DEPLOYING A VMWARE VCLOUD DIRECTOR® INFRASTRUCTURE-AS-A-SERVICE (IAAS) SOLUTION WITH VMWARE CLOUD FOUNDATION™: ARCHITECTURAL GUIDELINES
# Table of Contents

1. Executive Summary ............................................ 4

2. Introduction to VMware Cloud Foundation ................. 5
   2.1 Overview of VMware Cloud Foundation ................. 5
   2.2 Architecture ............................................. 6
      2.2.1 Physical Architecture .......................... 6
      2.2.2 Imaging and Bring-Up ......................... 6
      2.2.3 Domains – Logical Pooling of Physical Resources 7
      2.2.4 Management Domains .......................... 9
      2.2.5 Workload Domains ............................ 12

3. VMware vCloud Director ...................................... 13
   3.1 Overview of VMware vCloud Director ................. 13
   3.2 Architecture ............................................. 14
      3.2.1 Core Terminology ................................ 14
      3.2.2 Management Cluster .......................... 15
      3.2.3 Resource Abstraction Layers ................ 17

4. vCloud Director with Cloud Foundation .................... 18
   4.1 Terminology Mapping .................................. 18
      4.1.1 vCloud Director Management Cluster and Cloud Foundation Management Domain 18
      4.1.2 vCloud Director Resource Group and Cloud Foundation VI Workload Domain 20
   4.2 Example Architectures: vCloud Director with Cloud Foundation ................. 21
      4.2.1 vCloud Director Deployment Models in the vCloud Architecture Toolkit 21
      4.2.2 Single Availability Zone – Self-Contained Deployment Model 21
      4.2.3 Multiple Availability Zones – Mixed Deployment Model 23
   4.3 Networking Options ..................................... 24
      4.3.1 General Considerations ........................ 24
      4.3.2 Physical Networking in Cloud Foundation .... 25
      4.3.3 External Network Connectivity of a Workload Domain 26
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.4 Example Logical Network Design in vCloud Director and Integration with Cloud Foundation</td>
<td>27</td>
</tr>
<tr>
<td>4.3.5 External Network Connectivity Options with Cloud Foundation</td>
<td>28</td>
</tr>
<tr>
<td>4.3.6 Summary</td>
<td>32</td>
</tr>
<tr>
<td>4.4 Storage Options</td>
<td>33</td>
</tr>
<tr>
<td>5. Conclusion</td>
<td>33</td>
</tr>
<tr>
<td>6. Appendix</td>
<td>34</td>
</tr>
<tr>
<td>6.1 References</td>
<td>34</td>
</tr>
<tr>
<td>6.2 Software Versions</td>
<td>34</td>
</tr>
</tbody>
</table>
1. Executive Summary

VMware vCloud Director® is a product available exclusively for service providers via the VMware vCloud® Air™ Network program to address their public and hybrid cloud infrastructure-as-a-service (IaaS) use cases. Originally released in 2010, it enables service providers to orchestrate the provisioning of Software-Defined Data Center (SDDC) services as complete virtual data centers that are ready for consumption in a very short time frame. vCloud Director applies the principles of pooling, abstraction, and automation to all data center services such as storage, networking, and security. Using vCloud Director, service providers can deliver a shared SDDC infrastructure to multiple customers—that is, tenants—while keeping the resources of these tenants isolated from each other. Essentially, vCloud Director enables a complete multitenancy SDDC platform as one of its key architectural principles.

To accelerate the customer journey to the SDDC, VMware has introduced VMware Cloud Foundation™, a new and unified SDDC platform for the private and public cloud. Cloud Foundation brings together VMware compute, storage, and network virtualization into a natively integrated stack that can be deployed on premises or run as a service from the public cloud. The Cloud Foundation stack consists of VMware vSphere®, VMware NSX®, and VMware vSAN™ along with the new VMware SDDC Manager™. The SDDC Manager component fully automates and orchestrates the bring-up, deployment, operation, and scalability of these underlying SDDC components along with the inherent rack infrastructure consisting of server and networking hardware. To maximize the benefits of this rapidly deployed hyper-converged SDDC infrastructure, VMware partners with several hardware vendors to deliver a validated and prebuilt SDDC stack using Cloud Foundation.

Designing and implementing a vCloud Director environment has typically been a time-consuming and complicated task. Although Cloud Foundation itself does not eliminate the design and implementation of vCloud Director components, it dramatically diminishes these tasks for the underlying SDDC platform stack—that is, vSphere, NSX, and vSAN—and the underlying hardware rack infrastructure, both of which can serve as the foundational platform for vCloud Director.

This technical paper is aimed at architects and designers who want to assess the benefits of deploying vCloud Director with Cloud Foundation and who lead the design and implementation of such an architecture on behalf of a service provider. It therefore offers a short overview of both products and their key terminologies as they pertain to this discussion, provides basic architectural guidance on how to deploy vCloud Director with Cloud Foundation, and discusses the benefits of this approach.
2. Introduction to VMware Cloud Foundation

2.1 Overview of VMware Cloud Foundation

VMware Cloud Foundation delivers a natively integrated SDDC stack consisting of vSphere, NSX, and vSAN as core technologies for server, storage, and network virtualization. Additional software components of VMware vRealize® Suite and the VMware Horizon® suite can be deployed natively on top as another option. Cloud Foundation relies on certified server hardware components—more or less a subset of VMware vSAN ReadyNode™—and certified network hardware components in accordance with the VMware Compatibility Guide for VMware Cloud Foundation. When deploying on-premises private clouds, customers can choose either to build their own hardware configuration ready for Cloud Foundation or to order a completely prebuilt and preconfigured rack configuration from one of several hardware vendors who are certified partners for delivering prebuilt Cloud Foundation configurations.

