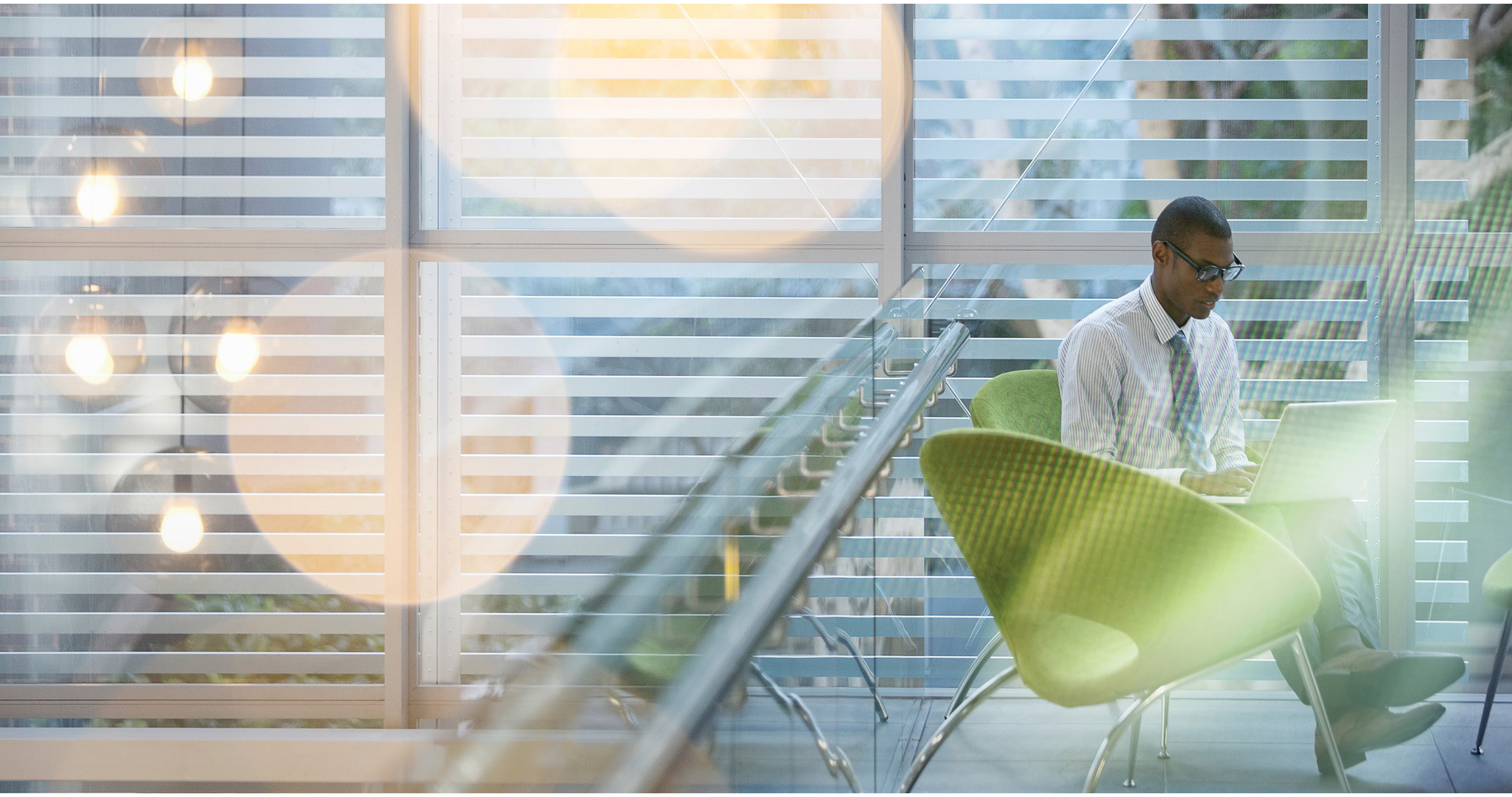
White Paper



Citrix Service Provider Reference Architecture on Microsoft CloudOS

Leveraging Citrix and Microsoft Capabilities to Deliver Applications, Desktops, and Data as a Service

Table of Contents

Executive Summary

The Citrix Service Provider Reference Architecture enables a new generation of multi-tenant application and desktop cloud services. Because the reference architecture uses a cloud service delivery approach, it scales easily while increasing workstyle mobility for an expanding user base. The architecture enables the delivery of Microsoft® Windows® applications and desktops on a pay-as-you-go basis from the Citrix Service Provider's hosted cloud and tenant on premise datacenters and branch offices, allowing tenants to move capital and management expenses to an operational cost model. Citrix Service Providers can take advantage of Microsoft and Citrix Service Provider licensing programs to deliver cost-effective services based on subscriber usage.

The reference architecture is easily adapted to meet specific provider and subscriber requirements, allowing Citrix® Service Providers to deliver a comprehensive set of Desktop-as-a-Service (DaaS) offerings and price points while simplifying management and scalability. All of this adds up to a cloud-ready services model that enables lower infrastructure and administrative costs, greater customer satisfaction, and increased business success.

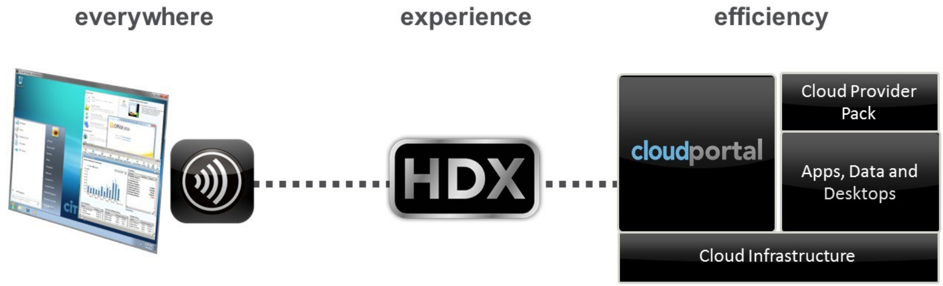


Figure 1: Citrix Service Provider – Conceptual Line of Sight

What's New in This Reference Architecture

The Citrix Service Provider Reference Architecture enables Citrix Service Providers to deliver Windows applications, desktops, and data as Desktop as a Service (DaaS) through an integrated set of Citrix and partner technologies:

- Citrix XenDesktop® unifies the delivery of hosted applications and desktops (Citrix XenApp®) with virtual desktops (XenDesktop) using a single architecture and management experience. Because of advancements in HDX™ technologies, this XenDesktop release improves the user experience, especially for mobile users on various endpoint devices (e.g., smartphones, tablets, laptops, PCs, or Macs) across diverse bandwidth connections.
- The Citrix Cloud Provider Pack (CPP) contains several Citrix Service Provider-specific enhancements that enable more effective multi-tenant management of the Citrix DaaS solution. Two key components of this CPP release are:
    - Citrix App Orchestration allows Citrix Service Providers to automate the delivery of applications and desktops in multi-tenant environments across multiple XenDesktop sites or XenApp farms, Microsoft Active Directory domains, and datacenters. App Orchestration enables Citrix Service Providers to build offerings with a defined set of apps, desktops, and resources accessible to tenant users that are selected from an application storefront.
    - Citrix CloudPortal™ Services Manager (CPSM) provides an easy-to-use web portal that helps Citrix Service Providers manage service delivery and subscriber offerings, simplifying delivery across datacenters.

The architecture makes application and desktop services available to users of any Citrix Receiver™ enabled endpoint device over secured Internet connections using Citrix NetScaler®. For subscriber locations that aggregate a number of endpoints in a single setting, such as a small retail business, accounting office, or medical clinic, Citrix Branch Repeater™ can be added to provide a high-definition user experience to multiple endpoints over an optimized network connection. The administrative simplicity provided through the integrated Citrix software components allows subscriber volumes at very large scale to be managed with a relatively modest number of Citrix Service Provider administrators and tenant on-boarding personnel as compared to other models.

Citrix Solutions Lab Implementation

The architecture is unique in its scalability and its ability to flex to meet a broad range of multi-tenancy requirements. In the Citrix Solutions Lab, test engineers built out a sample implementation to model real-world scenarios and best practice. While every deployment varies to meet specific tenant and subscriber requirements, the lab environment included ten sample tenants employing two types of multi-tenancy isolation models (for more detailed descriptions of these models, see the discussion on pages 61 and 62):

- **Tenants 1 and 2: Private Delivery Site isolation.** Private Delivery Site isolation dedicates resources exclusively to a single tenant. In the lab build-out, each Private Delivery Site tenant accesses services on machines and networks that are completely isolated from those of other tenants. This isolation model is appropriate for tenants that need the highest level of data and infrastructure isolation.

- **Tenants 3-9: Private Delivery Group/Shared Delivery Site isolation.** The Private Delivery Group/Shared Delivery Site isolation model uses private Delivery Groups to isolate application and desktop workers, but the XenDesktop deployment, managed by the Citrix Service Provider only, is implemented using a shared site. This model presents a lower cost of service delivery to the Citrix Service Provider (and as should follow, to the tenants) since management infrastructure components and expenses are more densely distributed across multiple tenants.
- **Tenant 10: Private Delivery Group/Shared Delivery Site isolation.** Tenant 10 uses the same Delivery Group isolation model as Tenants 3 through 9, taking advantage of shared resources in the Citrix Service Provider datacenter. However, this tenant represents a mixed use case in which a dedicated VLAN and other isolation mechanisms are employed to customize network level capabilities and tenant Service Level Agreements (SLAs). Tenant 10 capabilities and details will be provided in an addendum to this document.

The different isolation models are described in more detail in Appendix A: Multi-Tenancy Design Considerations. As described in Appendix B: Lab Implementation and Configuration Details, lab tenants were configured with different sized user populations and workloads for testing. The remainder of this document details the reference architecture and deployment considerations, and is intended to help Citrix Service Providers to put the solution into practice.

Note: This document may reference specific products that were used to deploy this reference architecture in the Citrix Solutions Lab. The details of any particular third-party product are not provided as a product endorsement or recommendation. These details are provided solely as a reference regarding the hardware and software configuration used in the lab environment, and in practice service providers can implement comparable products. Appendix B summarizes the hardware, software, and configurations used in the lab environment.

Introduction and Scope

This document provides architectural guidance for Citrix Service Providers that supply application, desktop, and data services to subscribers. The architecture can scale from a small subscriber base of a few tenants with few users to one that delivers millions of active application and desktop sessions for thousands of tenants across multiple geographies.

The Citrix Service Provider Reference Architecture can be implemented within virtually any cloud or datacenter infrastructure. For this series of tests, Citrix chose to implement the solution as an extension of Microsoft Windows Server 2012 R2 with Hyper-V and Microsoft System Center Virtual Machine Manager (SCVMM) 2012 R2. The solution documented in the Microsoft "Desktop Hosting Reference Architecture Guide" was used as an additional reference for this Citrix solution. By deploying Citrix software components on a cloud services infrastructure, Citrix Service Providers can construct an environment to deliver multi-tenant desktop, application, and data services to multiple tenants safely, securely, cost-effectively, and with industry-recognized best-in-class performance.

Citrix Software Integration with Microsoft Technologies

This is the fourth revision in the evolution of the Citrix Service Provider Reference Architecture. With this revision, the following Citrix product versions (as tested in the Solutions Lab) bring new capabilities:

- Citrix XenDesktop 7.1 unifies the delivery of hosted application and desktop sessions (via RDS) with the ability to deliver full virtual desktops (VDI) through a single control plane and management interface. Information for experienced XenApp administrators is available here: http://support.citrix.com/proddocs/topic/xendesktop-71/cds-overview-info-previous-xa-customers.html.
- Citrix App Orchestration 2.0 enables Citrix Service Providers to automate and manage, at high scale, the delivery of DaaS offerings in multi-tenant environments.
- CloudPortal Services Manager 11.0.1 supplies a portal to manage service delivery and subscriber offerings. It supports delegated management roles that enable down-channel partners and tenant administrators to self-provision services and monitor provisioning requests.

Note: At the time of this document's publication, XenApp 7.5, XenDesktop 7.5, and App Orchestration 2.5 have been released. An addendum to this reference architecture document will provide additional details of deploying with these newer releases.

In addition to the secure-by-design capabilities within the Citrix products, specific design and techniques for the integration of Citrix software components with Microsoft infrastructure, Hyper-V virtual servers, and Active Directory (AD) domains are key factors for a secure and scalable Citrix Service Provider solution. In this reference architecture, App Orchestration and CloudPortal Services Manager map to individual tenant-specific Organization Units (OUs) within a single Microsoft Active Directory Domain or alternatively to individual tenant-specific domains. Guest VMs are implemented in Hyper-V and managed by Microsoft System Center Virtual Machine Manager (SCVMM). Virtual network separation, augmented by Hyper-V Virtual Switch Extended Access Control Lists (ACLs), helps to enforce isolation between tenants. Tenant partitions and services are managed through centralized dashboards and monitoring systems from Citrix, Microsoft, and the hardware and storage vendors used for these tests.

A sample multi-tenant implementation as built within the Citrix Solutions Lab, based on Citrix XenDesktop Hosted Shared Desktops and Server VDI, Citrix App Orchestration, and Citrix CloudPortal Services Manager is referenced throughout this document.

High Availability (HA) capabilities are inherent within many components of the architecture. For example, software servers are deployed in Hyper-V clusters to create N+1 configurations, and Citrix NetScaler is used for client access and load balancing. Although beyond the scope of this architecture, Disaster Recovery (DR) designs are possible using Citrix NetScaler, Microsoft Hyper-V, and Microsoft System Center Data Protection Manager. Further details about HA and DR options are in the documentation for the respective components at http://www.citrix.com/edocs and http://technet.microsoft.com/en-us/library/cc507089.aspx.

Core Architectural Concepts and Features

Core concepts and features — such as endpoint ubiquity, subscription-based licensing, multi-tenancy, single instance management, and dynamic assembly — provide much of the simplified scalability and high level of user acceptance of the Citrix Service Provider model.

Endpoint ubiquity

Endpoint ubiquity enables wide adoption of desktop services that deliver high performance graphics and peripheral I/O capabilities —on any device over any network. Citrix Receiver enables this ubiquity through support for virtually every popular device and platform in the market and optimizations for low-bandwidth mobile networks. It enables a high-definition experience for users that increases acceptance and helps to grow demand.

Subscription-based licensing

Citrix Service Providers typically provide a pay-per-use or pay-per-month mechanism that enables businesses to treat desktop acquisition and maintenance as an operational expense rather than incurring the capital expense of building infrastructure. Citrix Service Providers can realize economies of scale since the solution accommodates multi-tenancy, dynamic assembly, and single instance management, which together create an attractive solution that keeps month-to-month costs relatively low for both the subscriber and the service provider.

To supply providers with a more flexible cost structure, Citrix Service Providers can take advantage of special Citrix and Microsoft licensing agreements:

- **The Citrix Service Provider program** is designed for service providers that provide hosted application, data, and desktop cloud services to end-user customers. The program extends the “right to use” for Citrix products to Citrix Service Providers, creating the core delivery infrastructure and giving providers the flexibility of a monthly “active subscriber” pricing and licensing model. Citrix Service Providers always have access to the current product versions in the program and pay only for actual end-user usage recorded in the previous calendar month.
- **The Microsoft Service Provider Licensing Agreement (SPLA)** is the Microsoft service provider program. SPLA allows providers with a hosted offering to license Microsoft products on a monthly basis to their end-user 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. (For details on the Microsoft SPLA program, see http://www.microsoft.com/hosting/en/us/licensing/splabenefits.aspx.)

Multi-tenancy

Multi-tenancy capabilities provide economies of scale on a single infrastructure while providing the required isolation and data protection. Providers can make trade-offs regarding price and features to meet individual tenant requirements. Appendix A: Multi-Tenancy Design Considerations describes the multi-tenancy isolation models enabled in this architecture, which are also depicted in Figure 2.

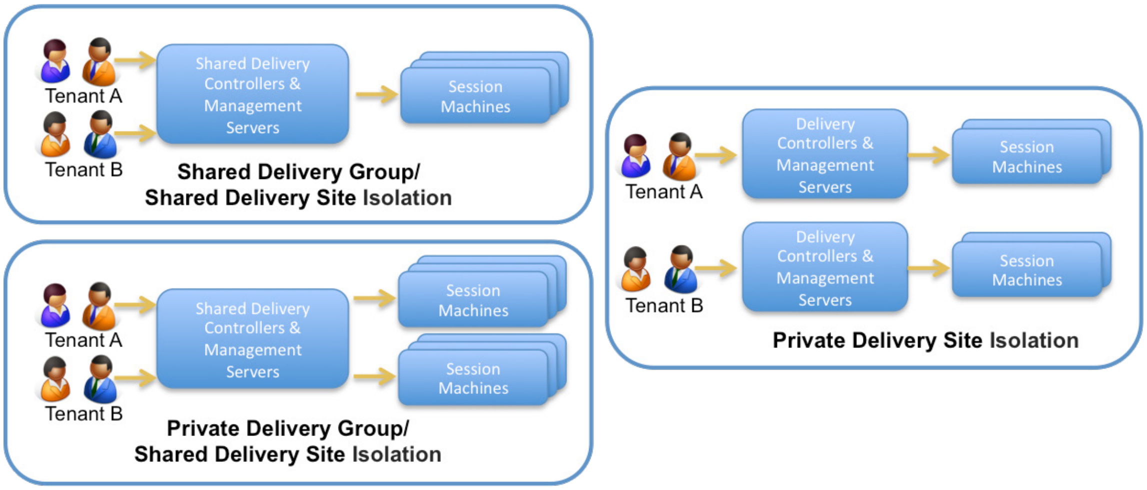

Tenant A
Tenant B
Shared Delivery Controllers & Management Servers
Session Machines
Shared Delivery Group/
Shared Delivery Site Isolation
Tenant A
Tenant B
Shared Delivery Controllers & Management Servers
Session Machines
Session Machines
Private Delivery Group/
Shared Delivery Site Isolation
Tenant A
Delivery Controllers & Management Servers
Session Machines
Tenant B
Delivery Controllers & Management Servers
Session Machines
Private Delivery Site Isolation

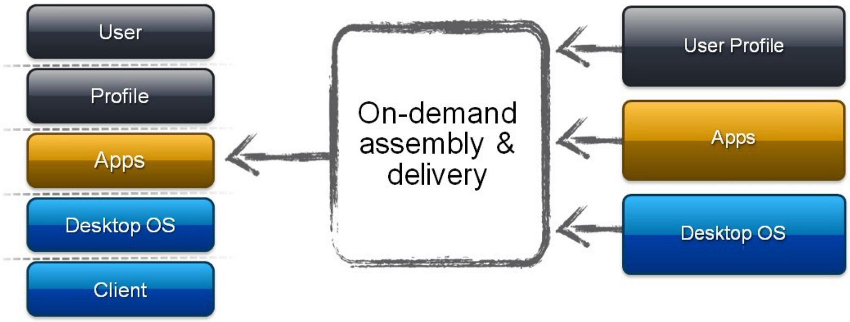
Figure 2: Multi-Tenancy Isolation Models

Single instance management

Single instance management provides the most efficient lifecycle maintenance of operating system workloads and Microsoft Windows-based applications. By creating a single read-only image of each critical workload and then streaming that workload onto virtual machines, Citrix Service Providers can maintain thousands of execution environments from a single source, requiring only a reboot of the individual machine to deploy the latest image.

Dynamic assembly

Dynamic assembly of operating system, application, and user personalization settings on a per-user, per-tenant basis enables efficient management and massive scale for DaaS services. Single instance images are assembled based on tenant-subscribed services. Images are dynamically assembled in different configurations for each tenant and user according to individual configuration and service level agreements.



A Multi-Tenant DaaS Architecture

Figure 3 shows the reference architecture as it might be integrated into an existing Citrix Service Provider environment serving multiple tenants. Network separation is one element in providing isolation between tenants.

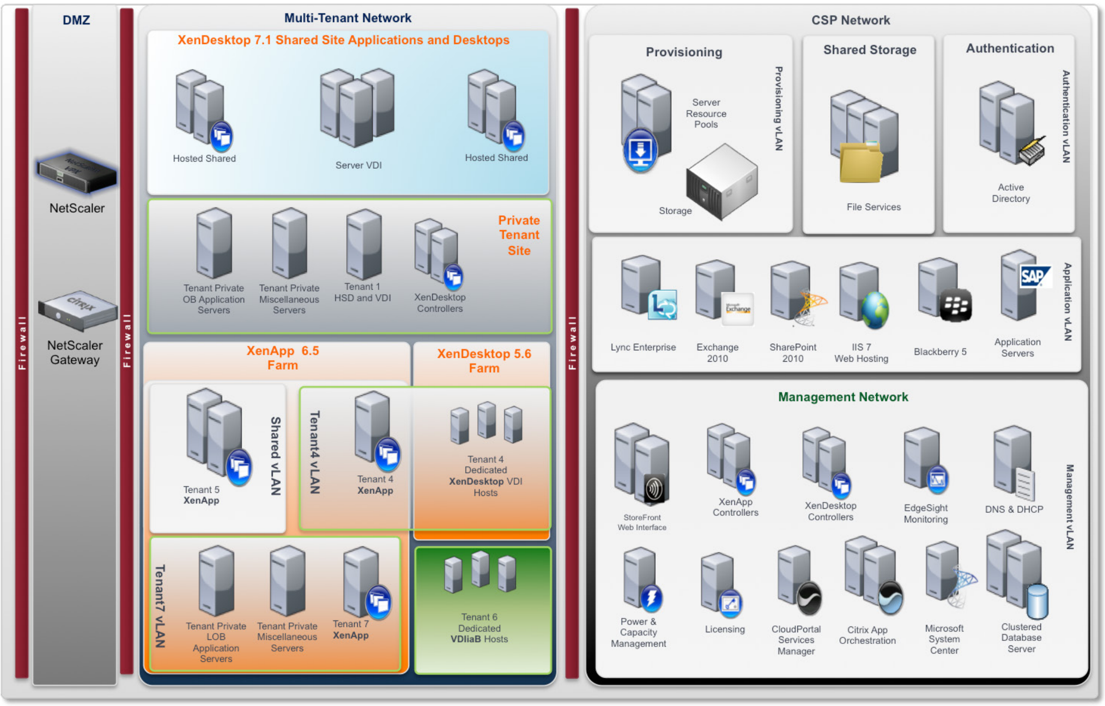


Figure 3: Citrix Service Provider Reference Architecture – Sample Implementation

The reference architecture encompasses the delivery of both hosted shared desktops and applications via RDS and hosted virtual desktops (VDI). These can both be deployed with XenDesktop 7.1, which can co-exist with earlier releases (e.g., XenApp 6.5 for RDS and XenDesktop 5.6 for VDI). Citrix XenDesktop 7.1 is based on the FlexCast® Management Architecture (FMA), which supplies a single set of administrative interfaces to deploy both paradigms. Unlike previous Citrix software releases that required separate Citrix XenApp and XenDesktop farms, this new release allows administrators to deploy a single XenDesktop infrastructure and use the same management tools and policies for mixed desktop and application session machines.

Citrix recommends that if you continue running deployments of past versions of XenApp or XenDesktop, you run them in parallel with the XenDesktop 7.1 site and continue running the management consoles with each release for that site. For administrators familiar with deploying XenApp, it may be helpful to read "Important information for XenApp administrators" to understand key differences between features and terminology for earlier XenApp releases and XenDesktop 7.1.

There are significant advantages for Citrix Service Providers to deploy this reference architecture using Citrix App Orchestration and CloudPortal Services Manager software. App Orchestration enables Citrix Service Providers to automate the delivery of applications and desktops in a Citrix prescribed multi-tenant environment across multiple products, product versions, XenDesktop sites, and datacenters. By deploying CloudPortal Services Manager in addition to App Orchestration, providers can more efficiently provision desktop, application, and data services to their tenants. Optionally CloudPortal

Service Manager may be used to provide a level of delegated self-service provisioning for tenants. App Orchestration and CloudPortal Services Manager technologies help Citrix Service Providers deliver applications and desktops and other services quickly and efficiently, allowing them to scale to support new tenants and more users with minimal additional administrative resources.

