vCloud Director 9.7 for Service Providers Release Notes

Updated on 06/19/2020

vCloud Director 9.7 for Service Providers | 28 March 2019 | Release Build 12990033 (installed build 12989839);

Check for additions and updates to these release notes.

What's in the Release Notes

The release notes cover the following topics:

What's New in this Release

For information on the new and updated features of this release, see the VMware Technical White Paper What's New with VMware vCloud Director 9.7.

System Requirements and Installation

Compatibility Matrix

See the VMware Product Interoperability Matrixes for current information about:

- vCloud Director interoperability with other VMware platforms
- Supported vCloud Director databases
- Upgrade paths

Supported vCloud Director Server Operating Systems

- CentOS 6
- CentOS 7
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7

Supported AMQP Servers

vCloud Director uses AMQP to provide the message bus used by extension services, object extensions, and notifications. This release of vCloud Director supports RabbitMQ versions 3.7, 3.7.9 and 3.8.2.

For more information, see the *vCloud Director Installation, Configuration, and Upgrade Guide*.

Supported Databases for Storing Historic Metric Data

You can configure your vCloud Director installation to store metrics that vCloud Director collects about virtual machine performance and resource consumption. Data for historic metrics is stored in a Cassandra database. vCloud Director supports Cassandra versions 3.*x.*

For more information, see the *vCloud Director Installation, Configuration, and Upgrade Guide*.

Disk Space Requirements

Each vCloud Director server requires approximately 2100MB of free space for the installation and log files.

Memory Requirements

Each vCloud Director server must be provisioned with at least 6GB of memory.

CPU Requirements

vCloud Director is a CPU-bound application. CPU overcommitment guidelines for the appropriate version of vSphere should be followed. In virtualized environments, regardless of number of cores available to vCloud Director, there must be a sensible vCPU to physical CPU ratio, one that doesn't result in extreme overcommitting.

Required Linux Software Packages

Each vCloud Director server must include installations of several common Linux software packages. These packages are typically installed by default with the operating system software. If any are missing, the installer fails with a diagnostic message.

```
alsa-lib
bash
chkconfig
coreutils
findutils
glibc
grep
initscripts
krb5-libs
libgcc
libICE
libSM
libstdc++
libX11
libXau
libXdmcp
libXext
libXi
libXt
libXtst
module-
init-
tools
net-
tools
pciutils
procps
redhat-
lsb
sed
tar
wget
which
```

In addition to these packages, which the installer requires, several procedures for configuring network connections and creating SSL certificates require the use of the Linux nslookup command, which is available in the Linux bind-utils package.

Supported LDAP Servers

vCloud Director allows you to import users and groups from the following LDAP services.

Platform	LDAP Service	Authentication Methods
Windows Server 2008	Active Directory	Simple
Windows Server 2012	Active Directory	Simple, Simple SSL, Kerberos, Kerberos SSL
Windows Server 2016	Active Directory	Simple, Simple SSL
Windows 7 (2008 R2)	Active Directory	Simple, Simple SSL, Kerberos, Kerberos SSL
Linux	OpenLDAP	Simple, Simple SSL

Supported Security Protocols and Cipher Suites

vCloud Director requires client connections to be secure. SSL version 3 and TLS version 1.0 have been found to have serious security vulnerabilities and are no longer included in the default set of protocols that the server offers to use when making a client connection. The following security protocols are supported:

- TLS version 1.1
- TLS version 1.2

Supported cipher suites include:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Note: Interoperation with releases of vCenter earlier than 5.5-update-3e and versions of `ovftool` earlier than 4.2 require vCloud Director to support TLS version 1.0. You can use the cell management tool to reconfigure the set of supported SSL protocols or ciphers. See the Cell Management Tool Reference in the *vCloud Director Administrator's Guide*.

Supported Browsers

The vCloud Director is compatible with the current and last major revision of browsers. Version 9.7 of vCloud Director was tested with and supports:

- Google Chrome 72.0.3626.109
- Mozilla Firefox 60.5.1ESR
- Microsoft Edge 42.17134.1.0
- Microsoft Internet Explorer 11.590.171340

Note: Flash must be enabled in the browser to access the vCloud Director Web Console.

Note: Use of Microsoft Edge is not supported with vCloud Director installations that use self-signed certificates. Edge also does not support plugins, so functions such as console redirection and OVF upload do not work with Edge.

Supported Guest Operating Systems and Virtual Hardware Versions

vCloud Director supports all guest operating systems and virtual hardware versions supported by the ESXi hosts that back each resource pool.