Cloud Foundation offers the following core features and benefits:

• Automated hardware and software bring-up – With SDDC Manager as its core automation component, Cloud Foundation can deploy a complete SDDC platform consisting of software and hardware in a fully automated way that requires only minimal user input and advance planning. Complete deployment of the Cloud Foundation stack, from initial rack power-up until it is user-workload ready, typically takes less than 8 hours.

• Simplified resource provisioning – Cloud Foundation creates and maintains logical pools of compute, storage, and network resources from the underlying physical rack hardware resources. For this purpose, these physical resources can be allocated and decommissioned dynamically “on the fly.”

• Automated lifecycle management – SDDC Manager orchestrates patch and upgrade management of the underlying SDDC software components in a fully automated way.

• Scalability and performance – Cloud Foundation delivers a private cloud instance, which can easily be integrated into an existing network. Certified hardware configurations range from a minimum of four servers to a multirack arrangement with up to eight racks. SDDC Manager can manage these hardware resources as a single capacity pool, which can be added in units as small as one server to existing or new logical pools.
2.2 Architecture

2.2.1 Physical Architecture

Figure 1. Cloud Foundation Physical Architecture

Figure 1 depicts the physical architecture of a Cloud Foundation configuration with the following components:

- One management switch per rack
- Two top-of-rack (ToR) switches per rack
- Up to 32 servers per rack
  - Currently, a single Cloud Foundation instance can scale up to eight racks.
- Two interconnect switches per Cloud Foundation instance (when deploying more than one rack)

The external network connection is realized via the ToR switches in rack 1.

In its current release, a Cloud Foundation instance is placed in a single data center or availability zone. Cloud Foundation does not implement the concept of multiple data centers or availability zones at this time.

2.2.2 Imaging and Bring-Up

A physical rack configuration for Cloud Foundation, as described in section 2.2.1, initially has factory-default hardware settings and does not contain any customized hardware or software. The automated installation and configuration of Cloud Foundation hardware and software components occur in a two-stage process: imaging and bring-up.
The details for executing these two installation stages are described in the official documentation for Cloud Foundation and in demo videos on the Cloud Foundation YouTube channel. Completion of the Cloud Foundation imaging stage executes a basic installation and configuration of the following components:

- Management switch
- ToR switches (2)
- Rack interconnect switches (2)
- All connected servers with VMware ESXi™

Cloud Foundation system components are deployed onto node 0, which is the first server at the bottom of rack 1. See section 2.2.4 for details on these components.

The next stage is called bring-up. Completion of this stage deploys the following fully configured and production-ready components:

- Four-node vSphere and vSAN cluster

**NOTE:** This cluster also forms the management domain, which will be explained in section 2.2.4.

- VMware vCenter Server® Appliance™, which manages the Cloud Foundation management domain
- Platform Services Controller™ instances configured in Enhanced Linked Mode
- NSX base installation consisting of VMware NSX Manager™ and VMware NSX Controller™ cluster

The following distinctions clarify why the process of installation and configuration is divided into the two stages of imaging and bring-up rather than being consolidated into one single stage:

- The imaging stage leads to a basic configuration that is identical for all customer environments with a given Cloud Foundation rack hardware configuration.
- The bring-up stage individualizes and instantiates a Cloud Foundation configuration based on individual customer requirements, especially regarding IP networking, and makes it production ready.

### 2.2.3 Domains – Logical Pooling of Physical Resources

Cloud Foundation introduces the concept of a domain to provision intelligent units of SDDC resources on the bare-metal Cloud Foundation hardware infrastructure described in section 2.2.1.

At the simplest level, a domain describes an aggregation of a specified number of hosts from the Cloud Foundation rack configuration.
Figure 2 shows an example of carving out several domains from within the Cloud Foundation rack configuration.

The concept of a domain has the following further characteristics or rules within Cloud Foundation:

- At its core, a domain is an aggregation of hosts with ESXi preinstalled and all necessary network infrastructure configured. This includes management network, VMware vSphere vMotion® network, and so on.
- When creating a domain, a new vCenter Server Appliance instance and a new NSX instance are deployed. The vCenter Server Appliance and NSX Manager instances of the new NSX installation are placed in the Cloud Foundation management domain, which will be introduced shortly afterward. The NSX Controller cluster will already have been deployed in the newly created domain.
• The vCenter Server Appliance instance is registered with one of the two Platform Services Controller instances within the management domain.

• The preinstalled ESXi hosts of the domain are configured production ready by the Cloud Foundation domain creation workflow and form a new vSphere cluster with a vSAN datastore.

• In the current Cloud Foundation release, exactly one vSphere cluster per domain is created. At this time, having more than one vSphere cluster per domain is not supported. This might be subject to change in future Cloud Foundation releases.

• In the current Cloud Foundation release, the user cannot directly select nodes to be included in a workload domain during creation. Rather, the Cloud Foundation system attempts to completely consume all nodes from one rack before moving on to the next rack. Therefore, the vSAN concepts of fault domains and stretched clustering are not supported with the current Cloud Foundation release. This also might be subject to change in future Cloud Foundation releases.

• A domain must have a minimum of 3 and a maximum of 64 hosts. These limits are basically defined by the configuration limits of vSphere 6.0, used within the current Cloud Foundation release, and the corresponding vSAN version.

• There are two domain types within Cloud Foundation. These will be described in more detail in a subsequent section:
  - Management domain – A management domain is primarily dedicated to hosting system components related to Cloud Foundation and further management components related to vSphere, NSX, and vRealize Suite.
  - Workload domain – A workload domain in the Cloud Foundation context is dedicated to hosting end-user or customer workloads.

