What’s New in VMware vCloud Director 8.20

Feature Overview
Table of Contents

Introduction ............................................................................................................. 3
Feature Updates ....................................................................................................... 3
  Advanced NSX Networking Features ................................................................. 3
  Custom Role-Based Access Control for Service Provider and
  Tenant Roles ........................................................................................................ 11
  VM to ESXi Host Affinity Rules ........................................................................... 13
Architecture Updates ............................................................................................... 14
  Importing Existing vCenter Managed Infrastructure into
  vCloud Director .................................................................................................. 14
  Automatic Import of VMs .................................................................................... 16
  HTML5 User Interface ........................................................................................ 17
Additional Changes ................................................................................................. 18
Summary .................................................................................................................. 18
More Information .................................................................................................... 18
About the Author ..................................................................................................... 18
Introduction

The VMware vCloud Director® 8.20 solution makes it easy for cloud service providers to manage and operate virtual data centers (VDCs) for multiple consumers. The solution can automate the creation of VDCs based on consumer resource needs and assign the appropriate policies necessary to maintain a proper allocation of resources. The vCloud Director solution also provides a unique portal for consumers to manage various cloud services and workloads on their own.

vCloud Director 8.20 is a milestone release that adds new networking services that support advanced workload management, improve security, and provide multiple ways to connect remotely with a hybrid cloud model.

Feature Updates

vCloud Director 8.20 includes major functional updates. The solution now integrates more closely with VMware NSX® network virtualization, which means that end users will be able customize many network settings.

Advanced NSX Networking Features

Service providers can now abstract and define more NSX features for individual tenants. This allows them to create new advanced service offerings that give tenants and organization VDC users more power to manage their workloads. This release makes the following NSX networking services available to tenants via self-service:

- **Dynamic routing** – Add Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) algorithms to automatically create routing tables between dynamic VMware NSX® Edge™ gateways.
- **Distributed firewall** – Define granular security policies on workloads connected on the same organization network, including firewall rules for traffic flowing within the organization VDC.
- **Tenant layer 2 (L2) VPN access** – Stretch on-premises workloads to vCloud Director organization networks to enable a hybrid cloud.
- **Tenant SSL VPN** – Access workloads placed in an organization’s VDCs remotely via an SSL client.
- **Load balancing** – Distribute incoming traffic to workloads dynamically to help applications maintain SLAs.

These services (except for the distributed firewall) are accessible by right-clicking the NSX Edge gateway and selecting Edge Gateway Services. If you are upgrading from an older version of vCloud Director software and have existing NSX Edge gateways deployed, you can convert these to NSX Edge gateway services by right-clicking the NSX Edge gateway and selecting Convert to Advanced Gateway. This action will redeploy the NSX Edge gateway, upgrade it to a higher version of NSX Edge software if it is version 5.5 or earlier, and enable the new HTML user interface (UI) for configuring the advanced NSX features.
Dynamic Routing

vCloud Director 8.20 adds support for configuring dynamic routing between different NSX Edge gateways. Previously, it only supported static routes between different vApp networks connected to the same or different organization VDC network. Defining routing paths is helpful in situations where two vApps need to talk to each other but are located on different L2 segments. Static routing can be defined at each NSX Edge gateway to determine what the next hop for the traffic originating from a specific vApp will be.

Dynamic routing reduces the need to configure manual routes when a virtual machine (VM) in an organization VDC network needs to talk to another VM in a different organization VDC network. Dynamic routing uses algorithms (vCloud Director software supports both OSPF and BGP) to share network routing tables between various NSX Edge gateways that have dynamic routing enabled. This reduces the overall time organization administrators spend maintaining network routing tables. In a hybrid cloud scenario, if the tenant using the organization network has an enterprise on-premises network connected via Multiprotocol Label Switching (MPLS) or Internet Protocol Security (IPSec), the dynamic routing protocols will help define the best route for transferring packets between the two data centers.

You can configure dynamic routing by right-clicking an NSX Edge gateway and selecting the Routing tab.