Extensions to the Citrix Service Provider Reference Architecture

Citrix Service Providers can add the following Citrix products to the reference architecture to enable additional offerings and provide a full complement of Citrix Mobile Workspace capabilities:

- **Citrix XenMobile**®. Citrix XenMobile is a comprehensive solution to manage mobile devices, apps, and data. Users have single-click access to all of their mobile, SaaS, and Windows apps from a unified corporate app store, including seamlessly integrated email, browser, data sharing, and support apps. IT gains control over mobile devices with full configuration, security, provisioning, and support capabilities. More information is available at http://www.citrix.com/products/xenmobile/overview.html.
- **Citrix ShareFile**®. Citrix ShareFile is an enterprise "follow-me" data solution that enables IT to deliver robust data sharing and sync services to meet collaboration needs while enforcing data security requirements. By making follow-me data a seamless and intuitive part of every user's environment, ShareFile improves productivity for a highly mobile workforce. For more information, see http://www.citrix.com/products/sharefile/overview.html.

Architectural Modules

As shown in Figure 4, the Citrix Service Provider Reference Architecture can be logically divided into four architectural modules: (1) Infrastructure-as-a-Service (IaaS), (2) Multi-Tenant Citrix Farms and Sites, (3) Dashboards and Management, and (4) Endpoints and Offices. The modules are introduced below. Subsequent sections discuss implementation details for the first three modules.

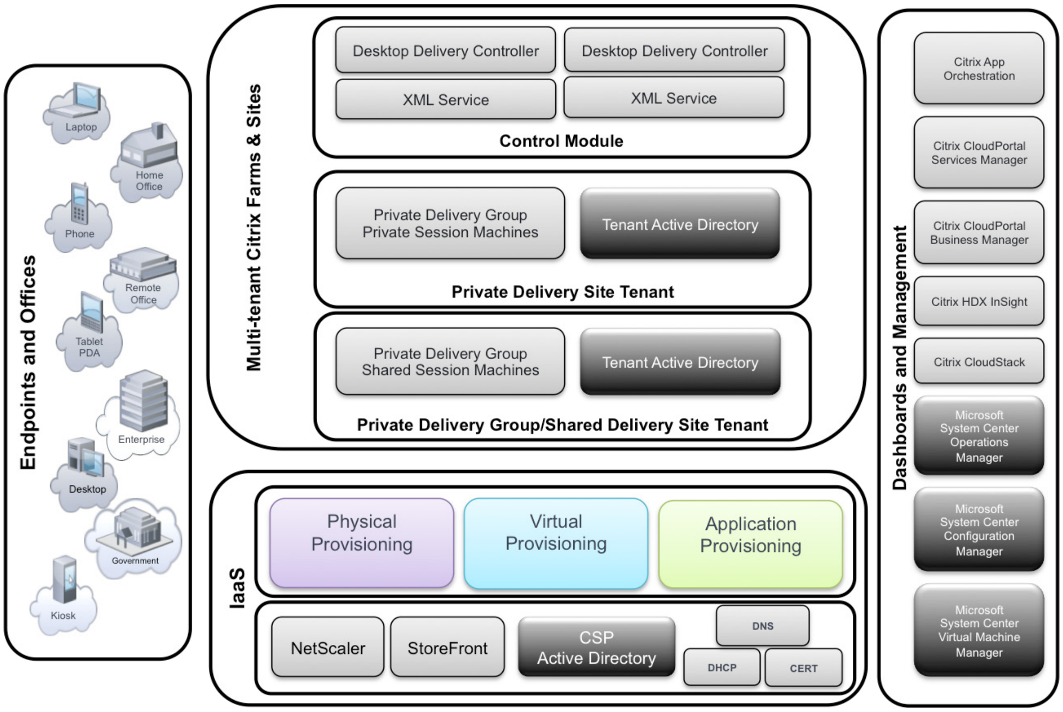

Endpoints and Offices
Laptop
Home Office
Phone
Remote Office
Tablet PDA
Enterprise
Desktop
Government
Kiosk
Multi-tenant Citrix Farms & Sites
Desktop Delivery Controller
Desktop Delivery Controller
XML Service
XML Service
Control Module
Private Delivery Group Private Session Machines
Tenant Active Directory
Private Delivery Site Tenant
Private Delivery Group Shared Session Machines
Tenant Active Directory
Private Delivery Group/Shared Delivery Site Tenant
IaaS
Physical Provisioning
Virtual Provisioning
Application Provisioning
NetScaler
StoreFront
CSP Active Directory
DNS
DHCP
CERT
Dashboards and Management
Citrix App Orchestration
Citrix CloudPortal Services Manager
Citrix CloudPortal Business Manager
Citrix HDX InSight
Citrix CloudStack
Microsoft System Center Operations Manager
Microsoft System Center Configuration Manager
Microsoft System Center Virtual Machine Manager

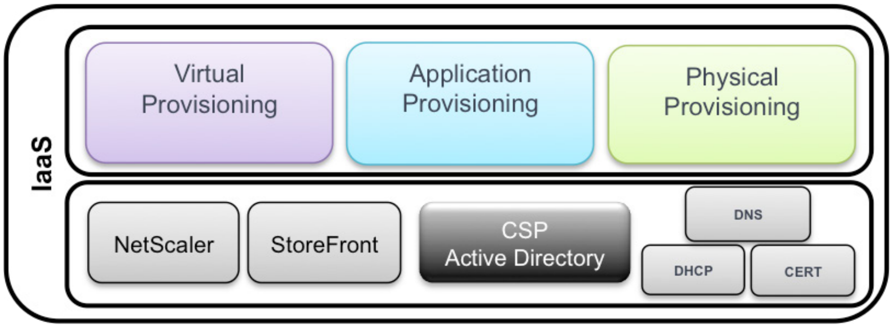
Figure 4: Four Logical Modules of Citrix Service Provider Reference Architecture

Infrastructure-as-a-Service (IaaS)

The foundation of the architecture is the Infrastructure-as-a-Service (IaaS) module, which is responsible for network, authentication, and provisioning functions. It has two sub-layers:

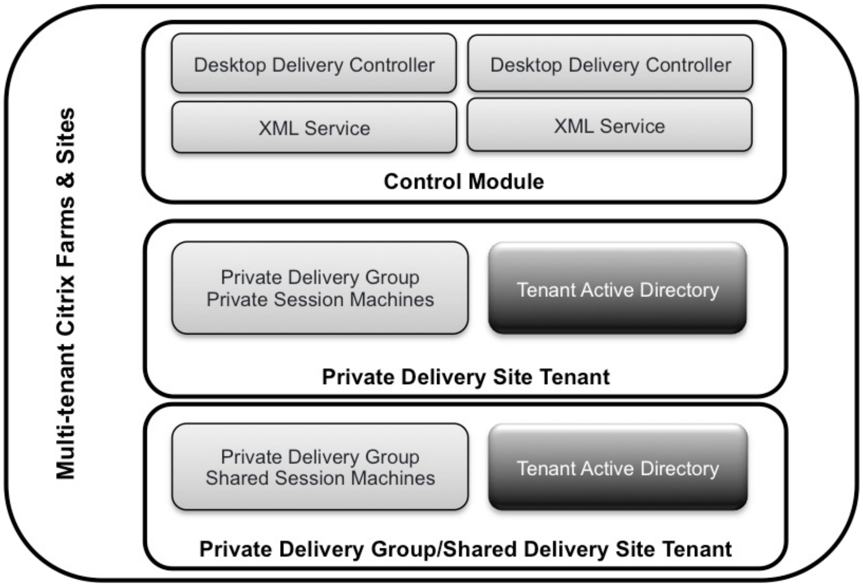
- Network infrastructure, including the implementation of Active Directory domains
- Provisioning infrastructure, including virtual, application, and physical provisioning

The IaaS module controls the system-wide network configuration, forest-level Active Directory management, remote access, and all layers of provisioning. Section 3 gives design considerations for the IaaS module.



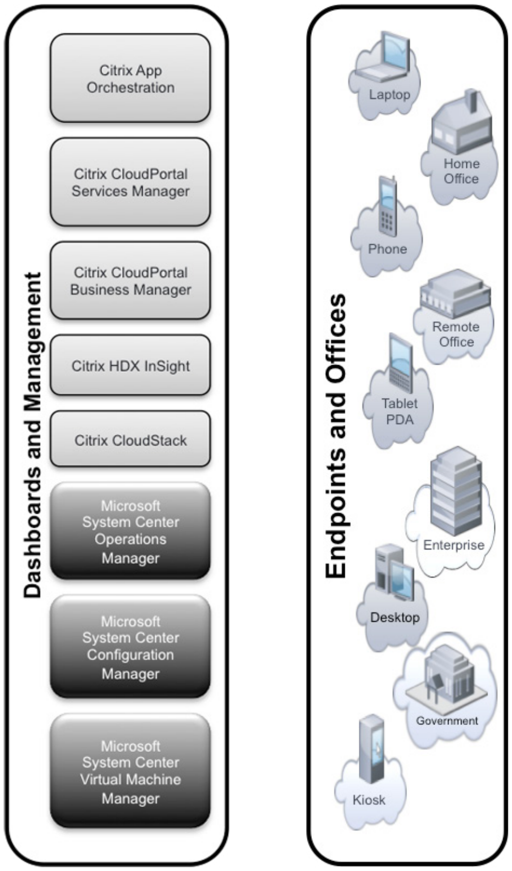
Multi-Tenant Citrix Farms and Sites

The Multi-Tenant Citrix Farms and Sites module is the core component of the service provider datacenter — this logical block controls application and desktop delivery within the multi-tenant architecture. (Note that in the unified XenDesktop 7.1 release, a “site” rather than a “farm” is the main XenDesktop environment consisting of Delivery Controllers and a database used to deliver both XenApp and XenDesktop services.) Within a multi-tenant datacenter, applications and desktops are virtualized and subscriber partitions and Active Directory boundaries are defined, while centralized XenDesktop Delivery Controllers govern application and desktop delivery across tenants. Section 4 discusses implementation details for this module.


Multi-tenant Citrix Farms & Sites
Desktop Delivery Controller
Desktop Delivery Controller
XML Service
XML Service
Control Module
Private Delivery Group Private Session Machines
Tenant Active Directory
Private Delivery Site Tenant
Private Delivery Group Shared Session Machines
Tenant Active Directory
Private Delivery Group/Shared Delivery Site Tenant

Dashboards and Cloud Platform Management

To successfully manage a service provider network, administrators need effective tools that are simple to use and scale efficiently as they add new tenants. Citrix App Orchestration and Citrix CloudPortal Services Manager enable a unified view across the entire infrastructure, across multiple datacenters, XenDesktop and XenApp 6.5 sites, and servers. This end-to-end view gives providers the detailed information and wide spectrum of control necessary to provision applications and quickly and maintain service level agreements for subscribers. Additional tools such as HDX Insight™ and the Citrix Usage Collector also facilitate ease of management. Section 5 describes App Orchestration, CloudPortal Services Manager, and other components for effective and scalable management of the Citrix Service Provider environment.


Dashboards and Management
Citrix App Orchestration
Citrix CloudPortal Services Manager
Citrix CloudPortal Business Manager
Citrix HDX InSight
Citrix CloudStack
Microsoft System Center Operations Manager
Microsoft System Center Configuration Manager
Microsoft System Center Virtual Machine Manager
Endpoints and Offices
Laptop
Home Office
Phone
Remote Office
Tablet PDA
Enterprise
Desktop
Government
Kiosk

Endpoints and Offices

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

With Citrix Receiver, Citrix Service Providers 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, Software-as-a-Service (SaaS), and native mobile applications.

With the introduction of Citrix's next-generation seamless application capabilities, applications that must execute on the endpoint device can now be presented within a user's cloud-hosted desktop. This capability enables 100% application compatibility within the Citrix Service Provider solution while also providing a smooth transition over time for application migrations from legacy endpoints and datacenters into the Citrix Service Provider hosted datacenter.

Infrastructure Module Deployment Considerations

This section discusses architectural considerations for the IaaS module as tested in the Citrix Solutions Lab implementation — the infrastructure layer that supports the reference architecture. The IaaS foundation encompasses the lowest layer of the design, starting with the physical machines and networks and ending with the virtual and application provisioning designs.

Building a Cloud Infrastructure on Microsoft Technologies

At the infrastructure layer, the Citrix Service Provider Reference Architecture complements the Microsoft guidelines for building infrastructure for the delivery of RDS Session Host delivery of Windows desktops. The Microsoft "Desktop Hosting Reference Architecture Guide" (http://www.microsoft.com/en-us/download/details.aspx?id=39285) discusses key Microsoft technologies enabling hosted applications and desktops.

The Microsoft guide describes a 1500-seat solution targeted at cloud providers who deliver services via the Microsoft Service Provider Licensing Agreement (SPLA) program. The document guides the implementation of a desktop hosting service that leverages Microsoft technologies including Windows Server 2012 Remote Desktop Session (RDS), Microsoft Active Directory services, Microsoft Windows System Center Virtual Machine Manager (SCVMM), and Windows Server 2012 with Hyper-V.

The Microsoft infrastructure design features three discrete layers: a physical layer, a virtualization layer, and a service layer. Hyper-V virtualization masks the specific server and networking hardware in the physical layer. Hyper-V servers host the required Windows Server 2012 operating system instances needed for storage virtualization and Hyper-V clustering support. At the service layer, the virtual machine instances, virtual subnets, and virtual storage support the services for each tenant as well as the provider's management and perimeter services.

This Citrix Service Provider Reference Architecture builds on these same concepts and technologies in its underlying Infrastructure-as-a-Service (IaaS) layer. These same concepts, enabled by Citrix design and testing on the Microsoft CloudOS platform, are a model found in other infrastructure enabling solutions like Citrix CloudPlatform, or public clouds (like Microsoft Azure and others) that have been the foundation for successful Citrix-based DaaS services — some for several years at the time of this revision.

Implementing the IaaS Module

As in the Microsoft reference architecture guide, Microsoft Hyper-V virtualization hides the details of the particular infrastructure hardware and networking components, and provides clusters of virtual machines to support the hosted desktop and application workloads.

Physical Provisioning and Infrastructure Components

The Citrix Solutions Lab used the following components to implement the reference architecture. Specific offerings are mentioned solely as examples and Citrix Service Providers can implement comparable products.

Server Hardware

The following types of physical servers were used to host the entire solution infrastructure:

- For virtualized servers hosting infrastructure control layer workloads (Microsoft AD, Microsoft System Center Virtual Machine Manager (SCVMM), Hyper-V Clusters, Scale-Out File Server Cluster): Eleven dual-socketed, quad-core Intel blade servers, such as HP BL460c G8 Blade Servers with Intel Xeon E5-2670 processors (2.60GHz, 8-core, 20MB)
- For virtualized servers hosting application and desktop workloads: 27 dual-socketed, quad-core Intel servers, such as HP BL460c G8 Blade Servers with Intel Xeon E5-2670 processors (2.60GHz, 8-core, 20MB)
- For virtualized servers hosting infrastructure client layer workloads: 22 dual-socketed, quad-core Intel servers, such as HP BL460c G7 Blade Servers with Intel Xeon X5650 processors (2.67GHz, 6-core, 12MB)

Networking Components

The following networking components were used:

- Switch chassis enabling Layer 3 routing and firewall between VLANs, such as Cisco Nexus 7010K
- Core switch for the Storage Network, such as Cisco Nexus 7010K
- VLAN edge switches, such as Cisco Nexus 7010K

The Citrix NetScaler, and Gateway designs are discussed later in this document (see page 38).

Storage Configuration

In a Citrix Service Provider environment, the availability and performance of the storage infrastructure are critical because storage outages or performance issues can impact thousands of users. Thus, the storage architecture must provide a level of availability and performance that is typically deployed to support business-critical applications. Citrix recommends that Citrix Service Providers choose a storage vendor that has software and hardware solutions to address required availability and performance requirements for large, scalable Citrix application and desktop delivery environments.

The Citrix Solutions Lab implementation used EMC VNX7600 unified storage behind a Microsoft Scale-Out File Server (SOFS) Cluster. As shown in Figure 5, clustered file servers convert iSCSI LUNs into CIFS shares, which are created and presented to Hyper-V as storage repositories. Link aggregation (based on Link Aggregation Control Protocol, LACP) enables a high availability storage design; it allows Ethernet ports from the same host to connect to the same switch, creating a virtual link with multiple IP addresses and providing redundancy for storage access.

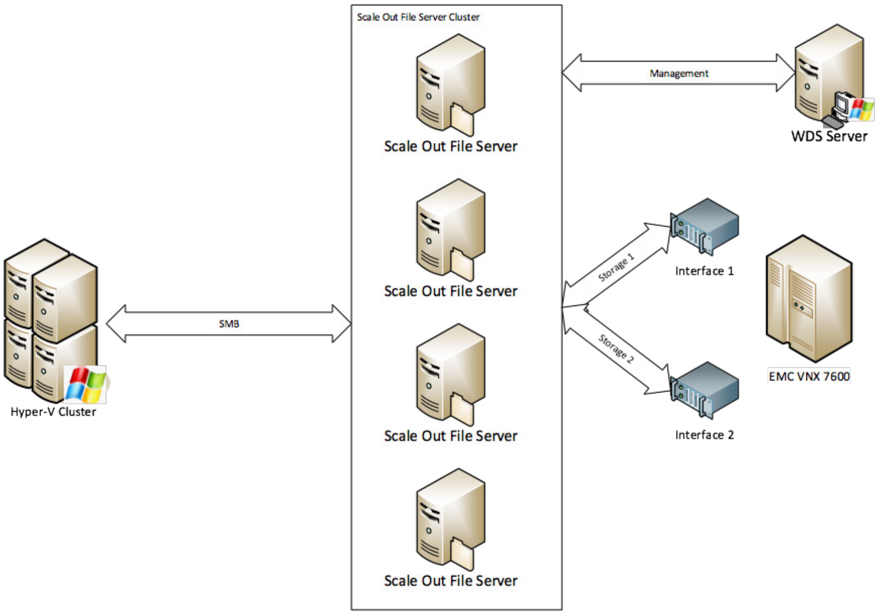


Figure 5: Sample storage configuration

Network Boundaries and VLANs

To configure a multi-tenant DaaS solution, the reference architecture defines several secured network zones. These provide tight security at critical boundaries between the management layers and tenant partitions. Figure 6 depicts the zones and networks: the Demilitarized Zone (DMZ), the multi-tenant network, and the Citrix Service Provider network. The figure also depicts VLANs in each network group.

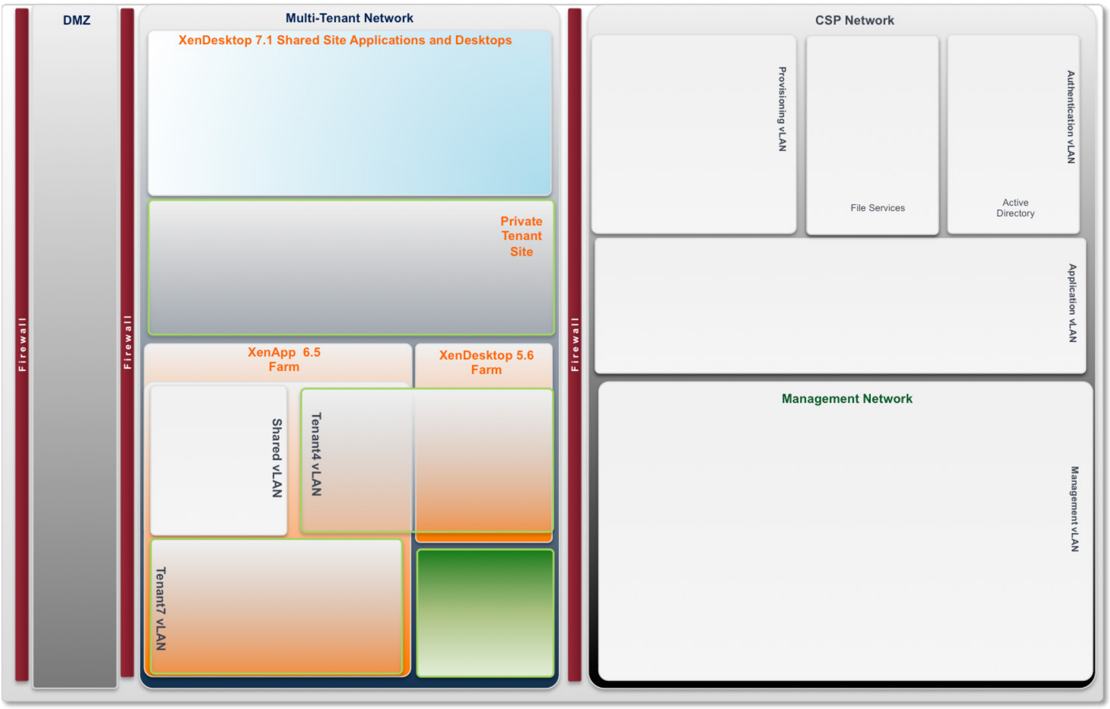
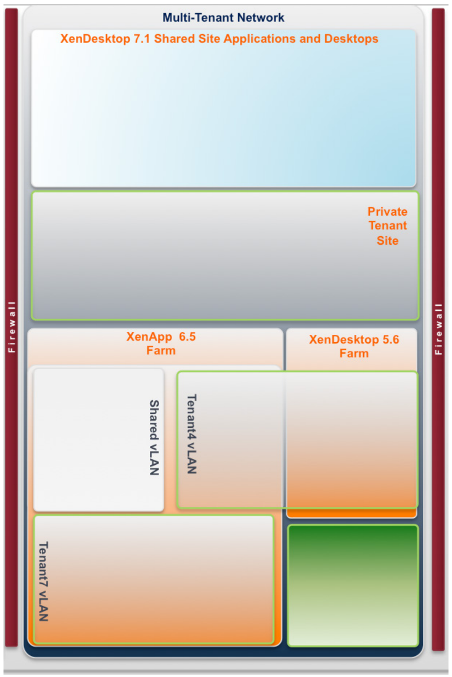


Figure 6: Citrix Service Provider Reference Implementation – Network Boundaries

DMZ - Demilitarized zone

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



Multi-tenant network

The multi-tenant network is behind the DMZ and further isolated from the Citrix Service Provider network by a firewall. The firewall ensures that management communications flow between the Citrix Service Provider and tenant networks in a manner that promotes the various multi-tenant isolation levels.

The multi-tenant network is implemented as separate VLANs:

- **Tenant 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 Citrix Service Provider.
- **Shared Tenant VLAN:** This VLAN presents a single network segment to XenDesktop and XenApp servers for tenants that do not require the security that a separate VLAN provides. 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. Service providers can potentially pass these savings to the subscriber.

Citrix Service Provider network

The Citrix Service Provider network hosts all of the Citrix Service Provider shared infrastructure for provisioning, authentication, back office services, management services, and dashboards. It encompasses these VLANs:

- **Trust/Authentication VLAN:** The authentication VLAN contains the Microsoft Active Directory Forest and Domains in a secured network. Authenticated access to Active Directory capabilities is enabled in this VLAN only for specific administrators, machines, and users from other networks.
- **Management VLAN:** The management VLAN contains core network services such as Domain Name Services, NTP, and SNMP, and other Citrix Service Provider-provided services.
- **Application VLAN:** This VLAN contains the back office applications that enable web, mail, collaboration, and line of business application back-end services. The Citrix Service Provider can leverage these VLANs and services across tenants or dedicate them to a specific tenant according to subscriber service level agreements.
- **Provisioning VLAN:** The provisioning VLAN provides a secure network for image management and infrastructure services — in particular, for Citrix Provisioning Services™ (PVS). In the lab implementation, multiple PVS VLANs were defined, one for each site-isolated tenant as well as a shared tenant PVS VLAN, to enable an effective provisioning configuration (see page 71 for implementation details).

Appendix B contains more information about specific VLAN configurations in the Citrix Solution Lab implementation.

Physical connections and additional networks

Beyond the DMZ and multi-tenant networks, two additional networks are enabled specifically for performance reasons across the infrastructure: one is dedicated to storage and the other to hypervisor management (in this case, Microsoft System Center Virtual Machine Manager).