2.2.4 Management Domains

A management domain within Cloud Foundation is primarily dedicated to hosting Cloud Foundation management components such as SDDC Manager as well as those related to VMware virtual infrastructure (VI) such as Platform Services Controller instances, VMware vCenter Server® instances, NSX Manager instances, and management components of vRealize Suite, all of which are part of the Cloud Foundation framework.

Placing end-user or customer workloads into a Cloud Foundation management domain is allowable and sensible in certain scenarios:

• Small Cloud Foundation configurations for which there are no resources to create a separate workload domain
• Management components of user workloads

However, consumers of a Cloud Foundation configuration must ensure proper sizing of the management domain to account for additional resource requirements imposed by their workloads. The standard size of a workload domain is four hosts; this can be expanded after initial deployment.
Figure 3 provides an overview of the Cloud Foundation management components within a Cloud Foundation management domain.

As depicted in Figure 3, the management domain consists of a vSphere cluster, initially with four hosts—that is, the first four hosts of the first rack. It hosts management VMs, which can be subdivided into the following areas:

1) Core Cloud Foundation management layer – The core Cloud Foundation management layer contains the minimal set of VMs available with every Cloud Foundation installation. The VMs in this layer in turn can be classified in the following way:

   a) Cloud Foundation system stack – This stack contains the basic system VMs hosting the Cloud Foundation configuration. Its components will be explained only briefly because they are not very relevant to a discussion related to vCloud Director architecture:

      • Infrastructure services VMs (ISVMs) – These three VMs contain among other things a distributed datastore service that holds all infrastructure-related configuration data and ensures and monitors the health of infrastructure system services related to Cloud Foundation. At its core, it is the central clustered repository for all configuration data related to Cloud Foundation.
• Cloud Foundation lifecycle management repository and backup – These VMs store Cloud Foundation patch and upgrade bundles.
• Virtual rack manager or SDDC Manager – SDDC Manager is the central gateway to Cloud Foundation configuration management. It offers among other things a Web user interface (UI) for administration, implements a workflow services engine, and provides a DNS and an NTP server as shared SDDC infrastructure services.

b) VI management stack – The VI management stack consists of standard management components related to vSphere and NSX:
• Platform Services Controller – Platform Services Controller instances provide shared platform services—VMware vCenter® Single Sign-On, for example—to VMware components such as vCenter Server and SDDC Manager. A detailed description of all Platform Services Controller services is beyond the scope of this document. There are two Platform Services Controller instances configured in Enhanced Linked Mode that form a vSphere domain. All vCenter Server instances, which are subsequently deployed when creating Cloud Foundation workload domains, are registered with one of the two Platform Services Controller instances.
• vCenter Server – This vCenter Server instance solely manages the vSphere cluster of the Cloud Foundation management domain.
• NSX Manager plus NSX Controller cluster (three VMs) – These VMs form the management or control plane of the NSX installation, which provides NSX networking services for the vSphere cluster in the management domain.

c) Operations management stack – The operations management stack consists of a VMware vRealize Log Insight™ instance and a VMware vRealize Operations™ instance. These components are optional and are separately licensed within Cloud Foundation. They therefore appear in light, transparent green in Figure 3.

2) Management layer for Cloud Foundation workload domains – With each instantiated Cloud Foundation workload domain, a set of certain management VMs are deployed. Because there are two types of Cloud Foundation workload domains, which will be explained in more detail in a following section, there are also two types of management layers for these workload domains:

a) Management layer for VI workload domains – The management layer for a VI workload domain consists of only two VMs, which are deployed with each VI workload domain:
• vCenter Server – This vCenter Server instance manages the vSphere cluster of the corresponding Cloud Foundation workload domain.
• NSX Manager – This NSX Manager instance connects to the vCenter Server instance of the Cloud Foundation workload domain to manage the NSX networking services for that workload domain.
b) Management layer for virtual desktop infrastructure (VDI) workload domains – VDI workload domains are not relevant to a discussion related to vCloud Director and are not described in detail here. The management layer also contains a vCenter Server instance and an NSX Manager instance, as is the case with the management layer of VI workload domains, but it additionally contains VMware Horizon management components.

2.2.5 Workload Domains

Workload domains are dedicated to hosting consumer or customer workloads within the Cloud Foundation configuration. They are created via the SDDC Manager Web UI by an administrator of the Cloud Foundation configuration.

As has already been mentioned, there are currently two types of workload domains available in the Cloud Foundation product:

a) VI workload domains – VI workload domains are reserved for VI workloads and will be discussed later in this document when the vCloud Director IaaS use case is described in more detail.

b) VDI infrastructure workload domains – VDI workload domains are created for hosting workloads related to VMware Horizon.

Figure 4 highlights the components of a VI workload domain with four hosts, which are deployed within Cloud Foundation:

Figure 4. VI Workload Domain

Many workflow tasks are managed behind the scenes when deploying a VI workload domain. The following is a summary of the tasks related to this discussion:

- Components deployed in the Cloud Foundation management domain – Although a VI workload domain deployment is initiated, some related components for managing the newly created VI workload domain are deployed in the Cloud Foundation management domain:
  - A new NSX Manager instance and a vCenter Server Appliance instance are deployed into the management domain and are configured automatically.
- The vCenter Server Appliance instance manages the VI workload domain. The NSX Manager instance is registered or connected with that corresponding vCenter Server instance.

- VI workload domain deployment – The VI workload domain is created by deploying and configuring the following components:
  - ESXi hosts (4)
  - VMware vSphere Distributed Switch™ (1)
  - vSphere cluster created with the four ESXi hosts
  - vSAN enabled within the vSphere cluster, creating a vSAN datastore
  - NSX Controller cluster corresponding to the newly deployed NSX installation or NSX Manager and consisting of three NSX Controller VMs

Note: The NSX Controller cluster, although not situated in the NSX data path, is deployed in the VI workload domain and not in the management domain. This is due to the close communication relationship between the managed ESXi hosts in the VI workload domain and the NSX Controller VMs.

