Citrix Service Provider Reference Architecture

Using Citrix Technologies to Enable the Hosted Delivery of Microsoft Windows-based Applications and Desktops as a Service

June, 2012
Contents

Executive Summary........................................................................................................................................... 3

Introduction and Scope....................................................................................................................................... 3

Conceptual Overview.......................................................................................................................................... 5

Core Concepts..................................................................................................................................................... 6

Overview of Reference Architecture Modules ................................................................................................. 8

CSP Reference Architecture Implementation .................................................................................................. 11

Multi-Tenancy Design Considerations............................................................................................................. 12

Securing the Networks ....................................................................................................................................... 27

Active Directory and Organization Unit Considerations................................................................................ 30

Virtual Provisioning of application and desktop host workloads .................................................................. 33

Application Provisioning ................................................................................................................................... 38

Active Directory Integration, XenApp Worker Groups and Policies ................................................................. 47

XenDesktop Considerations ............................................................................................................................... 51

Simplified Hosted VDI with VDI-in-a-Box .......................................................................................................... 55

Secure Access and Acceleration ......................................................................................................................... 56

Dashboards and Management ............................................................................................................................ 59

Citrix App Orchestration .................................................................................................................................... 59

Citrix CloudPortal Services Manager .............................................................................................................. 64

Citrix EdgeSight .................................................................................................................................................. 80

Conclusion .......................................................................................................................................................... 81

Appendix A: Online Resources ......................................................................................................................... 82
Executive Summary

The Citrix® Service Provider Reference Architecture guides partners in designing a new generation of application, data and desktop cloud services. These cloud services enable CSPs tenants’ businesses to move capital and management expenses to an operational cost model, while also increasing work-style mobility for subscribers. These services leverage the Microsoft® Service Provider License Agreement (SPLA) and Citrix Service Provider (CSP) licensing programs to deliver Microsoft Windows® applications and desktops on a pay-as-you-go basis to multiple tenant businesses from a service provider’s hosted cloud. This reference architecture is for service providers that will manage a multi-tenant application and desktop cloud service rather than an outsourced “IT as a Service” or Infrastructure as a Service (IaaS) datacenter where each end tenant manages their own resources.

Introduction and Scope

This document provides architectural guidance for Citrix Service Providers that will provide application, data and desktop subscription services from the smallest subscriber base of a few tenants with small numbers of subscribers, to one that must scale into the millions of active application and desktop workloads across thousands of tenants.

The Citrix solution presents users with a familiar Windows desktop and applications experience, enabled by Citrix XenApp™ and XenDesktop™, and the Citrix Service Provider Automation Pack extensions to the Microsoft® Windows Server® 2008 R2 - Remote Desktop Services base operating system. Service Providers can deliver these services to users of any Citrix Receiver™ enabled endpoint device over secured public internet connections with Citrix NetScaler®. For subscriber locations that aggregate a number of end-points in a single setting such as a small retail business, accountant office or medical clinic, Citrix Branch Repeater™ provides a high-definition user experience to all end-points over an optimized network connection.
A sample multi-tenant environment using Citrix XenApp 6.5 Worker Groups and App Orchestration for various modes of multi-tenancy is referenced throughout this document. XenApp Worker Groups map to individual subscriber-specific Organization Units within a single Microsoft Active Directory Domain, or alternatively to individual subscriber specific child domains within a single Microsoft Active Directory Forest. All subscriber partitions and services are managed through centralized dashboards and monitoring systems as provided by Citrix, Microsoft and 3rd parties. This document does not provide detailed guidance for CSPs requiring multi-tenant designs where a single farm is dedicated to each subscriber, although many of the concepts within this document apply to such designs.

This is the third revision in the evolution of the CSP Reference Architecture and with this revision we are introducing guidance on several major new capabilities for CSPs.

- App Orchestration enhancements for Multi-Farm management from a single console
- Enhanced Provisioning capabilities within CloudPortal Services Manager
- Next Generation Seamless Applications
- Clarification on VDI capabilities compliant with Citrix and Microsoft licensing programs

The sample design follows security best practices. A CSP must determine any deviations from these suggestions based on particular business needs. High Availability capabilities are inherent within many components of the architecture, whereas Disaster Recovery designs are enabled most effectively by Citrix NetScaler and Citrix XenServer. Further details of additional HA and DR options are in the product documentation for the respective components at http://www.citrix.com/edocs.
The Citrix® Service Provider Reference Architecture presents tenants and end subscribers with a cost effective, pay per month subscription to application, data and desktop services provided by a 3rd party Citrix Service Provider (CSP). This section provides an overview of the Conceptual Reference Architecture as well as the core technical concepts that enable this architecture.
Core Concepts

The core concepts of end-point ubiquity, subscription-based licensing, multi-tenancy, single instance management and dynamic assembly provide much of the simplified scalability and high user acceptance of this emerging service model.

End-point ubiquity

End-point ubiquity enables the widest adoption of desktop services capable of providing high performance graphics and peripheral IO capabilities for Windows desktops on any device over any network. In the CSP Reference Architecture, Citrix Receiver enables this ubiquity through support for virtually every popular device and platform in the market. Citrix Receiver enables a high-definition experience (HDX™) for users of cloud hosted application and desktop services, increasing user acceptance and helping to grow this emerging services market.

Subscription-based licensing

These services provide a pay per use, pay per month model which enables subscribers to treat desktop acquisition and maintenance as an operational expense for services rather than a capital expense of owning and building their own infrastructure. The savings recognized by the economies of scale that multi-tenancy, dynamic assembly and single instance management enable further enhance the business proposition of this licensing model by keeping month to month costs relatively low for both the subscriber and service provider.

Multi-tenancy

Multi-tenancy capabilities provide large economies of scale from a single infrastructure servicing multiple organizations. This provides different levels of trade-offs regarding price and performance in reference to an individual tenant’s service level requirements.

Single instance management

Single instance management provides the most efficient life-cycle maintenance of operating system workloads and Windows-based applications. By creating a single read-only image of each critical
workload, and then streaming that workload onto physical or virtual machines, CSPs can maintain thousands of execution environments from a single source, requiring only a reboot of the individual machine to deploy the latest image. Application virtualization provides a similar solution at the application layer where a single application image is maintained and patched and then streamed into a user’s execution environment at run-time. This single application image can be securely streamed to thousands of users, across multiple tenants.

Dynamic assembly

Dynamic assembly of the operating systems, applications, and user personalization settings on a per user, per tenant basis is a critical enabler of massive scale and efficient management for Windows-based desktops and applications within a multi-tenant service provider solution. This dynamic assembly leverages single instance managed images as components that are assembled for a user based upon the services subscribed to by the tenant. Single instance images are dynamically assembled in different configurations for each tenant/user based on their individual configurations and service level agreements.

Subscription licensing

Fundamental to the concept of applications, data and desktops as a cloud hosted service is the subscriber requirement that all IT services and products are purchased as an operational expense rather than the upfront capital expense of building or upgrading a datacenter. To facilitate these subscriber requirements many software vendors have begun to introduce subscription-based licensing programs made available through service providers to subscribers. The Citrix Service Provider (CSP) licensing program is the Citrix response to this emerging model.

- **Citrix CSP licensing**
  The Citrix Service Provider (CSP) program is designed specifically for service providers who provide hosted application, data and desktop cloud services to end-user customers. The CSP program addresses the service provider market for offsite, multi-tenant hosting where the end-user customer is not the licensee. The CSP program extends to service providers the “right to use” Citrix products as the underpinning of their delivery infrastructure and gives them the flexibility of a monthly “active subscriber” pricing and licensing model. Service providers always have access to the most current versions of Citrix products available in the program and only pay for actual end-user usage recorded during the previous calendar month.
Microsoft SPLA licensing
SPLA (Service Provider Licensing Agreement) is the Microsoft service provider program. SPLA enables service providers and ISVs with a hosted offering to license Microsoft products on a monthly basis to provide services and hosted applications to their end customers. SPLA is a well-known industry term that many service providers equate with the monthly pricing and licensing model used to charge for hosted software services. Citrix Service Provider program includes a similar CSP Program Agreement that defines service provider partner use rights.

Overview of Reference Architecture Modules

Infrastructure as a Service (IaaS)

The foundation of the service provider platform begins at the Infrastructure as a Service (IaaS) module, which has two sub-components:

1. Network infrastructure
2. Provisioning infrastructure

The IaaS module controls the system-wide network configuration, forest-level Active Directory management, remote access and all layers of provisioning.
Multi-Tenant Citrix Farms

The multi-tenant Citrix Farms module is the core component of the service provider datacenter(s)—this is what controls application and desktop delivery within the multi-tenant architecture. Within this module, applications and desktops are virtualized; subscriber partitions and Active Directory boundaries are defined, while centralized and shared XenApp and XenDesktop controllers govern the experience across tenants.

**Figure 1.4: Citrix Service Provider Reference Architecture – Conceptual View – Citrix Farms**

**Dashboards and management**

To successfully build and manage a service provider network, IT administrators need the correct set of management and troubleshooting tools. To do this efficiently, administrators need tools that are simple to use with a wide level of control. Citrix AppCenter, and CloudPortal Service Manager and other supporting management dashboards present a unified view across the entire infrastructure, from the datacenter to the device. This end-to-end view gives service providers the detailed information necessary to ensure that service level agreements for subscribers are maintained.
End-points and offices

When applications and desktops are delivered as a service, the user is the ultimate judge of the experience being delivered. Service providers must deliver a great, consistent experience across all networks to any device to capitalize on the largest subscriber base. How does a service provider do this when they do not manage the endpoint or the network? Citrix Receiver and HDX are the strategic components that make this a reality.

With Citrix Receiver, CSPs have complete control over security, performance and user experience with no need to own or manage the physical device or its location. Users simply install Citrix Receiver on their own device to gain access to their desktop and all of their business, web and SaaS applications.

With the introduction of Citrix’s next generation seamless app capabilities applications that must execute on the end-point device can now be presented within a user’s cloud hosted desktop. This capability now enables 100% application compatibility within the CSP solution while also providing a smooth transition for application migrations from a customer’s legacy end-points and datacenters into the CSP hosted datacenter over time.
The complete implementation of the reference architecture leverages multiple vLANs, security zones and a combination of physical and virtual server installations to enable a highly scalable, high performance and easily managed multi-tenant solution for service providers. This section describes the design, the various components and configurations used, and the best practices approach that can be employed to build a massively scalable solution. With the new use cases enabled by the inclusion of Citrix’s latest technologies like Hosted Server VDI and App Orchestration a Citrix Service Provider can potentially serve millions of active subscribers from a single system based on the concepts discussed within this reference architecture.
# Multi-Tenancy Design Considerations

Looking at the complete virtualization stack, one notices the several potential layers where multi-tenancy capabilities can be introduced within the environment. All of them have their advantages and disadvantages to an applications, desktops and data “as-a-Service” business. Note the following trade-offs of implementing multi-tenancy at a specific layer:

![Multi-tenant layers within the DaaS stack](image)

<table>
<thead>
<tr>
<th>Layer</th>
<th>Example</th>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical Network</td>
<td>Completely separate datacenters or networks</td>
<td>Greatest level of design flexibility and tenant isolation</td>
<td>Highest cost per tenant because all infrastructure is replicated per tenant</td>
</tr>
<tr>
<td>Virtual Network</td>
<td>Co-located datacenters using vLANs as the primary isolation layer</td>
<td>Very high level of design flexibility and tenant isolation</td>
<td>Only slightly less expensive than physical network isolation</td>
</tr>
<tr>
<td>Physical Server</td>
<td>Co-located datacenters renting dedicated physical servers to subscribers</td>
<td>Relatively high level of design flexibility</td>
<td>Network layer security can be compromised; still relatively high cost; intra-server communications can be cumbersome to design</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Dedicated Virtual Hosts; co-located</td>
<td>Relatively high level of design flexibility; lower</td>
<td>Network layer security can be compromised;</td>
</tr>
</tbody>
</table>
Citrix Service Providers leverage different multi-tenant approaches to deploy and manage a single instance of Citrix infrastructure (thus saving costs) while continuing to meet the individual tenant expectations. A CSP must take into account several considerations to determine the best approach for their business. This section discusses some of those considerations, as well as three example multi-tenant approaches used in the market today.