Deprecated and Discontinued Functionality

End of Life and End of Support Warnings

- End of Support for Java SDK and .NET SDK. Python SDK is fully supported.
- End of Support for creation of edge devices in the non-advanced mode.
- Upcoming End of Support Notice
    - vCloud Director 9.7 is the last release of vCloud Director to support Oracle Linux as a supported operating to install the vCloud Director application.
    - vCloud Director 9.7 is the last release of vCloud Director to support MS SQL as the vCloud Director Database. Going forward only PostgreSQL database will be supported.
    - vCloud Director 9.7 is the last release of vCloud Director to support vCloud API version 20. This API version is deprecated in this release and will not be supported in future releases.
    - vCloud API 32.0 (vCloud Director 9.7) contains APIs that are under accelerated deprecation and will be removed in future releases. See vCloud API Programming Guide for Service Providers.

Resolved Issues

- **New Unavailable documentation on migrating to vCloud Director appliance and restoring the appliance embedded database**

The vCloud Director 9.7 documentation does not contain instructions on how to migrate existing deployments to vCloud Director 9.7 appliance. Also, there are no instructions on how to restore a backed up appliance embedded database.

Known Issues

- **New When you associate two vCloud Director appliance sites, objects are not visible across the sites**

  If you make a site association and your sites have objects like organizations, organization VDCs, vApps, VMs, you cannot see the objects across sites. The HTML 5 UI displays an Internal server error message. The issue occurs during multisite fanout communication because the `/etc/hosts` file of the vCloud Director appliance does not have correct contents.

  Workaround: None

- **New During vCloud Director Appliance deployment, attempting to set a static route via the provided OVF parameters fails**

  During vCloud Director Appliance deployment, attempting to set a static route via the provided OVF parameters fails. Error messages related to inaccessible system directories appear in the `vcd-ova-netconfig` log file.

```
# cat /opt/vmware/var/log/vcd/networkconfig.log
find: './proc/852': No such file or directory
find: './proc/853': No such file or directory
find: './proc/854': No such file or directory
```

  Workaround: Contact VMware Global Support Services (GSS) for assistance with the workaround for this issue.

- **New The vCloud Director appliance management user interface Promote button and appliance console repmgr commands stop working**

  This issue occurs when the `postgres` user password has expired on one or more vCloud Director appliances. As a result, the vCloud Director appliance management user interface `Promote` button fails to update the selected standby to become the new primary node in a database HA cluster. Some replication manager (repmgr) tool commands fail with errors such as: `Nodes unreachable via SSH`. Upon startup, the appliance OS console displays error messages, such as `[FAILED] Failed to start User Manager`. The `postgres` user password is set to expire on May 25, 2019.

  Workaround:

  Set the `postgres` user account password to never expire. You must run the commands on all appliances individually.

  1. Log in directly or SSH to the vCloud Director appliance OS as `root`.

  2. Set the `postgres` user account and password to never expire by running this command:

```
chage -M -1 -d 1 postgres
```

  3. To confirm that your settings are applied, run the command `chage --list postgres` .

  The system output should confirm that the `postgres` user account and password are set to never expire.

- **New** **Promoting a standby cell to become a primary cell in a high availability cluster might result in an Nginx error screen**

  If a primary or a standby cell is offline at the moment when you attempt to promote a standby cell to become the new primary cell using the appliance management user interface, this might result in the following error message in your browser: `"An error occurred. Sorry, the page you are looking for is currently unavailable. Please try again later. If you are the system administrator of this resource then you should check the error log for details. Faithfully yours, nginx."`

  Workaround: Refresh your browser.

- **New** **Enabling SSL connection to database fails after unsuccessful renewal of certificates on the vCloud Director appliance cell**

  When you attempt to import certificates to the vCloud Director appliance cell, if the new certificate Common Name is the same as the previous Common Name, the import fails. As a result, when you attempt to enable SSL connection to the vCloud Director database, the database configuration fails with the following exception: `sun.security.validator.ValidatorException: PKIX path validation failed: java.security.cert.CertPathValidatorException: signature check failed.`

  Workaround:

  1. Run the following command: `sed -i '/import-trusted-certificates/ s/$/ --force /' /opt/vmware/appliance/bin/appliance-sync.sh`
  2. Wait for a minute and rerun the `configure-database` or `reconfigure-database` command to enable SSL connection to the database: `/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres --database-user vcloud --database-password --database-host --database-port 5432 --database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-director/certificates.ks --keystore-password --primary-ip --console-proxy-ip --console-proxy-port-https 8443.`