To summarize, a VI workload domain consists of an empty vSphere cluster prepared to provide virtualized compute, storage, and network resources. It is deployed and configured completely automatically.

3. VMware vCloud Director

3.1 Overview of VMware vCloud Director

VMware vCloud Director is a platform used by VMware service providers to deliver public and hybrid cloud data center services. From a provider perspective, it enables service providers to carve virtually isolated, multitenancy-enabled resources from a physical pool of compute, storage, and network resources. These virtual entities are also called virtual data centers. Within the construct of virtual data centers, vCloud Director currently is the only VMware SDDC automation product that implements secure multitenancy by isolating data center services at all virtual layers of data center resources.

The following are some of the most important additional features of vCloud Director:

- VMware vSphere vApp™ catalog – Tenants can create multi-VM configurations called vSphere vApps and store them as vApp templates in their own vApp catalog. This catalog is isolated from all catalogs of other tenants hosted on the same physical platform. The vApp templates are then used for repetitive deployment of vApps.

- Automated networking and security services based on NSX – Software-defined NSX networking and security services such as distributed switching based on VXLAN; distributed firewalls; and VMware NSX Edge™ services such as routing, NAT, VPN, and load balancing are consumed by vCloud Director—during vApp deployments, for example—in a fully automated way.

- Self-service Web portal – End users of the tenants using the vCloud Director platform have direct access to their vApp catalogs and deployed vApps through a modern, self-service Web portal.

- vCloud API – Tenants and providers can consume vCloud Director services via a comprehensive REST-based API. For example, providers can develop their own Web portal for consumption by their tenants.
3.2 Architecture

3.2.1 Core Terminology

vCloud Director introduces a layer of abstraction to pool compute, storage, and network resources while enabling complete multitenancy. Table 1 summarizes the most important terms pertaining to this paper.

<table>
<thead>
<tr>
<th>CONSTRUCT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization</td>
<td>An organization is the unit of multitenancy that represents a single logical security boundary. An organization contains users, virtual data centers, and networks.</td>
</tr>
<tr>
<td>Resource Group</td>
<td>A resource group is a set of compute, storage, and network resources dedicated to tenant workloads and managed by a single pairing of vCenter Server instance plus NSX Manager instance. vCloud Director manages the resources of all attached resource groups through API communication with vCenter Server and NSX Manager.</td>
</tr>
<tr>
<td>Provider Virtual Data Center</td>
<td>A provider virtual data center is a grouping of compute, storage, and network resources from a single vCenter Server instance. It consists of one or more resource pools with one primary—that is, initial—resource pool along with datastores connected to this resource pool. <strong>All resource pools must be from a single vCenter Server instance or resource group, so a single provider virtual data center cannot be spanned across vCenter Server instances.</strong> Provider virtual data centers typically are configured with root resource pools from a vSphere cluster. Therefore, cluster objects typically are assigned as resource pools for backing a provider virtual data center. Multiple organizations can share provider virtual data center resources.</td>
</tr>
<tr>
<td>Organization Virtual Data Center</td>
<td>An organization virtual data center is a subgrouping of compute and storage resources allocated from a provider virtual data center and assigned to a single organization. On the vSphere layer, a resource pool under each of the corresponding provider virtual data center resource pools is created and represents the organization virtual data center.</td>
</tr>
<tr>
<td>vSphere vApp</td>
<td>A vSphere vApp is a container for a distributed software solution and is the standard unit of deployment in vCloud Director. A vCloud Director vApp is different from a vSphere vApp in the manner it is instantiated and consumed in vCloud Director. It enables power operations to be defined and specifically ordered. It consists of one or more VMs and can be imported or exported as an Open Virtualization Format (OVF) package. A vCloud vApp can have additional constructs specific to vCloud such as vApp networks.</td>
</tr>
</tbody>
</table>

Table 1. Architectural Constructs of vCloud Director
3.2.2 Management Cluster

In a similar manner to that previously described for Cloud Foundation management components, components related to vCloud Director are placed into a management cluster. Figure 5 shows a typical example management cluster for a basic vCloud Director implementation.

![Figure 5. vCloud Director Management Cluster](image)

**NOTE:** Figure 5 depicts only the main, core vCloud Director management components required for establishing a basic vCloud Director deployment. Depending on the use case, more components and extensions might be deployed in the vCloud Director management cluster. However, these additional components are not relevant for a basic architectural discussion evaluating the feasibility of implementing vCloud Director with a Cloud Foundation installation and are therefore not shown here.

The vCloud Director management cluster, as depicted in Figure 5, consists of the following core components:

**Cloud Management Components**

- **vCloud Director cells** – vCloud Director cells are the central management components of a vCloud Director environment. They provide the following core functionalities:
  - Enable access to vCloud Director managed cloud resources—virtualized compute, storage, and network resources—to tenants. Two access points are built into the vCloud Director cells to access these resources:
    - UI/API access point – The vCloud Director UI is implemented as a Web console and provides the standard portal for setting up and managing an IaaS solution based on vCloud Director. The vCloud API supports developers who want to build their own customized interactive clients apart from the standard UI to better satisfy additional UI requirements a service provider might have for its individual use cases.

---

*VMware*
Remote console proxy – The remote console of deployed VMs or vApps is proxied through the remote console proxy service of vCloud Director cells. Because there is a central point of access, this alleviates the remote console access in service provider environments from a security perspective.