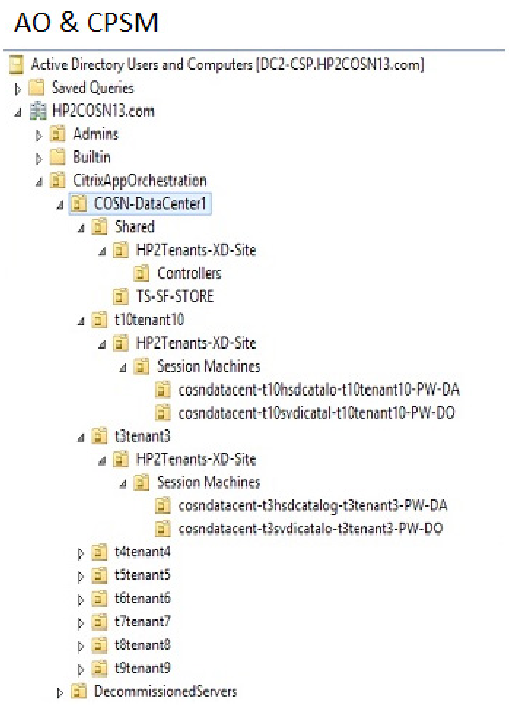
- **Storage:** This is an un-routable network that separates the storage and network data within the environment. All Hyper-V hosts have a direct connection to this network for SAN access.
- **Management:** This network separates management traffic from the data and storage traffic.

A network switch is physically connected to these networks to provide connectivity across them. The switch secures these distinct networks through prescriptive route and access-list tables. The network switch is directly connected to a pair of additional switches that provide connectivity to individual VMs.

In addition to physical switch configurations, Hyper-V 2012 R2 introduces support for Virtual Switch Extended Access Control Lists (ACLs). Hyper-V ACLs provide firewall protection and enforce security policies for tenant VMs. Appendix C: Configuring Hyper-V Extended ACLs (page 95) includes more information about how ACLs were implemented in the reference architecture and validated in the lab environment.

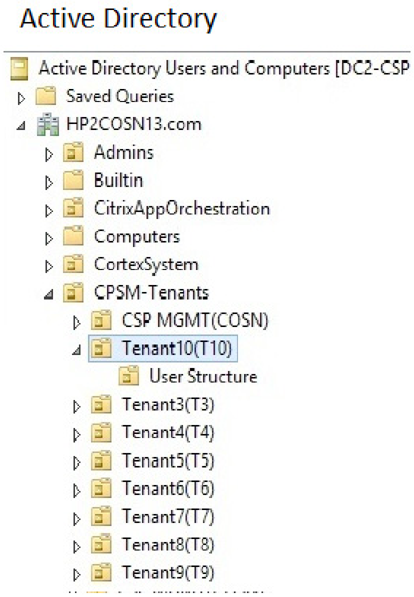
Active Directory and Organizational Unit Considerations

Windows-based applications and desktops "as-a-Service" are inherently based upon Microsoft Windows principles and technologies. As a result, Microsoft Active Directory (AD) plays a critical role in many aspects of the Citrix Service Provider Reference Architecture, most notably as the central account authority and as a foundational element to organizational and multi-tenant isolation capabilities. To facilitate the different tenant isolation models in the reference architecture, Delivery Groups in Citrix App Orchestration and CloudPortal Services Manager are mapped to specific Active Directory Organizational Units (OUs).



AO & CPSM

```
Active Directory Users and Computers [DC2-CSP.HP2COSN13.com]
  Saved Queries
  HP2COSN13.com
    Admins
    Builtin
    CitrixAppOrchestration
      COSN-DataCenter1
        Shared
          HP2Tenants-XD-Site
            Controllers
          TS-SF-STORE
        t10tenant10
          HP2Tenants-XD-Site
            Session Machines
              cosndatacent-t10hsdcatalo-t10tenant10-PW-DA
              cosndatacent-t10svdicatal-t10tenant10-PW-DO
        t3tenant3
          HP2Tenants-XD-Site
            Session Machines
              cosndatacent-t3hsdcatalog-t3tenant3-PW-DA
              cosndatacent-t3svdicatalo-t3tenant3-PW-DO
        t4tenant4
        t5tenant5
        t6tenant6
        t7tenant7
        t8tenant8
        t9tenant9
      DecommissionedServers
```



Active Directory

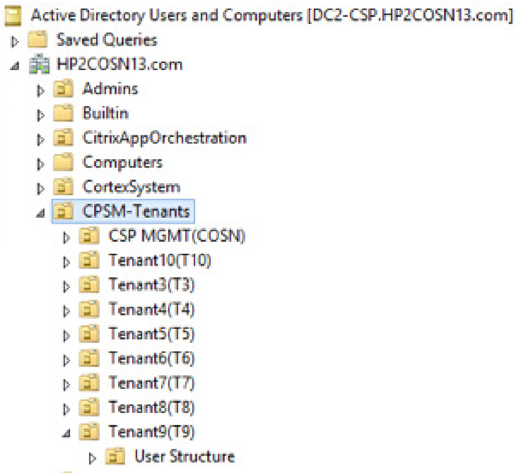
```
Active Directory Users and Computers [DC2-CSP
  Saved Queries
  HP2COSN13.com
    Admins
    Builtin
    CitrixAppOrchestration
    Computers
    CortexSystem
    CPSM-Tenants
      CSP MGMT(COSN)
      Tenant10(T10)
        User Structure
      Tenant3(T3)
      Tenant4(T4)
      Tenant5(T5)
      Tenant6(T6)
      Tenant7(T7)
      Tenant8(T8)
      Tenant9(T9)
```

The screenshots above highlight complementary structures within Citrix App Orchestration and CloudPortal Services Manager (application and desktop publishing and management) and the Microsoft Active Directory console (Account Authority and OU structure). Sub-nodes in each tree structure map to tenant-specific groups. In fact, the Citrix nodes are logical administrative folders that map directly to the Active Directory Organizational Units and/or tenant domains, providing tenant partitioning and enforcing isolation.

This section focuses solely on Active Directory design; the App Orchestration, CloudPortal Services Manager, and XenDesktop complements are discussed later in this document (see page 35).

Active Directory Organizational Units and Group Policy Objects

Active Directory considerations in this reference architecture follow industry best practices for SMB-focused Citrix Service Providers. Input from various cloud and service providers over the last few years corroborates the use of AD Organizational Units (OUs) as the preferred tenant partitioning mechanism for most deployments.



```
Active Directory Users and Computers [DC2-CSP.HP2COSN13.com]
  Saved Queries
  HP2COSN13.com
    Admins
    Builtin
    CitrixAppOrchestration
    Computers
    CortexSystem
    CPSM-Tenants
      CSP MGMT(COSN)
      Tenant10(T10)
      Tenant3(T3)
      Tenant4(T4)
      Tenant5(T5)
      Tenant6(T6)
      Tenant7(T7)
      Tenant8(T8)
      Tenant9(T9)
        User Structure
```

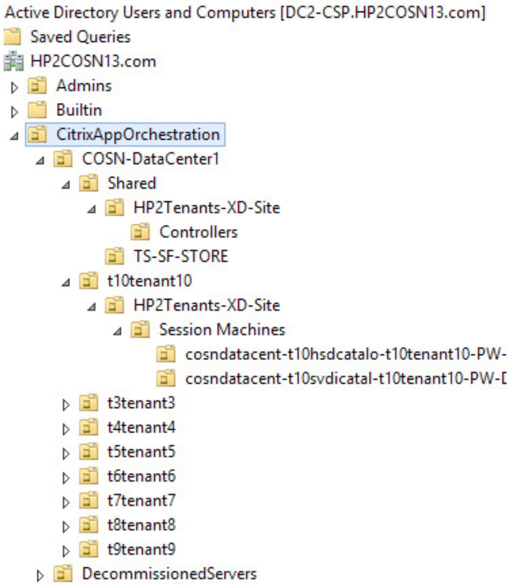
As shown in the graphic to the right, we created a separate OU for each tenant. This enables the use of AD Group Policy Objects (GPOs) as a mechanism for assigning properties to each tenant. Doing this simplifies administration and enforcement of Service Level Agreements (SLAs) for the configuration and security of each tenant.

Some tenants might be better served by a dedicated child domain, or in some cases their own isolated AD forest and isolated infrastructure. More details on these site-isolated tenants are discussed in the section on App Orchestration and its associated appendix.

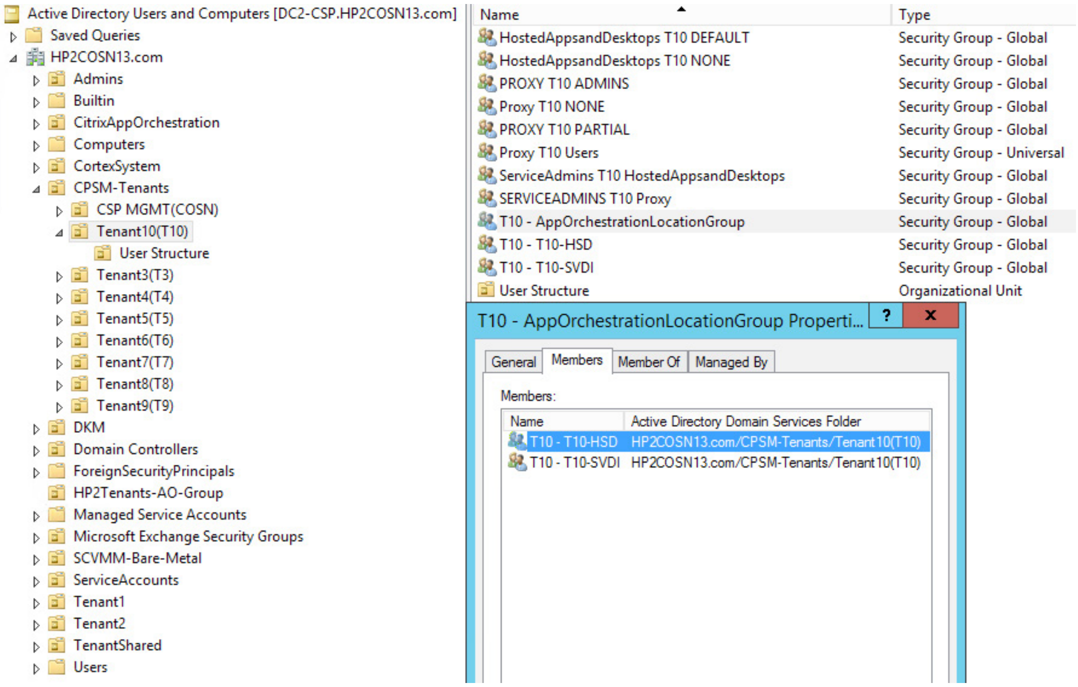
The advantage of cascading Group Policy in a multi-tenant environment is that it requires the least amount of customization with the greatest impact per tenant or SLA. For example, a Citrix Service Provider might begin their service offering with a generic GPO configuration that is applied at the Citrix Service Provider OU (such as “HP2COSN13.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 customizations that augment the generic offering. Troubleshooting a particular tenant configuration then usually requires only the consideration of the tenant’s GPO configuration.

The implementation of App Orchestration relies on the proper configuration of tenant OUs and linking GPOs to the App Orchestration root OU in the shared resources domain and resource OUs in the tenant domains. The screen excerpts below highlight App Orchestration root OU configurations in the shared and tenant domains. Appendix B gives additional examples of OU and GPO configurations.

Active Directory OUs define the set of privileged Citrix Service Provider administrators that perform management tasks across the Citrix Service Provider domain. One early implementation task for App Orchestration is to create an OU named Admins, add users to the Admins OU, and add them to the Domain Admin group.



```
Active Directory Users and Computers [DC2-CSP.HP2COSN13.com]
  Saved Queries
  HP2COSN13.com
    Admins
    Builtin
    CitrixAppOrchestration
      COSN-DataCenter1
        Shared
          HP2Tenants-XD-Site
            Controllers
          TS-SF-STORE
        t10tenant10
          HP2Tenants-XD-Site
            Session Machines
              cosndatacent-t10hsdcatalo-t10tenant10-PW-
              cosndatacent-t10svdicatal-t10tenant10-PW-[
        t3tenant3
        t4tenant4
        t5tenant5
        t6tenant6
        t7tenant7
        t8tenant8
        t9tenant9
      DecommissionedServers
```



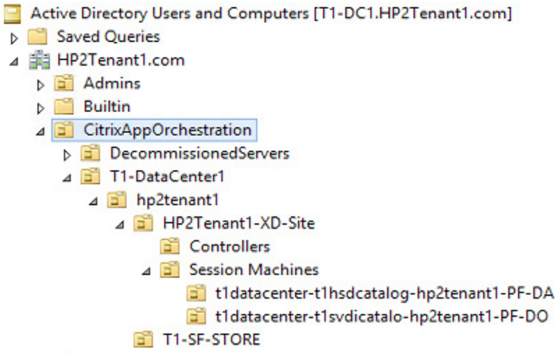
```
Active Directory Users and Computers [DC2-CSP.HP2COSN13.com]
  Saved Queries
  HP2COSN13.com
    Admins
    Builtin
    CitrixAppOrchestration
    Computers
    CortexSystem
    CPSM-Tenants
      CSP MGMT(COSN)
      Tenant10(T10)
        User Structure
      Tenant3(T3)
      Tenant4(T4)
      Tenant5(T5)
      Tenant6(T6)
      Tenant7(T7)
      Tenant8(T8)
      Tenant9(T9)
    DKM
    Domain Controllers
    ForeignSecurityPrincipals
    HP2Tenants-AO-Group
    Managed Service Accounts
    Microsoft Exchange Security Groups
    SCVMM-Bare-Metal
    ServiceAccounts
    Tenant1
    Tenant2
    TenantShared
    Users
```

Name	Type
HostedAppsandDesktops T10 DEFAULT	Security Group - Global
HostedAppsandDesktops T10 NONE	Security Group - Global
PROXY T10 ADMINS	Security Group - Global
Proxy T10 NONE	Security Group - Global
PROXY T10 PARTIAL	Security Group - Global
Proxy T10 Users	Security Group - Universal
ServiceAdmins T10 HostedAppsandDesktops	Security Group - Global
SERVICEADMINS T10 Proxy	Security Group - Global
T10 - AppOrchestrationLocationGroup	Security Group - Global
T10 - T10-HSD	Security Group - Global
T10 - T10-SVDI	Security Group - Global
User Structure	Organizational Unit

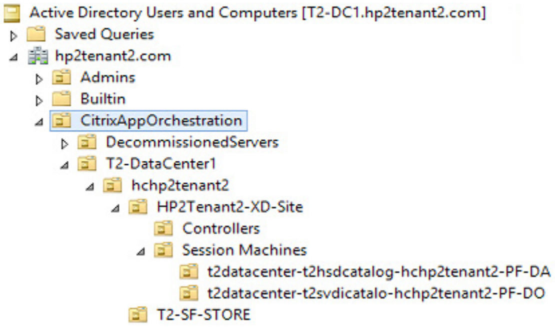
T10 - AppOrchestrationLocationGroup Properti...

Members:

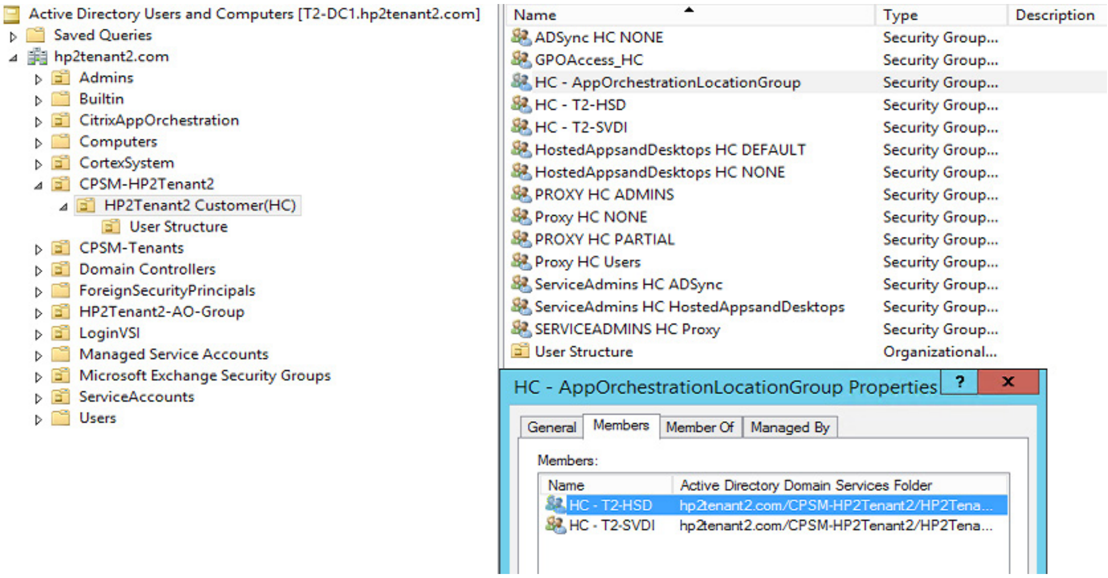
Name	Active Directory Domain Services Folder
T10 - T10-HSD	HP2COSN13.com/CPSM-Tenants/Tenant10(T10)
T10 - T10-SVDI	HP2COSN13.com/CPSM-Tenants/Tenant10(T10)



Active Directory Users and Computers [T1-DC1.HP2Tenant1.com]
- Saved Queries
- HP2Tenant1.com
  - Admins
  - Builtin
  - CitrixAppOrchestration
    - DecommissionedServers
    - T1-DataCenter1
      - hp2tenant1
        - HP2Tenant1-XD-Site
          - Controllers
          - Session Machines
            - t1datacenter-t1hsdcatalog-hp2tenant1-PF-DA
            - t1datacenter-t1svdicatalo-hp2tenant1-PF-DO
        - T1-SF-STORE



Active Directory Users and Computers [T2-DC1.hp2tenant2.com]
- Saved Queries
- hp2tenant2.com
  - Admins
  - Builtin
  - CitrixAppOrchestration
    - DecommissionedServers
    - T2-DataCenter1
      - hchp2tenant2
        - HP2Tenant2-XD-Site
          - Controllers
          - Session Machines
            - t2datacenter-t2hsdcatalog-hchp2tenant2-PF-DA
            - t2datacenter-t2svdicatalo-hchp2tenant2-PF-DO
        - T2-SF-STORE



Active Directory Users and Computers [T2-DC1.hp2tenant2.com]
- Saved Queries
- hp2tenant2.com
  - Admins
  - Builtin
  - CitrixAppOrchestration
  - Computers
  - CortexSystem
  - CPSM-HP2Tenant2
    - HP2Tenant2 Customer(HC)
      - User Structure
  - CPSM-Tenants
  - Domain Controllers
  - ForeignSecurityPrincipals
  - HP2Tenant2-AO-Group
  - LoginVSI
  - Managed Service Accounts
  - Microsoft Exchange Security Groups
  - ServiceAccounts
  - Users

Name	Type	Description
ADSync HC NONE	Security Group...	
GPOAccess_HC	Security Group...	
HC - AppOrchestrationLocationGroup	Security Group...	
HC - T2-HSD	Security Group...	
HC - T2-SVDI	Security Group...	
HostedAppsandDesktops HC DEFAULT	Security Group...	
HostedAppsandDesktops HC NONE	Security Group...	
PROXY HC ADMINS	Security Group...	
Proxy HC NONE	Security Group...	
PROXY HC PARTIAL	Security Group...	
Proxy HC Users	Security Group...	
ServiceAdmins HC ADSync	Security Group...	
ServiceAdmins HC HostedAppsandDesktops	Security Group...	
SERVICEADMINS HC Proxy	Security Group...	
User Structure	Organizational...	

HC - AppOrchestrationLocationGroup Properties

Members:

Name	Active Directory Domain Services Folder
HC - T2-HSD	hp2tenant2.com/CPSM-HP2Tenant2/HP2Tena...
HC - T2-SVDI	hp2tenant2.com/CPSM-HP2Tenant2/HP2Tena...

Active Directory Infrastructure

The table below shows server characteristics for the AD infrastructure.

Requirements	
Operating System	Microsoft Windows Server 2012 R2
Installed Roles	Active Directory Services
Additional Software	None
Hypervisor	Microsoft 2012 R2 with Hyper-V
AD Virtual Server Specifications	4 vCPU w/ 4GB RAM

The sample implementation includes multiple AD domain controller virtual machines provisioned with the global catalog role in the management zone to provide authentication services to tenants. Each AD 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:
http://technet.microsoft.com/en-us/library/cc268216.aspx.

Virtual Provisioning

Virtualization is the fundamental enabler of an efficient cloud datacenter. As a best practice, virtualizing workloads enables dynamic scale and simplifies management.

Microsoft System Center Virtual Machine Manager

The Citrix Service Provider Reference Architecture described in this document is founded on Microsoft guidelines for building a multi-tenant infrastructure (refer to the "Desktop Hosting Reference Architecture Guide" (http://www.microsoft.com/en-us/download/details.aspx?id=39285). The multi-tenant architecture relies on Microsoft Hyper-V and System Center 2012 Virtual Machine Manager (SCVMM) at the virtualization layer. (More information on SCVMM and Hyper-V can be obtained at the Microsoft web sites: http://technet.microsoft.com/en-us/systemcenter/hh278293 and http://www.microsoft.com/en-us/server-cloud/windows-server/default.aspx.)

SCVMM is deployed in the Citrix Service Provider management domain. Using SCVMM, Citrix Service Provider administrators create and configure the required infrastructure and tenant virtual machines and virtual networks. Multiple SCVMM consoles can be deployed if desired. In the lab implementation, for example, the first SCVMM console was installed on a physical server to build out the cloud infrastructure environment and deploy VMs and operating systems. The first SCVMM console could then be used to create a VM and build a second virtualized SCVMM console dedicated to VMs for multiple tenant environments.

Microsoft Hyper-V virtualization

Hyper-V is used to virtualize workloads in the reference architecture, and clustering is implemented to define N+1 configurations for redundancy. For Private Delivery Site tenants with dedicated infrastructure resources, the tenant is assigned its own Hyper-V cluster. A shared Hyper-V cluster is allocated for the Private Delivery Group/Shared Delivery Site tenants, and each tenant is then assigned one or more virtual machines (VMs) connected to an isolated virtual subnet. Two additional Hyper-V clusters were created to host shared cloud-based services, one for Scale-Out File Services and a second for other shared infrastructure services.

Virtual machines have multiple Hyper-V network adapters defined that connect to the appropriate networks through a Hyper-V network switch. The defined Hyper-V hosts are members of the Citrix Service Provider's Active Directory forest, and they are included in the Citrix Service Provider's SCVMM fabric as Hyper-V hosts. Appendix B describes the Hyper-V VM cluster and VLAN configurations implemented in the Citrix Solutions Lab and documents how virtual servers are defined and connected within the Citrix Service Provider Active Directory domain.

Hosted application and desktop workload provisioning

One of the primary enablers of efficient scale and management within a Desktop-as-a-Service solution is a robust yet simple workload provisioning system. Although there are many approaches to XenDesktop and XenApp provisioning, from physical unattended installations to VM cloning and other technologies, Citrix recommends Citrix Provisioning Services (PVS) for efficient scale and simplified lifecycle management of workloads in this reference architecture.

Application Provisioning

Application provisioning within the Citrix Service Provider 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 is one of the key enablers of dynamic assembly, separating applications from the underlying OS. This also allows lifecycle management of the application 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 Citrix Service Provider tenants, personalized for each tenant's SLA through the policies associated with that tenant's Delivery Group partition.

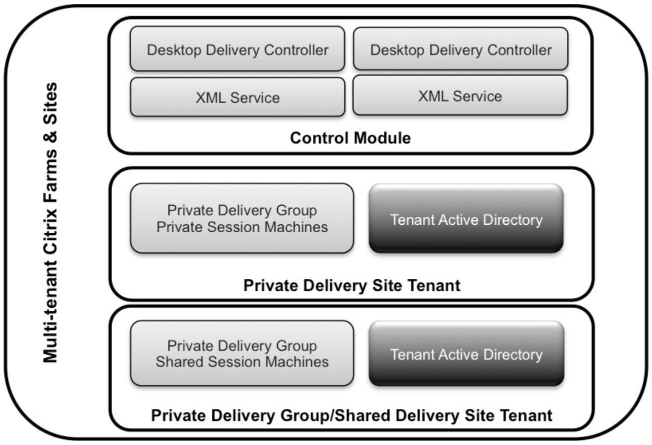
App Orchestration provides the means of allocating applications and desktops to subscribers based on Delivery Groups and Delivery Sites that map to specific Active Directory OUs. Configuring App Orchestration is discussed in more detail in the "Dashboards and Cloud Service Management" section (page 44).

