



# Release Notes for Cisco Virtual Application Cloud Segmentation Services, Release 6.0STV3.2

---

**First Published: 2017-02-10**

**Last Updated: 2017-02-10**

This document describes the features, limitations, and bugs for the Cisco Virtual Application Cloud Segmentation (VACS) Services software solution. Use this document in combination with the documents listed in [Related Documentation](#) and [Cisco VACS Documentation Matrix](#).

This document includes the following sections:

- [Overview, page 1](#)
- [New Features and Enhancements in Release 6.0STV3.2, page 2](#)
- [Software Compatibility, page 3](#)
- [Limitations and Restrictions, page 6](#)
- [Using the Bug Search Tool, page 9](#)
- [Bugs, page 10](#)
- [Related Documentation, page 11](#)
- [Cisco VACS Documentation Matrix, page 12](#)
- [Documentation Feedback, page 14](#)
- [Obtaining Documentation and Submitting a Service Request, page 14](#)

## Overview

Cisco Virtual Application Cloud Segmentation (VACS) Services is a software solution that automates the coordinated licensing, installation, and deployment of multiple virtual services in your data center to enable an easy and efficient setup of virtualized applications. Cisco UCS Director provides the management interface to deploy, provision, and monitor the Cisco VACS solution.

Cisco VACS provides a fully customizable, extended application container abstraction to simplify deploying and provisioning virtual services.



An application container is a set of virtual services such as virtual switches, routers, firewalls, and other network devices configured in a consistent manner to deploy different workloads. When you create and instantiate an application container template, Cisco VACS deploys virtual machines (VMs), and configures networks, the firewall, and virtual switches, and enables network and security provisioning at the virtual layer.

Cisco VACS allows you to define extended application container templates and instantiate them through automated setup and to provision the underlying virtual components. You can use the ready-to-use application container templates that define the rules for deploying a collection of VMs within a private network secured by a firewall.

Cisco VACS leverages the features in the following virtual components to build a secure multi-tenant cloud and create application container templates:

- Cisco Nexus 1000V
- Cisco Prime Network Services Controller (PNSC)
- Cisco Cloud Services Router (CSR) 1000V
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Virtual Security Gateway (VSG)
- Server Load Balancer (SLB)

Key features and benefits of Cisco VACS include:

- Single workflow automation to logically isolate virtual application workloads at the virtual layer.
- VMware vSphere support for interoperability across private cloud environments.
- Consistent provisioning and orchestration experience across physical and virtual assets through Cisco UCS Director.

## New Features and Enhancements in Release 6.0STV3.2

This release of Cisco VACS contains the following new features and enhancements:

### New Features

- Provides an option to import VSMs that are not installed as a part of the Cisco VACS infra components installation.
- Supports installation of multiple Cisco PNSC(s) per virtual account.
- Provides the following new REST APIs:
  - VACSImportVsm
  - VACSReleaseLockEntry
  - userAPIGetLockInfo
  - userAPIGetNetworkEntityPassword

### Enhancements

None

# Software Compatibility

The following table lists the compatibility information for Cisco VACS, Cisco UCS Director, and the relevant Cisco VACS components.