- Manage cloud resources based on vSphere and NSX; implement a logical abstraction layer by leveraging logical pooling of these resources; enable secure multitenancy by fully isolating virtual data center resources between multiple organizations or tenants

- vCloud Director database – Although the vCloud Director cells are stateless, the vCloud Director database is the central repository for storing the configuration data of a vCloud Director installation. The vCloud Director database must be deployed externally from the vCloud Director cells. Oracle and Microsoft SQL Server databases are supported for use with vCloud Director in accordance with the VMware Solution Interoperability Matrix.

- NFS transfer share – The NFS transfer share is a mandatory component of every vCloud Director installation. It provides temporary storage for concurrent OVF and ISO file transfers between resource groups. In Figure 5, it is depicted as a virtual appliance, but it can also be provided by an external NFS storage array.

- vCenter Server – vCenter Server as a cloud management component manages only the vSphere environment in which the cloud management components are hosted. This role is very similar to the vCenter Server role described in section 2.2.4 for the Cloud Foundation management domain.

- Load balancer – A load balancer is required to provide a single point of access in a multicell vCloud Director installation. vCloud Director cells have no extraordinary requirements regarding the load balancer product. If an NSX installation is available—directly within the management cluster, for example—an NSX Edge device can easily be configured as a load balancer for vCloud Director cells. Otherwise, a third-party load balancer can be used.

Resource Group Management Components
The management components of a vCloud Director resource group—one vCenter Server instance and one NSX Manager instance per resource group—are very similar to those already described for the management components of Cloud Foundation VI workload domains.
3.2.3 Resource Abstraction Layers

Figure 6 provides an example structure of the resource abstraction layers of vCloud Director.

- The base layers compose a resource group consisting of a vCenter Server and NSX Manager pair along with managed ESXi hosts.

**NOTE:** Although only one resource group is shown in Figure 6, a vCloud Director instance can manage up to 20 resource groups or vCenter Server instances. However, a resource group always marks a distinct border for the elasticity of a provider virtual data center.
• The resource group presents resource pools—typically vSphere clusters—to the vCloud Director installation.

• Within a vCloud Director installation, one or more provider virtual data centers are configured. As part of the configuration, each provider virtual data center can be assigned one or more resource pools or vSphere clusters.

• Within the next resource layer, an organization is configured for tenant access. In vCloud Director architectural discussions, the terms “tenant” and “organization” are used interchangeably. The vCloud Director UI, however, is not familiar with the term “tenant” and solely uses “organization.”

• Within an organization, one or more organization virtual data centers are configured. Each one carves out resources from exactly one provider virtual data center. Multiple organization virtual data centers can carve out resources from a single provider virtual data center. But in contrast, a single organization virtual data center cannot carve out resources from multiple provider virtual data centers.

• Organization users access the resources of organization virtual data centers and can use catalog items to deploy vApps in these data centers.

4. vCloud Director with Cloud Foundation

4.1 Terminology Mapping

To design a vCloud Director environment on top of a Cloud Foundation installation, it is helpful to understand the design terminology regarding Cloud Foundation and vCloud Director. There are only a few mappings necessary between vCloud Director and Cloud Foundation constructs because there are only a few overlapping abstraction layers between the two products. These mappings are described in the following subsections.

4.1.1 vCloud Director Management Cluster and Cloud Foundation Management Domain

The vCloud Director management cluster and the Cloud Foundation management domain share the purpose of hosting the following management components:

• Product-related system components and VMs—for example, Cloud Foundation management components and vCloud Director cell servers

• vCenter Server management components

• vCenter Server or NSX Manager instances of managed resources

**NOTE:** Managed resources include “resource groups” in the case of vCloud Director and “VI workload domains” in the case of Cloud Foundation.

• Optional enhanced management components such as a syslog server (vRealize Log Insight) or a system management server (vRealize Operations)
This mapping leads to the first design principle:

**Design principle 1: Place vCloud Director management components within the Cloud Foundation management domain or in a separate management cluster.**

1. Place vCloud Director management components within the Cloud Foundation management domain.

**Pros**

- Easy and straightforward – The Cloud Foundation management domain already exists in a Cloud Foundation installation.
- Minimal planning required – The management cluster already exists as a mandatory component of Cloud Foundation.

**Cons**

- Limited architectural flexibility regarding Platform Services Controller high availability – Cloud Foundation currently does not offer a load balancer option for this. If a vCloud Director instance integrates into a vCenter Single Sign-On or Platform Services Controller instance, a dedicated registration to one of the two Cloud Foundation Platform Services Controller instances is required with no automated failover.

2. Separate vCloud Director management components from the Cloud Foundation management domain. Certain requirements or constraints in an environment might lead to the decision to separate the vCloud Director management components from the Cloud Foundation management domain.

**Pros**

- Architectural flexibility – vCloud Director can be registered with a Platform Services Controller instance, which is configured for high availability with a load balancer. On a higher level of the architecture design, the option is available to protect the vCloud Director management components by a stretched cluster—that is, vSphere Metro Storage Cluster or vSAN stretched cluster—which is a feature currently not supported by Cloud Foundation. The registration of vCloud Director with a Platform Services Controller instance enables authentication of vCloud Director system users against an existing vSphere domain. Because a vCloud Director system must access a VMware vSphere Web Client instance to delegate authentication, at least one vCenter Server instance must be registered with the same Platform Services Controller instance.
- Existing management cluster – A management cluster already exists in a customer’s environment and will be used for the vCloud Director installation.
- Clear role distinction of Cloud Foundation – In this model, Cloud Foundation is a pure “resource provider” for the vCloud Director installation, along with other potential resource providers that serve different purposes and different SLAs.
Cons

- More planning required - Greater effort must be made, especially when the externally placed vCloud Director management components must traverse several security zones before reaching the Cloud Foundation components to communicate with—that is, vCenter Server, NSX Manager, and so on.
- Added resource consumption - Placing vCloud Director components apart from a vCloud Director system leads to additional resource consumption, which reduces ROI.

