly as follows:

```
<interfaces>
    <interface>
        <nicid>0</nicid>
        <network>automation-multi-vim-sim-net</network>
        <security_groups>
```

```
            <security_group>default</security_group>
        </security_groups>
    </interface>
</interfaces>
```

Or otherwise, user must disable the port-security as follows:

```
<interfaces>
    <interface>
        <nicid>0</nicid>
        <network>automation-multi-vim-sim-net</network>
        <port_security_enabled>false</port_security_enabled>
    </interface>
</interfaces>
```

Example for deployment via ETSI VNFD:

```
node_1_nic0:
      type: cisco.nodes.nfv.VduCp
      properties:
        layer_protocols: [ ipv4 ]
        protocol:
          - associated_layer_protocol: ipv4
        trunk_mode: false
        order: 0
        management: false
        name_override: nic0-backward-compatibility
        iface_type: virtual
        port_security_enabled: true
        binding_profile: "trusted=true, type=dict, physical_network=physnet_tenant"
        allowed_address_pairs:
          - ip_address: 192.168.0.0/18
      requirements:
        - virtual_binding: vdu_node_1
        - virtual_link: jenkins-internal-vnf-net-1
      metadata:
        security_groups: default
```

Note The mentioned port-security enhancements does not have any impact on the existing deployments when user upgrades from older ESC releases to ESC 5.10. But, when a new VNF is deployed using ESC 5.10, user must take care of the port-security settings for VNF to be managed by ESC.

- **ESC Documentation Update**
  - Cisco Elastic Services Controller Troubleshooting Guide—Explains the various troubleshooting activities related to ESC Installation, ESC HA, ESC Micro-services, ESC upgrades, ESC troubleshooting backup and restore, ESC ConfD and NETCONF API, and ESC VNF deployment. For more information, see the Cisco Elastic Services Controller Troubleshooting Guide

Deprecated Features

Starting ESC Release 5.4, some of the functionalities are deprecated. The table below lists the deprecated functionalities, and the new functionalities replacing them in ESC:

Table 1: Deprecated Functionalities

Deprecated Functionality	New Functionality	w
Data model pertaining to SOL001 v2.7.1	Data model pertaining to SOL001 v3.3.1	7 5
Data model, request/response structures and flows pertaining to SOL002 v2.5.1	Data model, request/response structures and flows pertaining to SOL002 v3.3.1	7 5
Data model, request/response structures and flows pertaining to SOL003 v2.5.1	Data model, request/response structures and flows pertaining to SOL003 v3.3.1	7 5
The Cisco-specific extensions on `tosca.datatypes.nfv.VnfHealOperationConfiguration`.	Moved to a standardised extension point: `cisco.datatypes.nfv.VnfcAdditionalConfigurableProperties`	4 3 6
The Cisco-specific extensions on `tosca.nodes.nfv.Vdu.VirtualBlockStorage` to specify the external volume UUID in the resource_id.	Moved to a standardised data structure: `tosca.nodes.nfv.Vdu.VirtualBlockStorage.virtual_block_storage_data.vdu_storage_requirements`	4 3 6
Some of the Cisco-specific extensions on `tosca.nodes.nfv.VduCp`.	All but allowed_address_pairs have moved to standardised data structures on `tosca.nodes.nfv.VduCp.virtual_network_interface_requirements` and `tosca.nodes.nfv.VnfVirtualLink.virtual_link_protocol_data`	4 3 6
The Cisco-specific extensions on `tosca.policies.nfv.SecurityGroupRule` to specify an out-of-band Security Group.	Moved to a standardised data structure: `tosca.nodes.nfv.VduCp.metadata.security_group`	4 3 6
The following Cisco-specific extensions on which serve as placeholders for the definition of fixed addresses and static IP pools in the SOL001 VNFD: `nodes.nfv.Vdu.Compute (vdu_profile.static_ip_address_pools)`	Use `InstantiateVnfRequest` for IP addressing requirements, using `cpProtocolData` data structures, as per the standards.	3 3 6

Starting with Cisco ESC Release 5.3, support for the following may end in any of the future releases without additional notice:

- The deprecated VMware vCenter versions 5.5 and 6.0.

- The deprecated VMware vCloud Director (vCD) version 8.2.
- The deprecated D-MONA 1:1 mapping

For more information, see the release documents available at http://www.cisco.com/c/en/us/support/cloud-systems-management/elastic-services-controller-esc/tsd-products-support-series-home.html.

Cisco Elastic Services Controller Bugs

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

Open Bugs

The table below lists the open issues in the Cisco Elastic Services Controller 5.10 release.

Table 2: Open Bugs in Cisco Elastic Services Controller 5.10

Bug ID	Description
CSCwd63865	After failed recovery of VM, the VM recovery again sends a notification with the wrong VM ID.

Resolved Bugs

The following table lists the resolved issues in the Cisco Elastic Services Controller 5.10 release.

Table 3: Resolved Bugs in Cisco Elastic Services Controller 5.10

Bug ID	Description
CSCwd97909	Problem is being observed in a Gateway with a sys uptime greater than 497 days.
CSCwe95602	PostgreSQL password decode issue (codec can't decode byte) fixed
CSCwe97020	Brownfield script throws an error
CSCwe30927	MONA does not execute rules during the daylight saving time (DST) transition back to standard time.
CSCwc46301	ESC unable to change openstack port attributes port_security & security_group_ids

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 5.9, 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.