**Table 1**      **Software Compatibility**

Cisco VACS	Cisco UCS Director	Cisco VACS Components
Release 6.0STV3.2	Release 6.0.1.0	<ul style="list-style-type: none"> <li>• VMware vSphere 5.5 or 6.0</li> <li>• Cisco Nexus 1000V 5.2(1)SV3(1.6)</li> <li>• Cisco PNSC 3.4.1d</li> <li>• Cisco VSG 5.2(1)VSG2(1.4)</li> <li>• Cisco CSR 1000V XE 3.16.1a</li> <li>• Cisco ASAv 9.6.2</li> <li>• Server Load Balancer (SLB)               <ul style="list-style-type: none"> <li>– Open Source HA-proxy, Release 1.5.2 1.5.2-2.el6 (on x86_64)</li> <li>– Keepalived 1.2.15</li> </ul> </li> </ul>
Release 6.0STV3.1.1	Release 6.0	<ul style="list-style-type: none"> <li>• VMware vSphere 5.5 or 6.0</li> <li>• Cisco Nexus 1000V 5.2(1)SV3(1.4)</li> <li>• Cisco PNSC 3.4.1b</li> <li>• Cisco VSG 5.2(1)VSG2(1.3)</li> <li>• Cisco CSR 1000V XE 3.16.1a</li> <li>• Cisco ASAv 9.6.1</li> <li>• Server Load Balancer (SLB)               <ul style="list-style-type: none"> <li>– Open Source HA-proxy, Release 1.5.2 1.5.2-2.el6 (on x86_64)</li> <li>– Keepalived 1.2.15</li> </ul> </li> </ul>
Release 5.5STV3.1	Release 5.5  <b>Note</b> <ul style="list-style-type: none"> <li>• Cisco UCS Director Release 6.0 is not supported.</li> </ul>	<ul style="list-style-type: none"> <li>• VMware vSphere 5.5 or 6.0</li> <li>• Cisco Nexus 1000V 5.2(1)SV3(1.4)</li> <li>• Cisco PNSC 3.4.1b</li> <li>• Cisco VSG 5.2(1)VSG2(1.3)</li> <li>• Cisco CSR 1000V XE 3.16.1a</li> <li>• Cisco ASAv 9.6.1</li> <li>• Server Load Balancer (SLB)               <ul style="list-style-type: none"> <li>– Open Source HA-proxy, Release 1.5.2 1.5.2-2.el6 (on x86_64)</li> <li>– Keepalived 1.2.15</li> </ul> </li> </ul>

Table 1 Software Compatibility (continued)

Cisco VACS	Cisco UCS Director	Cisco VACS Components
Release 5.4STV3.0	Release 5.4 and Release 5.4-based patch releases. <b>Note</b> <ul style="list-style-type: none"> <li>• Cisco UCS Director Release 5.4.0.3 is the recommended version.</li> <li>• Cisco UCS Director Release 5.5 is not supported.</li> </ul>	<ul style="list-style-type: none"> <li>• VMware vSphere 5.5 or 6.0</li> <li>• Cisco Nexus 1000V 5.2(1)SV3(1.4)</li> <li>• Cisco PNSC 3.4.1b</li> <li>• Cisco VSG 5.2(1)VSG2(1.3)</li> <li>• Cisco CSR 1000V XE 3.16.1a</li> <li>• Cisco ASAv 9.6.1</li> <li>• Server Load Balancer (SLB)               <ul style="list-style-type: none"> <li>– Open Source HA-proxy, Release 1.5.2 1.5.2-2.el6 (on x86_64)</li> <li>– Keepalived 1.2.15</li> </ul> </li> </ul>
Release 5.4STV2.1.2	Release 5.4.0.2 <b>Note</b> Release 5.3 and the Release 5.3-based patches are not supported.	<ul style="list-style-type: none"> <li>• VMware vSphere 5.1 or later</li> <li>• Cisco Nexus 1000V 5.2(1)SV3(1.4)</li> <li>• Cisco PNSC 3.4.1b</li> <li>• Cisco VSG 5.2(1)VSG2(1.3)</li> <li>• Cisco CSR 1000V XE 3.16.1a</li> <li>• Server Load Balancer (SLB)               <ul style="list-style-type: none"> <li>– Open Source HA-proxy, Release 1.5.2 1.5.2-2.el6 (on x86_64)</li> <li>– Keepalived 1.2.15</li> </ul> </li> </ul>
Release 5.4STV2.1.1	Release 5.4.0.2 <b>Note</b> Release 5.3 and the Release 5.3-based patches are not supported.	<ul style="list-style-type: none"> <li>• VMware vSphere 5.1 or later</li> <li>• Cisco Nexus 1000V 5.2(1)SV3(1.4)</li> <li>• Cisco PNSC 3.4.1b</li> <li>• Cisco VSG 5.2(1)VSG2(1.3)</li> <li>• Cisco CSR 1000V XE 3.16.1a</li> <li>• Server Load Balancer (SLB)               <ul style="list-style-type: none"> <li>– Open Source HA-proxy, Release 1.5.2 1.5.2-2.el6 (on x86_64)</li> <li>– Keepalived 1.2.15</li> </ul> </li> </ul>