Figure 2. VMware NSX Edge Gateway Dynamic Routing Global Configuration
Distributed Firewall

This vCloud Director release introduces the ability for a tenant to configure NSX distributed firewall rules on VMs in an organization VDC. The distributed firewall rules define the ways that traffic can flow between VMs on an organization VDC network.

In previous vCloud Director versions, you could configure the firewall on the NSX Edge gateway to control the traffic flowing between the external networks and the routed organization VDC networks, also known as “north-south” traffic. But this firewall could not define rules of traffic flow between VMs within the same organization VDC network or networks within the same organization VDC. Essentially, there was no way to limit “east-west” traffic flow.

The new distributed firewall available in vCloud Director 8.20 brings this “east-west” traffic under control via NSX network virtualization functions. The distributed firewall also further secures vCloud Director workloads by providing more granular security control.

To access the distributed firewall function, a user in the organization must have enough privileges to manage the firewall.

You can access distributed firewall settings by logging in to the vCloud Director portal and right-clicking Org vDC > Manage Firewall. This will open a new tab.
NSX kernel modules controlled with VMware NSX Manager™ software reside within each of the VMware ESXi™ hosts. Once you create firewall rules, they get published to every ESXi host that’s supporting the organization VDC. The vCloud Director portal allows organizations to define these rules in a similar fashion to the firewall on the NSX Edge gateway. You can create the rules using individual IP or MAC addresses, or a predefined group of IP/MAC address sets. You can apply the rules to individual ports or select from a predefined list of services (e.g., SNMP, ICMP, HTTP, etc.). Apart from individual services, the vCloud Director portal has predefined service groups (e.g., Microsoft Exchange, Oracle, etc.).

**Tenant L2 VPN Access**

L2 VPN access now allows tenants or users to create a tunnel between networks in an organization VDC to an on-premises network at their enterprise location. This tunnel creates an L2 broadcast domain between two sites and makes the two networks look seamless across the cloud by putting VMs on both sites on the same IP subnet. vCloud Director software uses the NSX L2 VPN server at the NSX Edge gateway and allows configuration by an authorized tenant user. An enterprise user consuming the organization VDC can connect to the L2 VPN server by using NSX network virtualization on-premises or by using the standalone NSX Edge appliance to talk to the NSX server. Once the client has configured the NSX L2 VPN server, the tenant can decide which L2 segment on-premises it wants to extend to the cloud. The client can extend an existing on-premises VXLAN or VLAN to the organization VDC network. The subnets on both ends (cloud and on-premises) must be the same. Alternatively, you can configure the organization VDC network as a client with the L2 server onsite.

You can only extend routed organization VDC networks using the L2 VPN tunnel. To extend an organization VDC network, you must convert it to a subinterface type, which allows vCloud Director software to identify the network it will use to extend via L2 VPN. The vCloud Director solution, with the help of NSX network virtualization, will create a trunk interface type for this network.
When creating a new organization VDC-routed network, select Create as Subinterface.

To enable the L2 VPN tunnel, the server site needs an encryption protocol and an authorization key, along with the networks (and interfaces) to be stretched. On the client site, you must select the same encryption protocol with appropriate authentication details and the network extended to the tunnel.

The L2 VPN can stretch networks regardless of whether the individual segments are VXLAN or VLAN.

**Tenant SSL VPN Access**

This vCloud Director release adds support for SSL VPN access, in addition to IPSec and L2 VPN options. With SSL VPN enabled, remote clients can connect to the SSL server configured on the NSX Edge gateway to access applications or organization VDC networks.

When an SSL connection is established from a remote client, the SSL server gives each connected client an IP address on the private network. This enables hybrid cloud deployments in which a remote client can connect to the workloads sitting in the cloud inside an organization VDC.