![Figure 2.3: DaaS Multi-Tenant parameters](image-url)
Although a specific CSP business model can consider more parameters, five primary considerations will influence most multi-tenant designs.

- **Isolation**: Isolating users of one tenant from users of other tenants to prevent leakage of sensitive information or from being affected by activities of other tenants.
- **Performance Guarantees**: Ensuring that performance of one tenant is not negatively affected by activities of other tenants.
- **Customized Experience**: Providing unique environmental, security or performance aspects to an individual tenant based on their specific service level agreement (SLA) within the multi-tenant environment.
- **Self-Service Administration**: Providing the ability for tenants to perform some level of administration for their specific services.
- **Cost**: Delivering the correct mix of the above capabilities at an appropriate cost.

The Citrix solution, based upon XenApp and XenDesktop, supports several options for multi-tenancy that provide different blends of isolation, performance management, customization, self-service and cost. CSPs can determine which of these options meet the needs of their customers and develop offerings and price-points accordingly.

The three most widely employed models of application and desktop multi-tenancy are shared (session layer isolation), partial isolation (machine layer isolation), or full isolation (farm or network layer isolation).
Session Isolation model

The shared (session layer isolation) model has one XenApp farm with infrastructure components and session hosts shared between tenants. Although not recommended from a best practice or security perspective, this is a common model in use for smaller providers today, particularly for those CSPs offering basic, standard desktop services where cost—not security—is the most significant business concern.

![Session Isolation Diagram]

Figure 2.4: Multi-tenancy: Session Isolation

The key characteristics of this model are shown in the sliding scale to the right:

- Users from multiple tenants can have sessions on a single XenApp session host. This requires appropriate lockdown of XenApp session hosts to minimize the possibility of a user of one tenant negatively affecting the users of another tenant. However, there is still a chance that a user could compromise a server (thus affecting users of another tenant).
- User performance guarantees established by using the XenApp CPU Utilization Management feature.
- A separate Web Interface site can provide custom branding for each tenant. In addition, Windows and Citrix policies in Active Directory can provide a highly customized experience to users, for example, wallpaper, theme, Citrix HDX settings and so on.
- This method of multi-tenancy is extremely cost effective because a CSP can spread all of the infrastructure costs across multiple tenants.
Server isolation model

The server isolation (machine layer isolation) model has one XenApp or XenDesktop farm with shared infrastructure components, but the session or desktop VM hosts are not shared. More and more CSPs are moving to this method. Although it does not provide the extreme security found in the network isolation model, this model provides arguably the most optimal blend of isolation, performance, customization, self-service admin and cost for most tenants—which translates into a very competitive price-point.

![Server Isolation Diagram](image)

Figure 2.5: Multi-tenancy: Server Isolation

The key characteristics of this model are shown in the sliding scale to the right:

- Each tenant has a dedicated pool of session host servers or dedicated desktop VMs ... XenApp Worker Groups and XenDesktop catalogs help easily create this deployment. As a best practice, administrators should still always lock down individual session hosts.
- Because users from one tenant can have sessions only on their designated XenApp servers, or dedicated XenDesktop VM a user cannot negatively impact the performance of another tenant’s users. Administrators can further guarantee performance to users by using additional capabilities within XenApp and XenDesktop.
- In addition to the customization capabilities mentioned in the shared deployment, each tenant can have custom machine images for XenApp session hosts.
- CSPs can allow tenants to perform some level of administration for their pool of session hosts or dedicated desktops, for example, helpdesk activity for viewing which users are logged onto which servers, shadowing a session or resetting a session.

Though each tenant has dedicated session hosts or desktops, the costs might not be much higher than that of the shared model. This deployment method offers a blend of multi-tenancy capabilities at a very reasonable cost.
Farm isolation model

In the Farm isolation model, one XenApp or XenDesktop farm, or VDI-in-a-Box Grid with dedicated infrastructure is deployed per tenant. None of the infrastructure components are shared and in most cases each farm will reside on a dedicated vLAN or physical network. This model is best suited for tenants with stringent confidentiality and security requirements, such as federal agencies, healthcare, and so on, or those with heavy-duty performance or customization needs. These capabilities come at a cost, but most CSPs typically charge a premium for this type of service. It is understandably less common to see deployments of this nature – but important to understand that the option exists. This option is recommended for those environments where the tightest possible security, regardless of cost, is the primary requirement.

![Figure 2.6: Multi-tenancy: Farm Isolation](image)

The key characteristics of this model are shown in the sliding scale to the right:

- Tenants are completely isolated, including dedicated brokering operations.
- Performance guarantees are similar to the partial isolation model.
- The customized experience aspects remain the same as that of the partial isolation model.
- Service providers have the option to allow the tenant to perform a much higher level of self-service administration for example, helpdesk activity, managing session hosts, managing applications, and so on.

The costs are higher for this model because the infrastructure components are not shared between tenants.
Creating the IaaS Layer

This section discusses the basic design considerations for the IaaS foundation that enables a secure and scalable solution. It begins at the lowest layer of the design and builds up from there, starting with the CSP datacenter network layout and ending with the virtual and application provisioning designs.

The layers addressed in this section are:

- Network boundaries, vLANs, and basic network services
- Active Directory and Organization Unit considerations
- Virtual Provisioning of DaaS workloads
- Application Provisioning

Note: We address the NetScaler, Branch Repeater, Access Gateway, and Web Interface designs in the Secure Access and Acceleration section after discussing subscriber partitions.
Network Boundaries and vLANs

**Network design**

The Citrix Reference Architecture for Multi-Tenant Desktop as a Service uses several secured zones to enable a flexible and scalable solution that provides for tight security at critical boundaries between the management layers and tenant partitions. These networks and zones are:

**DMZ - Demilitarized zone**

The DMZ is a network area isolated by firewalls on either side, providing a barrier between the public internet and the CSP datacenter operational environment. This network is the outside facing perimeter to the environment. The machines in this zone host the NetScaler and Access Gateway servers, the CloudPortal Services Manager Web.

**Multi-tenant network**

The multi-tenant network is behind the DMZ and further isolated from the CSP network by a standard firewall. The firewall at this layer ensures that management communications flow between the CSP and tenant networks in a manner that ensures the various levels of multi-tenant isolation and CSP delegated administration appropriate for each tenant. The multi-tenant network is further divided into separate vLANs:
When tenants require a separate network segment for their dedicated workloads and servers, it is recommended that you use per tenant vLANs. Service providers might choose to charge subscribers in these vLANs a slight premium for this level of security because of the slightly higher infrastructure and management costs to the CSP.

**Shared vLAN**

This vLAN presents a single network segment to XenApp worker servers within the farm for those tenants that do not require the sense of security that a separate vLAN can provide. At the service provider’s discretion, subscribers in this vLAN might recognize a slight advantage regarding cost of service because much of the infrastructure, including the network, is shared among tenants and service providers can pass these savings to the subscriber.

**CSP network**

The CSP network is the area hosting all of the CSP shared infrastructure for provisioning, authentication, back office services, management services and dashboards.

**Provisioning vLAN**

The provisioning vLAN provides a secure network for the single instance management images and infrastructure services that enable administrators to quickly provision XenApp and other tenant workloads from a shared read-only vDisk. This approach enables dynamic scaling of large-scale environments while using the minimal amount of backend storage.
and provides relatively simple life-cycle management as compared to most other methods.

**Authentication vLAN**
The authentication vLAN contains the Microsoft Active Directory Forest and Domains within a secured network. Only specific secured access to Active Directory capabilities are enabled in this vLAN for specific users, administrators and machines from the other networks.

**Management vLAN**
The management vLAN contains many of the foundational network services necessary in a hosted environment such as Domain Name Services, NTP and SNMP as well as other services provided by the CSP.

**Application vLAN**
This vLAN contains the back-office applications that enable web, mail, collaboration and line of business application backend services. Leverage these vLANs and services across tenants or dedicate them to a specific tenant, as determined by the CSP and subscriber service level agreements.
**Physical connections and additional networks**

Two additional networks are enabled specifically for performance reasons across the entire infrastructure: One network is dedicated to storage and the other to hypervisor management, in this example Citrix XenServer®.

**Storage** – The storage zone is an un-routable network that separates the storage and network data within the environment. All XenServer hosts have a direct connection to this zone for SAN access.

**XenServer Management** – The XenServer management zone separates XenServer-to-XenServer network traffic from the data and storage traffic.

A Cisco Catalyst 6513 layer-3 switch is physically connected to these networks to provide connectivity across them. The switch configuration secures these distinct networks through prescriptive route and access-list tables. The Cisco Catalyst 6513 is directly connected to a pair of Cisco Catalyst 3750G switches that provide connectivity to the individual XenServers. The above figure presents a view of the connections from the physical server to the switch.

This design delivers the foundation for a highly scalable system while providing physical separation necessary to meet the security requirements of a multi-tenant environment.
Note: The details of any particular 3rd party product are not provided as an endorsement or recommendation for the use of that product. These details are provided solely as a reference regarding the hardware and software used within the Citrix Cloud App Delivery Group lab environment when this document was written.

Each network in this sample uses a simple IP addressing scheme with a private network address set by RFC1918 and RFC4193. This design provides ample capacity for individual vLANs or security domains within the networks and eases the overhead of managing the routing and access-list tables.

![Figure 3.4: Detail of sample implementation TCP/IP addressing](image-url)
In a Citrix Service Provider environment, the availability and performance of the storage infrastructure are critical because thousands of users can be impacted by storage outages or performance issues. Thus the storage architecture must provide the level of availability and performance typical for business-critical applications. Citrix recommends that CSPs choose a storage vendor that has software and hardware solutions to address the availability and performance requirements for large, scalable Citrix application and desktop delivery environments.

The Citrix Cloud App Delivery Group lab implementation of the Citrix Reference Architecture for Multi-Tenant Desktop as a Service employed a NetApp FAS 3170 SAN with dual controllers. Each controller is individually connected to the storage shelves and clustered to provide the maximum amount of redundancy in case of a controller failure. From the raw storage, a single aggregate (Agg0) was created for each controller. From the aggregates, NFS volumes were created and presented to the XenServers as storage repositories.

Hypervisor Host Configuration

The CSP solution is hypervisor agnostic; a service provider can use any of the following hypervisors for the infrastructure or the worker servers that deliver the applications and desktops.

Citrix XenServer

Citrix XenServer is a complete, managed server virtualization platform built on the powerful Xen® hypervisor. Xen technology is widely acknowledged as the fastest and most secure virtualization software in the industry. XenServer is designed for efficient management of Windows and Linux®
Microsoft Hyper-V
Microsoft Windows Server 2008 R2 with Hyper-V® builds on the architecture and functions of Windows Server 2008 with Hyper-V by adding multiple new features that enhance product flexibility. Hyper-V is available in a Standard, Server Core and free Hyper-V Server 2008 R2 versions. More information on Hyper-V is on the Microsoft company website.