**Table 1**      **Software Compatibility (continued)**

<b>Cisco VACS</b>	<b>Cisco UCS Director</b>	<b>Cisco VACS Components</b>
Release 5.4STV2.1	Release 5.4 <b>Note</b> Release 5.3 and the Release 5.3-based patches are not supported.	<ul style="list-style-type: none"> <li>• VMware vSphere 5.1 or later</li> <li>• Cisco Nexus 1000V 5.2(1)SV3(1.4)</li> <li>• Cisco PNSC 3.4.1b</li> <li>• Cisco VSG 5.2(1)VSG2(1.3)</li> <li>• Cisco CSR 1000V XE 3.16.1a</li> <li>• Server Load Balancer (SLB)               <ul style="list-style-type: none"> <li>– Open Source HA-proxy, Release 1.5.2 1.5.2-2.el6 (on x86_64)</li> <li>– Keepalived 1.2.15</li> </ul> </li> </ul>
Release 5.3STV2.0.1	Release 5.3 or the later releases <b>Note</b> We recommend that you use the Cisco UCS Director Release 5.3.1.2.	<ul style="list-style-type: none"> <li>• VMware vSphere 5.1 or later</li> <li>• Cisco Nexus 1000V 5.2(1)SV3(1.4)</li> <li>• Cisco PNSC 3.4.1b</li> <li>• Cisco VSG 5.2(1)VSG2(1.3)</li> <li>• Cisco CSR 1000V XE 3.14.0</li> <li>• Server Load Balancer (SLB)               <ul style="list-style-type: none"> <li>– Open Source HA-proxy, Release 1.5.2 1.5.2-2.el6 (on x86_64)</li> <li>– Keepalived 1.2.15</li> </ul> </li> </ul>
Release 5.3STV2.0	<ul style="list-style-type: none"> <li>• Release 5.3 or the 5.3.1.0 patch</li> <li>• Release 5.2 or Release 5.2-based patch releases.</li> </ul>	<ul style="list-style-type: none"> <li>• VMware vSphere 5.1 or later</li> <li>• Cisco Nexus 1000V 5.2(1)SV3(1.4)</li> <li>• Cisco PNSC 3.4.1b</li> <li>• Cisco VSG 5.2(1)VSG2(1.3)</li> <li>• Cisco CSR 1000V XE 3.14.0</li> <li>• Server Load Balancer (SLB)               <ul style="list-style-type: none"> <li>– Open Source HA-proxy, Release 1.5.2 1.5.2-2.el6 (on x86_64)</li> <li>– Keepalived 1.2.15</li> </ul> </li> </ul>
Release 5.3STV1.1.2	<ul style="list-style-type: none"> <li>• Release 5.3</li> <li>• Release 5.2</li> </ul> <b>Note</b> Apply the Cisco UCS Director maintenance patch (patch 1, which is cucsd_patch_5_2_0_1.zip) before installing or upgrading to Cisco VACS Release 5.3STV1.1.2.  <ul style="list-style-type: none"> <li>• Release 5.1</li> </ul>	<ul style="list-style-type: none"> <li>• VMware vSphere 5.1 or later</li> <li>• Cisco Nexus 1000V5.2(1)SV3(1.1)</li> <li>• Cisco PNSC 3.2.2.b</li> <li>• Cisco VSG 5.2(1)VSG2(1.1)</li> <li>• Cisco CSR 1000V XE 3.14.0</li> </ul>