While an L2 VPN stretches an existing IP subnet across sites, an SSL VPN creates an interface with the same IP range for every incoming connection and releases it once the remote client has disconnected. An L2 VPN tunnel is always active once you have configured the two sites, but an SSL VPN tunnel can terminate once the client disconnects.
To configure an SSL VPN server, the server needs a public IP address (on the NSX Edge gateway), a pool of IP addresses to assign to incoming client connections, an authentication protocol, and a list of users who will be accessing it.

You can configure SSL servers by navigating to Edge Gateway > Edge Gateway Services > SSL VPN Plus.

Figure 8. SSL VPN Server Settings
Load Balancing

The NSX Edge load balancer now helps evenly distribute incoming traffic to a VDC workload with a pool of servers. Pools support a common application and can be based on HTTP, HTTPS, TCP, or UDP.

A pool of servers is defined using the Pools configuration, which also allows you to specify the IP addresses of the VMs that will be sharing the incoming traffic workload.

Figure 9. VMware NSX Edge Gateway Load Balancer Configuration

Figure 10. Edit a Pool
The load balancer also needs an IP address where the incoming traffic will originate. You can define this using a virtual IP address and it is typically a public IP address that’s configured for the NSX Edge gateway interface. The virtual server maps the public IP address for incoming traffic to the pool of servers.

You can manage the way the incoming traffic is redirected to the pool of servers with the Application Profiles settings. You can define an application profile according to multiple parameters, including redirection of URLs and the maintenance of persistent connections based on a source IP address, cookie, or session ID.
You can also assess the health of the pool of back-end servers using the Service Monitor setting. Figure 14 shows the overall process for configuring a load balancer on the NSX Edge gateway.

Custom Role-Based Access Control for Service Provider and Tenant Roles

A service provider administrator must perform many tasks to onboard new tenants to the cloud, maintain existing tenants, and maintain the underlying VMware infrastructure. By mapping specific roles to the meta-functions that the service provider administrator will perform, service providers can improve their security practices and operational visibility while maintaining compliance.
vCloud Director 8.20 allows the creation of custom roles for service provider tenants. You can define the roles based on functional tasks and subtasks within the vCloud Director system administration. To create a custom role, first select a function, then assign a user the new role. For example, if system administrators are going to use the VMware vSphere® platform to define and manage service provider VDCs in the data center, their custom role will be assigned the provider VDC, the VMware vCenter Server® application, datastores, provider network, and hosts functions.

Similarly, you can create custom roles for organization administrators. Although organization administrators are already created with predefined roles out-of-the-box, creating custom roles provides more granular access control. In addition, with custom roles, service providers can restrict access to just the features and functions that the tenant has signed up for. This feature helps restrict tenant access to tiered services.
VM to ESXi Host Affinity Rules

VM to host affinity rules allows you to pin certain VMs to a group of ESXi hosts backing the organization VDC resources. The affinity rules ensure that the VMs defined in the rule set are placed within the defined set of hosts.

A provider VDC is associated with a cluster of ESXi hosts. These clusters normally have VMware vSphere Distributed Resource Scheduler™ (DRS) enabled. When a tenant instantiates a VM for deployment, DRS uses an algorithm to select an appropriate ESXi host for the VM, and the total workload in that cluster is distributed evenly among the ESXi hosts. However, there may be certain scenarios where you need to place a VM in an organization VDC on a specific host not recommended by DRS. These scenarios include latency-sensitive applications or applications with licensing requirements that you need to place on a specific ESXi host or hosts.

Because affinity rules require visibility between both the VM, which is a tenant object, and an ESXi host, only system administrators can create them.

Take these steps to create affinity rules:

1. Create an ESXi host group in the vCenter Server application, which will create a host group inside the cluster that's backing the provider VDC. Log in to the vCenter Server application and navigate to Cluster > Manage Settings > Configuration > Host Groups.

2. Create a VM group in the vCloud Director portal, which will list the VMs that require affinity to the host group. Log in to the vCloud Director portal and navigate to Provider vDC > Resource Pools Tabs > Open the Resource Pool > VM Groups.