- **New** **After upgrading vCloud Director with an external Microsoft SQL database to version 9.7, registering or synchronizing a vCenter Server might fail**

  After upgrading a vCloud Director installation with an external Microsoft SQL database, if you try to register or sync a vCenter Server instance that contains opaque networks, the following error might occur:

  ```
  Violation of UNIQUE KEY constraint 'uq_opaq_netw_inv_vc_id_net_id'.
  Cannot insert duplicate key in object 'dbo.opaque_network_inv'.
  ```

  The opaque networks appear if a vCenter Server instance is associated with an NSX-T Manager and networks are created in that NSX-T Manager.

  Workaround:

  1. Delete all networks from the associated NSX-T Manager.
  2. Verify that there are no opaque networks in the vCenter Server instances and the opaque network inventory tables.
  3. Retry registering the vCenter Server instance or for an already registered vCenter Server instance, reconnect it via the menu option in the vCenter Server view.

  If you cannot delete the networks, there is no alternative workaround.

- **New** **The deployment of the primary appliance fails with an appliance management user interface message that no nodes are found in the cluster**

The deployment of the primary vCloud Director appliance fails because of insufficient access permissions to the NFS share. The appliance management user interface displays the message: `No nodes found in cluster, this likely means PostgreSQL is not running on this node`. The */opt/vmware/var/log/vcd/appliance-sync.log* file contains an error message: `creating appliance-nodes directory in the transfer share /usr/bin/mkdir: cannot create directory ‘/opt/vmware/vcloud-director/data/transfer/appliance-nodes’: Permission denied`.

Workaround:

1. Mount the NFS share on a Linux virtual machine.
2. Change the permissions on the mount point: `chmod -R 750 path-to-mountpoint`.
3. Retry the deployment.

- **New Accessing vCloud Director 9.7 with FQDN fails with an SSL version error**

  Accessing vCloud Director 9.7 with FQDN results in an error: `ERR_SSL_VERSION_OR_CIPHER_MISMATCH` because the SSL certificate keystore on the vCloud Director cell is shared by the HTTPS engine and PostgreSQL. The shared SSL certificate cannot process HTTPS requests that come in to the FQDN due to additional security measures applied by the Server Name Indication (SNI) extension of the TLS protocol.

  Workaround: In a vCloud Director environment that consists of a single cell, use the IP address instead of FQDN to access the vCloud Director UI or API.

  In a vCloud Director environment that consists of multiple cells, you must deploy a load balancer so that the IP is used to communicate with the cells in the back-end.

  1. Deploy a load balancer in front of the VCD cell or cells.
  2. Configure the SSL termination to occur on the load balancer.

- **New Cannot promote a new primary cell by using the appliance management user interface**

  The log rotation function might incorrectly set permissions on the appliance *failover.log* file, which results in promote operation failure.

  Workaround:

  1. SSH to each of the primary and standby appliances, and run the following command:
     `chmod 0664 /opt/vmware/var/log/vcd/failover.log`
  2. Retry the promote operation.

- **New After promoting one of the standby cells to become the new primary cell, vCloud Director cells might incorrectly connect to the old failed primary database**

  The `reconfigure-database` command runs periodically in the background and might incorrectly set vCloud Director cells in the server group to point to the original failed or inaccessible primary cell. As a result, the vCloud Director cells are unable to service any UI or REST API calls.

  Workaround:

  1. Promote a standby cell.
  2. Power off the failed primary appliance.
  3. SSH as root to one of the standby appliances.
  4. Switch to postgres user by running `su - postgres`.
  5. As a postgres user, run `/opt/vmware/vpostgres/current/bin/repmgr cluster show`.

6. From the output of `cluster show`, find the ID of the failed primary.
7. As a postgres user, run `/opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id` *`failed_primary_node_ID`*
   Where *failed_primary_node_ID* is the node ID of the failed primary cell from the previous command.

- **New The vCloud Director WebMKS console sends incorrect Ctrl+Alt+Delete input to the guest OS**

  The version of WebMKS, used in vCloud Director 9.5.0.2, 9.5.0.3, and 9.7, sends incorrect codes to the guest OS when you send the `Ctrl+Alt+Delete` input.

  Workaround:

  - Use either Internet Explorer or Edge browser.
  - Use the HTML5 Standalone VMRC console.
  - For Windows based machines, use the on-screen keyboard to send `Ctrl+Alt+Delete` input to the guest OS.