**Table 1**      **Software Compatibility (continued)**

Cisco VACS	Cisco UCS Director	Cisco VACS Components
Release 5.2STV1.1.1	<ul style="list-style-type: none"> <li>• Release 5.2</li> </ul> <p><b>Note</b> Apply the Cisco UCS Director maintenance patch (patch 1, which is <code>cucsd_patch_5_2_0_1.zip</code>) before installing or upgrading to Cisco VACS Release 5.3STV1.1.2.</p> <ul style="list-style-type: none"> <li>• Release 5.1</li> </ul>	<ul style="list-style-type: none"> <li>• VMware vSphere 5.1 or later</li> <li>• Cisco Nexus 1000V 5.2(1)SV3(1.1)</li> <li>• Cisco PNSC 3.2.2.b</li> <li>• Cisco VSG 5.2(1)VSG2(1.1)</li> <li>• Cisco CSR 1000V XE 3.14.0</li> </ul>
Release 5.2STV1.1	<ul style="list-style-type: none"> <li>• Release 5.2</li> </ul> <p><b>Note</b> Apply the Cisco UCS Director maintenance patch (patch 1, which is <code>cucsd_patch_5_2_0_1.zip</code>) before installing or upgrading to Cisco VACS Release 5.3STV1.1.2.</p> <ul style="list-style-type: none"> <li>• Release 5.1</li> </ul>	<ul style="list-style-type: none"> <li>• VMware vSphere 5.1 or later</li> <li>• Cisco Nexus 1000V 5.2(1)SV3(1.1)</li> <li>• Cisco PNSC 3.2.2.b</li> <li>• Cisco VSG 5.2(1)VSG2(1.1)</li> <li>• Cisco CSR 1000V XE 3.14.0</li> </ul>
Release 5.1STV1.0	Release 5.1	<ul style="list-style-type: none"> <li>• VMware vSphere 5.1 or later</li> <li>• Cisco Nexus 1000V 5.2(1)SV3(1.1)</li> <li>• Cisco PNSC 3.2.2.b</li> <li>• Cisco VSG 5.2(1)VSG2(1.1)</li> <li>• Cisco CSR 1000V XE 3.12.0</li> </ul>

## Limitations and Restrictions

This section describes the limitations and restrictions of Cisco VACS.

### General Cisco VACS Limitations

- Cisco VACS supports the following:
  - ESX versions 5.0 and later
  - vCenter versions 5.1 and later
- Only one Cisco PNSC can be deployed per vCenter, but there is no limit to the number of vCenters that can be managed as the virtual account and the number of Cisco Nexus 1000V deployed per vCenter.
- All VXLAN VTEPs added per host using the add host operation should be configured to be in the same subnet.
- During the add host operation, do not migrate the VSM VMs to VEM.
- If you upgrade to Cisco UCS Director patches after you upgrade Cisco VACS, you must reapply the Cisco VACS patch.
- Cisco VACS does not support multi-node Cisco UCS Director deployments.
- Cisco UCS Director supports only hosts or clusters under DC. It does not support any folder structures under DC.
- The add host operation could fail when you add a host that has a previous version of the Cisco Nexus 1000V VIB.

### License Limitations

- Each Cisco Nexus 1000V is licensed with 1024 licenses.

- Cisco VACS does not support ELA UCS Director licenses.
- When upgrading from Cisco VACS evaluation to Cisco VACS production licenses, note the following:
  - After installing the Cisco UCS Director production licenses, the Cisco VACS evaluation licenses are invalid. You must use a Cisco VACS production license.
  - After installing the Cisco VACS production licenses, the existing Cisco Nexus 1000V that was installed with the evaluation license does not get a permanent Cisco Nexus 1000V license. You must deploy a new Cisco Nexus 1000V so that it gets a permanent license.
  - A Cisco CSR 1000V or Cisco ASAv deployed during the Cisco VACS evaluation license (or with no Cisco ASAv licenses) comes up with default licenses and a maximum throughput of 100 Kbps.
  - After installing the Cisco VACS production licenses, the existing Cisco CSR 1000V or Cisco ASAv of deployed containers is not automatically licensed with permanent licenses. If required, you must manually apply the permanent licenses for the Cisco CSR 1000V or Cisco ASAv.

### Configuration Limitations

- IP pool limitations:
  - The IP pools used for management and uplink pools should have mandatory VLAN and Gateway fields.
  - The IP pools used for the port group-based VM networks in custom containers should not have the Gateway field.
  - The broadcast and network IP addresses should not be used as the IP addresses in the pool.
  - The IP subnet for the management and uplink networks must be different in a new Cisco VACS template, irrespective of the type of the edge gateway selected. For all existing templates, the same IP pool is supported for both these networks as long as the template is not edited.
- IP subnet pool limitations:
  - The subnet cannot contain fewer than 4 IP addresses, or more than 1024 IP addresses.
- IP address limitations when an IP needs to be entered for install actions, IP pools, and ERSPAN:
  - Do not use broadcast and network, Experimental/Use in research IP addresses.
- Cisco VACS does not configure the upstream switches and routers in the physical infrastructure. Cisco VACS only configures the virtual infrastructure for Cisco PNSC, Cisco Nexus 1000V, Cisco CSR 1000V, and Cisco ASAv.
- You must configure the upstream devices such that the path MTU between the VEMs has an MTU of greater than or equal to 1600.