3. Create a new affinity rule in the Resource Pools section to associate the VM group with the host group.
Architecture Updates

vCloud Director 8.20 also adds many updates to its architecture, including the way it manages the inventory of objects with the vCenter Server application and an additional API to configure networking services.

Importing Existing vCenter Managed Infrastructure into vCloud Director

The vCloud Director solution interacts with the underlying vCenter Server application to deploy and manage VMs. The vCenter Server application is responsible for placing these VMs on the appropriate ESXi hosts based on the distributed resource cluster’s calculations. The vCloud Director solution synchronizes with the vCenter Server application to keep track of the state and inventory of VMs. At the same time, vCloud Director software creates resource pools as container objects to place VMs created in an organization VDC. The resource pools have the allocation definitions assigned for compute, network, and storage, which means that vCloud Director software only synchronizes inventory under these resource pools. vCloud Director software will not recognize existing VMs that the vCenter Server application is managing.

This release makes it possible to import existing VMs in the vCenter Server application to an organization VDC in the vCloud Director portal. This will help service providers bring the multitenancy vCloud Director platform into already managed vCenter Server environments.

Imported VMs must be mapped to tenants or organization VDCs within the vCloud Director solution. Figure 17 explains the resource pool structure needed.

![Figure 17. Resource Pool Structure Required for Import](image-url)
To import existing VMs, first create a new provider VDC with RP1 as the resource pool. Once created, to adopt RP2 in the organization VDC, trigger the following API:

```xml
POST

Content-Type: application/vnd.vmware.admin.createVdcParams+xml

<?xml version="1.0" encoding="UTF-8"?>
<CreateVdcParams
  name="org26vdc1"
  xmlns="http://www.vmware.com/vcloud/v1.5">
  <Description>Example VDC</Description>
  <AllocationModel>AllocationVApp</AllocationModel>
  <ComputeCapacity>
    <Cpu>
      <Units>MHz</Units>
      <Allocated>2048</Allocated>
      <Limit>2048</Limit>
    </Cpu>
    <Memory>
      <Units>MB</Units>
      <Allocated>2048</Allocated>
      <Limit>2048</Limit>
    </Memory>
  </ComputeCapacity>
  <NicQuota>0</NicQuota>
  <NetworkQuota>100</NetworkQuota>
  <VdcStorageProfile>
    <Enabled>true</Enabled>
    <Units>MB</Units>
    <Limit>2048</Limit>
    <Default>true</Default>
    <ProviderVdcStorageProfile
      href="https://vcloud.example.com/api/admin/pvdcStorageProfile/101" />
  </VdcStorageProfile>
  <ResourceGuaranteedMemory>1</ResourceGuaranteedMemory>
  <ResourceGuaranteedCpu>1</ResourceGuaranteedCpu>
  <VCpuInMhz>2048</VCpuInMhz>
  <IsThinProvision>false</IsThinProvision>
  <NetworkPoolReference
    href="https://vcloud.example.com/api/admin/extension/networkPool/313" />
  <ProviderVdcReference
    name="Main Provider"
    href="https://vcloud.example.com/api/admin/providervdc/35" />
</CreateVdcParams>
```
In the preceding example, the existing resource pool setting on RP2 will be overwritten by the one defined by the allocation setting on the provider VDC and will be added to RP1. Also, because vCloud Director software creates vApp constructs, it will automatically add them around imported VMs.

**Automatic Import of VMs**

When you create a VM in a resource pool that's backing an organization VDC, vCloud Director software will automatically import the VMs as vApps in the organization VDC cloud. As part of its periodic inventory update with the vCenter Server application, any time vCloud Director software sees any new VM objects in a resource pool that maps to a tenant organization, it will automatically import them, generate a vApp construct around them, and start to include them as managed objects in its updated inventory.

This feature helps achieve consistency across vSphere and vCloud Director environments. Not all service providers will want to always have automatic import running, so the feature has an on/off switch to enable or disable it.

You can apply automatic import of VMs at the system, organization, or organization VDC level, with the settings overwriting each other in that order.