Citrix StoreFront provides users an enterprise app store that aggregates offerings in one place. Each StoreFront user is able to subscribe to their favorite application and desktop resources, which can then follow the user automatically between devices. In this reference architecture, App Orchestration configures private or shared StoreFront catalogs that manage desktop and application offerings for subscribers.

If application streaming is required in addition to virtualized application and desktop, a Citrix Service Provider can extend this reference architecture and add Microsoft® App-V. More information is available on the Microsoft App-V web site: http://www.microsoft.com/en-us/windows/enterprise/products-and-technologies/mdop/app-v.aspx.

Deploying Application and Desktop Workloads

The Citrix XenDesktop site is a primary building block for the application and desktop services module within this reference architecture. A XenDesktop site is divided into various modules and partitions to provide a scalable solution for over 1,000 RDS workloads that can provide services for more than 100,000 active users per site.



Software Architecture for XenDesktop 7.1

The software architecture of XenDesktop 7.1 differs from earlier versions of XenDesktop in that it creates a unified infrastructure to deploy mixed application and desktop workloads, enabling the deployment of both hosted shared desktops (RDS) and hosted virtual desktops and servers (VDI). Figure 7 depicts the major components in a single XenDesktop 7.1 site.

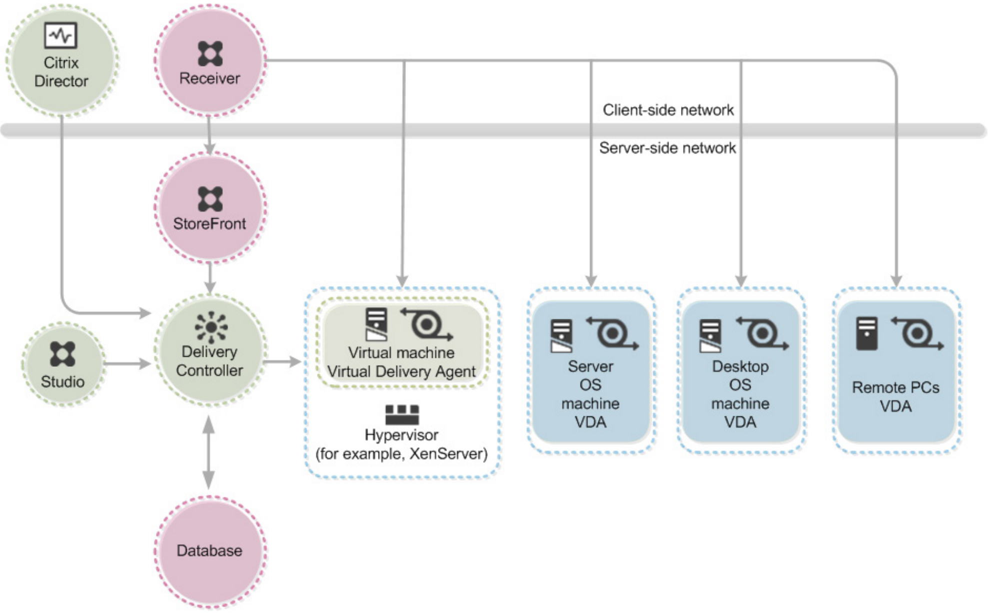


Figure 7: Single-Site Software Architecture of XenDesktop 7.1 and its major components

The major components for a single-site deployment of XenDesktop 7.1 include:

- **Receiver.** Installed on user devices, Citrix Receiver provides users with on-demand access to Windows, Web, and Software-as-a-Service (SaaS) applications.
- **StoreFront.** StoreFront authenticates users to sites hosting resources and manages stores of desktops and applications that users access.
- **Studio.** Studio is a management console that can configure and manage a XenDesktop site.
- **Delivery Controllers.** Delivery Controllers are responsible for distributing applications and desktops, managing user access, and optimizing connections to applications.
- **Virtual Delivery Agent.** A Virtual Delivery Agent is installed on each virtual or physical machine (within the server or desktop OS) and manages each user connection for application and desktop services. The agent allows OS machines to register with the Delivery Controllers and governs the HDX connection between these machines and Citrix Receiver.
- **Server OS Machines.** These are XenDesktop 7.1 virtual or physical machines (based on a Windows Server operating system) that deliver RDS applications or hosted shared desktops to users.
- **Desktop OS Machines.** These are XenDesktop 7.1 virtual or physical machines (based on a Windows Desktop operating system) that deliver personalized VDI desktops or applications that run on a desktop operating system.

Note: XenDesktop Server OS Machines and Desktop OS Machines are implemented through Session Machines in App Orchestration. In App Orchestration terminology, Session Machines are simply the virtual or physical machines that host desktop and app sessions to support server and desktop OS instances.

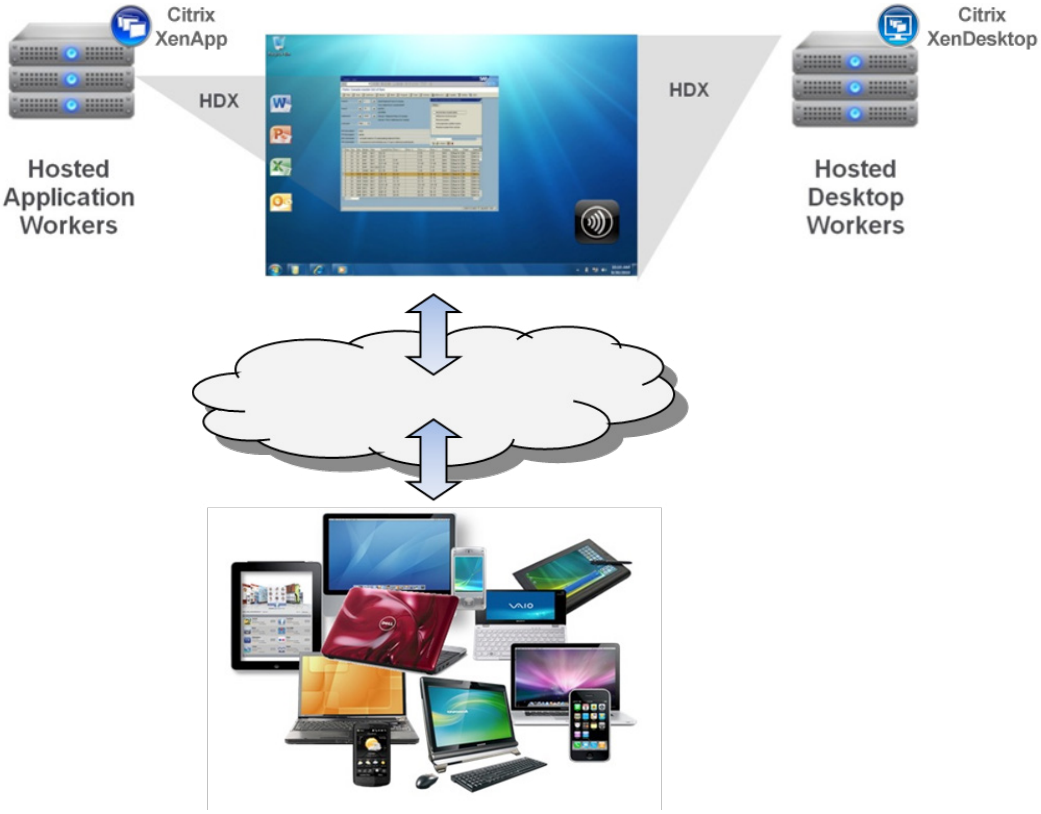
- **Director.** Director helps administrators quickly troubleshoot and resolve issues. It supports real-time assessment, site health and performance metrics, and end user experience monitoring. Citrix EdgeSight® reports are available from within the Director console and provide historical trending and correlation for capacity planning and service level assurance.
- **SQL Database.** An SQL database is a central repository for all XenDesktop configuration information.

For the majority of users, Citrix Service Providers are provisioning hosted shared applications and desktops through Citrix extensions to RDS. The next section highlights deployment considerations for Citrix hosted shared workloads. The same XenDesktop infrastructure can be leveraged also for virtual desktop (VDI) delivery.

Deploying Hosted Application Workloads (RDS)

Hosted applications execute on XenDesktop servers and are presented to the user 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.

Please note: This section is specific to the use of XenApp for the delivery of Windows applications via hosted shared desktops based on Windows Server 2012 R2 Remote Desktop Services (RDS).



Creating the Multi-Tenant Citrix XenDesktop Site Layer

The reference architecture requires the configuration of several different servers within the multi-tenant Citrix XenDesktop site layer.

AlwaysOn SQL Database Clusters

Several Citrix software components in this architecture require SQL databases, including XenDesktop 7.1, App Orchestration, and CloudPortal Services Manager. For this reason, the architecture relies on Microsoft® SQL Server™ as the database management system. SQL Server 2012 adds new high availability and disaster recovery solutions, including AlwaysOn clusters and availability groups, which were implemented to increase the reliability of the Citrix Service Provider Reference Architecture lab deployment.

AlwaysOn Availability Groups provide an enterprise-level alternative to database mirroring. Introduced in SQL Server 2012, AlwaysOn Availability Groups maximize the availability of user databases. An availability group supports failover for a set of databases that fail over together.

The previous version of this reference architecture used an IMA (Independent Management Architecture) data store to house configuration information. In this version, XenDesktop 7.1 uses a Microsoft SQL Server database as the data store for both configuration and session information. A typical single-site XenDesktop 7.1 deployment consists of three databases, as follows:

- Site configuration database: Stores the current configuration and XenDesktop state.
- Monitoring database: Stores historical data for display within Director.
- Configuration logging database: Tracks XenDesktop configuration changes.

A typical deployment also makes use of a Temporary Database (TempDB) provided by SQL Server.

During XenDesktop server startup, each server queries the database for initialization information. This is the most CPU-intensive action for the database since the initialization process makes sure that the local host cache (LHC) is consistent with the database. When multiple servers boot, multiple simultaneous requests for initialization information are made to the database.

During typical site operation, each server accesses the database periodically to ensure its cache is current. The database is also accessed if Citrix Studio, App Orchestration, or other utilities modify the site configuration or request static information. However, the database is not accessed when a user logs in, disconnects, or reconnects. All information needed for a client to establish a connection to a XenDesktop server is stored in cache, with the exception of licensing details.

SQL Database server characteristics are shown below.

Database Software Requirements	
Operating System	Microsoft Windows Server 2012 R2
Installed Roles/Features	Microsoft .NET Framework 4.0
Additional Software	Microsoft SQL Server 2012 SP1
Hardware Used	
Server	4 vCPU, 16GB RAM
Scalability	1,000 XenDesktop RDS Workers

For guidance on estimating database capacities for XenDesktop 7.1, please see the Citrix knowledge base article: http://support.citrix.com/article/CTX139508.

Delivery Controllers

In earlier XenApp releases, there is a zone master or data collector responsible for user connection requests and communication with hypervisors. In the XenDesktop 7.1 release, this functionality is distributed evenly across the Delivery Controllers for the XenDesktop site. Delivery Controllers manage the state of sessions and desktops, starting and stopping them based on demand and administrative configuration. Each site has one or more Delivery Controllers; to optimize availability, they are typically set up in an N+1 configuration for each XenDesktop Delivery Site.

Sizing guidelines

The Delivery Controllers store 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 records the data collector can process in conjunction with managing dynamic information.

Delivery Controller Software Requirements	
Operating System	Microsoft Windows Server 2012 R2
Installed Roles/Features	During a wizard-based XenDesktop installation, the installer deploys component prerequisites automatically. For more information on XenDesktop installation, see: http://support.citrix.com/proddocs/topic/xendesktop-71/cds-system-requirements-71.html
Additional Software	XenDesktop 7.1
Hardware Used	
Server	4 vCPU, 8GB RAM
Scalability	1,000 XenApp Session Machines

Citrix License Server

When users connect to a site, the Session Machine checks out a license from the Citrix license server on behalf of the client device. Subsequent connections from the same client share the same license.

Sizing guidelines

One of the most important considerations in determining Citrix 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 site and the number of simultaneous client connections dictate the CPU power of the server needed for the licensing feature.

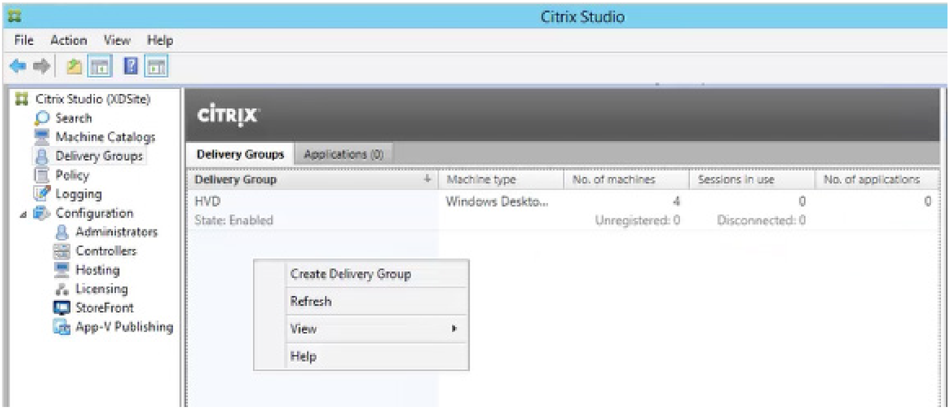
To appropriately size the license server, determine the number of client logins per second in the deployment by using performance monitor counters and the load evaluator logging feature. This analysis determines the processor speed needed for optimal license server performance.

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.

License Server Software Requirements	
Operating System	Microsoft Windows Server 2012 R2
Installed Roles	None
Additional Software	Citrix License Server 11.11.1
Hardware Used	
Server	4 vCPU, 4GB RAM
Scalability	446,400 users

Citrix Studio

Citrix Studio is the console that configures and manages the XenDesktop 7.1 deployment, eliminating the need for separate consoles for application and desktop management. Studio is a Microsoft Management Console snap-in that displays all of the objects in the deployment. Instead of using folders and Worker Groups to organize applications, servers, and other resources, in Studio you organize those resources using a combination of machine catalogs, tags, Delivery Groups, and Delegated Administrators.



Delivery Group	Machine type	No. of machines	Sessions in use	No. of applications
HVD State: Enabled	Windows Deskto...	4 Unregistered: 0	0 Disconnected: 0	0

Citrix Studio Requirements	
Operating System	Windows 7, Windows 8, Windows Server 2012, or Windows Server 2008 R2 SP1
Installed Roles/Features	Microsoft Management Console 3.0 (included with all supported operating systems). During the wizard-based XenDesktop installation, the installer deploys component prerequisites automatically.
Hardware Used	
WorkStation minimum	Varies per platform
Scalability	XenDesktop site-wide management

Configuring Trust

In the Solutions Lab implementation of the Citrix Service Provider Reference Architecture, trust relationships were used to permit access to Citrix Service Provider resources external to a Private Delivery Site tenant's Active Directory (AD) domain. The direction of trust defines the trust path for authentication.

Between the "trusting" Citrix Service Provider Management domain and "trusted" private tenant AD domains, one-way, non-transitive trusts are used. In the reference architecture, there are no two-way trusts and trusts are non-transitive.

Figure 9 shows how the Citrix Service Provider Management domain trusts Private Delivery Site tenant domains, allowing those tenants to access resources within the Citrix Service Provider domain.

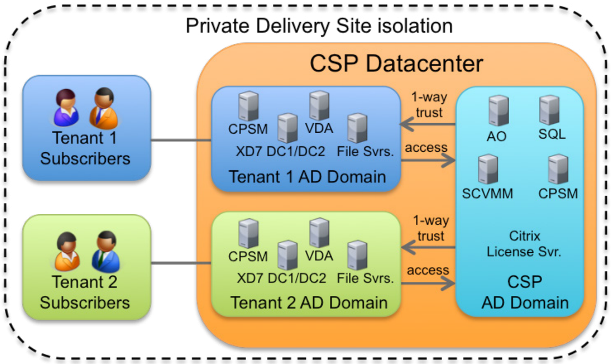
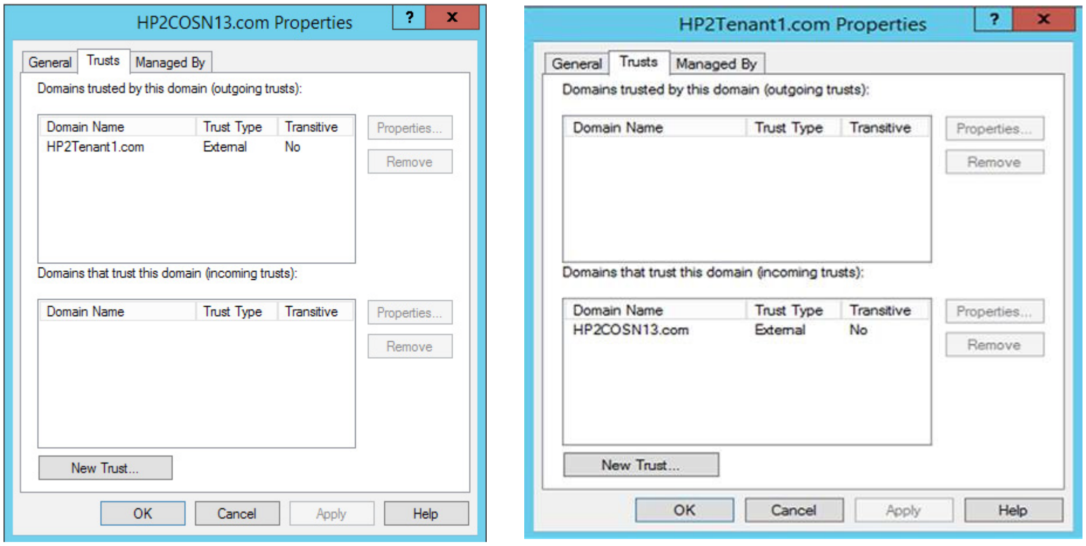


Figure 9: Configuring Trust — Private Delivery Site-Isolated Tenants.

AD Properties must be set to properly configure trust relationships. In the reference architecture implementation, the Citrix Service Provider Management domain (H2COSN13.com) is configured to trust the Private Delivery Site tenant domains (e.g., HP2Tenant1.com), as shown in AD Properties dialogs below (Figure 10).



HP2COSN13.com Properties

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
HP2Tenant1.com	External	No

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive

HP2Tenant1.com Properties

Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
HP2COSN13.com	External	No

Figure 10: Active Directory trusts for the Citrix Service Provider management and tenant domains.

Note: At the time of this document's publication, XenApp 7.5, XenDesktop 7.5, and App Orchestration 2.5 have been released. An addendum to this reference architecture document will provide additional details of deploying with these newer releases.

Active Directory Integration with App Orchestration

Administrators manage all user and server settings through a combination of App Orchestration, CloudPortal Services Manager, and Active Directory policies and settings. Access to published applications, hosted desktops, or virtual desktops are controlled through App Orchestration mechanisms known as Delivery Groups and Delivery Sites. In addition to Active Directory controls and Access Control List-enforced security on virtual switches, these App Orchestration features are one of the primary mechanisms for implementing site multi-tenancy within this reference architecture (Figure 11).

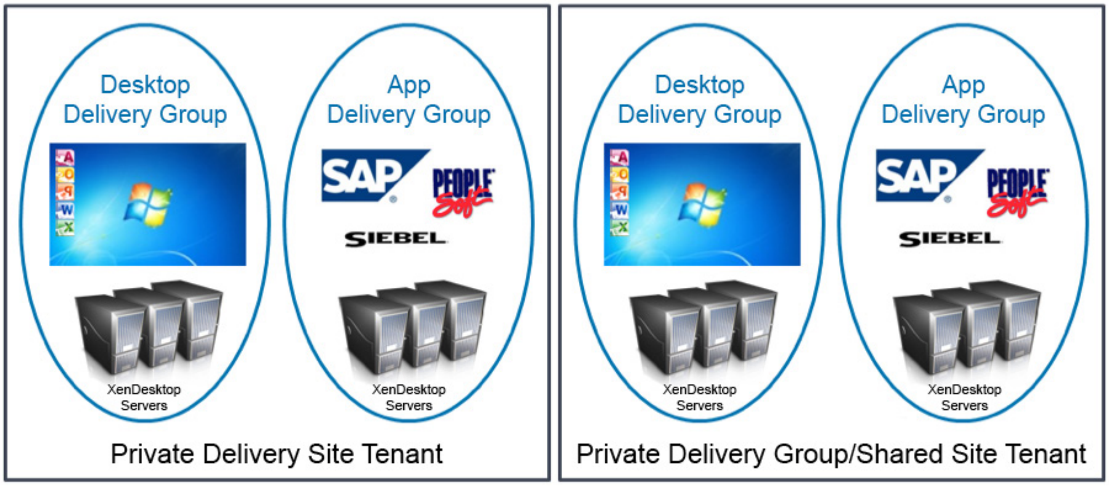


Figure 11: Delivery Groups and tenant isolation

App Orchestration uses Delivery Sites and Delivery Groups to provision application and desktop services in this reference architecture:

- **Delivery Sites.** A Delivery Site is the core environment that contains the XenDesktop Delivery Controllers and the SQL Database used to deploy XenApp and XenDesktop services. Delivery Sites provision desktops and applications to users through App Orchestration.
- **Delivery Group.** A Delivery Group is a container for one or more virtual machines used to deliver applications and desktops to a specific group of users. A Delivery Group is associated with a shared or private Delivery Site. A Delivery Group can be shared among tenants or dedicated to a specific tenant, according to the isolation level of the subscriptions it is hosting.

When you create App Orchestration offerings, you choose a means of isolation for tenants who subscribe to the app or desktop. The isolation level refers to whether the Delivery Controllers and Session Machines used for the offering are shared with other tenants or private to the subscribing tenant.

Three App Orchestration isolation levels are available:

- **Shared Delivery Group.** Both Session Machines and the Delivery Site are shared with other tenants.
- **Private Delivery Group.** Session Machines are private, but the Delivery Site is shared.
- **Private Delivery Site.** Both Session Machines and the Delivery Site are private and are not available to other tenants.

You can create App Orchestration environments that deploy XenDesktop in complex, multiple-forest Microsoft Active Directory environments. After setting up the App Orchestration environment and configuring trust, subscribing a tenant to an offering involves creating a Delivery Group according to the appropriate isolation level. The Delivery Group restricts access to the offering, ensuring only the specified users can access the offering. (See page 44 for additional information about App Orchestration.)

To facilitate isolation in a multi-tenant environment, Delivery Groups are mapped to Active Directory Organizational Units in this architecture. With on-demand provisioning through App Orchestration, using Active Directory automates this step by creating a base image for hosted shared desktops with all of the applications installed. To add capacity, the administrator simply creates a new instance of the base image and adds it to the desired tenant OU. The server receives its server settings from Active Directory, joins the appropriate Delivery Groups and begins hosting published applications or desktops. Creating separate Delivery Groups for desktops and applications gives Citrix Service Providers the flexibility to easily expand their tenant base.

Delivery Groups and Citrix policy filters

Citrix Service Provider administrators can filter all XenDesktop server policies by Delivery Groups, thereby restricting Group Policy Objects (GPOs) to a specific set of servers in the site. For policies configured in Citrix Studio, 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.

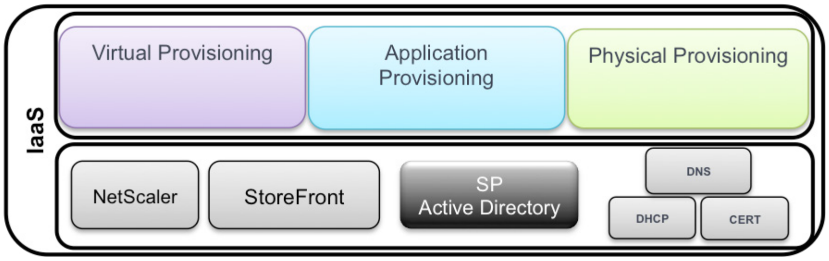
AD GPOs are used to manage the settings in the XenDesktop site. For all user and site settings GPOs can be linked to the XenDesktop OUs without any filters. However, if a setting is required specifically for a particular tenant's servers, a Delivery Group filter can be added to the policy to limit it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

Citrix policy configuration

In XenDesktop, nearly all server, site, 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. XenDesktop provides site-based group policies through the policies node in the management console. Such policies are written to the XenDesktop database and propagated to all servers in the site.