VMware vSphere
VMware vSphere consists of the management infrastructure or virtual center server software and the hypervisor software that virtualizes the hardware resources on the servers. It offers features such as Distributed resource scheduler, vMotion, HA, Storage vMotion, VMFS, and a multi-pathing storage layer. More information on vSphere is on the VMware company website.

The following server types were used to host the infrastructure for the entire Citrix solution.

Server hardware used in the Citrix lab implementation

2 x HP DL360
Dual – Quad core Intel E5335 @ 2.00 GHz
16GB – PC3 1066MHz
6 x 1GbE NICs

10 x HP DL380
Dual – Quad core Intel E5335 @ 2.00 GHz
96GB – PC3 1066MHz
6 x 1GbE NICs
Securing the Networks

Administrators can secure communications between the various CSP networks through firewall configurations that deny all traffic to those networks other than that necessary to provide and manage secure services across multiple tenants.

<table>
<thead>
<tr>
<th>Port</th>
<th>Source to Destination</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP: 443</td>
<td>Public Internet to DMZ</td>
<td>End-point to Access Gateway SSL connectivity</td>
</tr>
<tr>
<td>TCP: 1494/2598</td>
<td>DMZ to Tenant Network</td>
<td>Access Gateway to Sessions, applications and desktops, HDX/ICA® connectivity for endpoints. This protocol is encapsulated in 443/SSL from the end-point to Access Gateway in the line item above.</td>
</tr>
<tr>
<td>TCP: 80/443</td>
<td>DMZ to Tenant Network</td>
<td>Citrix Web Interface or CloudGateway/StoreFront connections</td>
</tr>
<tr>
<td>TCP/UDP: 389/636/3268</td>
<td>DMZ to Management Network</td>
<td>Active Directory communications and authentication</td>
</tr>
<tr>
<td>TCP: 53</td>
<td>DMZ to Management Network</td>
<td>DNS</td>
</tr>
<tr>
<td>TCP: 123</td>
<td>DMZ to Management Network</td>
<td>NTP</td>
</tr>
<tr>
<td>TCP: 161-162</td>
<td>DMZ to Management Network</td>
<td>SNMP</td>
</tr>
<tr>
<td>Port</td>
<td>Source to Destination</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>UDP: 6901-30 / 10802-3</td>
<td>Tenant Network to Management Network</td>
<td>Provisioning Server vDisk streaming</td>
</tr>
<tr>
<td>SMB: 445</td>
<td>Tenant vLANs to Application vLAN</td>
<td>File Shares and Citrix Streaming</td>
</tr>
<tr>
<td>TCP/UDP: 389/636/3268</td>
<td>Tenant Network to Management Network</td>
<td>Active Directory communications and authentication</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Source to Destination</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP: 53</td>
<td>Tenant to Management</td>
<td>DNS</td>
</tr>
</tbody>
</table>

Page 28
<table>
<thead>
<tr>
<th>Network</th>
<th>TCP: 123</th>
<th>Tenant to Management Network</th>
<th>NTP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TCP: 161-162</td>
<td>Tenant to Management Network</td>
<td>SNMP</td>
</tr>
<tr>
<td></td>
<td>TCP: 1433-1434</td>
<td>Tenant to Management Network</td>
<td>Microsoft SQL Services</td>
</tr>
<tr>
<td></td>
<td>TCP: 80/443/9035</td>
<td>Tenant to Management Network</td>
<td>Citrix EdgeSight Services App Studio XenDesktop VDA</td>
</tr>
<tr>
<td></td>
<td>TCP: 11161</td>
<td>Tenant to Management Network</td>
<td>Citrix Power and Capacity Management</td>
</tr>
<tr>
<td></td>
<td>TCP: 2512</td>
<td>Tenant to Management Network</td>
<td>Citrix Independent Management Architecture communications</td>
</tr>
<tr>
<td></td>
<td>TCP: 135 / 27000</td>
<td>Tenant to Management Network</td>
<td>Citrix Licensing Services</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Software Used</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Cisco IOS</td>
</tr>
<tr>
<td>Hardware Used</td>
<td>Cisco Catalyst 6513</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 4900M</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 3750G</td>
</tr>
</tbody>
</table>
Active Directory and Organization Unit Considerations

Windows-based applications and desktops “as a Service” are inherently based upon Microsoft Windows principals and technologies. As a result Microsoft Active Directory plays a critical role in many aspects of the Citrix designs, most notably as the central account authority and as a foundational element to organizational and multi-tenant capabilities.

The above graphic highlights the complementary structures within the Citrix XenApp 6.5 AppCenter Console (application and desktop publishing and management) and the Microsoft Active Directory Console (Account Authority and organizational structure). Sub-nodes in each tree view map to tenant specific groups. In fact, the Citrix nodes are logical administrative folders that map directly to the Active Directory Organization Units and/or child domains that provide the basic tenant partitioning and security from an account perspective for this solution.

This section focuses solely on the Active Directory design; the XenApp complement is discussed in the Hosted Applications section later in this document. We have also added guidance regarding VDI-in-a-Box and XenDesktop integration within this architecture. Although the AD mappings are conceptually the same some terminology differs within the XenDesktop and VDI-in-a-Box documentation. Additionally, when Citrix CloudPortal Services Manager is included within a CSPs
designs it should be noted that CSPM will provision tenants and their associated OUs within Active Directory under the CPSM parent OU, integrating the XenApp and XenDesktop objects within the CSPM created AD tenant containers aids in the seamless integration of these systems within CPSMs provisioning.

**Active Directory Organization Units and Group Policy Objects**

The Active Directory (AD) considerations for the CSP Reference Architecture follow Microsoft recommended best practices for AD designs. We have also followed current industry best practice implementations for the SMB focused Citrix Service Providers as understood through conversations with providers across the spectrum over the last few years. The result of this combined set of considerations points to the Organization Unit (OU) as the preferred tenant partitioning mechanism within AD for most instances.

As discussed in the earlier section on multi-tenancy, some subscribers might be better served by a dedicated child domain, or in extreme cases their own isolated AD forest and all other infrastructure. Those two scenarios represent the edge case in the SMB-focused service provider market, and as such are not addressed in detail in this reference architecture. The context of this document and all further design considerations within this document use a single AD OU structure as its basis.

As shown in the graphic to the right, we created a separate OU for each tenant, labeled Tenant1, Tenant2, and so on. This enables the leverage of AD Group Policy Objects (GPOs) as a foundational mechanism for assigning properties to each tenant. Doing so ensures easy, quick administration and enforcement of Service Level Agreements (SLAs) regarding the configuration and security of each tenant.

Subordinate OUs to each tenant enable further granularity of management with regards to separate applications, desktops and users/user groups within a single tenant. This OU structure provides a clearly navigable solution for troubleshooting individual tenant configurations, while also leveraging the cascading aspects of Group Policy.

The advantage of cascading Group Policy in a multi-tenant environment is that it enables the least amount of customization with the greatest impact per tenant or SLA. For example, a CSP might begin their service offering with a generic GPO configuration that is applied at the CSP OU (CSPDemo.com in the graphic). This GPO is applied to all subordinate OUs (Tenants) by default. Any tenant that requires a modification to this generic base GPO is then assigned an additional GPO for their OU container that contains only those configuration customizations that augment the generic offering. Troubleshooting a particular tenant configuration thus usually only requires consideration of the GPO for that tenant.
Active Directory infrastructure

<table>
<thead>
<tr>
<th>Software Requirements</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Microsoft Windows Server 2008 R2</td>
</tr>
<tr>
<td>Installed Roles</td>
<td>Active Directory Services</td>
</tr>
<tr>
<td>Additional Software</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hardware Used</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
<td>XenServer 5.6 SP1</td>
</tr>
<tr>
<td>Virtual Server Specifications</td>
<td>4 vCPU w/ 4GB RAM</td>
</tr>
</tbody>
</table>

The sample implementation includes two AD domain controller virtual machines provisioned with the global catalog role in the management zone to provide authentication services to the tenants. Each virtual machine is sized to support up to 10,000 users. Additional domain controllers are required if the CPU within the virtual machine exceeds 50%.

For more information regarding Microsoft Active Directory designs, see:
Virtual Provisioning of application and desktop host workloads

Hypervisor

Virtualization is the fundamental enabler of an efficient cloud datacenter. As a best practice, enabling dynamic scale and simplified management within the CSP Reference Architecture for, all workloads are virtualized except for Citrix Provisioning Services™ (discussed in the next section). Because the reference architecture is hypervisor agnostic, no proprietary capabilities within any of the more popular hypervisors are discussed. Each VM is simply used as a compute engine and container for workloads within the reference architecture. An example configuration as implemented within the Citrix Cloud App Delivery Group labs provides a guide for efficient network and storage configuration of the host servers.

Workload provisioning

One of the primary enablers of efficient scale and management within the solution is a robust yet simple workload provisioning system. Although there are many approaches to provisioning, from physical unattended installations to VM cloning and other more recent technologies, Citrix recommends Citrix Provisioning Services (PVS) for the most efficient scale and simplified life-cycle management of XenApp and other service enabling workloads.

The remainder of this section describes the implementation within the reference architecture.
**Note:** Because of the intense IO requirements for vDisks in this environment Citrix recommends installing the PVS on a physical server. However, PVS can be virtualized in certain conditions. Please refer to our knowledge base article: [http://support.citrix.com/article/CTX128645](http://support.citrix.com/article/CTX128645) (Design Considerations for Virtualizing Provisioning Services) for more information.

**Provisioning Server infrastructure**

<table>
<thead>
<tr>
<th>Software Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating System</strong></td>
</tr>
<tr>
<td><strong>Installed Roles</strong></td>
</tr>
<tr>
<td><strong>Additional Software</strong></td>
</tr>
<tr>
<td><strong>Server(s)</strong></td>
</tr>
<tr>
<td><strong>Server</strong></td>
</tr>
<tr>
<td><strong>Scalability</strong></td>
</tr>
</tbody>
</table>

**Provisioning Services streaming technology**

The Provisioning Services infrastructure is based on software-streaming technology. This technology allows computers to be provisioned and re-provisioned in real-time from a single shared-disk image. In doing so, administrators can completely eliminate the need to manage and patch individual systems. Instead, all image management is done on the master image. The local hard-disk drive of each system can be used for runtime data caching or, in some scenarios, removed from the system entirely, which reduces power usage, system failure rates and security risks.

**Provisioning Services solution**

Using Provisioning Services, administrators prepare a device (master target device) for imaging by installing any required software on that device, create a vDisk image from the master target device’s hard-disk drive, and saves the image to the network (on a Provisioning Server or storage device).

When the vDisk is available from the network, the target device no longer needs its local hard-disk drive to operate; it boots directly across the network. The Provisioning Server streams the contents of the vDisk to the target device on demand in real time. The target device behaves as if it is running from its local drive. Unlike thin-client technology, processing takes place on the target device.
Provisioning Services implementation

The PVS servers are directly connected to the core switch and storage network with separate network adaptors. This design separates the I/O traffic for vDisk input (loaded from the NFS share) and vDisk output (delivered to the Target Devices), providing a high level of performance (maximum IOPs), reliability (redundant devices and network connections) and scalability (increased target devices).

![Diagram of Citrix Provisioning Service sample implementation](image)

Figure 5.2: Citrix Provisioning Service sample implementation

The implementation includes two physical servers running Windows Server 2008 R2 and the File Services Role, with Provisioning Services installed.

