Table of Contents

Purpose and Overview ................................................................. 3
  1.1 Background ............................................................... 3
  1.2 Target Audience ......................................................... 3

Design of the Outsourced Data Center ..................................... 3
  2.1 Deploy vCloud Networks ................................................. 4
      2.1.1 Configure Firewall and NAT Rules ................... 5
  2.2 Connect Networks to On-Premises Data Center ................. 6
  2.3 Deploy Directory and DNS Services ............................ 7
  2.4 Migrate Templates and Virtual Machines ..................... 8

Conclusion .............................................................................. 9

About the Author ..................................................................... 9
Purpose and Overview

VMware vCloud® Air™ has been developed with a vast number of use cases in mind. The purpose of this paper is to provide an example of the enterprise IT/outsourced data center in the form of a case study. This use case forms the foundation for subsequent solution briefs. By understanding this foundational building block, users will be better prepared to fully grasp the concepts described in other solution briefs.

This study focuses primarily on the need for organizations to leverage public cloud resources for enterprise IT use. When enterprise IT has access to public cloud resources, it can react to business requests more rapidly while still maintaining the level of control that today’s enterprises demand.

The focus of this case study is on describing the basic foundation of the outsourced data center as it relates to modern enterprise IT operations.

1.1 Background

Enterprise IT customers are approaching a crossroads where on-premises capacity is becoming limited. In addition, the speed of the business is in many cases outpacing the speed at which IT can deliver the necessary infrastructure. Previously, IT teams have been required to design, procure, install, configure and manage an increasing number of discrete infrastructures to satisfy the business’s needs. This process takes time to complete and can slow down the progress of business itself. Even the seemingly simple task of adding capacity to existing VMware vSphere® infrastructure often must go through a long internal vetting and approval process.

vCloud Air provides IT organizations with quick and easy access to compute, memory and storage resources by adding capacity derived from VMware vCloud Suite® to their on-premises data center. By having infrastructure as a service (IaaS) based on VMware technology readily available, IT organizations can quickly deploy new workloads and migrate existing ones to vCloud Air without having to modify components at the application layer. However, to make a functional outsourced data center and hybrid cloud, the following key considerations must be addressed before this process of deployment and migration of new and existing workloads begins:

• Establishing and configuring cloud networks
• Connecting on-premises vSphere to vCloud Air
• Deploying supporting infrastructure
• Migrating templates and media

After these four basic issues have been properly addressed, users can view their outsourced data center as ready to accept workloads. This document aims to improve users’ understanding of these considerations so they are fully prepared to embrace the cloud at their own pace in this new era of IT as a service.

1.2 Target Audience

This document is intended for vSphere architects as well as administrators. Although this will not be an in-depth, step-by-step walk-through on how to configure the concepts discussed, both groups will gain a better understanding of how various aspects of an outsourced data center might work and can therefore adapt these concepts to their own environments. Because the requirements of each subscriber can greatly differ, we will not address the following specific topics in detail in this case study:

• Compliance
• Licensing
• Third-party tools

Design of the Outsourced Data Center

Understanding how to design an outsourced data center is relatively simple. In most cases, it should be viewed and treated like any other data center the IT department controls. Instead of a physical, brick-and-mortar computing environment, this design, with respect to what is exposed to the end users and administrators, is different because it is entirely software defined. By providing subscription-based access to vCloud Air, VMware has eliminated the need to build, manage and update the actual infrastructure. Users can design and configure the core services
they need, and then start deploying workloads immediately. This enables IT organizations to focus on meeting business needs instead of on managing the underlying infrastructure itself. It is assumed that users already have decided to subscribe to one or both of the following two currently available “compute” options:

- VMware vCloud Air Virtual Private Cloud
- VMware vCloud Air Dedicated Cloud

2.1 Deploy vCloud Networks

With both compute service options, every customer is given access to a VMware vCloud Networking and Security Edge™ gateway. In the case of vCloud Air Dedicated Cloud, users can choose to deploy additional vCloud Networking and Security Edge gateways. Each deployed gateway delivers as many as nine interfaces that can be used to define vCloud Air networks. All of these networks share the following attributes that can and should be unique to each network. Not all of them must be configured according to the use case presented, but they are all made available as part of each offering.