4.1.2 vCloud Director Resource Group and Cloud Foundation VI Workload Domain

The vCloud Director resource group and the Cloud Foundation VI workload domain have the common characteristic that both constructs describe a group of vSphere compute and storage resources as well as NSX networking resources managed by a single vCenter Server and NSX Manager pair. The key differences are that a "generic" vCloud Director resource group is more flexible regarding resource provisioning in terms of provider virtual data center configuration. A "generic" vCloud Director resource group can consist of many vSphere clusters managed by a single vCenter Server instance. Therefore, many vSphere clusters are assigned to one or multiple provider virtual data centers. The Cloud Foundation VI workload domain, however, is currently constrained by having a single vSphere cluster beneath a vCenter Server instance.

This terminology mapping leads to the second design principle:

**Design principle 2: Use a Cloud Foundation VI workload domain as a resource group within the vCloud Director installation.**

This design principle must be followed when implementing vCloud Director with Cloud Foundation. There are two possible alternative approaches for following this design principle:

1. **All vCloud Director resource groups are represented by Cloud Foundation VI workload domains.** This design principle, when chosen in conjunction with design principle 1a—that is, having vCloud Director management components within a Cloud Foundation management domain—is straightforward and leads to a fully self-contained, PoD-like configuration in which nearly all software components are hosted within Cloud Foundation.
2. **Only a subset of vCloud Director resource groups are represented by Cloud Foundation VI workload domains.** This design principle, although not as easy and straightforward as the previous one, offers the highest architectural and service flexibility:
Different types of resource groups serving different SLAs can be configured within one vCloud Director installation. For example, Cloud Foundation VI workload domains as a resource group type serving an SLA that is tied to a single availability zone can be combined with a vSphere Metro Storage Cluster resource group, for example, that is stretched across two availability zones and therefore serves a higher SLA. With this approach, it is recommended or mandatory that the vCloud Director management cluster be separate from the Cloud Foundation management domain—see design principle 1b—in a disaster-tolerant configuration.

4.2 Example Architectures: vCloud Director with Cloud Foundation

4.2.1 vCloud Director Deployment Models in the vCloud Architecture Toolkit

The VMware vCloud Architecture Toolkit™ describes many generic design approaches for a vCloud Director environment. The following example architectures for deploying vCloud Director with Cloud Foundation are based on a subset of vCloud Director deployment models described in the toolkit.

4.2.2 Single Availability Zone – Self-Contained Deployment Model

This deployment model is based on the following design principles:

• All vCloud Director and Cloud Foundation management components are hosted within the Cloud Foundation management domain.
• All vCloud Director resource groups are mapped to VI workload domains within the same single Cloud Foundation instance.

Following these design principles produces a fully self-contained vCloud Director environment in which all components—that is, management stack and resource groups—are hosted within a single Cloud Foundation installation. This approach enables easy configuration and operational procedures. As a downside, all components are hosted within a single availability zone. The loss of this availability zone implicates a loss of service for the vCloud Director and Cloud Foundation pair as well.
Figure 7 provides an overview of this deployment model.

![Diagram](image-url)

**Figure 7. vCloud Director with Cloud Foundation – Self-Contained Deployment Model**
4.2.3 Multiple Availability Zones – Mixed Deployment Model

Figure 8 shows an example of a mixed deployment model with resource groups other than Cloud Foundation vSphere environments as well as vSphere environments hosted by Cloud Foundation.

Pros

• Disaster recovery – vSphere Metro Storage Cluster offers disaster recovery for the vCloud Director management platform and for resource groups other than Cloud Foundation ones. This clustering is only one option to protect the vCloud Director management components, as well as workloads hosted within resource groups, against a disaster or failure of an availability zone. Other approaches—for example, protecting workloads with VMware Site Recovery Manager™ in conjunction with compliant storage replication technologies—are also possible options for a disaster-tolerant configuration.

• Storage options – Other storage services, along with SLAs other than vSAN, can be offered in this model if necessary.

• Separation – A clear and strict separation of the vCloud Director management layer and Cloud Foundation resource consumption units is achieved. This is especially beneficial if vCloud Director resource groups must be managed in data centers separate from the vCloud Director management layer.
Cons

• More complicated – For greenfield scenarios, the overall architecture is more complicated than in the deployment model described in section 4.2.1.

• Separate management platform – A separate vCloud Director management platform is established because the existing Cloud Foundation management domain is not used by vCloud Director components.

• Increased planning – More-extensive planning efforts might be necessary, especially in greenfield scenarios—for example, for planning the communication relationships and potential firewall rules between Cloud Foundation environments and those other than Cloud Foundation ones or for designing and implementing different vSphere environments.

4.3 Networking Options

4.3.1 General Considerations

VMware NSX for vSphere is the core component within a vCloud Director implementation for providing automated software-defined networking services. In accordance with the VMware Product Interoperability Matrix, a version of NSX compatible with a corresponding vCloud Director version must be used.

As previously described, a separate NSX Manager and vCenter Server pair is deployed with a VI workload domain within Cloud Foundation. When the vCloud Director instance registers the vCenter Server installation of a VI workload domain as a resource group, it also actively registers and uses the NSX Manager instance as an API endpoint for providing software-defined networking services within this resource group.

The NSX instances that automatically spin off with every VI workload domain deployment are full-featured NSX installations with no limitations or special rules imposed by Cloud Foundation. Therefore, these instances can be consumed by the vCloud Director instance without special limitations.

The only rules to be evaluated when designing a vCloud Director solution with Cloud Foundation are those related to the network constructs that are introduced by Cloud Foundation. These constructs are briefly described in the following section.