**Note:** Use Network Interface Card (NIC) – Teaming to increase the reliability and the I/O between the Provisioning Servers, File Server and Target Devices. Also, use dedicated NICs for loading the vDisks and for delivering the vDisks to the Target Devices.

The following diagram outlines a basic Provisioning Server and Windows Network File System (NFS) architecture:

![Diagram of Provisioning Server architecture](image)

**Figure 5.3: Basic Provisioning Server architecture**

The SAN is configured to present NFS volumes to the PVS servers.

This scenario compares the PVS server’s IOPS usage when streaming one XenApp server verses ten XenApp servers running a medium Microsoft Office 2007™ workload. The workload was generated using EdgeSight® for Load Testing (ESLT) version 3.6 to scale up to fifty users per server over a fifteen-minute period. The test was run with the PVS cache located on the device hard disk, the recommended deployment configuration when streaming a XenApp workload.
The data below captures the start of the workload as users initially begin to log on to the XenApp servers and continues for the duration of the test. The ESLT scripts perform the following actions:

1. Scale up to the maximum defined user count over fifteen minutes.
2. Continue to run at the maximum defined user count for five additional minutes.
3. Scale down to no users over five minutes.

![XenApp Load Test - vDisk IOPs](image)

**Figure 5.4: XenApp Load Test - vDisk IOPs**

The graph contains only the IOPS of the vDisk. The write cache and operating systems are located on separate physical drives to allow their IO to be analyzed independently.

There is little to no disk IO regardless of the number of XenApp servers and users involved in the test. The initial spike in IOPS was relatively small compared to the peak observed during the boot scenario.

Best Practices for Configuring Provisioning Server on a Network
[http://support.citrix.com/article/CTX117374](http://support.citrix.com/article/CTX117374)

Hotfix CPVS56SP1E029 - For Citrix Provisioning Services 5.6 SP1
[http://support.citrix.com/article/CTX129381](http://support.citrix.com/article/CTX129381)
Application Provisioning

Application provisioning within the CSP reference architecture provides a key element to the “Dynamic Assembly” capabilities within the system. Dynamic assembly is the process by which separate elements are combined in real-time to present a user with their specific, familiar, and personalized environment of operating system, desktop, application and personalization settings.

Application virtualization and streaming

Application virtualization provides one of the key components of dynamic assembly, the separation of applications from the underlying OS. Separating the application from the OS enables management of the application and its total life-cycle as a discreet object. A further advantage to this separation of OS and application is the ability to deliver and manage a single application image across CSP tenants; personalized for each tenant’s SLA through the policies associated with that tenant’s worker group based partition.

Within the XenApp system, Citrix streaming and Microsoft® App-V combine to provide a complete and seamless solution with mature and proven application compatibility.

Figure 6.1: Application Virtualization and Streaming architectural overview
Packaging applications with the profiler/sequencer

To enable single instance management of applications from a single application hub (AppHub) across tenants within a Citrix Service Provider datacenter, package the applications into a virtualized instance using either the Citrix Streaming Profiler or Microsoft App-V Sequencer. For details and best practices of the sequencing and profiling process, refer to the Citrix Streaming and Microsoft App-V integration kit documentation found in the Citrix eDocs “XenApp 6.5” library at http://www.citrix.com/edocs.

The resources required for both of these packaging utilities are basically the same, with only a few differences regarding the underlying machine configurations.

<table>
<thead>
<tr>
<th>Citrix Streaming Profiler Requirements</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server 2008 R2</td>
</tr>
<tr>
<td>Installed Roles</td>
<td>Roles as installed on the XenApp worker servers</td>
</tr>
<tr>
<td>Additional Software</td>
<td>Citrix Streaming Profiler</td>
</tr>
<tr>
<td><strong>Hardware Used</strong></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>2 vCPU, 4GB RAM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Microsoft App-V Sequencer Requirements</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server 2008 R2</td>
</tr>
<tr>
<td>Installed Roles</td>
<td>Roles as installed on the XenApp worker servers</td>
</tr>
<tr>
<td>Additional Software</td>
<td>Microsoft App-V Sequencer</td>
</tr>
<tr>
<td><strong>Hardware Used</strong></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>2 vCPU, 4GB RAM</td>
</tr>
</tbody>
</table>

**The AppHub**

The AppHub provides the central storage and streaming services that enable delivery of a single application image into the worker servers. The image is assembled on-demand for each user. Within the CSP Reference Architecture implementation, the AppHub has two enabling technologies: Standard file storage for the images themselves and the Microsoft App-V Streaming Server.
Delivering applications to tenant users and groups

After the application image is uploaded to the AppHub, the next step is to publish it for subscriber access. The Citrix AppCenter Console is the central administrative interface for configuring published applications across all tenants. The published applications are then streamed into the hosted desktop through the Offline and App-V plug-ins for Citrix Receiver. For more information about the Delivery Services Console, see “Citrix Delivery Services Console” later in this document.

See the knowledge base article: “How to Sequence an App-V Virtual Application and Stream XenApp Server to be Published Seamlessly to Users” [http://support.citrix.com/article/CTX126082](http://support.citrix.com/article/CTX126082)
Hosted applications execute on XenApp servers and are presented to the desktop through Citrix Receiver and HDX technologies. The applications themselves are either installed on the XenApp worker servers or virtualized and streamed into those servers as described in the preceding section. Because XenApp infrastructure and workers are leveraged in much the same way for both application and desktop delivery, we discuss configuration and scalability of Hosted Applications in Creating the Multi-Tenant Layer section, next.
Creating the Multi-Tenant Layer

The Citrix farm is the primary building block for the multi-tenant module within the reference architecture. The farm is divided into various modules and partitions to provide a scalable yet simplified management scope for over 1,000 XenApp workloads providing services for over 100,000 active users per farm/block.

Please note: This section is specific to the use of XenApp for the delivery of Windows applications and Hosted Shared Desktops, based on Windows Server 2008 R2 Remote Desktop Services. Although conceptually similar in many areas we have created two separate sections to address XenDesktop and VDI-in-a-Box (VDIiaB) concepts within this particular solution.

The section titled “XenDesktop Considerations” has been added in an effort to build upon the concepts introduced in this section, and also to clarify those points that are specific to the additional desktop models that XenDesktop brings to this solution.

The section title “Simplified VDI with VDI-in-a-Box” outlines the implementation of VDIiaB as a complement to the CSP reference architecture for those CSPs wanting to offer VDIiaB grids as part of their services for SMB tenants.
The major modules and components of the Citrix Farm are:

- XenApp Data Store
- XenApp Data Collector
- XenApp Workers
- XenApp Worker Groups
- Citrix License Server
- Microsoft Active Directory
IMA Data Store

The Independent Management Architecture (IMA) data store is a central repository for all of the configuration information for the XenApp farm. This includes items such as published applications, worker groups and load evaluators. During server startup, the IMA Service queries the data store for initialization information. This is the most CPU-intensive action for the data store, as the IMA Service initialization process ensures that the local host cache (LHC) is consistent with the data store. When multiple servers boot, multiple simultaneous requests for initialization information are made to the data store.

During normal farm operation, each server accesses the data store every thirty minutes to ensure its LHC is current. The data store is also accessed if the Delivery Service Console (DSC) or other Citrix query-based utilities modify the farm configuration or request static information. However, the data store is not accessed when a user logs in, disconnects, or reconnects to the farm. All the information needed for a client to establish a connection to a XenApp server is stored in the LHC, with the exception of licensing details.

<table>
<thead>
<tr>
<th>Data Store Software Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operating System</strong></td>
</tr>
<tr>
<td><strong>Installed Roles/Features</strong></td>
</tr>
<tr>
<td><strong>Additional Software</strong></td>
</tr>
</tbody>
</table>

**Data Collector**

The data collector manages all of the dynamic information in the farm. Dynamic information consists of items that change often such as connected sessions, disconnected sessions and server loads. The data collector is responsible for knowing the global state of the farm. The data collector also performs resolutions—a process where, upon user request, the data collector determines the least-loaded server that is hosting a load-balanced published application or desktop.

**Sizing guidelines**

The data collector stores all dynamic information in memory therefore the data collector needs enough RAM to store all of the records. Memory usage varies based on the number of published applications, number of servers and number of user sessions in the farm. The CPU plays an
important role in determining the number of resolutions the data collector can process in conjunction with managing dynamic information.

<table>
<thead>
<tr>
<th>Data Collector Software Requirements</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Microsoft Windows Server 2008 R2</td>
</tr>
<tr>
<td>Installed Roles/Features</td>
<td>During a wizard-based XenApp installation, the Server Role Manager (using the Server Role Installer) automatically installs all prerequisite software and Windows Server roles. For more information on XenApp server installation: <a href="http://support.citrix.com/proddocs/topic/xenapp6-w2k8/ps-system-requirements-w2k8-xa6.html">http://support.citrix.com/proddocs/topic/xenapp6-w2k8/ps-system-requirements-w2k8-xa6.html</a></td>
</tr>
<tr>
<td>Additional Software</td>
<td>XenApp 6</td>
</tr>
<tr>
<td>Hardware Used</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>4 vCPU, 8GB RAM</td>
</tr>
<tr>
<td>Scalability</td>
<td>1,000 XenApp Workers</td>
</tr>
</tbody>
</table>

License Server

The license server stores and manages Citrix licenses. When users connect to a farm, the worker server checks out a license from the license server on behalf of the client device. Subsequent connections from the same client device share the same license.

Sizing guidelines

One of the most important considerations in determining license server requirements is processor speed. Although CPU usage is not usually high, CPU time increases as license checkout requests are made and License Management Console activity increases. The time it takes to execute these transactions is dependent on the speed of the CPU. In general, the size of the farm and the number of simultaneous client connections dictate the power of the server needed for the licensing feature.

To appropriately size the license server, determine the number of client logins per second in the farm deployment by using the Performance Monitor counters and the load evaluator logging feature. This analysis determines the processor speed needed for optimal license server performance.

Additionally, the license server process is single threaded, so multiple processors do not increase performance. The license server uses approximately 4.5KB of memory for every session license and 39KB of memory for every start-up license that is in use. The license server is capable of processing 248 license checkout requests per second. In a scenario where all users log in over the course of thirty minutes, a single license server can handle 446,400 users.
The AppCenter Console is the user interface of the XenApp “Control Module.” A Microsoft Management Console (MMC) snap-in enables CSPs to perform a number of DaaS and SaaS management functions.

CSPs can configure…

- XenApp servers
- Server farms
- Published desktops
- Published applications
- Policies
- Printers
- Load balancing

…and monitor:

- Alerts
- Hotfix information
- Administrative changes

Install the AppCenter Console on a standalone workstation VM or publish it from a XenApp Controller Server within the Control Module.