- **NAT and firewall** – Both of these are enabled by default, with no firewall rules defined and all traffic denied as the default rule.
- **A vCloud Networking and Security Edge gateway IP address** – This is the address that will be assigned to the vCloud Networking and Security Edge gateway interface where the network is routed.
- **Domain Name System (DNS) server configuration** – vCloud Networking and Security Edge gateway can provide DNS, but an alternate server can be specified.
- **Static IP pool range** – This is a pool of NAT IP addresses that will be consumed when deploying virtual machines.
- **DHCP**
- **Load balancing**
- **IPsec virtual private network (VPN)**

*NOTE:* vCloud Networking and Security Edge gateways support 10 interfaces, but one interface is used for “external” access when a public IP is assigned to it. Subscribers are given public IP addresses as part of the subscription service with both offerings, and additional IP addresses can be added at any time through the service interface.

Figure 1 is a logical diagram showing various networks as well as example IP addresses.

![Figure 1: Figure 1. Various Networks and IP Addresses](image)
2.1.1 Configure Firewall and NAT Rules

After the basic network segments have been decided on, it is important to create some firewall rules. Previously, it was noted that by default there are no rules configured. As mentioned, subscribers are also given a number of public IP addresses they can use with both offerings. That number, by default, depends on the service type but can be expanded at any time. The following are examples of rules that might be necessary to create, using the networks shown in the diagram as reference:

<table>
<thead>
<tr>
<th>RULE</th>
<th>SOURCE</th>
<th>DESTINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow All Outbound</td>
<td>Internal:Any</td>
<td>External:Any</td>
</tr>
<tr>
<td>Allow Private to Desktop</td>
<td>192.168.50.0/24:Any</td>
<td>192.168.51.0/24:Any</td>
</tr>
<tr>
<td>Allow Desktop to Private</td>
<td>192.168.51.0/24:Any</td>
<td>192.168.50.0/24:Any</td>
</tr>
</tbody>
</table>

**NOTE:** All virtual machines on a vCloud Networking and Security Edge gateway segment use the vCloud Networking and Security Edge gateway as their default gateway. The preceding rules enable all segments to get direct Internet access but also enable the “private” segment to communicate to the “desktop” network. The “DMZ” is denied access to both.

For machines to get direct access to the Internet, one or more source NAT (SNAT) rules also must be defined.

<table>
<thead>
<tr>
<th>TYPE</th>
<th>ORIGINAL IP</th>
<th>ORIGINAL PORT</th>
<th>TRANSLATED IP</th>
<th>TRANSLATED PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNAT</td>
<td>192.168.50.0/24</td>
<td>Any</td>
<td>74.204.180.41</td>
<td>Any</td>
</tr>
<tr>
<td>SNAT</td>
<td>192.168.51.0/24</td>
<td>Any</td>
<td>74.204.180.41</td>
<td>Any</td>
</tr>
<tr>
<td>SNAT</td>
<td>192.168.52.0/24</td>
<td>Any</td>
<td>74.204.180.41</td>
<td>Any</td>
</tr>
</tbody>
</table>

---

Figure 2: Source NAT Rules Defined
2.2 Connect Networks to On-Premises Data Center

The new vCloud Air networks described can access the Internet. In the case of two networks, desktop and private, they can also now communicate with each other through the vCloud Networking and Security Edge gateway via the previously defined firewall rules. This is useful, but they as of yet have no connection back to the on-premises data center. To bridge these networks, we provide the following three options to connect vCloud Air to the on-premises data center:

- IPsec VPN
- Direct connect
- Data center extension/stretch deploy

**NOTE:** Although an MPLS-based direct connection has been announced, this connectivity option will be discussed in a follow-up document. In addition, data center extension is currently available and will be discussed in another document.

For the purposes of this case study, we will focus on IPsec VPN. vCloud Air Edge gateways can work with any number of IPsec-compliant devices on premises. Figure 3 is an example of a configured IPsec VPN in vCloud Air. (Refer [here](#) for more information about configuring IPsec VPN.)

![Configured IPsec VPN in vCloud Air](image-url)
After configuration, the IPsec tunnel will be established. However, firewall rules must still be defined to allow traffic to pass. As mentioned previously, by default there are no rules defined. For this use case, the private network in vCloud Air must allow traffic to the corporate network on premises and vice versa. Therefore, the rules in the vCloud Networking and Security Edge gateway might resemble the following:

<table>
<thead>
<tr>
<th>RULE</th>
<th>SOURCE</th>
<th>DESTINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Private to OnPrem</td>
<td>192.168.50.0/24:Any</td>
<td>192.168.110.0/24:Any</td>
</tr>
<tr>
<td>Allow onPrem to Private</td>
<td>192.168.110.0/24:Any</td>
<td>192.168.50.0/24:Any</td>
</tr>
</tbody>
</table>

At this point, traffic can flow successfully between the networks. This configuration provides the most basic connectivity through the IPsec VPN tunnel between the two networks without any port restrictions.