### Container Limitations

- You are not allowed to execute the post container operations in parallel. You must wait for the current task to be completed before you proceed with the next task.
- Do not cancel the service request of any of the post container operations, such as add VM, delete VM, configure SNAT, configure ERSPAN, power on and power off a container.
- You cannot resubmit failed service requests for most of the container add-on operations (except for the manage VM networks operation).
- Rollback of successfully completed container add-on operations is not supported. To undo, you must use the UI for the add-on operation.
- You can roll back the failed add VM network service requests for the manage VM networks operation.
- Currently, all service options that are a part of Cisco PNSC are not available in Cisco UCS Director. The only available service options are http and https. To access the other service options, you must enter the appropriate standard port number by ignoring the type selection.

- During container deployment, the storage policy occasionally selects storage that does not belong to a shortlisted host from the compute policy.
- For cluster mode compute policy deployments, all hosts under the cluster must be a part of Cisco Nexus 1000V and must have the same common storage.
- If the network adapter type is VMXNET3, the container deployment fails intermittently on VMware ESXi 5.1.0 build-1483097 (ESXi 5.1.0 Update 2).
- When multiple application containers with SLB/CSR VMs are deployed, deployment fails for some of these application containers. You must resubmit the failed application containers after the other application containers are deployed successfully.
- Parallel deployment of application containers is serialized at the SLB task, which delays container deployment.
- Container deployment might take longer than expected if the containers are deployed in parallel and have SLB VMs.
- After the containers are deployed from a non-overlapped pool, the pool should not be made overlapped.
- Supports overlapping IP for Static IP Pools. See the *About Overlapping IP* section in the *Cisco Virtual Application Cloud Segmentation Services Configuration Guide*.
- When secure reports are enabled, end users who are a part of the default group can view additional VMs that are discovered with Virtual Account that are not installed using Cisco VACS.
- When a post container operation is canceled, the service request is terminated without releasing the lock.
- Effective Cisco VACS Release 6.0STV3.2, if you import Cisco Nexus 1000V, you cannot add hosts using Cisco VACS.

#### SLB Limitations

- When workload VMs are added or deleted from the SLB zone, traffic impact for 2 to 3 seconds. This delay occurs because HA proxy must restart for the changes to take effect.

#### Secure Reports and VM Options Limitations

- The Accounting tab in the Self-Service Portal displays the service VM details, even when the secure container details option is enabled.
- The container icon (under the Options tab) available in the Self-Service Portal displays the total number of VMs (including service VMs), even though the secure container details option is enabled.



**Note** These limitations can mislead the end user about VM details that are displayed.

- Administrator-made changes in the Options menu do not reflect in the Self-Service Portal until the Refresh action is performed (Virtual Resources > Application Containers > Container Icon > Refresh).

#### Scale Limitations

Cisco VACS has the following scale limitations:

- Number of containers per Cisco VACS license are:
  - 10—with one Cisco CSR 1000V each
  - 05—with two Cisco CSR 1000V (HA) each
  - Any number without Cisco CSR 1000V, provided there are sufficient Cisco UCS Director host licenses required to deploy the VMs.
- Number of containers: 250
- Number of VMs per container: 60\*(20 VMs in each zone of a 3-tier container)



- Number of containers per host: 15\*
- Number of containers that can be deployed in parallel: 5\*

\*-These scale limits are the soft limits. The number of containers can vary, and it mainly depends on the below parameters:

- If Cisco VSG is present in the container or not (as one Cisco PNSC instance can support 128 Cisco VSGs)
- The Size of the containers (Small/Medium/Large)
- The vCPU/memory capacity of the individual hosts
- The type of Service VMs that are included in the container
- The Workload VM reservations in terms of vCPU/memory
- The defined VLAN/VXLAN/IP pool limits
- The Compute and storage policies

## Using the Bug Search Tool

Use the Bug Search Tool to search for a specific bug or to search for all bugs in a release. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

For more information about the Bug Search Tool, see the [Bug Search Tool Help & FAQ](#).

---

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

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



### Note

You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for it 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:

- In the Search For field, enter **Cisco Virtual Application Cloud Segmentation (VACS) Services** and press **Enter**. (Leave the other fields empty.)
- 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 status, severity, modified date, and so forth.