## Citrix AppCenter Console (XenApp configuration and management)

<table>
<thead>
<tr>
<th>License Server Software Requirements</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Microsoft Windows Server 2008 R2</td>
</tr>
<tr>
<td>Installed Roles</td>
<td>None</td>
</tr>
<tr>
<td>Additional Software</td>
<td>Citrix License Server 11.9</td>
</tr>
</tbody>
</table>

## Delivery Service Console Software Requirements

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Windows XP and Higher</th>
</tr>
</thead>
</table>
| Installed Roles/Features | Microsoft Management Console (MMC):
- For Windows Vista, Windows 7, and Windows Server 2008 R2: MMC 3.0 (installed by default)
- For other supported Windows operating systems: MMC 2.0 or 3.0 |

The XenApp Server Role Manager deploys the following software,
if it is not already installed:

• Microsoft .NET Framework 3.5 SP1
• Microsoft Windows Installer (MSI) 3.0
• Microsoft Windows Group Policy Management Console
• Microsoft Visual C++ 2005 SP1 Redistributable (x64)
• Microsoft Visual C++ 2008 SP1 Redistributable (x64)
• Microsoft Visual C++ 2008 SP1 Redistributable
• Microsoft Visual C++ 2005 SP1 Redistributable
• Microsoft Primary Interoperability Assemblies 2005

<table>
<thead>
<tr>
<th>Hardware Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>WorkStation minimum</td>
</tr>
<tr>
<td>Scalability</td>
</tr>
</tbody>
</table>

**Active Directory Integration, XenApp Worker Groups and Policies**

The release of XenApp 6 adds powerful new features for XenApp administrators through AD integration. Administrators can now manage all user and server settings through AD policies and can manage published applications, hosted desktops, load balancing and farm multi-tenancy through a new container known as a worker group.

![WorkerGroups and tenant isolation](image)

Figure 8.1: WorkerGroups and tenant isolation

A worker group is a collection of XenApp servers in the same farm, where administrators can associate objects such as published applications, published desktops, and policies. Worker groups allow a set of similar servers to be grouped and managed as a single entity. Worker groups are closely related to the concept of application silos. However, they streamline the creation of application silos by providing a way to synchronize the published applications and server settings across a set of XenApp servers.
Worker groups are dynamic. For example, when AD containers are associated with a worker group, changes in the AD container are automatically reflected in the server's worker group memberships.

Servers can be added to worker groups by AD Organizational Units or Server Groups. This provides for the dynamic update of worker groups based on AD memberships of servers. That is, as servers are added or removed from the AD containers, they are automatically added to or removed from the respective worker groups.

In anticipation of future expansion, two sets of worker groups are created: One set to group servers by tenant and one set to group applications by tenant. When the administrators add capacity for an existing tenant, they do not need to modify the servers list of published applications or desktops assigned to that tenant. Instead, they simply add another XenApp server to the tenant’s OU.

With dynamic provisioning, as may be enabled through the App Orchestration capabilities described later in this document, AD use automates this step by creating a base image for XenApp with all of the applications installed. To add capacity, simply create a new instance of the base image and add it to the desired tenant OU. The server receives its server settings from AD, joins the appropriate worker groups and begins hosting published applications or desktops. Creating separate worker groups for desktops and applications gives CSPs the flexibility to easily expand their tenant base.
Worker groups and Citrix policy filters

CSP administrators can filter all XenApp server policies by worker groups, thereby restricting Group Policy Objects (GPOs) to a specific set of servers in the farm. For policies configured in the Delivery Services Console, this is the only way to assign different settings to different groups of servers because all policies are replicated to all servers, completely independent of AD.

AD GPOs are used to manage the settings in the XenApp farm. For all user and site settings GPOs can be linked to the XenApp OUs without any filters. However, if a setting is required specifically for a particular tenant's servers, a Worker Group filter added to the policy limits it to the appropriate tenant.

Citrix policy configuration

In XenApp 6 nearly all server, farm and user settings are governed by group policies.

Administrators create a GPO containing the desired Citrix policy settings and link the GPO to the appropriate tenant OUs. However, for Citrix administrators who do not have control over their AD environment or whose organizations do not use AD for directory services, XenApp 6 provides farm-based group policies through the policies node in the management console. Such policies are written to the XenApp data store and propagated to all servers in the farm.

Administrators create Citrix policies at different OU structure levels as shown in the following graphic. In this case, the priority of policies enforcement is as follows:

- Policy created at the Default Domain Policy
- Policy created at the top OU level
- Policy created at the middle level OU
- Policy created at lowest level OU
The XenApp General GPO applies to the XenApp farm as a whole. For each tenant, the CSP administrator creates new GPOs or links existing GPOs to the tenant’s OU structure. For example, the Tenant1 GPO is a general tenant GPO created to apply policies to all of the Tenant1 downstream OUs. The CTXRestrictedComputer GPO is linked to the Tenant1 computer OU (Tenant1_Computers) and CTXRestrictedUser and XASession GPOs are linked to the Tenant1 user OU.

The resultant Citrix policies applied to the Tenant1 computer and user OUs are the merged settings from all four GPOs. If there is a conflict among the policy settings of these GPOs, the settings in the Computer and User GPOs have the highest priority and overwrite the settings in the Tenant1 GPO, XenApp General GPO and Domain GPO.
XenDesktop Considerations

Many of the fundamental scale and design parameters within the CSP reference architecture can be cross referenced with the enterprise focused XenDesktop 5 Modular reference architecture. The business impact of the nuances that a multi-tenant service offering from a single CSP cloud presents can be significant, and in some cases completely cost prohibitive for certain VDI scenarios. Over the last several years, as the Cloud, Service Provider, and Virtual Desktop market has evolved, the confusion over how “VDI” (Windows Client OS based virtual desktops) can and should be hosted as a cloud based service has been rather prolific. Various vendor licensing models for different layers of the solution stack (as well as the aggressive marketing of some startups) has added to the confusion over time. Citrix continues to work with all of our ecosystem partners to help bring clarity, both to service providers as well as to Citrix and other ISVs, regarding the current best approach to multi-tenancy designs for Windows application and desktop delivery as a service. This revision of the CSP Reference Architecture represents Citrix’s guidance on the current most cost effective approach for the integration of VDI desktop scenarios within the solution.

In order to address the broadest set of considerations in a cost effective manner Citrix has added several offerings to our XenDesktop line. In this section we will provide guidance on implementing XenDesktop Hosted VDI (based on Windows Client OS) and XenDesktop Server VDI (based on the Windows Server OS) within the overall CSP Reference Architecture.

XenDesktop Hosted Server VDI

XenDesktop Server VDI is compliant with all service provider subscription licensing models, and can leverage the greatest number of shared resources within a CSPs cloud datacenters. For this reason it is the preferred approach for the lowest cost delivery of almost all VDI use cases. From a technical perspective the Server VDI solution can be applied to virtually all use cases that have traditionally driven the need for Windows Client VDI by some users. These use cases include:

- The requirement to dedicate an entire OS to a single user:

  This use case is usually driven by a need for a particular user to frequently perform administrative level tasks such as install software, reboot the OS at will without affecting other users, or experiment with different settings as would be the case for a test or development engineer.

- The requirement to use an application that cannot be confirmed to run in a Microsoft Remote Desktop Services Session Host environment:

  Some legacy applications and sadly some new applications that are not written to Microsoft published best practices are incapable of executing in an environment where the Microsoft RD Session Host Role is active. Citrix XenDesktop Server VDI does not rely on this role and therefore does not expose the applications incompatibility.
• The installation of peripheral devices that are not compatible in a RD Session Host environment:

Like some applications there are some peripheral devices that can only operate securely in an environment that is dedicated to a single user. Again, Server VDI effectively serves this use case.

![Figure 9.1: A conceptual view of Hosted Server VDI](image)

As shown above on the left hand side of the graphic, an example of the XenDesktop Hosted Server VDI implementation, within the CSP Reference Architecture using the Server Isolation multi-tenancy model would place the XenDesktop components within a single XenDesktop farm. In this model all hardware, delivery controllers and VM provisioning systems are shared across multiple tenants. This model provides for the highest density of VDI workloads and the most streamlined management workflow within a CSPs datacenter.

On the right in the graphic the Farm Isolation multi-tenancy model is shown. This model isolates the entire farm, including the XenDesktop Controllers. Isolation at this level should be considered when a tenant requires their own Active Directory Forest for authentication or when any given tenants total VDI footprint requires one or more entire XenDesktop Pods as described in the [XenDesktop 5 Modular Reference Architecture](#). Isolation at this level for a tenant with small numbers of Hosted Server VDI subscribers, although technically valid, will present a more expensive solution than the previously discussed Server Isolation model.

The diagram below outlines the components and their placement within the appropriate network segments of the overall solution in blue.
XenDesktop Hosted VDI for CSPs

The cloud hosting of Windows Client OS desktops is growing in popularity as a request from prospective tenants. Although the technical implementation of such an offering may at first appear to be straightforward, the business considerations and their ultimate effect on a valid design can present a few challenges. These challenges point to a few conclusions, not the least of which is the tendency for most tenants to ultimately realize that a Hosted Shared or Hosted Server VDI subscription meets their needs and budget most appropriately. Nevertheless there is still a niche of use cases and user types that ultimately do require a Windows Client OS in order to be most productive. In these scenarios relative cost is often much less of a concern than the overall use case for that particular user. When these niche use cases can be served within a broader offering that includes Hosted Shared or Hosted Server VDI models tenants receive a full complement of services from a single provider at the most attractive price in aggregate. It is for this reason that much effort has gone into understanding Hosted VDI as a Service and the resulting design requirements presented here.

Some history should be acknowledged before we describe the VDI solutions presented. It has become clear that today there are many views regarding the definition of Desktop as a Service (DaaS). This is pretty typical in emerging markets, especially the sub-markets making up “the cloud” including DaaS. Since the 1990’s Citrix has played a leading role in many of the business and technology discussions that have evolved to represent several of the major cloud markets. Needless to say Citrix has played a leading role in the evolution of the Windows applications and desktops as a cloud service market since its earliest days, and has made many investments in research projects, startups and in some cases acquisition of those startups over more than a decade.
Over the last several years, as the Citrix Service Provider program was being conceptualized and implemented, we have continued to work to provide guidance for the best practice and cost effective use of Citrix products in CSP offerings. XenDesktop has been part of the CSP program since the beginning and we have CSPs that have delivered the various XenDesktop FlexCast models as appropriate for their tenants. By working with our partners and the CSP channel we have determined that there are two key Hosted Virtual Desktop architectures and business models that need to be discussed; **Desktops as a Service**, and **Desktop Infrastructure as a Service**.

![Server Isolation](image1.png)

![Farm Isolation](image2.png)

**Figure 9.3: A conceptual view of Hosted VDI for DaaS CSPs**

**Desktop as a Service:**

Desktop as a Service is a complete service offering where complete desktop and application integration as well as life-cycle management is provided by the CSP as a monthly subscription. Tenants are usually businesses that have a very small or no IT department, or are business units within larger organizations that have a need that is more efficiently addressed by engaging with a CSP while the corporate IT focuses on other IT needs of the corporation.

In the graphic above you will notice that the concept of the server and farm isolation multi-tenancy models remain relevant, but with one very distinct design change, the physical hosts for the desktop VMs are represented as dedicated pools (Dedicated Virtual Infrastructure) per tenant. This dedicated hardware is explicitly required due to the current licensing specifics of the Windows Client OS according to Microsoft. Additionally it should be a best practice for these workloads to be
hosted on tenant dedicated hardware, in order to simplify the management of tenant specific SLAs as determined by the niche use cases that usually map to applications with intense compute needs, these in turn typically drive the requirement for a client OS VDI solution. It has been our experience that these use cases make up a very small percentage of DaaS requirements, perhaps lower than 5% of a tenant’s total DaaS subscriber base.

**Desktop Infrastructure as a Service:**

Desktop Infrastructure as a Service can be described as a cloud service that provides the basic network, storage and compute infrastructure to enable a tenant to build and maintain their own virtual desktop infrastructure. This service type typically does not provide any life cycle maintenance for the tenants VMs or applications. Although some do provide basic VM templates that include fundamental components such as the OS and perhaps a particular brand of Anti-Virus agent, the service that is provided is at a root level and the associated SLAs are typically for network uptime and perhaps VM back-ups.