Secure Access and Acceleration Using NetScaler

Citrix NetScaler is a modular platform upon which several critical network security and acceleration functions are built. For Citrix Service Providers focused on small to medium businesses, Citrix NetScaler Gateway capabilities are fundamental to the secure delivery of desktops and applications as a service.



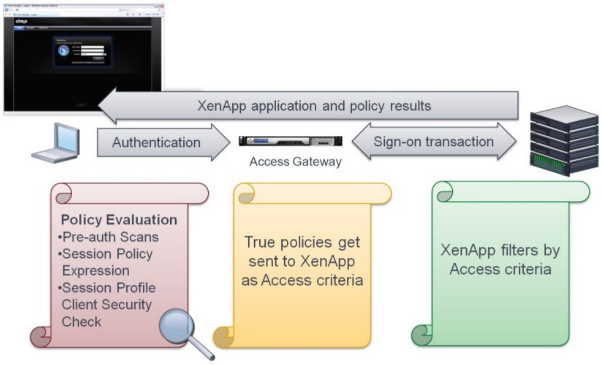
The NetScaler Access Gateway™ functionality within Citrix NetScaler provides secure access to the Citrix Service Provider environment over SSL (TCP 443) across the public Internet. Multi-tenant support is implemented either within a single NetScaler platform, a physical appliance HA pair, or across segregated networks and VLANs through the use of a dedicated 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 networks.

Citrix Solutions Lab implementation

The NetScaler Gateway Enterprise Edition virtual server is an entity within a NetScaler appliance that is a representative of all the configured services available to clients. The virtual server is also the point through which clients access these services. Configuring multiple vServers on a single appliance allows one NetScaler appliance to serve multiple user communities (multiple tenants in our example) with different authentication and resource access requirements.

NetScaler Gateway VPX™ Configuration	
Operating System	NetScaler VPX™ on XenServer
Hardware Used	
Server	Varies – See Appendix
Scalability	Varies – See Appendix

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 best fits your particular requirements.


XenApp application and policy results
Authentication
Access Gateway
Sign-on transaction
Policy Evaluation
•Pre-auth Scans
•Session Policy Expression
•Session Profile Client Security Check
True policies get sent to XenApp as Access criteria
XenApp filters by Access criteria

Deploying Server and Client VDI Workloads

Many of the fundamental scale and design parameters within the Citrix Service Provider reference architecture can be cross-referenced with enterprise-focused XenDesktop 7 reference architectures. See the Citrix XenDesktop 7 Blueprint (http://support.citrix.com/article/CTX138981) and available XenDesktop 7 reference architectures (http://www.citrix.com/products/xendesktop/tech-info.html).

The business impact from the nuances of a multi-tenant Citrix Service Provider cloud offering 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 have evolved, the confusion has been rather prolific over whether VDI desktops (Windows Client OS-based virtual desktops) can and should be hosted as cloud-based services. Various licensing models for different layers of the solution stack (and aggressive marketing from some startups) have added to the confusion. Citrix continues to work with its ecosystem partners to help bring clarity both to service providers and ISVs regarding the best approach to multi-tenancy designs for Windows application and desktop delivery as a service. This revision of the Citrix Service Provider Reference Architecture represents Citrix's guidance on the most current and cost-effective approach for integrating VDI desktops within a provider solution.

To address the broadest set of subscriber requirements in the most cost-effective manner, this section provides guidance on implementing XenDesktop for Hosted Shared Desktop or Hosted Server VDI (based on a Windows Server OS) and Hosted VDI (based on a Windows Client OS) within the reference architecture.

XenDesktop Server VDI

XenDesktop Server VDI is compliant with all service provider subscription licensing models, and can leverage the greatest number of shared resources within the Citrix Service Provider's cloud service datacenters. For this reason it is the preferred approach because it implies the lowest cost delivery of almost all use cases. From a technical perspective, some users can apply the Server VDI solution to virtually all use cases that have traditionally driven the need for Windows Client VDI. 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, which might 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 (RDS) 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 RDS Host Role is active. Citrix XenDesktop Server VDI does not rely on this role and therefore does not expose application incompatibility.
- The installation of peripheral devices that are not compatible in a RDS 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.

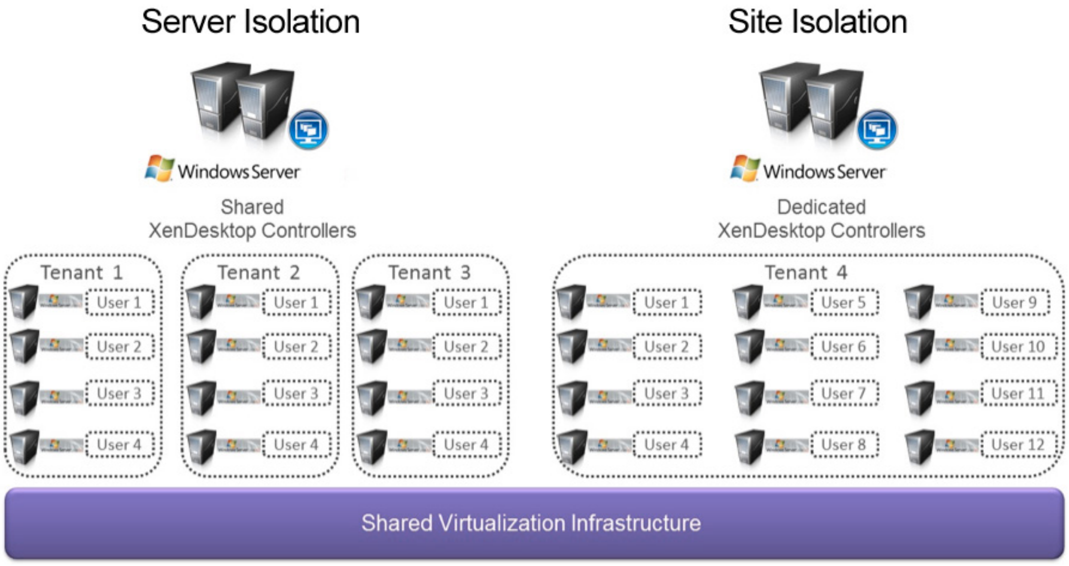


Figure 12: A conceptual view of Hosted Server VDI

As shown above on the left-hand side of Figure 12, an example of a Hosted Server VDI implementation using the Private Delivery Group/Shared Delivery Site Isolation multi-tenancy model would place the XenDesktop components within a single XenDesktop site. In this model all hardware, XenDesktop 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 Citrix Service Provider's datacenters.

The right side of Figure 12 depicts the Private Delivery Site Isolation multi-tenancy model. This model isolates the entire site, including the XenDesktop Delivery 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 (see http://www.citrix.com/products/xendesktop/tech-info.html for information on scalable enterprise XenDesktop reference architectures). 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 isolation model.

Figure 13 outlines the components and their placement (in blue) within the appropriate network segments of the overall solution.

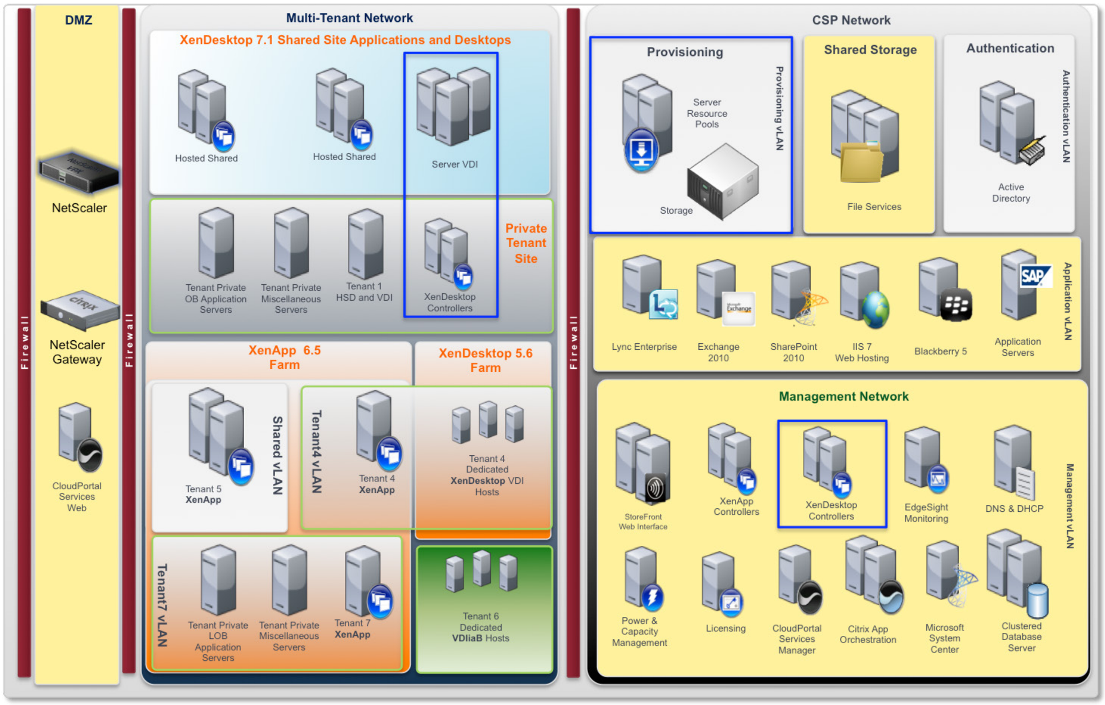


Figure 13: Component placement for Hosted Server VDI

XenDesktop Hosted VDI for Citrix Service Providers

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 describing different VDI solutions. It has become clear that today there are many views regarding the definition of Desktop-as-a-Service (DaaS). This is fairly typical in emerging markets, especially the sub-markets making up the cloud, including DaaS. Since the 1990s, Citrix has played a leading role in many business and technology discussions that have evolved into several major cloud markets. Needless to say, Citrix has played a significant role in the evolution of delivering Windows applications and desktops as cloud services since the earliest days, and has made many investments in research projects, startups, and technology acquisitions for more than a decade.

As the Citrix Service Provider program evolves, Citrix continues to provide best practices and guidelines for the cost-effective use of Citrix products in Citrix Service Provider offerings. XenDesktop has been part of the Citrix Service Provider program since the beginning and there are Citrix Service Providers that have delivered various XenDesktop FlexCast models needed for their tenants. By working with partners and the Citrix Service Provider channel, there are two key Hosted Virtual Desktop architectures and business models that predominate: Desktops-as-a-Service (DaaS) and Desktop-Infrastructure-as-a-Service (DIaaS).

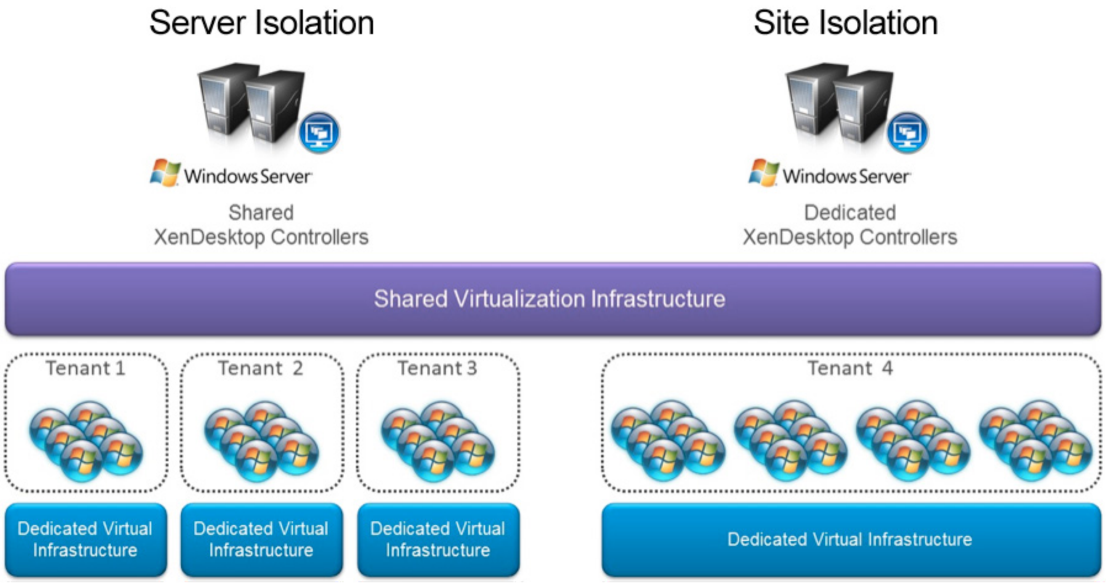

Server Isolation
Windows Server
Shared
XenDesktop Controllers
Site Isolation
Windows Server
Dedicated
XenDesktop Controllers
Shared Virtualization Infrastructure
Tenant 1
Tenant 2
Tenant 3
Tenant 4
Dedicated Virtual Infrastructure
Dedicated Virtual Infrastructure
Dedicated Virtual Infrastructure
Dedicated Virtual Infrastructure

Figure 14: A conceptual view of Hosted VDI for DaaS

Desktops-as-a-Service (DaaS)

Desktops-as-a-Service (DaaS) is an end-to-end service offering in which complete desktop and application integration as well as lifecycle management is provided by the Citrix Service Provider 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 Citrix Service Provider while corporate IT focuses on other IT needs of the organization.

In Figure 14, the concept of Private Delivery Group/Shared Delivery Site Isolation and Private Delivery Site 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 best practice for these workloads to be hosted on tenant-dedicated hardware to simplify management of tenant-specific SLAs determined by niche use cases. These use cases usually map to applications with intense compute needs, which in turn typically drive the requirement for a client OS VDI solution. Typically 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 (DIaaS)

Desktop-Infrastructure-as-a-Service (DIaaS) 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 lifecycle maintenance for the tenant's 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 up-time and perhaps VM back-ups.

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

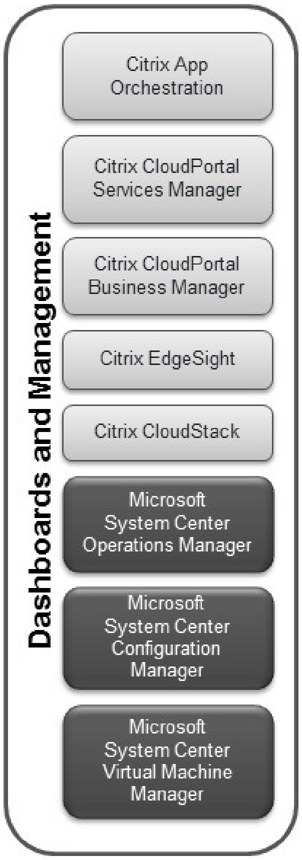
More information about Microsoft licensing requirements for Windows Client OS based VDI can be found at: http://download.microsoft.com/download/1/1/4/114A45DD-A1F7-4910-81FD-6CAF401077D0/Microsoft%20VDI%20and%20VDA%20FAQ%20v3%200.pdf

Dashboards and Cloud Service Management

Administering a complete application and desktops "as-a-Service" offering can be a significantly complex consideration. Comprehensive tools and dashboard views are critical to simplifying large-scale cloud administration for multi-tenant solutions.

Several Citrix-provided consoles enable deep control across the various solution components. The Citrix App Orchestration console allows Citrix Service Providers to build out deployments to massive scale using multi-site and multi-version configuration management across the entire Citrix Service Provider cloud. Citrix CloudPortal Services Manager enables delegated provisioning and administration across components with an easy-to-use web-based interface. Performance monitoring tools (such as Citrix HDX Insight) are also part of this reference architecture environment.

This section provides technical data and guidance regarding these dashboards and management consoles. It highlights CloudPortal Services Manager and App Orchestration as a means of cross-product integration and cloud-scale administration to simplify management of multi-tenant systems across datacenters. This section also introduces the monitoring tools available. In the Citrix Solutions Lab, test engineers integrated these software components to validate management capabilities (see Appendix B).


Dashboards and Management
Citrix App Orchestration
Citrix CloudPortal Services Manager
Citrix CloudPortal Business Manager
Citrix EdgeSight
Citrix CloudStack
Microsoft System Center Operations Manager
Microsoft System Center Configuration Manager
Microsoft System Center Virtual Machine Manager

Citrix App Orchestration

Citrix App Orchestration allows Citrix Service Providers to orchestrate and automate the delivery of applications and desktops in multi-tenant environments and across multiple products, sites, and datacenters. With App Orchestration, hosted service providers can:

- Manage XenApp and XenDesktop across multiple locations, including multiple datacenters in multiple versions, sites or farms, Active Directory domains, and datacenters
- Provide consistent configuration across global deployments spanning multiple delivery sites, eliminating configuration drift and issues
- Define tenant and user affinity to deliver offerings to primary and backup locations, for optimum continuity and fault tolerance
- Provision desktops and applications on any supported hypervisor. App Orchestration can incorporate externally provisioned VMs (e.g., provisioning via PVS as in this reference architecture).

App Orchestration 2.0 works with XenDesktop 7.1 to automate deployment of machine catalogs, Delivery Sites, and Delivery Groups for delivering applications and desktops (known as “offerings”) to users. Offerings are containers that help Citrix Service Providers define a set of apps, desktops, and resources. They are designed so that tenant users can select them as needed from an application storefront.

For detailed information about planning, installing, and configuring Citrix App Orchestration, refer to the App Orchestration documentation on the Citrix eDocs site (http://www.citrix.com/edocs). App Orchestration provides a configuration system that enables a multi-tenant data model with flexible isolation concepts at its core (permitting separate isolation models for each service). It also features a simple user interface and automated workflows that control XenDesktop, Active Directory, and other components.

App Orchestration follows the principle of "Desired State". When a change to an orchestrated deployment occurs, such as creating a Delivery Site or adding a Session Machine to a catalog, the change is saved as a desired configuration in the database. The App Orchestration engine then issues all of the actions required to apply the change. These actions are called workflows, which the administrator can monitor from the App Orchestration management console. The configuration server applies changes asynchronously, allowing multiple operations to occur across different products in the correct sequence and over extended periods of time. If any failures result, they can be corrected and the system will complete the change.

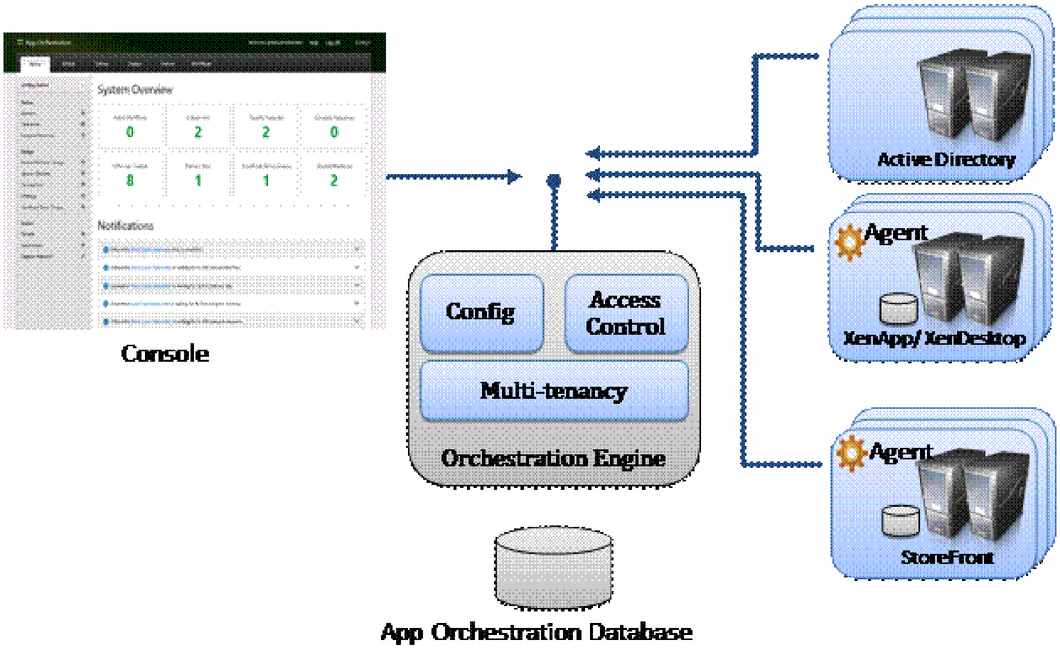


Figure 15: Citrix App Orchestration

App Orchestration 2.0 features

App Orchestration 2.0 provides the following features to simplify cloud-scale administration for service providers:

- **Simplified management across datacenters.** App Orchestration simplifies how Citrix technologies can be provisioned and deployed on virtual servers across datacenters. Given pools of XenDesktop Session Machines and Delivery Controllers, App Orchestration automatically manages capacities across multiple sites and datacenters, even managing multiple product versions and farms/sites in physically different domains.

- **Multi-tenant configuration.** Support for different types of isolation models (e.g., Session-based, Server-based, and Site-based) on a per-application or per-desktop basis. There are two areas in App Orchestration 2.0 in which you can specify isolation levels: delivery isolation and tenant StoreFront isolation.
- **Quick application and desktop configuration.** App Orchestration enables the harmonious configuration and integration of XenDesktop, XenApp, NetScaler, and Active Directory. This helps automate the installation of farms/sites, Session Machines and StoreFront server groups. Automatic discovery of application information (including name, icon, command line, working directory, etc.) from a XenDesktop RDS host can save valuable administrative time.
- **App Orchestration web management console.** App Orchestration supplies a web-based management console to control App Orchestration activities. You can use the console to monitor workflows for deployment actions, such as creating Delivery Sites or adding Session Machines.
- **Easier Patching of XenDesktop RDS hosts.** When you create a new version of a XenDesktop RDS host, App Orchestration can automate the tasks of gradually draining users from the older version servers to the newer ones, without any downtime or manual intervention.
- **Tenant management.** The administrator defines tenants into the system, their desired level of isolation, and assigns resources to them directly. The console allows the administrator to easily view which resources (applications, desktops, XenDesktop RDS hosts, sites, etc.) are allocated to which tenants.
- **CloudPortal Services Manager integration.** Using App Orchestration with CloudPortal Services Manager, Citrix Service Providers can enable multi-tenant self-servicing of application and desktop offerings that are configured through App Orchestration. This capability empowers a degree of self-support, delegating control to the tenant administrator to manage user subscription offerings.

For Citrix Service Providers unfamiliar with Citrix App Orchestration, see the App Orchestration documentation at the Citrix eDocs site, http://www.citrix.com/edocs.

Orchestrating multi-tenant isolation

Citrix App Orchestration simplifies the complex task of multi-tenant isolation by implementing the three primary isolation models discussed earlier in this document. All three multi-tenancy isolation models — Shared Delivery Group, Private Delivery Group/Shared Delivery Site, and Private Delivery Site — can be delivered from the same datacenter. The reference architecture implements these isolation models through App Orchestration Delivery Groups, Active Directory OUs, and Group Policy Objects (GPOs). When administrators create a subscriber offering, they must specify the level of delivery isolation. They must also specify the level of StoreFront isolation for each tenant imported into App Orchestration to define whether the StoreFront server group is shared and whether the tenant uses a private or shared store.

Citrix CloudPortal Services Manager

Citrix CloudPortal Services Manager (CPSM) is a self-service portal that helps providers manage the delivery of cloud services and customer offerings. It drives App Orchestration operation by associating desired states with tenants and allowing services to be provisioned to users. CPSM provides out-of-the-box support for Desktop-as-a-Service and Windows applications (powered by Citrix XenApp and Citrix XenDesktop), as well as popular business applications and services like Microsoft Exchange, Office, SharePoint, Lync, web and data hosting, and virtualization service management. Customers and sub-customers (i.e., such as a reseller's customers) that lack IT expertise can add or change services, view reports, manage users, and perform day-to-day administration tasks through the self-service interface.