**NOTE:** If browser or Web traffic is required to route through an on-premises proxy, a “local” Web browser can be configured to do so. Direct Internet routing also can be forced back through on-premises gateways by defining the next hop via a static route in the vCloud Air vCloud Networking and Security Edge gateway and removing the appropriate firewall and SNAT rules. The advanced networking capabilities of the vCloud Networking and Security Edge gateway are flexible enough to create the chosen solution, based on a wide variety of requirements. In some cases, experimentation with the various options and capabilities might be necessary.

2.3 Deploy Directory and DNS Services

At this point, we have a functional virtual data center inside vCloud Air that is connected to an on-premises data center. Firewall rules and a VPN connection have been created and configured, but a potential missing component is a Microsoft Active Directory or other directory service, as well as some basic infrastructure services such as DNS. For this case study, it is assumed that deployed workloads will be net new and Microsoft Windows based; therefore, this environment should be treated as a new Active Directory “site.” A Windows template from the global catalog can be chosen and configured to meet the required specifications for a domain controller, or a custom template can be uploaded and deployed.
At a minimum, the following operations should be completed or taken into consideration:

- Deploy redundant virtual domain controllers.
  - Join an existing corporate, secondary, or tertiary domain.
- Configure a new Active Directory “site.”
  - Add vCloud networks to Active Directory “Sites and Services” and assign to the new “site.”
- Edit vCloud network settings to use the new domain controllers for DNS instead of the vCloud Networking and Security Edge gateway.

Previously when the vCloud networks were configured, the DNS was set to use the vCloud Networking and Security Edge gateway itself. Now that Active Directory and DNS are deployed in the cloud, changing this to represent the local servers, as shown in Figure 5, is advised. This will enable new virtual machines deployed in the cloud to reflect the updated settings without the need to reconfigure this for each new virtual machine upon deployment.

If DHCP is configured on the vCloud Networking and Security Edge gateway for any network segment, changing this option on each vCloud network applies to all DHCP requests handled by this edge gateway.

### 2.4 Migrate Templates and Virtual Machines

At this point, a decision can be made to identify the templates that can be migrated from the on-premises vSphere environment to the vCloud Air private catalog. Leveraging VMware vCloud Connector® makes the manual migration process easy, but it might be worthwhile to leverage the catalog sync feature to automate the synchronization and migration of templates between this catalog, other VMware infrastructure-based clouds and the on-premises data center.

vCloud Connector also can easily migrate existing virtual machines to vCloud Air with minimal changes, if any, to the guest operating system. If it is required to maintain the existing IP and MAC addresses of a virtual machine, the data center extension feature can be employed for this purpose. In most cases, however, an application can survive an IP and MAC address change.
VMware vCloud Connector documentation can be referred to for more information on specific features and setup instructions for the vCloud Connector server and nodes. vCloud Air provides a node that is preconfigured, eliminating the need to manually deploy and configure one in this environment. To securely communicate with the nodes in each cloud, the vCloud Connector server must be deployed on premises with access to the Internet.

**NOTE:** Although it is not discussed here, each individual organization must understand and comply with Windows server license portability. Due to the nature of Windows License Mobility conditions, the ability of organizations to bring their own licenses is currently available only in the vCloud Air Dedicated Cloud offering of vCloud Air.

**Conclusion**

Providing the basic networking and infrastructure services that a physical data center typically requires is the foundation of building an outsourced data center. The remarkable difference between configuring these software-defined infrastructure and services versus the traditional model is that it can be done in hours with VMware vCloud Air rather than in months or days using conventional means. Further, new levels of business and IT agility can be achieved due to the decoupling of the infrastructure layer from the application. After these tasks have been completed, the pool of resources can be rapidly and reliably leveraged to deploy new and migrate existing workloads with ease.

**About the Author**

Chris Colotti is a Principle Technical Marketing Architect with the vCloud Air team. Chris has more than 10 years of experience in working with IT hardware and software solutions. He holds a bachelor of science degree in information systems from Daniel Webster College. Prior to coming to VMware, he served a Fortune 1000 company in southern New Hampshire as a systems architect and administrator, designing VMware solutions to support new application deployments. At VMware, in the role of consulting architect, Chris has guided partners as well as customers in establishing a VMware practice and consulted on multiple customer projects ranging from data center migrations to long-term residency architecture support. Currently, Chris is working on the newest vCloud Air solutions and architectures for vSphere customers wanting to migrate to VMware vCloud Air. Chris is also a VMware Certified Design Expert, (VCDX #37).