Although Citrix provides technologies for DIaaS scenarios and we are evolving these capabilities to meet next generation requirements within our Project Avalon initiative, this revision of our reference architecture continues our focus on the more complete set of services provided by DaaS models and service providers.

More information about Microsoft licensing requirements for Windows Client OS based VDI can be found here:


More information regarding XenDesktop scaling and best practices can be found in the XenDesktop 5 Modular Reference Architecture [http://support.citrix.com/article/CTX133162](http://support.citrix.com/article/CTX133162)

**Simplified Hosted VDI with VDI-in-a-Box**

For those CSPs that anticipate providing relatively simple VDI services, where dedicated hardware per tenant will be used for execution of the VMs as well as for storage and provisioning, VDI-in-a-Box presents an attractive alternative at small scale.

Both the Server isolation model and the farm/grid isolation model can be provided when Hosted Server VDI desktops are the enabling OS for DaaS.

Similar to the Farm Isolation model for Hosted VDI, a VDIiaB Grid can be dedicated to a single tenant for the delivery of Windows Client OS VDI desktops.
More information about VDI-in-a-Box can be found in Citrix eDocs


A large catalog of VDI-in-a-Box videos and walk-throughs are also available at

http://www.citrix.com/tv/#tags/vdi-in-a-box

Secure Access and Acceleration

For the sake of clarity in the integration flow we now return to the IaaS module to integrate NetScaler and Access Gateway within our multi-tenant module.

Citrix NetScaler and Access Gateway

Citrix NetScaler presents a modular platform upon which several critical network security and acceleration functions are built. For those CSPs focused on the small to medium business, the Citrix Access Gateway capabilities within NetScaler are fundamental to the secure delivery of desktops and applications as a service.

Access Gateway multi-tenancy with NetScaler

The Access Gateway functionality within Citrix NetScaler VPX™ (Virtual Appliance) provides secure access to the CSP environment over SSL (TCP 443) across the public internet. Access Gateway multi-tenant support is implemented either within a single NetScaler VPX, physical appliance HA pair, or across segregated networks and vLANs through the use of a dedicated NetScaler appliance per tenant vLAN. From a software configuration perspective all of these scenarios are fundamentally the same with regards to the integration points between the DMZ and Multi-Tenant network.
Implementation within the Citrix Cloud App Delivery lab environment

NetScaler - virtual servers

Not to be confused with a XenServer guest, the Access Gateway Enterprise Edition virtual server is an entity within a NetScaler VPX that is a representative of all the configured services available to clients. The virtual server is also the access point through which clients access these services. Configuring multiple virtual servers on a single appliance allows one Access Gateway appliance to serve multiple user communities (Tenants in our example) with differing authentication and resource access requirements.

NetScaler - profiles and policies

Configuration of authentication, authorization and accounting (AAA) allows users to log on to the Access Gateway with credentials that are recognized by either the Access Gateway or by authentication servers, such as LDAP or RADIUS, located in the secure network. Authorization policies define user permissions, determining which resources a given user is authorized to access.

The CSP Reference Architecture uses a single AD domain with multiple OUs; each OU represents one tenant. The figure to the right shows the AD infrastructure. The “servers” OU for each tenant contains that tenant’s dedicated worker servers and the “users” OU contains that tenant’s user accounts. Each tenant also has an associated AAA policy that enables subscribers to securely and seamlessly log on to their CSP hosted resources.

A session profile contains the settings for client connections and they are associated to session policies. You can create profiles separately from the policy using the configuration utility and then use the profile for multiple policies. Only one profile can be used with a policy.

A single Citrix XenApp farm with a load balanced pair of Microsoft Windows Server 2008 R2 servers running Citrix Web Interface supports all tenants in this implementation. Additional Web Interface servers can provide greater scale as more tenants are brought on-board.

A NetScaler HA VPX pair, enabling Citrix Access Gateway capabilities is located in the DMZ to provide secure access for tenants to their resources.
A firewall appliance in front of the Access Gateway provides NAT from the external Internet to the internal Access Gateway interface (virtual server) and blocks all unwanted traffic from entering the CSP environment from the public network.

### NetScaler AG VPX Configuration

<table>
<thead>
<tr>
<th>Operating System</th>
<th>NetScaler VPX</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware Used</strong></td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>4vCPU, 4 GB RAM</td>
</tr>
<tr>
<td>Scalability</td>
<td>300 Concurrent SSL-VPN Connections</td>
</tr>
</tbody>
</table>

**Note:** The NetScaler VPX class of products has been used as a flexible means to enable multiple virtual appliances to be implemented in various configurations throughout the different networks within the architecture. There may be scenarios where larger throughput needs and economics are better served by the physical NetScaler lines such as the MPX or SDX. Please refer to the NetScaler product page for more information on which product line may fit your particular designs.

### Integration with Web Interface

After the Access Gateway is configured it must be associated with a CloudGateway/StoreFront, or Citrix Web Interface site, in order to provide subscriber access to subscribed services.

In this typical scenario, tenants use a web browser or end-point running Citrix Receiver to access a secure logon point hosted by the CSP. After providing the appropriate credentials, users are directed to their organization’s customized Citrix Web Interface to access their subscribed resources.

**Please Note:** While the Citrix CloudGateway and StoreFront represent the path forward for service advertisements automation of these components by Citrix App Orchestration technology was not yet available at the time this document was written. As a result all architectural validation of automated configuration of services advertisement for this reference architecture was done using Citrix Web Interface.
Dashboards and Management

Administering a complete applications and desktops as-a-Service offering can be a significantly complex consideration. The right tools and dashboard views are critical to simplifying and delegating administration for these solutions. Several core consoles enable a deep level of native control across the various components within the system. Citrix App Orchestration and the App Studio Console empower CSPs to build to massive scale through multi-farm and multi-version preferred configuration management across their entire cloud. In addition, Citrix CloudPortal Services Manager enables delegated provisioning and administration across these components from a simplified interface. This section of the reference architecture provides technical data and guidance regarding some of the core native consoles, as well as a look at the CloudPortal Services Manager as an example of the cross product integration and delegated administration capabilities that enable simplified management of these multi-tenant systems.

Citrix App Orchestration

App Orchestration is a groundbreaking technology that automates the design, configuration, deployment and lifecycle maintenance of Windows apps and desktops hosted by CSPs for multiple tenants, across multiple farms.

App orchestration achieves these goals by providing a configuration system that has a multi-tenant data model with flexible isolation concepts at its core (such as being able to choose separate isolation modes per-service), a simple UI, and automated workflows that control XenApp, Active Directory, Web Interface, and other products behind the scenes.

App orchestration provides the following features to simplify multi-tenant cloud-scale administration:

**Simplified Farm Management** - Just create your pools of XenApp 6.5 Session Hosts and pools of XenApp Controllers – the tasks of joining these to manage capacities across multiple XenApp farms happen automatically.
Multi-tenant Configuration - Support for different types of isolation environments, i.e.; Session-based, Server-based and Farm-based on a per-app/desktop basis.

Quick App & Desktop Configuration - Tired of running the 10-step XenApp App Publishing wizard? App orchestration discovers most of the app information (app-name, icon, command-line, working directory, etc.) from a XenApp Session Host, thus saving you from having to enter all of this info.

Web Interface Management: App orchestration automatically configures Web Interface servers to point to the correct farms based upon the tenant’s desired level of isolation, any time a new farm/tenant is introduced in the system.

Easier Patching of XenApp Session Hosts: When you create a new version of a XenApp Session Host, this new technology can automate the tasks of gradually draining users from the older version servers to the newer ones, without any down time or manual intervention.

Desired State Configuration: The entire configuration is done using the principles of Desired-State. This allows you to specify complex configuration in a few seconds without having to worry about sequencing things in the right order – app orchestration takes care of that for you.

Tenant Management: You can define Tenants into the system, their desired level of isolation and assign resources to them directly. No more coming up with naming patterns and crazy folder hierarchies to represent tenants in XenApp. Furthermore, the App Studio (web console) allows you to easily view which resources (apps, desktops, XenApp session hosts, farms, Web Interface resources) are allocated to which tenants.

CloudPortal Services Manager integration: The apps and desktops you advertise are automatically available for self-service consumption via the Hosted Apps and Desktop service in our control panel – thus enabling tenants to subscribe to what they need.

App Orchestration: Concepts & Terminology

This section introduces concepts and terminology which might be unfamiliar to CSPs new to Citrix App Orchestration. A list of terms follows to help you understand these concepts.

Citrix App Studio: A web based console that allows simplified management of App Orchestration deployment.

Advertisement: An advertisement represents an app or desktop offering from a service provider. As part of creating an advertisement, a service provider can specify the level of multi-tenant isolation required for that app/desktop as well as associate it with a specific farm catalog. These two parameters play an important role in determining the price at which app/desktop is offered as a service to tenants. For example

- Microsoft Word 2010 with session-based isolation offered from a Silver tier farm
• SAP with a server-based isolation offered from a Gold tier farm A bundle of advertisements is represented as a user plan in CloudPortal Services Manager and offered to tenants for self-service purchase.

Workload Catalog: A workload catalog is a collection of identical XenApp session hosts i.e., typically machines created from a single image (OS + XenApp + the apps to be delivered). The machines in a workload catalog are not joined to any farm – app orchestration uses the free machines from the catalog and joins them to a specific farm when needed. A workload catalog has an Active Directory organizational unit (OU) associated with it and machines placed in that OU become members of that catalog as long as they are identical.

Farm Catalog: A farm catalog is a collection of identical XenApp controller deployments. A controller deployment consists of one or more XenApp controller servers configured to point to an IMA data store e.g. an app orchestration deployment could consist of 2 farm catalogs:

• Silver Tier farm catalog: Each farm in this catalog has 2 XenApp controllers configured to point to a SQL IMA data store.
• Gold Tier farm catalog: Each farm in this catalog has 3 XenApp controllers configured to point to a mirrored SQL IMA data store. Like a workload catalog, a farm catalog has an Active Directory OU associated with it and controller deployments placed in that OU become members of that catalog as long as they are identical in configuration. In order to deliver apps or desktops to a tenant, app orchestration picks a free (i.e., unallocated) controller deployment from a farm catalog and unallocated machine(s) from a workload catalog to create a farm.

Tenant: A Tenant is a customer of a service provider and is typically on boarded into the CSP environment using a portal like CloudPortal Services Manager – which creates the appropriate objects in Active Directory (OUs, user/group accounts) as well as pushes the tenant info into the app orchestration system. App orchestration allows apps/desktops to be associated directly with tenants and it automatically tracks resources used by a tenant.

Subscription: A subscription is created when a tenant subscribes to an advertisement for an app/desktop. It is associated with a workload (defined below) and user accounts from a tenant. A subscription maps to a published app object in a XenApp farm.

Workload: A workload is a collection of servers (from a specific workload catalog) that are designated to host app/desktop subscriptions. A workload is associated with a specific XenApp farm and it may be shared between tenants or dedicated for a tenant – depending upon the multi-tenant isolation level of the subscriptions it is hosting. A workload maps to a Worker Group object in a XenApp farm and an Active Directory OU with which policies for the workload servers can be associated.
Orchestrating Multi-tenant Isolation

Citrix App Studio simplifies the complex task of multi-tenant isolation by implementing the three primary isolation models discussed earlier in this reference architecture. All three multi-tenancy models can be delivered from the same datacenter. A quick review of each model follows:

**Session Isolation:** This model leverages RD Session Host and XenApp sessions as the isolation layer between subscribers. This model represents the highest density for applications and desktop services and therefore can be the least expensive per user service.