The vCloud Architecture Toolkit also describes design best practices regarding external network connectivity for certain vCloud Director deployment models. When designing vCloud Director environments with Cloud Foundation, it is essential to understand the following external network connectivity options offered by Cloud Foundation.
4.3.2 Physical Networking in Cloud Foundation

Figure 9 shows the physical networking architecture of a multirack Cloud Foundation installation.

The following design principles are implemented:

- Each physical rack consists of two ToR switches.
- Each of the two ToR switches per rack connects upstream with two 40Gbps network interfaces to the two rack interconnect switches. One port of the ToR switch connects to interconnect switch 1; another ToR switch port connects to interconnect switch 2.
- Each node—that is, ESXi host—has two 10Gbps network interfaces that connect to the two ToR switches using LACP.
- The pair of ToR switches along with the pair of rack interconnect switches form a large layer 2 domain using double-sided virtual port channels (VPCs).
- The two ToR switches of the first rack implement a connection to the upstream corporate network or Internet via two upstream routers or switches. Each first-rack ToR switch connects with two uplinks to the two upstream routers or switches—one link per upstream router or switch. The links to the upstream routers or switches can be either 10Gbps or 40Gbps and can be extended to up to four uplinks per ToR switch.

4.3.3 External Network Connectivity of a Workload Domain

Figure 10 shows the external network connectivity of a workload domain in a multirack view.

Each workload domain directly hosts the NSX Controller cluster, which is deployed automatically upon workload domain creation. The vCenter Server and NSX Manager pair managing the corresponding workload domain is not hosted within the workload domain itself, but rather in a Cloud Foundation management domain.

Network connectivity from a workload domain is realized in two basic ways:

a) Via a direct connection to a VLAN-based vSphere Distributed Switch port group

b) Via deployment of an NSX Edge device that provides routing capabilities between workload domain internal virtual wires to external VLAN-based port groups. In a vCloud Director environment, these devices are deployed and configured by the vCloud Director instance’s accessing the NSX API.

In Figure 10, there are two external networks, VLAN 110 and VLAN 120. These types of external networks are deployed by an SDDC Manager instance. Cloud Foundation supports VLANs in the range of 21–3199. The connections of these VLANs to networks outside of the Cloud Foundation instance are physically routed via the ToR switches of the first rack, as has been discussed, and are logically realized via various layer 2 and layer 3 connection options described in the following subsections.
4.3.4 Example Logical Network Design in vCloud Director and Integration with Cloud Foundation

Figure 11 depicts an example logical network design in vCloud Director as well as its integration into the networking constructs of Cloud Foundation.

The logical network design example depicted in Figure 11 has the following characteristics:

- The NSX Controller cluster is hosted in a Cloud Foundation VI workload domain and is automatically created there as part of a VI workload domain deployment workflow.
- Upon workload domain creation, an SDDC Manager instance automatically deploys and configures a distributed port group with VLAN 120, along with configuration of physical switches for Cloud Foundation external network connectivity. SDDC Manager can deploy additional VLANs anytime as well. Although deployed by SDDC Manager, the port group \textit{dvPG-External} must be registered within vCloud Director as an external network of one or more provider virtual data centers in order to be consumed by vCloud Director workflows.
- The NSX Edge device is situated at the border between the external VLAN 120 and the internal VXLAN-based virtual wires. Both the NSX Edge device and the VXLAN-based virtual wires belong to an organization virtual data center and are therefore completely managed within vCloud Director. For provisioning these NSX entities, vCloud Director leverages the NSX installation automatically deployed by Cloud Foundation and SDDC Manager upon VI workload domain creation.
4.3.5 External Network Connectivity Options with Cloud Foundation

Network design is an essential topic when creating a vCloud Director environment. As already outlined in section 4.3.2, Cloud Foundation offers special prescribed physical connection options for external network connectivity from a Cloud Foundation installation to the data center network. Based on these physical options, several logical connection options can be implemented. Not all of them are discussed in this paper, but examples of the most common ones are provided.

4.3.5.1. Layer 2 Connections

A layer 2–based connection is the most common way to interconnect a Cloud Foundation installation with the data center network. Figure 12 shows an example of such a configuration with Cloud Foundation.

![Figure 12. Double-Sided Virtual Port Channel with Cloud Foundation](image)

The configuration depicted in Figure 12 has the following characteristics:

- The green switches are the ToR switches of the Cloud Foundation installation located in the first rack. They are interconnected with two Cloud Foundation external upstream switches in the data center.
- The two ToR switches of the Cloud Foundation instance are configured as VPC peers and form a VPC domain.
- The two Cloud Foundation external upstream switches also form a VPC domain, but with a different VPC domain ID.
- Both the Cloud Foundation VPC peers and the upstream switch VPC peers are configured with a VPC consisting of eight links.
With this configuration, the ToR switches of the Cloud Foundation installation along with the Cloud Foundation external upstream switches form a large, highly resilient, and highly performant layer 2 domain.

4.3.5.2. General Layer 3 Connection Options
There are two basic options for connecting a Cloud Foundation installation to an external data center network other than Cloud Foundation via layer 3:

a) Cloud Foundation ToR switches as a layer 3 routing boundary
b) Cloud Foundation external upstream routers as a layer 3 routing boundary

Figure 13 depicts the first of these options.

![Layer 3 Networking with ToR Boundary](image)

This configuration has the following characteristics:

- The Cloud Foundation ToR switches are connected using equal cost multipathing (ECMP) toward the upstream routers.
- The NSX Edge device connects to the VRRP routing instance of the Cloud Foundation ToR switches via static routing.
- The NSX Edge device is only one option to connect from a Cloud Foundation workload domain to the ToR routing boundary. An overview of uplink connection options from a workload domain is presented in section 4.3.5.3.
Figure 14 depicts the second option, the implementation of Cloud Foundation external upstream routers as a routing boundary.