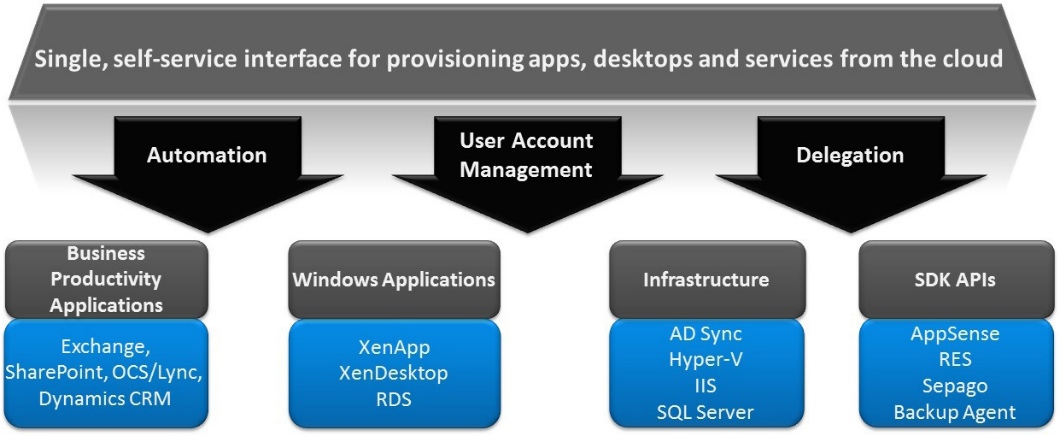

Single, self-service interface for provisioning apps, desktops and services from the cloud
Automation
User Account Management
Delegation
Business Productivity Applications
Exchange, SharePoint, OCS/Lync, Dynamics CRM
Windows Applications
XenApp XenDesktop RDS
Infrastructure
AD Sync Hyper-V IIS SQL Server
SDK APIs
AppSense RES Sepago Backup Agent

Figure 16: Citrix CloudPortal Services Manager provisioning capabilities

CloudPortal Services Manager features

CloudPortal Services Manager provides the following features to simplify and streamline application service provisioning within the Citrix Service Provider reference architecture:

- **Secure delegation of administrative tasks.** Day-to-day administrative tasks, such as creating users, resetting passwords, and provisioning applications and services, are delegated to the customer (or sub-customer in reseller situations) for streamlined management, reduced support costs, and improved quality of service and response time.
- **Simplified user interface.** The easy-to-use self-service web portal interface enables help desk staff and customers to manage their application and service offerings without requiring intense training or expensive skill sets.
- **Consolidated management of multiple customer environments.** Multiple customers in a multi-tenant infrastructure can be managed from a single web-based interface, simplifying administration and enabling faster response times.
- **Wizard-driven interface for adding new customers and users.** Adding new users and customers is easy and simple — required information fields are displayed in a familiar, web-based form. The User Copy feature allows an existing user's profile and services to be replicated to a new user for even faster user creation. Multiple users can also be imported from a simple Microsoft Excel spreadsheet, allowing customers to get started quickly and efficiently.
- **Customer resource and limit configuration.** Establishing limit configurations prevents customers from over-provisioning services.
- **Reporting.** By tracking and monitoring the environment, CPSM supports the creation of customized reports for usage and billing.

CloudPortal Services Manager considerations

CPSM provides detailed management for customers, users, services, and applications through a single interface. It supports:

- **Channel and reseller enablement.** Sub-customers can be nested within other customers to create a hierarchy for reseller and channel use cases. CPSM sites can be branded for a personalized reseller experience.

- **Layered services.** Services can be enabled at various layers — service provider, customer, and user — for easier and faster management.

Key CPSM Components

The CPSM cloud platform has four primary components, listed in the table below with the corresponding DNS alias and shown in Figure 17.

Component (DNS Alias)	Note
CPSM Web/User Interface (CortexWeb)	This is the Web server that is the user frontend. This server hosts the portal as well as the APIs that are used to access CPSM.
Provisioning Engine (CortexProvisioning)	This is the backend for the CPSM environment. The provisioning engine is workflow rules-based. The engine consists of MSMQ and the queue monitoring process. Rules and actions are stored in the SQL database.
Database (CortexSQL)	This is the SQL database used by the frontend and provisioning engine.
Reporting Services (CortexReports)	This server is used to generate reports regarding usage.

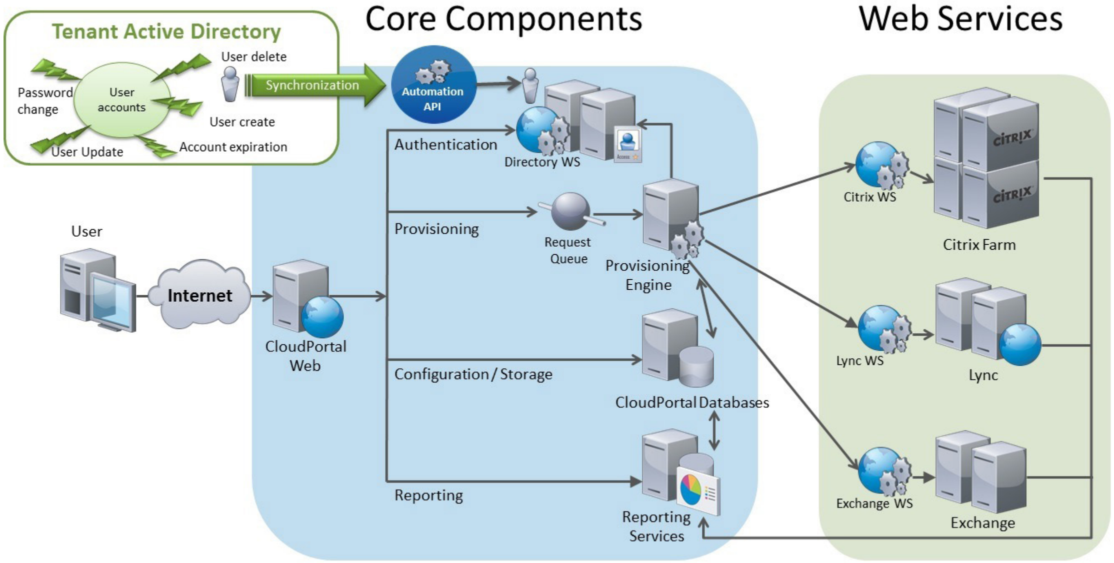
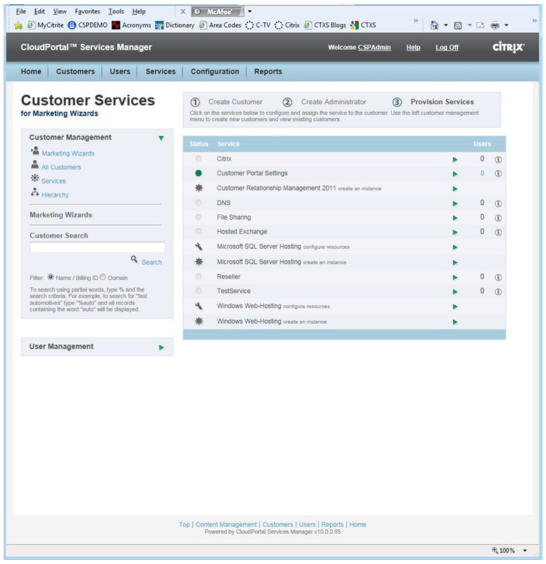


Figure 17: Citrix CloudPortal Services Manager Architecture

CloudPortal Services Manager user interface

CloudPortal Services Manager (CPSM) provides a unified interface for Citrix Service Provider administration as well as 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.


File Edit View Favorites Tools Help
McAfee
MyCitrite CSPDEMO Acronyms Dictionary Area Codes C-TV Citrix CTXS Blogs CTXS
CloudPortal™ Services Manager
Welcome CSPAdmin Help Log Off
CiTRIX
Home Customers Users Services Configuration Reports
Customer Management
Marketing Wizards
All Customers
Services
Hierarchy
Marketing Wizards
Customer Search
Search
User Management
100%

Customer Services
for Marketing Wizards

① Create Customer ② Create Administrator ③ Provision Services

Click on the services below to configure and assign the service to the customer. Use the left customer management menu to create new customers and view existing customers.

Filter: ● Name / Billing ID ○ Domain

To search using partial words, type % and the search criteria. For example, to search for "fast automotives" type "%auto" and all records containing the word "auto" will be displayed.

Status	Service		Users	
○	Citrix	▶	0	ⓘ
●	Customer Portal Settings	▶	0	ⓘ
✸	Customer Relationship Management 2011 create an instance	▶		
○	DNS	▶	0	ⓘ
○	File Sharing	▶	0	ⓘ
○	Hosted Exchange	▶	0	ⓘ
🔧	Microsoft SQL Server Hosting configure resources	▶		
✸	Microsoft SQL Server Hosting create an instance	▶		
○	Reseller	▶	0	ⓘ
○	TestService	▶	0	ⓘ
🔧	Windows Web-Hosting configure resources	▶		
✸	Windows Web-Hosting create an instance	▶		

Top | Content Management | Customers | Users | Reports | Home
Powered by CloudPortal Services Manager v10.0.0.85

CPSM system databases

A Microsoft SQL Server (CortexSQL) provides the backbone of the CPSM system. The CPSM databases store configuration information for all provisioned services, as well as all customer and user details. The databases also act as a cache mechanism for Active Directory, ensuring rapid user response without the need for slower AD queries. In addition, the databases store logging and auditing information for all provisioning transactions that pass through the system.

CPSM provisioning engine

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

The provisioning rules are easily customized using a simple Windows-based graphical interface that also provides a simple way to understand specific provisioning processes, which is helpful when troubleshooting problems. 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

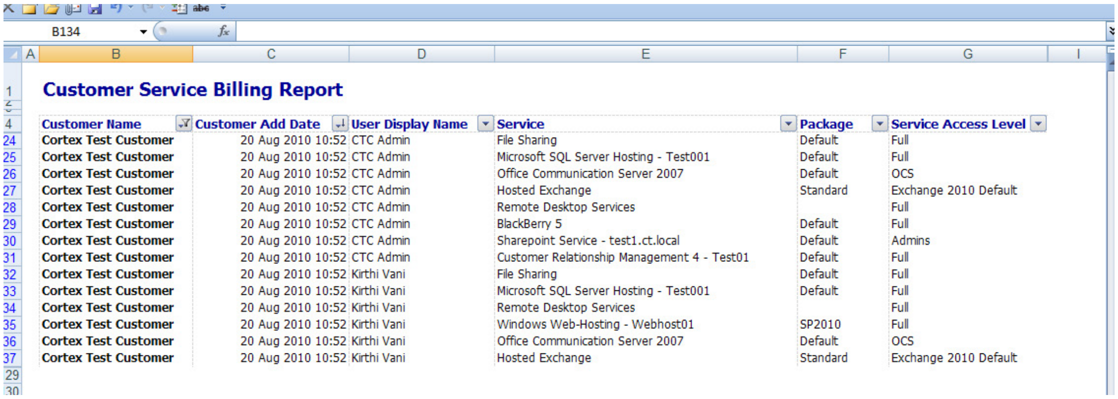
All provisioning processes are built using provisioning actions, enabling quick setup with little coding, while giving the service providers visibility into the processes being executed in their environment.

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

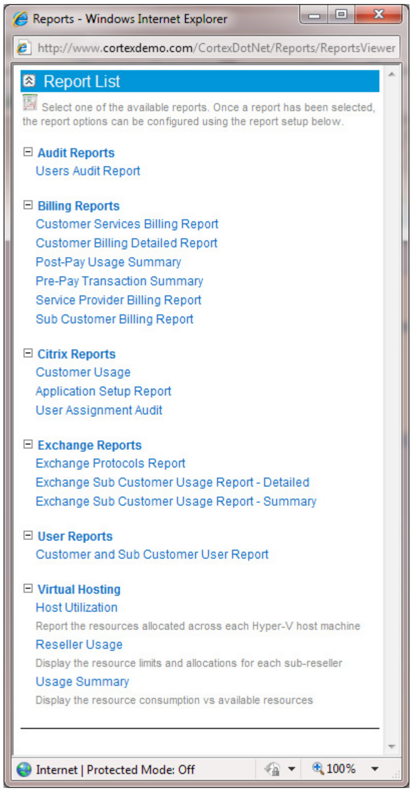
CPSM uses Microsoft SQL Server Reporting Services to deliver usage reporting capability through the CloudPortal Services Manager user interface. CloudPortal Services Manager interacts directly with the reporting services web service interface and allows controlled publishing of reports to all users of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



B134

Customer Service Billing Report

	Customer Name	Customer Add Date	User Display Name	Service	Package	Service Access Level
24	Cortex Test Customer	20 Aug 2010 10:52	CTC Admin	File Sharing	Default	Full
25	Cortex Test Customer	20 Aug 2010 10:52	CTC Admin	Microsoft SQL Server Hosting - Test001	Default	Full
26	Cortex Test Customer	20 Aug 2010 10:52	CTC Admin	Office Communication Server 2007	Default	OCS
27	Cortex Test Customer	20 Aug 2010 10:52	CTC Admin	Hosted Exchange	Standard	Exchange 2010 Default
28	Cortex Test Customer	20 Aug 2010 10:52	CTC Admin	Remote Desktop Services		Full
29	Cortex Test Customer	20 Aug 2010 10:52	CTC Admin	BlackBerry 5	Default	Full
30	Cortex Test Customer	20 Aug 2010 10:52	CTC Admin	Sharepoint Service - test1.ct.local	Default	Admins
31	Cortex Test Customer	20 Aug 2010 10:52	CTC Admin	Customer Relationship Management 4 - Test01	Default	Full
32	Cortex Test Customer	20 Aug 2010 10:52	Kirthi Vani	File Sharing	Default	Full
33	Cortex Test Customer	20 Aug 2010 10:52	Kirthi Vani	Microsoft SQL Server Hosting - Test001	Default	Full
34	Cortex Test Customer	20 Aug 2010 10:52	Kirthi Vani	Remote Desktop Services		Full
35	Cortex Test Customer	20 Aug 2010 10:52	Kirthi Vani	Windows Web-Hosting - Webhost01	SP2010	Full
36	Cortex Test Customer	20 Aug 2010 10:52	Kirthi Vani	Office Communication Server 2007	Default	OCS
37	Cortex Test Customer	20 Aug 2010 10:52	Kirthi Vani	Hosted Exchange	Standard	Exchange 2010 Default



Reports - Windows Internet Explorer
http://www.cortexdemo.com/CortexDotNet/Reports/ReportsViewer

Report List

Select one of the available reports. Once a report has been selected, the report options can be configured using the report setup below.

Audit Reports
- Users Audit Report

Billing Reports
- Customer Services Billing Report
- Customer Billing Detailed Report
- Post-Pay Usage Summary
- Pre-Pay Transaction Summary
- Service Provider Billing Report
- Sub Customer Billing Report

Citrix Reports
- Customer Usage
- Application Setup Report
- User Assignment Audit

Exchange Reports
- Exchange Protocols Report
- Exchange Sub Customer Usage Report - Detailed
- Exchange Sub Customer Usage Report - Summary

User Reports
- Customer and Sub Customer User Report

Virtual Hosting
- Host Utilization
  Report the resources allocated across each Hyper-V host machine
- Reseller Usage
  Display the resource limits and allocations for each sub-reseller
- Usage Summary
  Display the resource consumption vs available resources

Scalability and Capacity planning

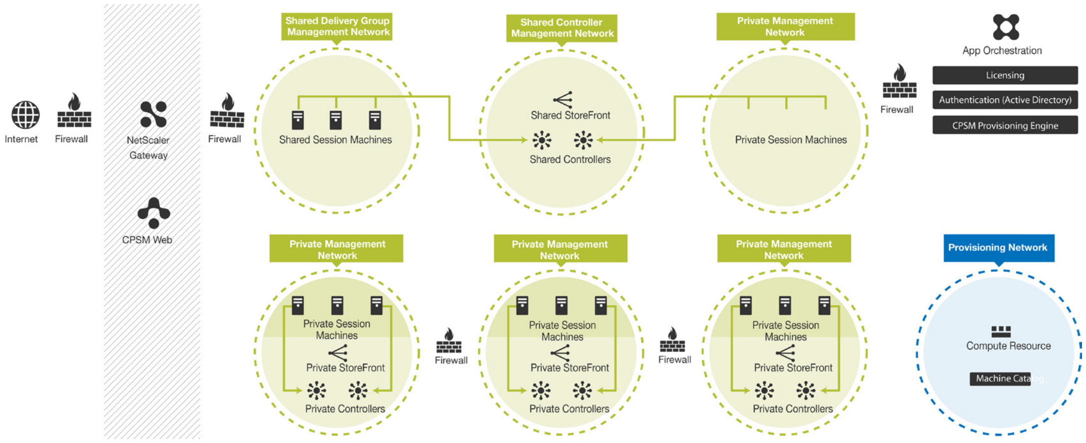
The table below provides a few sample scenarios with regards to capacity planning for CPSM:

Scenario	Scalability type	CPSM Server Requirements
100 - 1000 users	Basic Setup for Hosted Exchange – Single Server Setup	CPU: One 2.0GHz Xeon processor (Dual Core) or equivalent Memory: 2GB RAM, preferably 4GB RAM Disk: 36GB disk space
1000 - 5000 users	Basic Setup for Hosted Exchange – Dual Server Setup (Separate SQL Server)	Database Server: CPU: One 2.0GHz Xeon processor (Dual Core) or equivalent Memory: 2GB RAM, preferably 4GB RAM Disk: 36GB disk space Web Server: CPU: One 2.0GHz processor. Memory: 1GB RAM minimum, 2GB Recommended Disk: 36GB disk space
5000+ users	Basic Setup for Hosted Exchange – Triple Server Setup (All Components on Separate Servers)	Database Server: CPU: Two 2.0GHz Xeon processor (Dual Core) or equivalent Memory: 4GB RAM minimum Disk: 36GB disk space Web Server: CPU: Two 2.0GHz processors Memory: 2GB RAM minimum Disk: 36GB disk space Provisioning Engine Server: CPU: Two 2.0GHz processors Memory: 2GB RAM minimum Disk: 36GB disk space
100 000+ User	Advanced Setupregarding usage.	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)

Integrating CPSM with App Orchestration

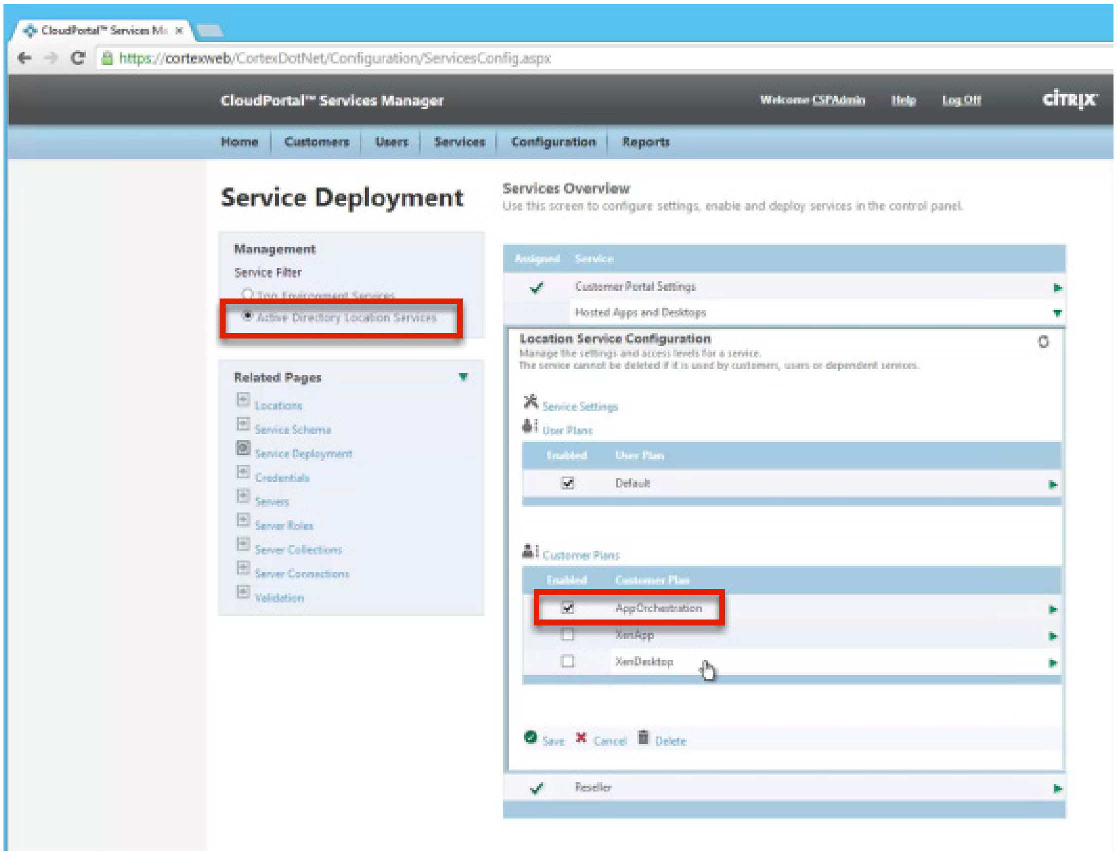
Using App Orchestration with CloudPortal Services Manager (as shown below), service provider partners can:

- Enable multi-tenant self-service of app and desktop offerings configured through App Orchestration
- Empower tenants and resellers to support themselves, and delegate control to the tenant or reseller administrator to manage their user subscription offerings



Configuring CPSM and App Orchestration

A video (http://www.citrix.com/tv/#videos/9766) outlines the deployment and configuration of the Hosted Apps and Desktops within CloudPortal Services Manager. The configuration in this video is specific to App Orchestration 2.0 as the Citrix delivery mechanism, which is precisely the configuration followed in this reference architecture. During the configuration steps for CPSM, the administrator specifies service deployment through Active Directory Location Services, App Orchestration as the method of deployment, and the name of the App Orchestration server. The administrator also specifies whether StoreFront services will be private or shared.



https://cortexweb/CortexDotNet/Configuration/ServicesConfig.aspx

Service Deployment

Management

Service Filter

○ Top Environment Services

● Active Directory Location Services

Services Overview

Use this screen to configure settings, enable and deploy services in the control panel.

Assigned	Service
✓	Customer Portal Settings
	Hosted Apps and Desktops

Location Service Configuration

Manage the settings and access levels for a service.
The service cannot be deleted if it is used by customers, users or dependent services.

Enabled	User Plan
☑	Default

Enabled	Customer Plan
☑	AppOrchestration
□	XenApp
□	XenDesktop

Assigned	Service
✓	Reseller

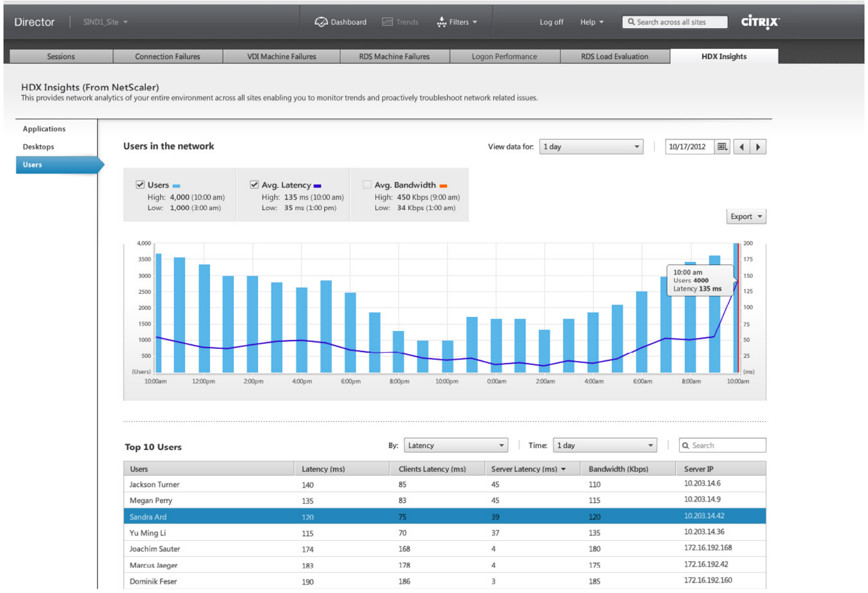
CPSM implementation details and customer onboarding example

A description of App Orchestration and CPSM integration and implementation steps can be found in Appendix D. The appendix also provides a detailed walk-through of the customer on-boarding process using CPSM.

Performance Monitoring and Management Tools

Citrix HDX Insight

HDX Insight is the integration of EdgeSight Network Inspector and EdgeSight Performance management with Director to provide real-time assessment and historical trending and advanced analytics of ICA® traffic in a deployment.



HDX Insights (From NetScaler)

This provides network analytics of your entire environment across all sites enabling you to monitor trends and proactively troubleshoot network related issues.