**Server Isolation:** This model leverages Active Directory OUs and XenApp Worker Groups as the isolation layer between tenants. This level of isolation enables tenant specific SLAs, customization of workloads, and a higher level of security than the Session Isolation model at the same or a slightly higher cost for infrastructure.

**Farm/Network Isolation:** This model isolates tenants at the Citrix Farm layer and potentially at the Active Directory Forest layer if the tenant desires it. Because much of the service provider’s infrastructure is duplicated in this scenario a higher cost of service per tenant is probable.

![Figure 11.1: Citrix App Orchestration](image)

**App Orchestration Deployment**

A Citrix App Orchestration basic deployment consists of:

- An Active Directory domain,
- At least one Microsoft SQL Server,
- At least one Citrix App Studio management server
- At least one Citrix XenApp 6.5 Controller
• At least one Citrix XenApp 6.5 Data Collector
• Citrix XenApp 6.5 Workers

All servers require Windows Server 2008 R2 and...

.NET 4.0 installed and...

.NET 3.5 installed as a server role.

All servers can be either physical machines or virtual machines running on one or more hypervisors.

A sample Configuration

A sample configuration as built in Citrix’s Cloud App Delivery Group’s engineering labs used...

- 1 Active Directory 2008R2 Forest with a single domain,
- 2 dual vCPU with 4GB of RAM Configuration servers,
- 1 dual vCPU with 4GB of RAM Web Service servers and
- 1 dual vCPU with 4GB of RAM SQL database server.

All infrastructure components were virtualized on XenServer 5.5 SP2 with independent 1GB network connections to its data and storage networks.
Citrix CloudPortal Services Manager

Citrix CloudPortal Service Manager (CPSM) provides CSPs with a single integrated interface for the management of desktops, applications and backend services.

CloudPortal Services Manager User Interface

CloudPortal Services Manager (CPSM) provides a single unified interface providing both system administration and delegated administration to resellers and end-customers. The CPSM Web UI (CortexWeb) is loosely coupled with the other CPSM components. This loose coupling provides several security benefits. The web server has no dependency on Active Directory so it can essentially operate outside of the managed domain. The website can be locked down and run with minimal administrative permissions while still allowing the CPSM system to complete administrative tasks.
CPSM system databases

SQL Server provides the backbone of the CPSM system. The database stores configuration information for all services provisioned by CPSM, as well as all customer and user details. The SQL database also acts as a cache mechanism for Active Directory ensuring rapid user response without the need for slower AD queries.

The CPSM databases also store logging and auditing information for all provisioning transactions that pass through the system.

CPSM provisioning engine

The CPSM provisioning engine runs as a Windows Service. It monitors the provisioning queues (MSMQ) for provisioning requests. When the provisioning engine receives a request, it uses provisioning rules to determine the actions required to complete the provisioning.

The provisioning rules are easily customized using a simple Windows-based graphical interface that also provides a simple way to understand specific provisioning processes, helpful for problem diagnosis. This interface can also be used to customize the provisioning process and to integrate new rules for custom services.

Each provisioning action performs a reusable piece of work, typically associated with provisioning applications. CPSM includes over 100 provisioning actions. Example actions include:

- Creating an Active Directory user
- Creating a security group in Active Directory
- Creating a folder in a file system
- Creating an address list in Microsoft Exchange
- Running a shell command or a visual basic script

All provisioning processes are built using provisioning actions, enabling quick setup with little coding, while giving the service providers visibility into the processes being executed in their environment.

**Active Directory web service (ADWS)**

The Active Directory web service provides a secure and simple interface to Active Directory. The CPSM website uses this service to perform real time tasks such as user authentication and password expiry status.

**Reporting**

CPSM uses Microsoft SQL Server Reporting Services to deliver usage reporting capability through the CloudPortal Services Manager user interface. CloudPortal Services Manager interacts directly with the reporting services web service interface and allows controlled publishing of reports to all users of the CloudPortal Services Manager system.
A sample implementation of Citrix CloudPortal Services Manager

This section describes the logical and physical design for a sample CSP.

**CloudPortal Services Manager Components**

The CloudPortal Services Manager platform (CPSM) as described within this document has the following high level components:

<table>
<thead>
<tr>
<th>Components</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSPM User Interface(s)</td>
<td>This is the frontend server. This server will host the portal as well as the API's that will be used accessing the CPSM.</td>
</tr>
<tr>
<td>Provisioning Engine(s)</td>
<td>This is the backend for the CPSM environment. The provisioning engine is rules (workflow kind) based. This component consists of MSMQ and the queue monitoring process. Rules and actions are stored in the SQL database.</td>
</tr>
<tr>
<td>Database</td>
<td>This is the SQL database providing database services to be used by the frontend and the provisioning engine.</td>
</tr>
</tbody>
</table>

**Logical design**

The following diagram shows the logical design diagram of the CPSM infrastructure.
Within the logical design the following components can be identified:

- The CSP cloud platform. Observed from the perspective of this document the CSP cloud platform contains the following components:
  - CPSM Provisioning Engine (CortexProvisioning)
  - CPSM Database (CortexSQL)
  - CPSM User Interface (CortexWeb)
- On-premise AD's using the CPSM tool ADSync to synchronize new directory objects and passwords with the private cloud environment through CPSM. The tool as such will interact with the APIs as published by the frontend servers. The ADSync is only required for those tenants that do have their own Active Directory services on premise.
- Users connecting to the environment to manage services will use the CPSM User Interface Web page.

Please Note: The following are mentioned as CSP cloud components but the implementation of these items is not detailed within this reference architecture.

- Infrastructure Services (Directory Services, etc…)
- Messaging Services

Systems and Roles

The following table enlists all systems, names and their roles within this CPSM platform:

<table>
<thead>
<tr>
<th>System name</th>
<th>Role</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSPCLOUDPCP01</td>
<td>CPSM Frontend Servers</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>CSPCLOUDPCP02</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSPCLOUDVPC01</td>
<td>CPSM Frontend HLB Name</td>
<td>HLB Virtual Name</td>
</tr>
<tr>
<td>CSPCLOUDPES01</td>
<td>Provisioning Engine Servers</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>CSPCLOUDPES02</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSPCLOUDVPE01</td>
<td>Provisioning Engine Server Cluster Name</td>
<td>Cluster Virtual Name</td>
</tr>
<tr>
<td>CSPCLOUDVPC01\CSPCLOUDVPC01-</td>
<td>SQL Server instance name dedicated to CPSM</td>
<td>SQL. Cluster</td>
</tr>
<tr>
<td>SQL01</td>
<td>CSPCLOUDVCP01</td>
<td>SQL Cluster Virtual Name</td>
</tr>
<tr>
<td>------------</td>
<td>---------------</td>
<td>--------------------------</td>
</tr>
</tbody>
</table>
## High Availability

The CPSM platform contains various solution components on different layers within the application. All solution components as such are redundant through the solution. The table below lists the different solution components and the high availability concepts applied:

<table>
<thead>
<tr>
<th>Service</th>
<th>High Availability Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPSM User Interface Web Frontend</td>
<td>Network load balanced using NetScaler VPX</td>
</tr>
<tr>
<td>CPSM Provisioning Engine</td>
<td>CPSM based failover cluster (Active/Passive)</td>
</tr>
<tr>
<td>Directory Web Service</td>
<td>CPSM based failover cluster (Active/Passive)</td>
</tr>
<tr>
<td></td>
<td>(Directory Web services are installed on each of the</td>
</tr>
<tr>
<td></td>
<td>provisioning engine nodes)</td>
</tr>
<tr>
<td>Exchange Web Service</td>
<td>CAS Array/NetScaler LB</td>
</tr>
<tr>
<td></td>
<td>(WebService will be installed on all CAS array members.</td>
</tr>
<tr>
<td></td>
<td>Communication will be initiated with the</td>
</tr>
<tr>
<td></td>
<td>CAS Array name (CSPCLOUDVCA01), requests as such are load</td>
</tr>
<tr>
<td></td>
<td>balanced over the different CAS servers)</td>
</tr>
<tr>
<td>SQL. Database Services</td>
<td>Clustered SQL Server named instance</td>
</tr>
</tbody>
</table>
CloudPortal Services Manager Component requirements

CloudPortal Services Manager Provisioning Engine

The CPSM Provisioning engines is responsible for processing the provisioning request submitted accordingly to the technical business rules as exist within this component. An essential component within the provisioning work stream is Microsoft Message Queuing.

The front end applications submit the provisioning request into the message queue as exists within the Provisioning engine systems. A queue monitoring process monitors the queues; request messages that are retrieved from the queue are processed by the provisioning engine.

Every message goes through a provisioning flow called the rules. Rules define the actions to be taken for each provisioning request. All rules and actions are stored in the CPSM databases.

Rules and actions are customized according to the requirements

The provisioning engine server also hosts the Directory Webservice. The directory webservice is specifically for all AD services related actions.

Message Queues

Following Private Queues are created during the provisioning Engine installation:

- **CortexBulkRequest**: This queue is used when doing bulk provisioning. For example: Reprovisioning a customer and all his users.
- **CortexRequest**: All regular provisioning actions are sent to this queue
- **CortexResponse**: This queue is only used when using remote locations (remote Active Directory domains).
- **CortexUsageData**: Agents on different server send requests to this queue to gather usage information.
Message Structure

Each message consists of following properties:

- **Message Label**: This property defines what type of request is sent. Ex.: Customer Create, Customer Update, Customer Service Add, etc…

- **General Properties**: Because the cortex frontend can be used to manage different domains, messages sent from the frontend to the provisioning engine, must contain all necessary information like: Customer Name, Customer OU Name. An extract is shown below:

- **Service and location specific properties**: These properties vary depending on the service provisioned. For exchange it might mention the database names to be used, mailbox size, etc.
Provisioning Engine Hardware Configuration

The hardware estimates for the solution are based on the breadth of experience with providers servicing a subscriber base at or near 50,000 total users.

The deployment will use virtual servers to run the provisioning engine. The following table contains the specifications for the virtual provisioning engine server:

<table>
<thead>
<tr>
<th>Hardware Specification</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of virtual servers</td>
<td>2</td>
</tr>
<tr>
<td>CPU</td>
<td>4 Cores</td>
</tr>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
</tbody>
</table>
| Virtual NIC                    | 1 x NIC Zone 2 Network  
                                | 1 x NIC Heart beat network |
| System drive (C:)              | 100 GB        |

Provisioning Engine Software Configuration


The following Server Roles and Server Features are required:

- .NET Framework 3.5.1
- .NET Framework 4.0
- Power Shell 2.0 (default in Windows Server 2008 R2)
- Web Server
  - Application Development
    - ASP.NET
  - Security
    - Windows Authentication
  - Management Tools
    - IIS Management Console
    - IIS Management Scripts and Tools
    - IIS 6 Management Compatibility
    - IIS 6 Metabase Compatibility
- Message Queuing
  - Message Queuing Services
  - Message Queuing Server
- Remote Server Administration Tools
  - Role Administration Tools
  - AD DS and AD LDS Tools
- Telnet Client
- Windows PowerShell

**Database Services**

Database services are obtained from the private cloud platform through the default instance on CSPCLOUDVQS01.