### Tip

To export the results to a spreadsheet, click the **Export Results to Excel** link.

---


# Bugs

The following are descriptions of the open and resolved bugs in Cisco VACS Release 6.0STV3.2. The bug ID links you to the [Cisco Bug Search Tool](#).

**Table 2**      **Open Bugs**

Bug ID	Headline
<a href="#">CSCva43239</a>	On a fresh setup, when the first instance of the Add Single Host wizard is opened, the VM port profiles are not displayed in the VM Migration screen.
<a href="#">CSCvb53564</a>	In the classic view of Cisco UCS Director, Release 6.0, when you perform any browser related actions, a flickering issue is seen and the screen does not load.
<a href="#">CSCuo95017</a>	When the workload VM includes a logical interface such as “virb0” in Linux, the ERSPAN feature does not work.
<a href="#">CSCur34625</a>	IP validations do not include a broadcast address.
<a href="#">CSCur91980</a>	If the container name and the VM include special characters such as % and \$, the container deployment fails because the Cisco Nexus 1000V does not create port profiles that include special characters.
<a href="#">CSCus09994</a>	When an Ubuntu version 14.04 template is used, the correct IP address and the hostname are not assigned to the IP address/host. IP addresses are not reflected in the VMs.
<a href="#">CSCus17034</a>	During HA deployments, if the VSG deployment fails, the rollback does not delete stale IP addresses.
<a href="#">CSCus74629</a>	The Add Host wizard occasionally does not display the VLAN ID for existing VMKNICs on the vSwitch.
<a href="#">CSCuu32360</a>	When there is an SLB switchover, the existing traffic sessions are not load-balanced efficiently.
<a href="#">CSCuu32387</a>	Under heavy traffic, the web-based SLB statistics are not displayed properly.
<a href="#">CSCuu87503</a>	When VMs are added to a container but one of the SLB HA VMs is not available, the configuration files of the SLB VMs are not synchronized.
<a href="#">CSCuv15551</a>	The container icon (under the Options tab) available in the Self-Service Portal displays the total number of VMs (including service VMs), even though the secure container details option is enabled.
<a href="#">CSCuv16831</a>	When you create a zone using the port profile name attribute and deploy the container, the workload VMs do not consider the port profile name attribute. Instead they are created based on the VM network.
<a href="#">CSCux81459</a>	Although the local datastore of the host has enough space, there is a insufficient disk space error displayed during the container deployment.
<a href="#">CSCuy99791</a>	When containers are deployed in parallel, sometimes the VSG data interface goes to a down state and data traffic is not policed.
<a href="#">CSCuz14537</a>	During the delete vNICs operation, a wrong IP address gets configured.
<a href="#">CSCuz45718</a>	Sometimes the add host operation fails because the PNIC does not get added to the DVS, resulting in a failure at the VC.
<a href="#">CSCvc84118</a>	When you cancel a post container operation, it results in the termination of the service request without releasing the lock.
<a href="#">CSCvc84181</a>	Sometimes you can create templates when the Cisco PNSC and the VSM versions are incompatible.
<a href="#">CSCvc85024</a>	When you cancel the service request for the manage zone operation, the workflow is not terminated,
<a href="#">CSCvc95548</a>	When you cancel the deployment of a service VM and initiate a rollback request, the service VM remains in a “in progress” state.

**Table 3**      **Resolved Bugs**

Bug ID	Headlines
<a href="#">CSCvb62287</a>	<p data-bbox="337 331 1518 394">During the Add VM Network operation, when you cancel the service request, the lock is not released in the database.</p>  <p data-bbox="337 457 1518 491"><b>Note</b>      This behavior is observed during the cancellation of all post container operations.</p>
<a href="#">CSCvb54945</a>	<p data-bbox="337 510 1518 573">When the end user policy is created without the end user VM operations, the VACS Add vNICS, VACS delete vNICS, VACS delete VM, and the UCSD Delete VM end user options are visible to the end user.</p>
<a href="#">CSCvb60323</a>	<p data-bbox="337 588 1518 646">Due to changes made to the Cisco IT infrastructure that supports tools.cisco.com, licensing of Cisco ASA v either fails or is delayed.</p>
<a href="#">CSCux21233</a>	<p data-bbox="337 665 1518 724">If a container name ends with a non-alphanumeric character, the container deployment completes but the policies are not applied. This causes traffic problems.</p>