You can change the system setting by navigating to the System > Administration > System Settings > General > Miscellaneous section.

To change the settings on an organization VDC, make a GET API call:

```
GET https://[vCD-cell-address]/api/admin/vdc/[Org-vDC-ID]
```

Change the `VmDiscoveryEnabled` tag to `True` via a PUT request:

```
PUT https://[vCD-cell-address]/api/admin/vdc/[Org-vDC-ID]
Accept:application/*+xml;version=27.0
x-vcloud-authorization:[authorization code]
Content-Type:application/vnd.vmware.admin.vdc+xml

<?xml version="1.0" encoding="UTF-8"?>
<AdminVdc xmlns="http://www.vmware.com/vcloud/v1.5" name="vdc-test">
  <AllocationModel>AllocationVApp</AllocationModel>
  <ComputeCapacity>
    <Cpu>
      <Units>MHz</Units>
      <Allocated>0</Allocated>
      <Limit>0</Limit>
      <Reserved>0</Reserved>
      <Used>0</Used>
      <Overhead>0</Overhead>
    </Cpu>
    <Memory>
      <Units>MB</Units>
      <Allocated>0</Allocated>
      <Limit>0</Limit>
      <Reserved>0</Reserved>
      <Used>0</Used>
      <Overhead>0</Overhead>
    </Memory>
  </ComputeCapacity>
</AdminVdc>
```
There are still some scenarios in which importing a VM might not work. Typically, the VM being imported needs to conform its hardware settings to the organization VDC that it’s being mapped into. If not, vCloud Director software will not be able to import the VM and will log the reason in the events log. Example scenarios include a VM that has a disk drive stored in a datastore that the organization VDC doesn’t have access to; or a VM that is attached to a virtual network that’s not mapped to the organization VDC network; or a VM with a hardware profile that is higher or lower than the parent provider VDC.

**HTML5 User Interface**

With this release, parts of the vCloud Director UI have been rearchitected to begin the transition from the current Flex-based technology to an interface based on HTML5. All the NSX Edge gateway networking services and distributed firewall configurations available to organizations have been moved to the HTML5 interface, while the rest of the UI elements are still Flex-based. When logging in to the vCloud Director portal, you will still see the old UI, until you navigate to an NSX Edge gateway that’s been converted to an advanced gateway. Users do not need to re-enter login credentials, and the user experience will be seamless. To access the new UI, right-click the NSX Edge gateway and select Configure Services. Another way to see the new UI is to right-click an organization VDC and select Manage Firewall.

![New User Interface for an NSX Edge Gateway Converted to an Advanced Gateway](image)
Additional Changes

In addition to the feature and architectural updates already mentioned in this document, this vCloud Director release includes other useful functionality. For instance, upgrading vCloud Director installations with multiple cells is now much easier with upgrade automation scripts. This release also allows network pools backed by vCloud Director network isolation (vCDNI) to be converted to VXLAN-backed network pools.

Summary

VMware vCloud Director 8.20 is packed with major new features that will help service providers and their consumers further secure their workloads with the distributed firewall functions; better manage their workloads in the cloud with advanced load-balancing capabilities; and deploy multiple hybrid channels to the cloud using L2 or SSL VPN services.

More Information

For more information about the VMware vCloud Director solution, visit the product pages at https://www.vmware.com/products/vcloud-director.html.

Access the documentation for vCloud Director software at https://www.vmware.com/support/pubs/vcd_sp_pubs.html.


To purchase the vCloud Director solution or to find out how you can join the VMware vCloud Air™ Network service provider program, visit http://www.vmware.com/go/partner-enrollment.

About the Author

Boskey Savla is a senior technical marketing manager for the vCloud Air Network group at VMware. She works on developing resources for vCloud Air Network partners with various VMware product stacks, focusing on the VMware vCloud Director software solution. She has more than 12 years of experience in systems and solution engineering. She has worked with various VMware partners in certifying and architecting Software-Defined Data Centers and hybrid cloud solutions.