The database service to comply with the following:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCPU</td>
<td>4 cores</td>
</tr>
<tr>
<td>Memory</td>
<td>16Gb</td>
</tr>
<tr>
<td>SQL Server version</td>
<td>SQL 2008 R2</td>
</tr>
<tr>
<td>Authentication</td>
<td>Mixed</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Enabled</td>
</tr>
<tr>
<td>Named Pipes</td>
<td>Enabled</td>
</tr>
<tr>
<td>IP Address</td>
<td>10.250.18.50</td>
</tr>
<tr>
<td>Port</td>
<td>1436</td>
</tr>
<tr>
<td>Disk space data files</td>
<td>60Gb</td>
</tr>
<tr>
<td>Disk space log files</td>
<td>20Gb</td>
</tr>
</tbody>
</table>

The following databases and users are created by CPSM:

<table>
<thead>
<tr>
<th>Database Name</th>
<th>Description</th>
<th>SQL User and Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSP</td>
<td>core database for customer and user information</td>
<td>CSPUser: dbowner</td>
</tr>
</tbody>
</table>
| CSPReports     | used for storing reporting data                           | CSPUser: dbowner  
CSPReportsUser: dbowner  
CortexProp: dbowner |
| ExchangeLogs   | used for storing Exchange information                      | CSPUser: dbowner  
ExchangeLogsUser: dbowner |

A number of SQL Jobs will be installed onto this server. These are related to the data collection processes for reporting purposes.

- Gather Daily Stats Data
Gather Monthly Stats Data

**Reporting Services**

Reporting services are installed on CPSM Provisioning engine CSPCLOUDPES01.

The CPSM reports are deployed on the reporting services machine CSPCLOUDPES01; the actual data is stored on the dedicated SQL instance on the central SQL cluster as described in the previous chapter.

CPSM will need to create an account for reporting services which needs to have administrative privileges on SQL Reporting Services.

**CloudPortal Services Manager Web Frontend Servers**

The CPSM User Interface Web Frontend serves are responsible to host the CPSM user interface web application as well to publish the provisioning API where the ADSync components will communicate with.

**Frontend Hardware Configuration**

The deployment uses virtual servers to host the frontend servers. The following table contains the specifications for the virtual frontend servers:

<table>
<thead>
<tr>
<th>Hardware Specification</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of virtual servers</td>
<td>2</td>
</tr>
<tr>
<td>CPU</td>
<td>4 Cores</td>
</tr>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td>Virtual NIC</td>
<td>1 x NIC</td>
</tr>
<tr>
<td>System drive (C:)</td>
<td>100 GB</td>
</tr>
</tbody>
</table>

**Software Configuration**


The following Server Roles and Server Features are required:

- .NET Framework 3.5.1
- .NET Framework 4.0
- Power Shell 2.0 (default in Windows Server 2008 R2)
- Web Server
  - Application Development
    - ASP.NET
  - Security
    - Basic Authentication
    - Windows Authentication
  - Management Tools
    - IIS Management Console
    - IIS Management Scripts and Tools
- Message Queuing
  - Message Queuing Services
  - Message Queuing Server
- Telnet Client
- Windows PowerShell
- Microsoft Report Viewer 2008 SP1 Components
- Microsoft SQL Server System CLR Types
- Microsoft SQL Server 2008 Management Objects

Service Offering integration

_CloudPortal Services Manager Exchange Web service_

Each Exchange Client Access Server will have a CloudPortal Services Manager web service installed. These web services are used by the CPSM solution to interact with the Microsoft Exchange environment for provisioning purposes.

The web services are load balanced through NetScaler and will be installed on the provisioning engine server.

The FQDN is CSPCLOUDVPE01.cspname.local

_Software Configuration_

The following software prerequisites are required:

- Microsoft Exchange 2010 SP1 Management Tools
- .Net Framework 4.0
## Scalability and Capacity planning

The table below provides a few sample scenarios with regards to capacity planning:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Scalability type</th>
<th>Hardware Requirements</th>
</tr>
</thead>
</table>
| **1** 100 - 1000 users | **Basic Setup for Hosted Exchange – Single Server Setup** | Laptop: One 2.0GHz Xeon processor (Dual Core) or equivalent  
Memory: 2 GB RAM, preferably 4 GB RAM  
Disk: 36 GB disk space |
| **2** 1000 - 5000 users | **Basic Setup for Hosted Exchange – Dual Server Setup (Separate SQL Server)** | **Database Server:**  
CPU: One 2.0 GHz Xeon processor (Dual Core) or equivalent  
Memory: 2 GB RAM, preferably 4 GB RAM  
Disk: 36 GB disk space  
**Web Server:**  
CPU: One 2.0 GHz processor.  
Memory: 1Gb RAM minimum, 2Gb Recommended  
Disk: 36 GB disk space |
| **3** 5000+ users | **Basic Setup for Hosted Exchange – Triple Server Setup (All Components on Separate Servers)** | **Database Server:**  
CPU: Two 2.0 GHz Xeon processor (Dual Core) or equivalent  
Memory: 4 GB RAM minimum  
Disk: 36 GB disk space  
**Web Server:**  
CPU: Two 2.0 GHz processors  
Memory: 2Gb RAM minimum  
Disk: 36 GB disk space  
**Provisioning Engine Server:**  
CPU: Two 2.0 GHz processors  
Memory: 2Gb RAM minimum  
Disk: 36 GB disk space |
| **4** 100 000+ User | **Advanced Setup** | **SQL Server Cluster:**  
2 or more SQL Servers.  
**Load balanced Web Servers:**  
2 or more Windows 2003/2008 Web servers.  
**Provisioning Server Cluster:**  
2 or more Clustered Windows Servers.  
Or  
Redundant Provisioning Server (Warm standby) |
Tenant premise to Service Provider Active Directory Synchronization

For those tenants that require synchronization with their on-premise AD, Citrix CloudPortal Services Manager ADSync utility can be employed to ensure consistency between the on-premise accounts and their CSP hosted counterparts.

The overall concept is summarized as follows:

- User object on premise identity information is synchronized through ADSync with related user object within the private cloud
- On premise password change occurrences are intercepted and replicated through ADSync to related user object within the private cloud
- New on premise user objects are provisioned by ADSync into the cloud environment. Within the cloud environment the user objects as is identified as a not activated object without any service offering applied
- Deletion of an on premise user object will result in deletion of the user object and it's assigned service offerings in the private cloud
- Resource mailboxes are treated in a similar concept as user objects.
- Synchronization direction will be from on premise into the private cloud
- Once the users are synchronized to the CSP cloud hosted AD, the CPSM Migration Tool will be used to import the migrated objects into CPSM.

CloudPortal Services Manager ADSync utility

The solution centers around a windows service “ADSync” that is deployed onto each domain controller in a tenants AD forest. As changes are made in the tenant’s own Active Directory, the changes are replicated across to the hosting environment using the standard CPSM XML based provisioning API.

CloudPortal Services Manager API Secure Requests

Requests are sent to the CPSM infrastructure using HTTPS. The CPSM secure API request utilizes a combination of a public/private key and a symmetric key (RSA and AES) to securely transfer data and credentials. This ensures the data cannot be intercepted or diverted to another source. The data in the request is also hashed (SHA1) to prevent unauthorized changes.

Authentication method used is Basic Authentication
CloudPortal Services Manager integration with ADSync

The CPSM user interface has been adapted to assist in the management and deployment of the ADSync utility as well as restricting the changes that can be made for synchronized users.

Users in CPSM that have been synchronized by the ADSync utility are flagged and the CPSM user interface will display non-editable user information. This is to avoid user information being updated in CPSM and then being overwritten by changes made via the customers Active Directory. User Services are still provisioned and managed through CPSM.

Installing ADSync on the On-Premise Domain Controllers

The ADSync utility is required to be installed on all on premise domain controllers. The component as such contains a password filter that runs within the Local Security Authority process of every Domain Controller in the domain. It intercepts all the password change events, the intercepted password will be replicated to the private cloud environment.
Citrix EdgeSight (monitoring, reporting and troubleshooting)

EdgeSight integration provides HDX monitoring and troubleshooting capabilities. Use of EdgeSight can also simplify Citrix CSP License reporting, for use in CSP billing systems as well as for their monthly license reporting.

The EdgeSight inherent multi-tenant architecture enables CSPs to delegate certain reporting and monitoring capabilities to their tenants.

Because this component is shared across the entire CSP infrastructure, the EdgeSight Server is integrated within the Management vLAN of the CSP Network. The CSP can grant EdgeSight web console access from any client or DaaS session. All traffic to and from the EdgeSight service is secured through the Firewall and vLAN configurations as discussed at the beginning of this document.

CSP-specific report templates are available for download from the Citrix Developer Network CSP community site at http://community.citrix.com/p/csp#.

For more information you can also download the Citrix Service Providers Guide to using Citrix EdgeSight from http://www.citrix.com/skb/articles/RDY2947.
Conclusion

Companies of all sizes are looking for a smarter approach to managing the applications and data they use to run their business. More devices, more applications and more places to work means business owners have to spend an increasing amount of time on IT. Citrix Service Providers can shift the focus for their subscribers back to where it matters the most—growing the business. By offering a bundle of applications, desktops, and IT services, customers get what they want in a familiar, pay-as-you-go subscription model.

This Citrix CSP Reference Architecture represents a common view of those best practices as recommended by Citrix and employed by some of today’s most successful Citrix Service Providers. With core architectural innovations across products and the Citrix eco-system, a reliable, scalable, and high-performance solution is now available for those CSPs wanting to provide monthly subscriptions to Windows based application and desktop services. The CSP licensing program and product innovations provide the foundation for aggregating thousands of servers, capable of servicing millions of active subscribers across multiple tenants, into a single management scope. Ultimately this provides a solution that enables Citrix Service Providers to build flexible, scalable, and cost effective solutions and services to meet their customers’ needs at an attractive price.
Appendix A: Online Resources

The Citrix Service Provider Toolkit
http://community.citrix.com/kits/#/kit/734024

Top 10 Considerations for Delivering Desktops in the Cloud
http://support.citrix.com/article/CTX128899

XenDesktop 5 Modular Reference Architecture
http://support.citrix.com/article/CTX133162

How to Deliver a Cloud Desktop using XenApp 6

Scaling Big – SaaS and DaaS Deployments for Citrix Service Providers
http://support.citrix.com/article/CTX129106

Citrix Service Providers Guide to using Citrix EdgeSight
http://www.citrix.com/skb/articles/RDY2947

App Orchestration for Service Providers
http://www.citrix.com/skb/articles/RDY6234

Secure Multi-tenant Desktop as a Service Access with NetScaler VPX
http://www.citrix.com/skb/articles/RDY4105

XenApp 6.5 Scaling Capabilities for multi-tenant DaaS
http://www.citrix.com/skb/articles/RDY5921
About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) transforms how businesses and IT work and people collaborate in the cloud era. With market-leading cloud, collaboration, networking and virtualization technologies, Citrix powers mobile workstyles and cloud services, making complex enterprise IT simpler and more accessible for 260,000 organizations. Citrix products touch 75 percent of Internet users each day and it partners with more than 10,000 companies in 100 countries. Annual revenue in 2011 was $2.21 billion. Learn more at www.citrix.com.

©2012 Citrix Systems, Inc. All rights reserved. Branch Repeater™, Citrix®, Citrix Access Gateway™, Citrix Merchandising™ Server, Citrix Provisioning Services™, Citrix Receiver™, EdgeSight®, HDX™, ICA®, NetScaler®, VPX™, XenApp™, XenDesktop®, and XenServer® are trademarks or registered trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. Xen® is a trademark of Citrix Systems, Inc. managed on behalf of Xen.org, and may be registered in the U.S. Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.