This configuration has the following characteristics:

- The Cloud Foundation ToR switches are connected via non-VPC links to the upstream routers via a transit VLAN.
- An NSX Edge device can peer with the upstream routers using a dynamic routing protocol such as eBGP. This is possible only when not terminating the route-peering relationship for the NSX Edge device on a VPC peer.
- Another option, not depicted, is to configure the links between Cloud Foundation ToR switches and upstream routers as double-sided VPC links. In this case, however, the NSX Edge device cannot peer with the upstream routers using a dynamic routing protocol; rather, it must use static routing.
Figure 15 shows a special variant of the second option.

In this variant, NSX Edge devices are used in ECMP mode, which is useful for certain scenarios in order to gain more bandwidth and availability for north-south traffic. A full discussion of these scenarios is beyond the scope of this document.
4.3.5.3. Workload Domain Uplink Options

Figure 16 summarizes these external networking connectivity options for a Cloud Foundation installation from a different angle, showing how the uplink options appear from the perspective of a workload domain.

The options shown in Figure 16 adhere to the following principles:

- Physical network connectivity for a VM in a workload domain to a Cloud Foundation external network environment can be implemented either via direct layer 2 links or via the Cloud Foundation ToR switches acting as a redundant pair of routers.
- With either physical option, an additional logical separation can be achieved by placing NSX Edge devices and NSX distributed logical routers into the network communication chain.

4.3.6 Summary

Cloud Foundation internal networking is deployed automatically by Cloud Foundation deployment workflows. It therefore offers a great simplicity at this layer. However, Cloud Foundation external networking options are mostly implemented manually as has been described. They therefore offer a high degree of flexibility when integrating a Cloud Foundation configuration into an existing data center. Due to this flexibility and to the highly network vendor-specific ways of implementing network technologies such as VPCs, the options described for external network connectivity are not meant as a complete list of all available and possible options. They should rather be considered as examples.
4.4 Storage Options

vSAN is the storage layer natively embedded in Cloud Foundation. Because vSAN is inherently built into the vSphere hypervisor, it is the natural choice as a storage layer for hyper-converged infrastructure (HCI) platforms based on vSphere.

vCloud Director can consume vSAN storage service offerings and integrates with the Storage Policy-Based Management (SPBM) implementation of vSAN. In this context, Cloud Foundation does not introduce any special rules for consuming vSAN storage.

Certain aspects must be considered that are not recommended to be realized with vSAN—for example, regarding public catalog offerings within vCloud Director. But these are limitations specific to vSAN that are not tied to Cloud Foundation. Even when relying on vSAN as a primary storage option within vCloud Director, there are alternative, NFS-based solutions that can be additionally deployed.

A detailed discussion on how to develop a storage strategy for vCloud Director with vSAN is presented in the VMware technical paper *Developing a Hyper-Converged Storage Strategy for VMware vCloud Director with VMware vSAN*.

5. Conclusion

Tests internally conducted at VMware have clearly demonstrated the technical feasibility of implementing a pairing of VMware vCloud Director with VMware Cloud Foundation. This technical paper describes architectural options and provides guidance on how to design such an environment.

With its unique capabilities to provide automated Software-Defined Data Center (SDDC) hardware and software, stack bring-up services, and automated lifecycle management, Cloud Foundation is an excellent choice for service providers who are using vCloud Director and want a way to quickly and efficiently spin up SDDC resources ready for consumption with vCloud Director. Cloud Foundation deploys these resources with a self-contained architecture that is verified and validated by VMware.

Customers and service providers can avoid going through iterative, time-consuming design and architecture cycles to implement an SDDC stack consisting of VMware vSphere, VMware vSAN, and VMware NSX. Cloud Foundation “consumption-ready” units of SDDC deploy resources in an automated, repeatable, and quality-assured manner.

Service providers can face the requirement of hosting VMware vCloud managed resources onsite at their customers’ data centers for data security and compliance reasons. Cloud Foundation enables them to achieve efficient integration into these data centers because it is a fully self-contained configuration that provides clear and easy interfaces with an existing data center, greatly simplifying deployment and reducing overall complexity.
6. Appendix

6.1 References
VMware vCloud Architecture Toolkit for Service Providers Documentation Center
VMware vCloud Director Product Page
VMware Cloud Foundation Product Page
VMware Cloud Foundation Blog Page
VMware Cloud Foundation Quick Reference Page

6.2 Software Versions
This paper relies on an evaluation’s being conducted with the following software versions, which are the current versions of the corresponding products as of the time of writing this document:

- VMware Cloud Foundation 2.1.x and the corresponding versions for VMware vSphere, VMware NSX, and VMware vSAN. See VMware-Cloud Foundation Release Notes 2.1.3.
- VMware vCloud Director 8.20

When planning a vCloud Director environment with Cloud Foundation or an upgrade of such an environment, ensure that the resulting software bill of materials complies with the VMware Product Interoperability Matrix. Concerning the versions of vSphere, NSX, and vSAN, the Cloud Foundation architecture ensures interoperability of these product versions shipped within a particular Cloud Foundation release. vCloud Director, however, is an external component from the perspective of Cloud Foundation. Interoperability between particular versions of vCloud Director and those of vSphere, NSX, and vSAN within a Cloud Foundation release must be verified when planning an installation or upgrade of such an environment.

Design rules and configuration limits presented in this document are applicable for the software versions mentioned. Regarding upcoming Cloud Foundation releases, these design rules and configuration limits might be subject to change, and additional options might become available.