## Related Documentation

In addition to these release notes, you can find documentation for Cisco VACS and the relevant components at the following locations on Cisco.com:

- [Cisco Virtual Application Cloud Segmentation Services Documentation](#)
- [Cisco Nexus 1000V for VMware vSphere Documentation](#)
- [Cisco Prime Network Services Controller Documentation](#)
- [Cisco Cloud Services Router 1000V Documentation](#)
- [Cisco Adaptive Security Virtual Appliance \(ASAv\) Documentation](#)
- [Cisco Virtual Security Gateway Documentation](#)
- [Cisco UCS Director Documentation](#)

# Cisco VACS Documentation Matrix

Not all Cisco VACS guides are updated for each release. The following table lists the guides that correspond to each Cisco VACS release.

**Table 4** Cisco VACS Documentation Matrix

<b>This Cisco VACS Release</b>	<b>Corresponds with These Guides</b>
6.0STV3.2	<ul style="list-style-type: none"> <li>• <i>Cisco Virtual Application Cloud Segmentation Services 6.0STV3.2 Release Notes</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Installation and Upgrade Guide, Release 6.0STV3.2</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Configuration Guide, Release 6.0STV3.2</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services End User Portal Guide, Release 6.0STV3.1.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Self-Service Portal User Guide, Release 5.5STV3.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services REST API Guide, Release 6.0STV3.2</i></li> </ul>
6.0STV3.1.1	<ul style="list-style-type: none"> <li>• <i>Cisco Virtual Application Cloud Segmentation Services 6.0STV3.1.1 Release Notes</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Installation and Upgrade Guide, Release 6.0STV3.1.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Configuration Guide, Release 5.5STV3.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services End User Portal Guide, Release 6.0STV3.1.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Self-Service Portal User Guide, Release 5.5STV3.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services REST API Guide, Release 6.0STV3.1.1</i></li> </ul>
5.5STV3.1	<ul style="list-style-type: none"> <li>• <i>Cisco Virtual Application Cloud Segmentation Services 5.5STV3.1 Release Notes</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Installation and Upgrade Guide, Release 5.5STV3.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Configuration Guide, Release 5.5STV3.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Self-Service Portal User Guide, Release 5.5STV3.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services REST API Guide, Release 5.5STV3.1</i></li> </ul>
5.4STV3.0	<ul style="list-style-type: none"> <li>• <i>Cisco Virtual Application Cloud Segmentation Services 5.4STV3.0 Release Notes</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Installation and Upgrade Guide, Release 5.4STV3.0</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Configuration Guide, Release 5.4STV3.0</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Self-Service Portal User Guide, Release 5.4STV3.0</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services REST API Guide, Release 5.4STV3.0</i></li> <li>• <i>Open Source Used in Cisco Virtual Application Cloud Segmentation Services, Release 5.4STV3.0</i></li> </ul>

Table 4 Cisco VACS Documentation Matrix (continued)