- **New Existing organization VDC networks that are operational are showing non-operational status in the vCloud Director tenant portal.**

  If you upgrade to vCloud Director 9.7 and you have organization VDC networks that you have not modified in the last month, the networks show a red operational status instead of green.

  Workaround:

  - Isolated and routed organization VDC networks: Update the description in the UI or perform an operation on it every month.
  - Direct networks: Update the description through the flex UI every month.

- **New Updating the properties of a shared direct organization VDC network in the tenant portal H5 UI causes it to be unshared if not in use by a VM or vApp, or causes it to fail, if in use by a VM or vApp.**

  When trying to update the name or description of a shared direct organization VDC network on the tenant portal H5 UI, if the network is shared and not in use, it becomes unavailable to other VDCs in the organization. If the network is in use, it fails with an error message saying that the network is in use. This is because the UI is not sending the shared flag and triggers an unsharing operation.

  Workaround: Update properties of a direct organization VDC network through the Flex UI.

- **New Cell startup fails intermittently**

  An intermittent race condition in the cell causes startup failure with the following error message in the cell-runtime.log file: com.vmware.cell.heartbeat.NonFatalHeartbeatException: org.hibernate.NonUniqueResultException: query did not return a unique result

  Workaround: None.

- **Cannot access an SDDC proxy if vCloud Director uses legacy self signed certificates**

  After the upgrade to vCloud Director 9.7, connecting to an SDDC proxy might fail with the error message: `verify error:num=20:unable to get local issuer certificate`. This issue happens if you generated the self signed certificates by using the cell management tool in vCloud Director 9.5 or earlier.

Workaround: After the upgrade to vCloud Director 9.7, regenerate and update the self signed certificates.

- **After the upgrade to vCloud Director 9.7 (vCloud API v.32.0), custom links that you added by using branding OpenAPI calls are removed**

  In vCloud API v.32.0, type `UiBrandingLink` that is used for custom links is replaced by type `UiBrandingMenuItem`. These types have different elements. This change is backward incompatible. As a result, API calls from versions 31.0 or earlier that attempt to process or set `customLinks` within a `UiBranding` object fail.

  Workaround: Update your API calls to the new data type.

- **Changing the compute policy of a powered on VM might fail**

  When trying to change the compute policy of a powered on VM, if the new compute policy is associated with a provider VDC compute policy that has VM Groups or Logical VM Groups, an error occurs. The error message contains: `Underlying system error: com.vmware.vim.binding.vim.fault.VmHostAffinityRuleViolation`.

  Workaround: Power off the VM, and retry the operation.

- **When using the vCloud Director Service Provider Admin Portal with Firefox, you cannot load the tenant networking screens**

  If you are using the vCloud Director Service Provider Admin Portal with Firefox, the tenant networking screens, for example, the **Manage Firewall** screen for an organization virtual data center, might fail to load. This issue happens if your Firefox browser is configured to block Third-Party cookies.

  Workaround: Configure your Firefox browser to allow third-party cookies.

- **Cannot configure the system to use a SAML identity provider by using the vCloud Director Service Provider Admin Portal**

  After you configure your system to use a SAML identity provider by using the vCloud Director Service Provider Admin Portal, you cannot log in again to the vCloud Director Service Provider Admin Portal.

  Workaround: Configure your system to use a SAML identity provider by using the vCloud Director Web Console.

- **vCloud Director 9.7 supports only a list of input parameters of vRealize Orchestrator workflows**

  vCloud Director 9.7 supports the following input parameters of vRealize Orchestrator workflows:

  - `boolean`
  - `sdkObject`
  - `secureString`
  - `number`
  - `mimeAttachment`
  - `properties`
  - `date`
  - `composite`
  - `regex`
  - `encryptedString`
  - `array`

  Workaround: None

- **A fast-provisioned virtual machine created on a VMware vSphere Storage APIs Array Integration (VAAI) enabled NFS array, or vSphere**

Virtual Volumes (VVols) cannot be consolidated

In-place consolidation of a fast provisioned virtual machine is not supported when a native snapshot is used. Native snapshots are always used by VAAI-enabled datastores, as well as by VVols. When a fast-provisioned virtual machine is deployed to one of these storage containers, that virtual machine cannot be consolidated .

Workaround: Do not enable fast provisioning for an organization VDC that uses VAAI-enabled NFS or VVols. To consolidate a virtual machine with a snapshot on a VAAI or a VVol datastore, relocate the virtual machine to a different storage container.