Users in the network

View data for: 1 day 10/17/2012

☑ Users
High: 4,000 (10:00 am)
Low: 1,000 (3:00 am)

☑ Avg. Latency
High: 135 ms (10:00 am)
Low: 35 ms (1:00 pm)

□ Avg. Bandwidth
High: 450 Kbps (9:00 am)
Low: 34 Kbps (1:00 am)

Top 10 Users

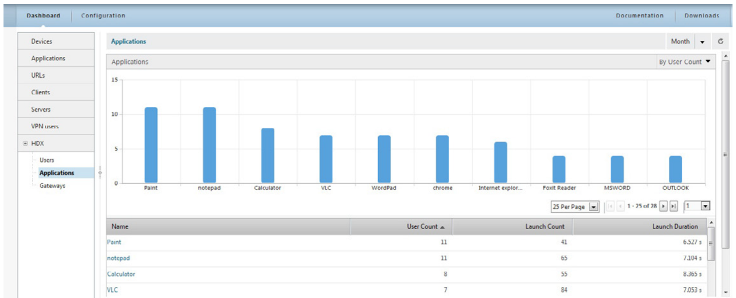
By: Latency Time: 1 day

Users	Latency (ms)	Clients Latency (ms)	Server Latency (ms)	Bandwidth (Kbps)	Server IP
Jackson Turner	140	85	45	110	10.203.14.6
Megan Perry	135	83	45	115	10.203.14.9
Sandra Ard	120	75	39	120	10.203.14.42
Yu Ming Li	115	70	37	135	10.203.14.36
Joachim Sauter	174	168	4	180	172.16.192.168
Marcus Jaeger	183	178	4	175	172.16.192.42
Dominik Feser	190	186	3	185	172.16.192.160

Citrix HDX Insight integration provides monitoring, reporting, and troubleshooting capabilities.

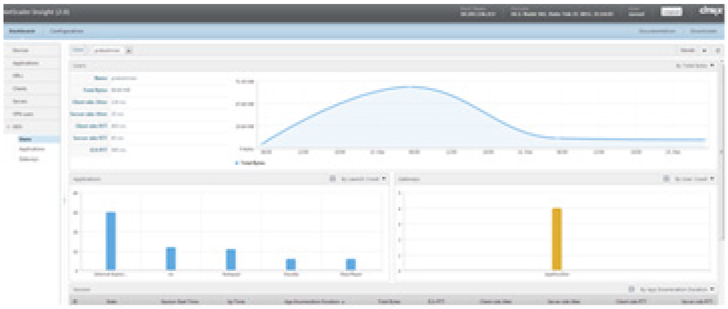
HDX Insight is deployed on redundant XenServer VMs. Since it is shared across the entire Citrix Service Provider infrastructure, the HDX Insight Server is integrated within the Management VLAN of the Citrix Service Provider network. The Citrix Service Provider can grant HDX Insight web console access from any client or DaaS session. All traffic to and from the HDX Insight service is secured through firewall and VLAN configurations.

Documentation for HDX Insight is available at http://support.citrix.com/proddocs/topic/ni-10-1-map/ni-hdxinsight-overview-con.html.



Applications

Name	User Count	Launch Count	Launch Duration
Paint	11	41	6.527 s
notepad	11	65	7.104 s
Calculator	8	55	8.365 s
VLC	7	84	7.053 s



NetScaler Command Center

NetScaler Command Center is a comprehensive management and monitoring solution for centralized configuration and control of all NetScaler platforms. It provides an easy way to define application delivery and load balancing policies via a simple declarative policy engine that requires no programming expertise.

Citrix Usage Collector 1.0

Citrix Usage Collector 1.0 collects and reports billable license consumption for Citrix Service Providers directly to Citrix for efficient billing. With Citrix Usage Collector, you can specify which license servers to poll for usage data, exempt certain users from billing, configure which users and groups can view and modify usage reports, set up usage alerts, and view current and past usage reports. Reporting details are shown on the Citrix Usage Collector home page and include product name, the number of in-use licenses and exceptions for the selected monthly/daily billing period, and informational, warning, and error notifications. For convenience, you can export reports to a .csv format for archiving.

No additional hardware is needed to run Citrix Usage Collector in this reference architecture. Documentation for Citrix Usage Collector 1.0 is available at http://support.citrix.com/proddocs/topic/citrix-usage-collector-10/lic-citrix-usage-collector-10.html.

Citrix Insight Services

Citrix Insight Services is a free online troubleshooting platform and health-checker for Citrix environments. It's exactly the same tool that Citrix tech support experts use every day to diagnose and fix hundreds of known issues. Citrix Auto Support analyzes log files, profiles the virtualization environment, and scans for known problems. It takes only a few minutes to obtain clear, actionable advice customized to a deployment.

To use Citrix Insight Services, the administrator uploads log files from XenDesktop, XenServer, XenApp and NetScaler (support for additional products is being added over time). When it discovers a known issue, it suggests hot fixes, patches and updates with red/yellow/green priorities. It will also analyze a configuration and provide best-practice advice, with links to relevant articles or white papers.

Citrix Insight Services is a great way to give a deployment a quick health check, allowing Citrix Service Providers to proactively resolve issues before they become real problems. Citrix Technote CTX#135408 describes how to get started.

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 these customers back to where it matters the most — growing their business. By offering a bundle of applications, desktops, and IT services, customers can get the applications and desktops they need in an easy-to-use, pay-as-you-go subscription model.

This Citrix Service Provider Reference Architecture represents a common view of technologies and best practices as recommended by Citrix and employed by many successful Citrix Service Providers. With core architectural innovations and cross-product integration, Citrix Service Providers can build a reliable, scalable, and high-performance solution in order to provide to provide tenants monthly subscriptions to Windows-based application and desktop services. The Citrix Service Provider licensing program and Citrix technologies provide a foundation for aggregating servers that can service millions of active subscribers across multiple tenants, while creating a single, comprehensive management view. Ultimately this provides a solution that enables Citrix Service Providers to build flexible, scalable, and cost-effective solutions that meet customer needs at an attractive and competitive price point.

Appendix A: Multi-Tenancy Design Considerations

Looking at the complete virtualization stack (Figure 18), there are several layers where multi-tenancy capabilities can be introduced. The table below highlights trade-offs of implementing multi-tenancy within a specific layer.

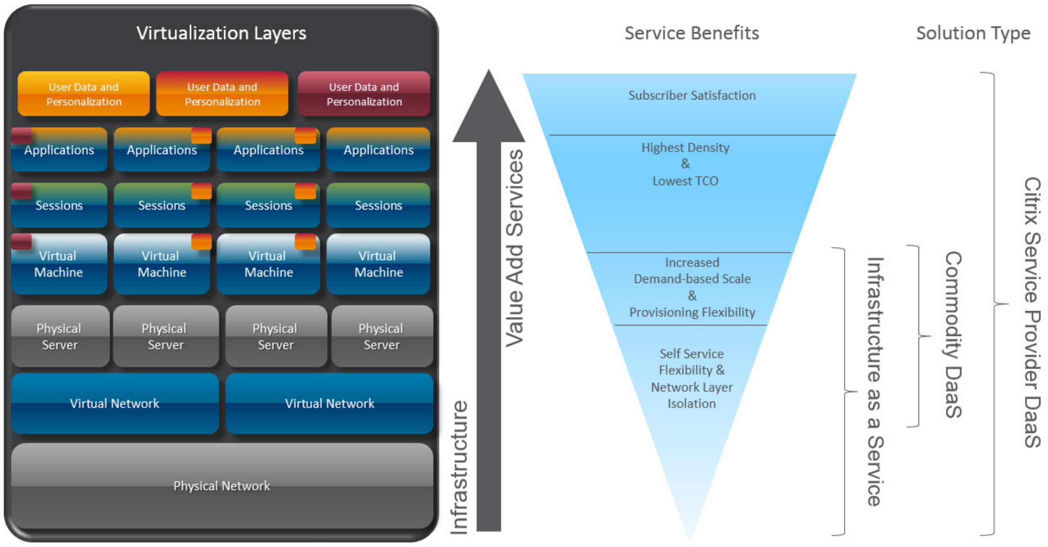


Figure 18: Multi-tenant layers within the DaaS stack

Layer	Example	Advantage	Disadvantage
Physical Network	Completely separate datacenters or networks	Greatest level of design flexibility and tenant isolation	Highest cost per tenant because all infrastructure is replicated for each tenant
Virtual Network	Co-located datacenters using VLANs as the primary isolation layer	Very high level of design flexibility and tenant isolation	Only slightly less expensive than physical network isolation
Physical Server	Co-located datacenters renting dedicated physical servers to subscribers	Relatively high level of design flexibility	Network layer security can be compromised; still relatively high cost; intra-server communications can be cumbersome to design
Virtual Machine	Dedicated Virtual Hosts; co-located VMs within a single datacenter and network	Relatively high level of design flexibility; lower per machine cost for provider and tenant since hardware is shared; dynamic scaling and provisioning	Network layer security can be compromised; intra-server communications can be cumbersome to design
Session Layer Virtualization	Hosted Shared Desktops	Highest subscriber density; lowest infrastructure and management costs	Lower design flexibility per tenant than machine and lower layer partitioning
Application Virtualization	Microsoft App-V	Enables dynamic assembly of OS and applications on-demand for each user; enables single instance management for application workloads across tenants; enables offline access to Citrix Service Provider managed applications	Requires repackaging of applications for streaming and virtualization; some applications not deliverable in this manner

Citrix Service Providers can leverage different multi-tenant approaches to deploy and manage a Citrix infrastructure (thus saving costs) while continuing to meet individual tenant needs. A Citrix Service Provider must take into account design considerations (Figure 19) to determine the best approach.

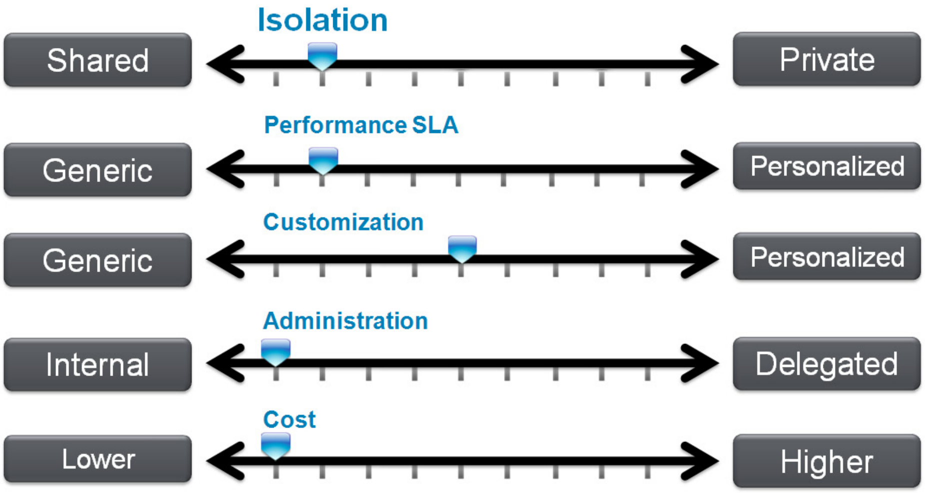


Figure 19: DaaS multi-tenant parameters

Although a specific Citrix Service Provider 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 being affected by activities of other tenants. Isolation is one of the most critical differentiators among methods of implementing multi-tenancy.
- **Performance SLA:** Ensuring that performance of one tenant is not negatively affected by activities of other tenants.
- **Customization:** Providing unique environmental, security, or performance aspects to an individual tenant based on their specific Service Level Agreement (SLA) within the multi-tenant environment.
- **Administration:** Providing the ability for tenants to perform some level of self-service administration for their own environment.
- **Cost:** Delivering the correct mix of the above capabilities at an appropriate cost.

The Citrix Service Provider reference architecture supports several options for multi-tenancy that provide different blends of isolation, performance management, customization, self-service, and cost. Citrix Service Providers can determine which of these options meet the needs of their customers, and develop offerings and price-points accordingly.

Isolation Models for Multi-Tenancy

There are three common multi-tenant approaches used in the market today that this reference architecture enables. They differ according to the type of isolation that they employ. In the lab implementation described in Appendix B, only the Private Delivery Site and Private Delivery Group/ Shared Delivery Site isolation models were implemented in order to validate the heightened security inherent in these models. (Note: "Delivery Site" refers to a XenDesktop Delivery Site and not to the private or shared StoreFront Site configured in App Orchestration.)

Shared Delivery Group/Shared Delivery Site isolation model

With the Shared Delivery Group/Shared Delivery Site isolation model, tenants share a single site infrastructure and session host, but each tenant's applications and desktops run within an isolated session on the same virtual machine. This approach is not recommended from a best practice or security perspective, but it is a common model in use for smaller providers today, particularly for those Citrix Service Providers offering basic, standard desktop services where cost — not security — is the most significant business concern.

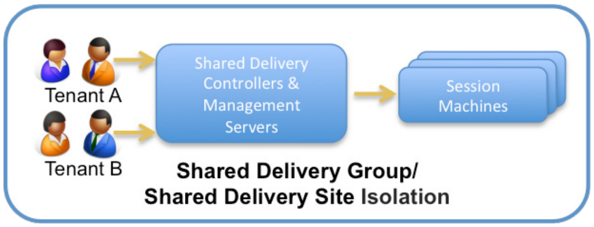

Tenant A
Tenant B
Shared Delivery Controllers & Management Servers
Session Machines
Shared Delivery Group/
Shared Delivery Site Isolation

Figure 20: Multi-tenancy: Shared Delivery Group isolation

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

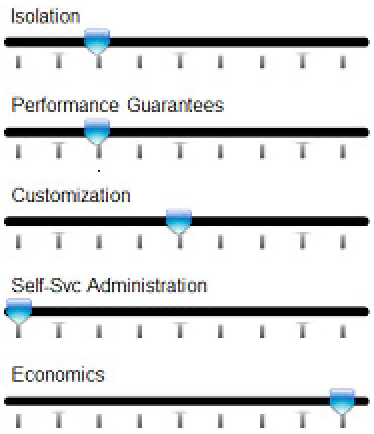


Figure x: Characteristics of a Shared deployment

- Users from multiple tenants have isolated sessions on a shared virtual machine (called a Session Machine). This requires appropriate lockdown of Session Machines to minimize the possibility of a user on one tenant negatively affecting users of another tenant. However, there is still a chance that a user can compromise a server (thus affecting another tenant's users).
- User performance guarantees can be established by using the CPU Utilization Management feature.
- A separate web interface site can provide custom branding for each tenant. In addition, Microsoft Windows and Citrix policies in Active Directory can provide a highly customized experience to users (e.g., wallpaper, theme, Citrix HDX settings, and so on).
- This method of multi-tenancy is extremely cost-effective because a Citrix Service Provider can spread infrastructure costs across multiple tenants.

Private Delivery Group/Shared Delivery Site isolation model

The Private Delivery Group/Shared Delivery Site isolation model provides isolation at the virtual machine layer. Tenants share a single XenDesktop Delivery Controller management network (including a shared XenDesktop site and infrastructure components). Session Machines, on the other hand, are connected to the tenant's private management network, supplying isolation through tenant-specific virtual machines. More and more Citrix Service Providers are moving to this method. Although it does not provide the strict security of the Private Delivery Site isolation model (which is described next), for many tenants this model provides arguably the most optimal blend of isolation, performance, customization, self-service administration, and cost — a combination that translates into a very attractive offering.

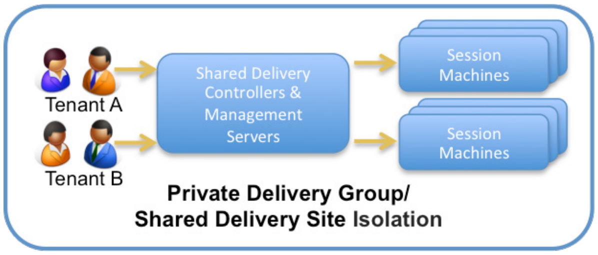

Tenant A
Tenant B
Shared Delivery Controllers & Management Servers
Session Machines
Session Machines
Private Delivery Group/
Shared Delivery Site Isolation

Figure 21: Multi-tenancy: Private Delivery Group/Shared Delivery Site isolation

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

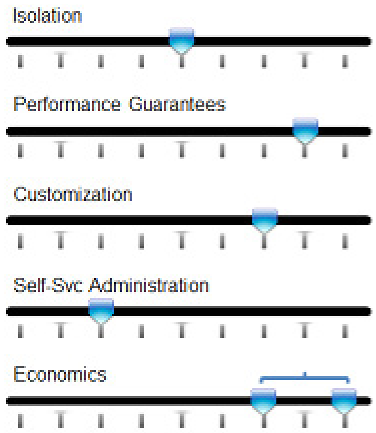


Figure x: Characteristics of a Partial Isolation deployment

- Each tenant has a dedicated pool of session servers. Delivery Groups and Session Machine Catalogs in App Orchestration simplify deployment. As a best practice, administrators should still always lock down individual Session Machine hosts.
- Because users from one tenant can have sessions only on designated servers, a user cannot negatively impact the performance of another tenant's users. Administrators can further guarantee performance to users by using additional capabilities within XenDesktop.
- In addition to the customization capabilities mentioned in the shared deployment, each tenant can have customized machine images for RDS and VDI workloads.
- Citrix Service Providers can allow tenants to perform some level of administration for their pool of session hosts or dedicated desktops (e.g., 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.

Private Delivery Site isolation model

In the Private Delivery Site isolation model, one XenDesktop site (or VDI-in-a-Box grid with dedicated infrastructure) is deployed per tenant. None of the infrastructure components are shared and Session Machines and Delivery Sites are connected to the tenant's private management 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 Citrix Service Providers 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.

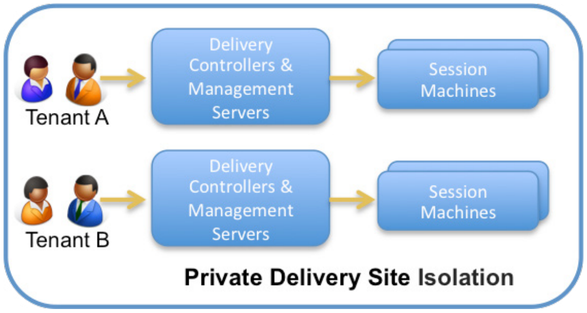

Tenant A
Delivery Controllers & Management Servers
Session Machines
Tenant B
Delivery Controllers & Management Servers
Session Machines
Private Delivery Site Isolation

Figure 22: Multi-tenancy: Private Delivery Site isolation

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

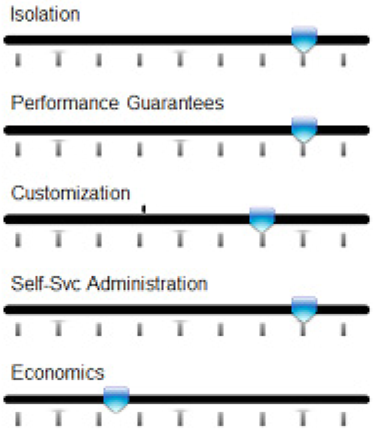


Figure x: Characteristics of a Full Isolation deployment

- Tenants are completely isolated including dedicated brokering operations.
- Performance guarantees are similar to the Private Delivery Group/Shared Delivery Site isolation model.
- The customized experience aspects remain the same as that of the Private Delivery Group/Shared Delivery Site isolation model.
- Service providers have the option to allow the tenant to perform a much higher level of self-service administration (e.g., help desk activity, managing session hosts, managing applications, etc.).
- The costs are higher for this model because the infrastructure components are not shared between tenants.

Appendix B: Lab Implementation and Configuration Details

In the Citrix Solutions Lab, test engineers validated this reference architecture by creating a sample deployment. While every implementation varies to meet specific tenant and subscriber requirements, the lab implementation instantiated a multi-tenant model that used Private Delivery Site isolation as well as Private Delivery Group/Shared Delivery Site isolation. (The Shared Delivery Group/Shared Delivery Site model was not implemented in the lab implementation because it has less stringent security demands.) Multiple tenants with different sized subscriber populations and application and desktop workloads (as shown in Figure 23 and detailed subsequently) were deployed and tested.

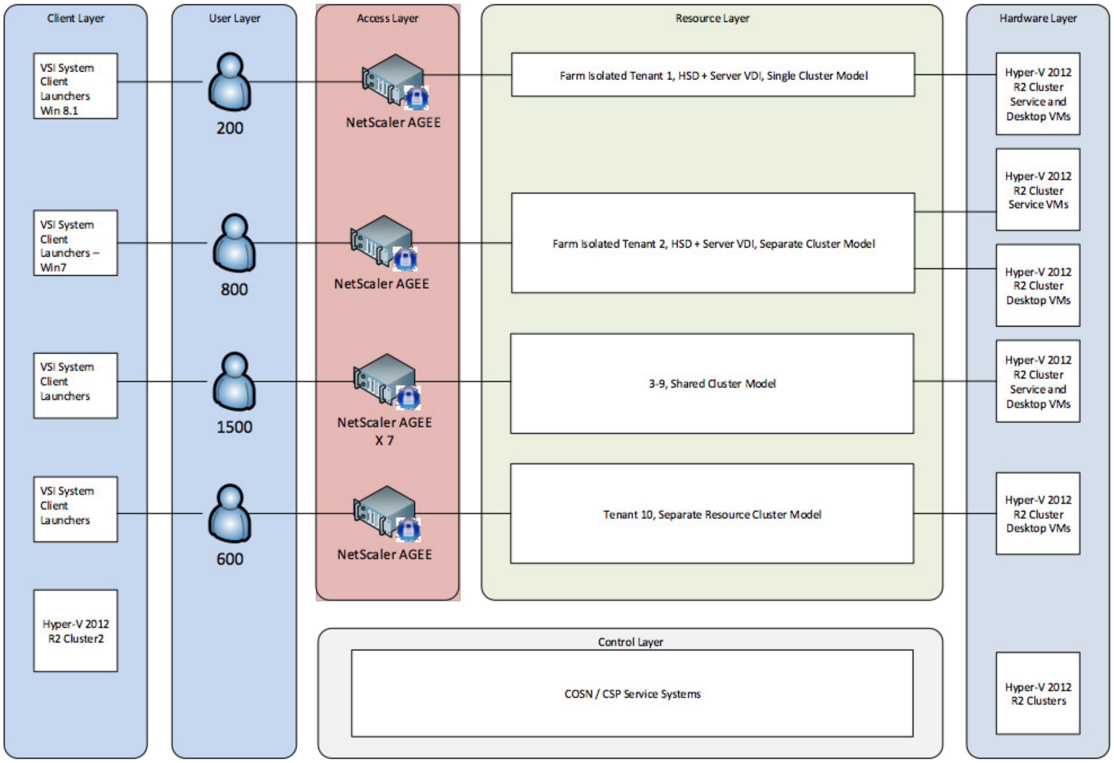

Client Layer
VSI System Client Launchers Win 8.1
VSI System Client Launchers – Win7
VSI System Client Launchers
VSI System Client Launchers
Hyper-V 2012 R2 Cluster2
User Layer
200
800
1500
600
Access Layer
NetScaler AGEE
NetScaler AGEE
NetScaler AGEE X 7
NetScaler AGEE
Resource Layer
Farm Isolated Tenant 1, HSD + Server VDI, Single Cluster Model
Farm Isolated Tenant 2, HSD + Server VDI, Separate Cluster Model
3-9, Shared Cluster Model
Tenant 10, Separate Resource Cluster Model
Control Layer
COSN / CSP Service Systems
Hardware Layer
Hyper-V 2012 R2 Cluster Service and Desktop VMs
Hyper-V 2012 R2 Cluster Service VMs
Hyper-V 2012 R2 Cluster Desktop VMs
Hyper-V 2012 R2 Cluster Service and Desktop VMs
Hyper-V 2012 R2 Cluster Desktop VMs
Hyper-V 2012 R2 Clusters

Figure 23: Citrix Solutions Lab Reference Architecture – Sample Implementation

This appendix outlines configuration details of the Citrix Solutions Lab implementation. It presents specific implementation considerations and best practices that were followed. It summarizes hardware configurations, software versions, storage components, and VLAN and VM configurations. It also describes important nuances that help in configuring and integrating the various reference architecture components.