This Cisco VACS Release	Corresponds with These Guides
5.4STV2.1.2	<ul style="list-style-type: none"> <li>• <i>Cisco Virtual Application Cloud Segmentation Services 5.4STV2.1.2 Release Notes</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Installation and Upgrade Guide, Release 5.4STV2.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Configuration Guide, Release 5.4STV2.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Self-Service Portal User Guide, Release 5.4STV2.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services REST API Guide, Release 5.4STV2.1.1</i></li> <li>• <i>Open Source Used In Cisco Virtual Application Cloud Segmentation Services, Release 5.4STV2.1</i></li> </ul>
5.4STV2.1.1	<ul style="list-style-type: none"> <li>• <i>Cisco Virtual Application Cloud Segmentation Services 5.4STV2.1.1 Release Notes</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Installation and Upgrade Guide, Release 5.4STV2.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Configuration Guide, Release 5.4STV2.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Self-Service Portal User Guide, Release 5.4STV2.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services REST API Guide, Release 5.4STV2.1.1</i></li> <li>• <i>Open Source Used In Cisco Virtual Application Cloud Segmentation Services, Release 5.4STV2.1</i></li> </ul>
5.4STV2.1	<ul style="list-style-type: none"> <li>• <i>Cisco Virtual Application Cloud Segmentation Services 5.4STV2.1 Release Notes</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Installation and Upgrade Guide, Release 5.4STV2.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Configuration Guide, Release 5.4STV2.1</i></li> <li>• <i>Cisco Virtual Application Cloud Segmentation Services Self-Service Portal User Guide, Release 5.4STV2.1</i></li> <li>• <i>Open Source Used In Cisco Virtual Application Cloud Segmentation Services, Release 5.4STV2.1</i></li> </ul>
5.3STV2.0.1	<ul style="list-style-type: none"> <li>• <i>Cisco Virtual Application Container Services 5.3STV2.0.1 Release Notes</i></li> <li>• <i>Cisco Virtual Application Container Services Installation and Upgrade Guide, Release 5.3STV2.0.1</i></li> <li>• <i>Cisco Virtual Application Container Services Configuration Guide, Release 5.2STV2.0.1</i></li> <li>• <i>Cisco Virtual Application Container Services Self-Service Portal User Guide, Release 5.2STV2.0.1</i></li> </ul>
5.3STV2.0	<ul style="list-style-type: none"> <li>• <i>Cisco Virtual Application Container Services 5.3STV2.0 Release Notes</i></li> <li>• <i>Cisco Virtual Application Container Services Installation and Upgrade Guide, Release 5.3STV2.0</i></li> <li>• <i>Cisco Virtual Application Container Services Configuration Guide, Release 5.2STV2.0</i></li> <li>• <i>Cisco Virtual Application Container Services Self-Service Portal User Guide, Release 5.2STV2.0</i></li> </ul>
5.3STV1.1.2	<ul style="list-style-type: none"> <li>• <i>Cisco Virtual Application Container Services 5.3STV1.1.2 Release Notes</i></li> <li>• <i>Cisco Virtual Application Container Services Installation and Upgrade Guide, Release 5.3STV1.1.2</i></li> <li>• <i>Cisco Virtual Application Container Services Configuration Guide, Release 5.2STV1.1</i></li> <li>• <i>Cisco Virtual Application Container Services Self-Service Portal User Guide, Release 5.2STV1.1</i></li> </ul>

**Table 4** Cisco VACS Documentation Matrix (continued)

This Cisco VACS Release	Corresponds with These Guides
5.2STV1.1.1	<ul style="list-style-type: none"> <li>• <i>Cisco Virtual Application Container Services 5.2STV1.1.1 Release Notes</i></li> <li>• <i>Cisco Virtual Application Container Services Installation and Upgrade Guide, Release 5.2STV1.1</i></li> <li>• <i>Cisco Virtual Application Container Services Configuration Guide, Release 5.2STV1.1</i></li> <li>• <i>Cisco Virtual Application Container Services Self-Service Portal User Guide, Release 5.2STV1.1</i></li> </ul>
5.2STV1.1	<ul style="list-style-type: none"> <li>• <i>Cisco Virtual Application Container Services 5.2STV1.1 Release Notes</i></li> <li>• <i>Cisco Virtual Application Container Services Installation and Upgrade Guide, Release 5.2STV1.1</i></li> <li>• <i>Cisco Virtual Application Container Services Configuration Guide, Release 5.2STV1.1</i></li> <li>• <i>Cisco Virtual Application Container Services Self-Service Portal User Guide, Release 5.2STV1.1</i></li> </ul>
5.2STV1.0	<ul style="list-style-type: none"> <li>• <i>Cisco Virtual Application Container Services 5.2STV1.0 Release Notes</i></li> <li>• <i>Cisco Virtual Application Container Services Installation Guide, Release 5.2STV1.0</i></li> <li>• <i>Cisco Virtual Application Container Services Configuration Guide, Release 5.2STV1.0</i></li> <li>• <i>Cisco Virtual Application Container Services Self-Service Portal User Guide, Release 5.2STV1.0</i></li> </ul>

## Documentation Feedback

To provide technical feedback on this document or report an error or omission, please send your comments to:

- [nexus1k-docfeedback@cisco.com](mailto:nexus1k-docfeedback@cisco.com)

We appreciate your feedback.

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2014-2017 Cisco Systems, Inc. All rights reserved.