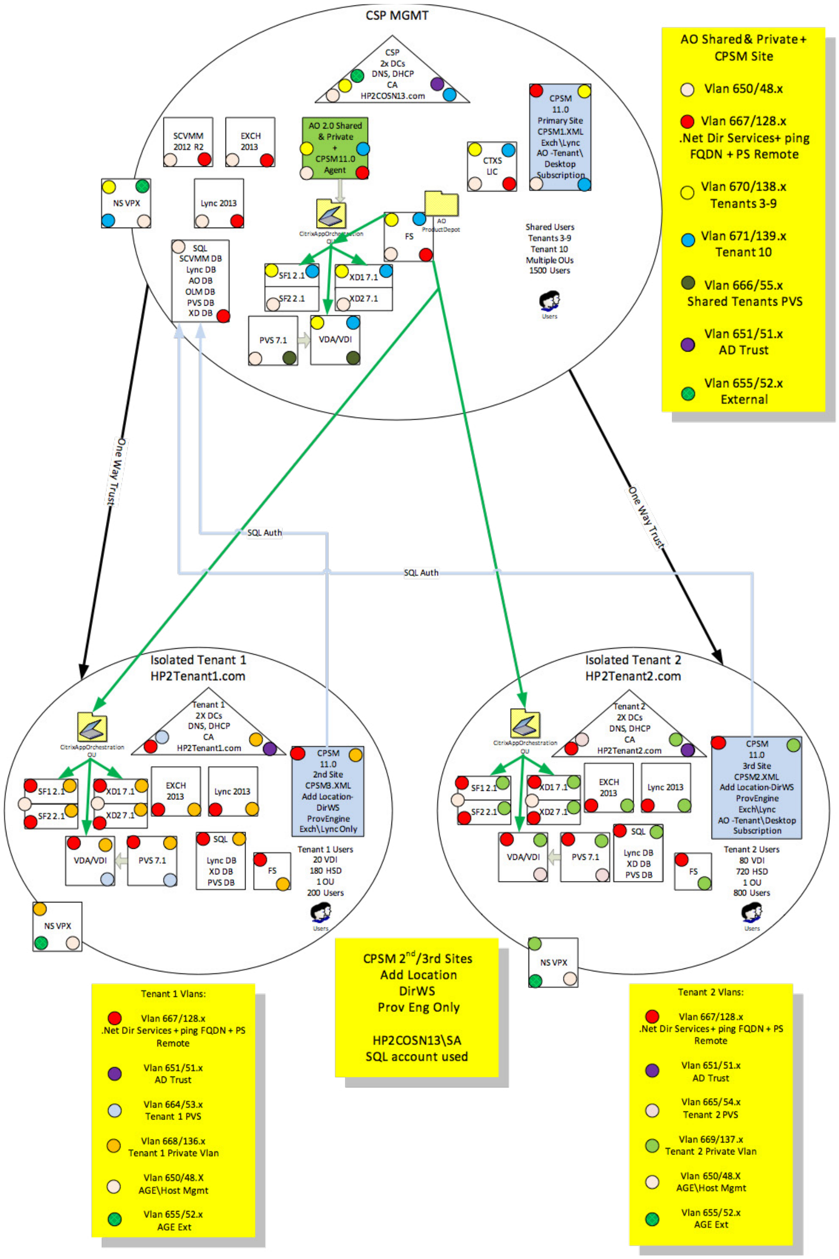

CSP MGMT
CSP
2x DCs
DNS, DHCP
CA
HP2COSN13.com
SCVMM 2012 R2
EXCH 2013
AO 2.0 Shared & Private + CPSM11.0 Agent
CTXS LIC
CPSM 11.0 Primary Site CPSM1.XML Exch\Lync AO -Tenant\ Desktop Subscription
NS VPX
Lync 2013
CitrixAppOrchestration OU
AO ProductDepot
FS
SQL SCVMM DB Lync DB AO DB OLM DB PVS DB XD DB
SF1 2.1
SF2 2.1
XD1 7.1
XD2 7.1
PVS 7.1
VDA/VDI
Shared Users Tenants 3-9 Tenant 10 Multiple OUs 1500 Users
Users
AO Shared & Private + CPSM Site
Vlan 650/48.x
Vlan 667/128.x .Net Dir Services+ ping FQDN + PS Remote
Vlan 670/138.x Tenants 3-9
Vlan 671/139.x Tenant 10
Vlan 666/55.x Shared Tenants PVS
Vlan 651/51.x AD Trust
Vlan 655/52.x External
One Way Trust
One Way Trust
SQL Auth
SQL Auth
Isolated Tenant 1
HP2Tenant1.com
Tenant 1
2X DCs
DNS, DHCP
CA
HP2Tenant1.com
CitrixAppOrchestration OU
SF1 2.1
SF2 2.1
XD1 7.1
XD2 7.1
EXCH 2013
Lync 2013
CPSM 11.0 2nd Site CPSM3.XML Add Location-DirWS ProvEngine Exch\Lync Only
VDA/VDI
PVS 7.1
SQL Lync DB XD DB PVS DB
FS
Tenant 1 Users 20 VDI 180 HSD 1 OU 200 Users
Users
NS VPX
Tenant 1 Vlans:
Vlan 667/128.x .Net Dir Services + ping FQDN + PS Remote
Vlan 651/51.x AD Trust
Vlan 664/53.x Tenant 1 PVS
Vlan 668/136.x Tenant 1 Private Vlan
Vlan 650/48.X AGE\Host Mgmt
Vlan 655/52.x AGE Ext
CPSM 2nd/3rd Sites
Add Location
DirWS
Prov Eng Only
HP2COSN13\SA
SQL account used
Isolated Tenant 2
HP2Tenant2.com
Tenant 2
2X DCs
DNS, DHCP
CA
HP2Tenant2.com
CitrixAppOrchestration OU
SF1 2.1
SF2 2.1
XD1 7.1
XD2 7.1
EXCH 2013
Lync 2013
CPSM 11.0 3rd Site CPSM2.XML Add Location-DirWS ProvEngine Exch\Lync AO -Tenant\Desktop Subscription
VDA/VDI
PVS 7.1
SQL Lync DB XD DB PVS DB
FS
Tenant 2 Users 80 VDI 720 HSD 1 OU 800 Users
Users
NS VPX
Tenant 2 Vlans:
Vlan 667/128.x .Net Dir Services + ping FQDN + PS Remote
Vlan 651/51.x AD Trust
Vlan 665/54.x Tenant 2 PVS
Vlan 669/137.x Tenant 2 Private Vlan
Vlan 650/48.X AGE\Host Mgmt
Vlan 655/52.x AGE Ext

Figure 24: Citrix Solutions Lab Reference Architecture – High Level Architecture

Figure 24 shows a high-level view of the lab architecture. Tenants 1 and 2 are Private Delivery Site tenants and use tenant-specific Active Directory domains (represented by triangles) and site-isolated servers (represented by rectangles) within each dedicated pool of tenant resources (the two bottom ovals). The Citrix Service Provider Management domain (top, Figure 24) depicts the shared resource pool for Tenants 3 through 10, which are Private Delivery Group/Shared Delivery Site tenants. Colored dots show the VLANs that isolate traffic for various functions in the architecture.

The primary site for Cloud Portal Services Manager (CPSM) is defined in the Citrix Service Provider Management domain, with tenant-specific CPSM sites defined in the Tenant 1 and Tenant 2 domains, enabling delegated on-boarding and management capabilities.

Summary of Implementation Details

This table captures important implementation nuances and considerations for providers that deploy the Citrix Service Provider Reference Architecture. Many of these points are "lessons learned" during the integration of solution components in the lab implementation. Refer to the relevant product documentation on the Citrix site (http://www.citrix.com/edocs) and the Citrix Partner site for Citrix Service Providers (https://www.citrix.com/partnercentral) for additional details.

Component	Description
Networking	• Separate virtual networks were defined to maintain functional isolation for security and performance reasons. The reference architecture uses VLANs for separation rather than Hyper-V Gateways and NVGRE (Network Virtualization using Generic Routing Encapsulation). NVGRE was not utilized in this implementation but may be used in a future reference architecture design. • Trust Management VLAN was secured using Hyper-V Extended Virtual Switch Access Control Lists (ACLs). See Appendix C for details. • A PVS network was created for each Private Delivery Site tenant as well as one PVS network for the tenants using a Shared Delivery Site.
Active Directory	• Dedicated OUs were defined for each tenant AD domain and are used to facilitate isolation. The Trust Network was used for inter-domain communication. • For Private Delivery Site tenants: One-way external non-transitive trust was established from the root Citrix Service Provider management domain to the Private Delivery Site tenant AD domains. • For Private Delivery Group/Shared Delivery Site tenants: One-way external non-transitive trust was established from the shared resource domain to the root Citrix Service Provider management domain. • AD OUs map to App Orchestration and CloudPortal Services Manager entities to integrate these components. • App Orchestration requires that all VMs it will touch during the installation must reside initially in the App Orchestration root OU (see Active Directory requirements in "Getting Started with App Orchestration" in the App Orchestration documentation on Citrix eDocs at http://www.citrix.com/edocs). To improve management visibility once App Orchestration is installed, the AO Service Designer can subsequently organize the VMs in an appropriate tree structure under the App Orchestration OU. • To facilitate Citrix Service Provider management, create users in the Admins OU and add them to Domain Admins group.
Microsoft SCVMM	• Physical Microsoft SCVMM 2012 console manages Hyper-V Cluster for infrastructure servers. Virtualized Microsoft SCVMM manages tenant Hyper-V Clusters.
Hyper-V	• Infrastructure systems were virtualized on Hyper-V servers in a dedicated Hyper-V shared services cluster. • Hyper-V Network Virtualization Gateway was virtualized on dedicated 2-host cluster.
Storage	• Scale-Out File Server (SOFS) cluster provides SMB storage to all systems in the environment. • SOFS was added to SCVMM to allow easier centralized management of SMB storage.
App Orchestration	• App Orchestration (AO) was used to deploy Citrix server components for the tenants. • Desktops were externally provisioned with PVS and imported into AO. • The script "New-CamGPO.ps1" should be run on all AD Domain Controllers that will be used by AO. The script creates a GPO that must be linked to the AO root OU in the Citrix Service Provider management, shared resource domain, and isolated tenant resource domains.
CloudPortal Services Manager	• CPSM and its required systems were deployed in conjunction with App Orchestration (see Appendix D). Citrix provides an App Orchestration (AO) agent that supports CPSM and App Orchestration integration. Remove the default CPSM Hosted Apps and Desktops (HAAD) role and replace it with the Hosted Apps and Desktops 11.2 version that supports CPSM and AO integration. (Citrix Service Provider partners can download the Hosted Apps and Desktops 11.2 package from the Citrix partner site. The download is available in the Citrix Cloud Provider Pack; for example, see http://www.citrix.com/downloads/xenapp/product-software/citrix-cloud-provider-pack.html.) • Exchange Schema was added into the root AD Forest; IIS certificates were used for SSL connections to the Web server. • Configure the AD Sync service within CPSM and AD Sync clients on the remote location's Domain Controllers. • Possible errors: - An Internet Explorer 11.0 browser issue has an incompatibility with the CPSM web console (use IE11 in IE mode or the Firefox browser). - During the provisioning process there may be a "Model state is invalid" error on ImportTenantModel. An App Orchestration 2.0 Hotfix may be required (problem case #62337775).
HDX Insight	• Implemented on two virtual servers running XenServer.

Physical Environment

Server and Networking Hardware

Server Hardware	Specifications	Purpose
11x HP ProLiant BL460c Gen 8	2x Intel Xeon E5-2670 processors (2.60GHz, 8-core, 20MB cache) or similar	Virtualized servers hosting infrastructure control layer workloads
27x HP ProLiant BL460c Gen 8	2x Intel Xeon E5-2670 processors (2.60GHz, 8-core, 20MB cache) or similar	Virtualized servers hosting application and desktop workloads
Networking Hardware	**Specifications**	**Purpose**
Cisco Nexus 7010K	8x32/10G	• Switch chassis enabling Layer 3 routing and firewall between VLANS • Core switch for storage network • VLAN edge switches

Storage Configuration

The Citrix Solutions Lab implementation of this reference architecture used EMC VNX7600 unified storage. Clustered file servers converted iSCSI LUNs into CIFS shares, which were created and presented to Hyper-V as storage repositories. The table below shows the LUNs defined, their purpose, and cluster assignment.

Storage Space (GB)	Name	Purpose	Storage Protocol
432	T1HSD	T1 Desktop & Service Cluster	CIFS
2976	T1Infra	T1 Desktop & Service Cluster	CIFS
162	T1Server VDI	T1 Desktop & Service Cluster	CIFS
54	T1User Profile	T1 Desktop & Service Cluster	CIFS
675	T1vDisk	T1 Desktop & Service Cluster	CIFS
864	T2HSD	T2 Desktop Cluster	CIFS
2819	T2Infra	T2 Desktop Cluster	CIFS
2	T2Quorum Witness	T2 Desktop Cluster	CIFS
648	T2Server VDI	T2 Desktop Cluster	CIFS
216	T2User Profile	T2 Desktop Cluster	CIFS
675	T2vDisk	T2 Desktop Cluster	CIFS
50	Misc Storage	SOFS Cluster	iSCSI
5679	T3-10 Shared Cluster Infrastructure LUN	T3-10 Shared Cluster	CIFS
2783	T3-10 Tenant Desktop LUN	T3-10 Shared Cluster	CIFS
200	SSC SCVMM Library	SSC Cluster	CIFS
3105	SSC VM Storage	SSC Cluster	CIFS
1	SSC Cluster Witness	SSC Cluster	CIFS
200	SSC SQL AlwaysOn	SSC Cluster	CIFS
1	SOFS Cluster Witness	SSC Cluster	iSCSI
135	SSC File Server LUN	SOFS Cluster	CIFS

Software Versions

Vendor	Product	Version
Citrix	App Orchestration CloudPortal Services Manager License Server NetScaler AGEE Provisioning Services Received for Windows StoreFront User Profile Manager XenDesktop	2.0 11.0.1 11.11.1 10.1.x (.120.13) 7.1 4.1 2.1 5.x 7.1
Microsoft	Office Lync Exchange SCVMM SQL Server Windows (Clients Only) Windows Server	2013 2013 2013 2012 R2 2012 R2 7 x64 SP1 and 8.1 2012 R2 with Hyper-V

VLAN Details

Separate virtual networks (Figure 25) were defined to maintain functional isolation for security and performance reasons:

- Citrix Service Provider Host Management Network (1 VLAN)
- Citrix Service Provider Shared Services Management (1 VLAN)
- AD Trust Network (1 VLAN)
- Hyper-V Storage Network (1 VLAN), as well as Storage VLANs connected to the Scale-Out File Server Cluster (2 VLANs)
- Tenant VM Network (1 VLAN per tenant)
- PVS Provisioning (1 VLAN per Private Delivery Site tenant plus 1 VLAN shared tenant)
- External (1 VLAN for Internet/WAN & NetScaler VPX)

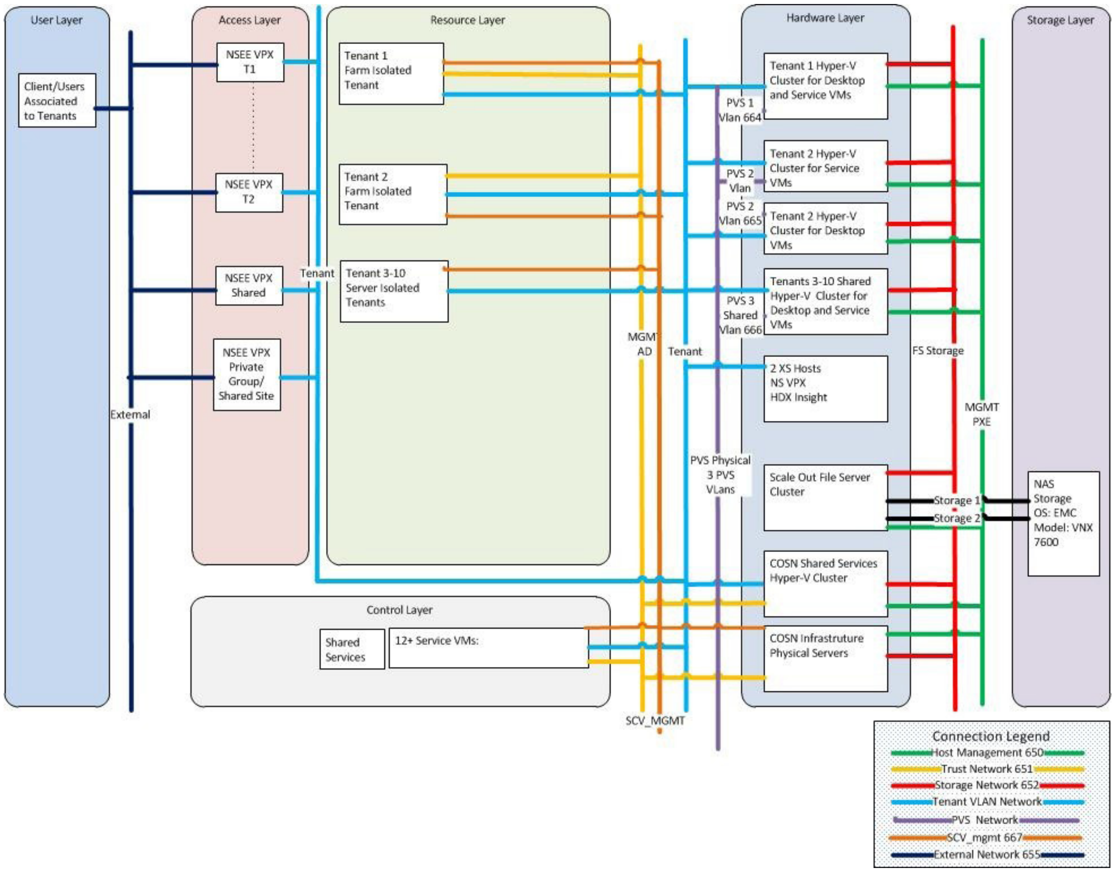

User Layer
Client/Users Associated to Tenants
External
Access Layer
NSEE VPX T1
NSEE VPX T2
NSEE VPX Shared
NSEE VPX Private Group/ Shared Site
Tenant
Resource Layer
Tenant 1 Farm Isolated Tenant
Tenant 2 Farm Isolated Tenant
Tenant 3-10 Server Isolated Tenants
MGMT AD
Tenant
PVS 1 Vlan 664
PVS 2 Vlan
PVS 2 Vlan 665
PVS 3 Shared Vlan 666
PVS Physical 3 PVS VLans
Hardware Layer
Tenant 1 Hyper-V Cluster for Desktop and Service VMs
Tenant 2 Hyper-V Cluster for Service VMs
Tenant 2 Hyper-V Cluster for Desktop VMs
Tenants 3-10 Shared Hyper-V Cluster for Desktop and Service VMs
2 XS Hosts NS VPX HDX Insight
Scale Out File Server Cluster
COSN Shared Services Hyper-V Cluster
COSN Infrastruture Physical Servers
FS Storage
MGMT PXE
Storage 1
Storage 2
Storage Layer
NAS Storage OS: EMC Model: VNX 7600
Control Layer
Shared Services
12+ Service VMs:
SCV_MGMT
Connection Legend
Host Management 650
Trust Network 651
Storage Network 652
Tenant VLAN Network
PVS Network
SCV_mgmt 667
External Network 655

Figure 25: Citrix Solutions Lab Implementation – VLANs

Each network in the sample implementation 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.

VLAN	Description
Citrix Service Provider Host Management	• Citrix Service Provider Root AD Domain primary device network • Physical hardware host management interface network • Hyper-V Host Management via SCVMM • Windows Deployment Services (WDS) from bare metal WDS/SCVMM console
AD Trust Network	• Active Directory Trust communication between domain AD DCs and Tenant AD DCs • Configured to allow Tenant to Citrix Service Provider Root AD DC communication only; secured using Extended Virtual Switch ACLs at Hyper-V host level.
Hyper-V Storage	• Hyper-V Host communication to Scale Out File Servers (SOFS)
iSCSI Storage	• Storage VLANs connected from EMC VNX iSCSI to the SOFS Cluster
External Network	• External WAN network for cloud environment
PVS	• PVS VLAN required for each tenant in addition to a shared PVS VLAN • Used for PVS Server streaming and PXE booting of streamed desktop VMs in tenants
Citrix Service Provider Shared Services Management	• Communication between shared services: Root AD, App Orchestration, CPSM, SCVMM, XenDesktop servers (DC, PVS, StoreFront, VDA), Citrix Licensing, desktop VMs, etc. • Hyper-V Extended Virtual Switch ACLs configured to prevent tenant VMs from seeing other tenant communications. Requires consistent tenant naming in all VMs.
Tenant	• Tenant private system communication, 1 VLAN per tenant

Tenant Details

The lab implementation characterized each tenant as having a 90:10 mix of Hosted Shared Desktops and VDI workloads.

Tenant	Isolation Model	HSD/VDI Workloads	Hyper-V Clustering
1	Private Delivery Site	200 Users: 180 Hosted Shared Desktops 20 Server VDI (Random Pooled Desktops)	1 Hyper-V cluster (Service & Desktop VMs)
2	Private Delivery Site	800 Users: 720 Hosted Shared Desktops 80 Server VDI (Random Pooled Desktops)	2 Hyper-V clusters (1 for Service VMs, 1 for Desktop VMs)
3	Private Delivery Group/Shared Delivery Site	50 Users: 40 Hosted Shared Desktops 10 Server VDI (Random Pooled Desktops)	Single shared Hyper-V cluster (Shared Service VMs & Tenant-specific Desktop VMs)
4		50 Users: 40 Hosted Shared Desktops 10 Server VDI (Random Pooled Desktops	
5		50 Users: 40 Hosted Shared Desktops 10 Server VDI (Random Pooled Desktops	
6		50 Users: 40 Hosted Shared Desktops 10 Server VDI (Random Pooled Desktops	
7		100 Users: 90 Hosted Shared Desktops 10 Server VDI (Random Pooled Desktops	
8		200 Users: 180 Hosted Shared Desktops 20 Server VDI (Random Pooled Desktops)	
9		400 Users: 360 Hosted Shared Desktops 40 Server VDI (Random Pooled Desktops)	
10	Private Delivery Group/Shared Delivery Site	600 Users: 540 Hosted Shared Desktops 60 Server VDI (Random Pooled Desktops)	1 Hyper-V Cluster (Resource VMs & Desktop VMs)

Tenant Environment and Size

Tenant	Desktop VMs	Service VMs	Required Hosts	N+1
Tenant 1 Cluster	24	18	4	5
Tenant 2 Clusters	-- 96	18 --	3 5	4 6
Tenant 3-9 Cluster	108	18	9	10
Tenant 10 Cluster	71	0	4	5
Total	299	54	25	30

Infrastructure Implementation

Private Delivery Site Tenant

Figure 26 depicts the infrastructure implemented in the lab to deploy a Private Delivery Site tenant (Tenant 1).

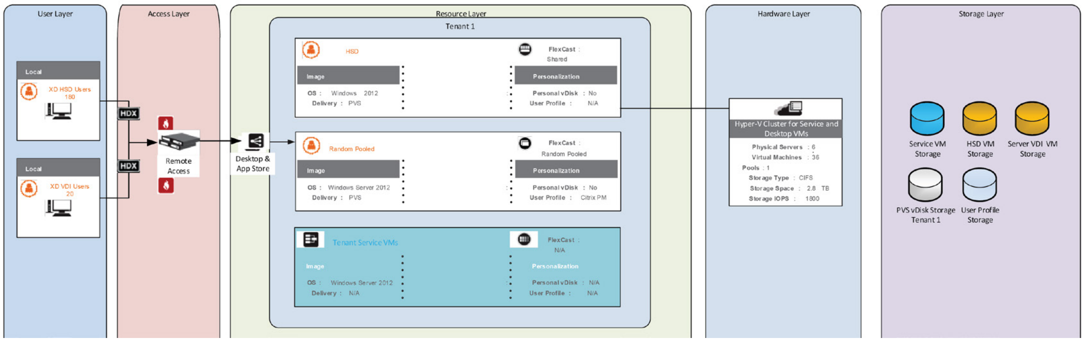


Figure 26: Implementation Detail for Private Delivery Site Tenant

Private Delivery Group/Shared Delivery Site Tenant

Figure 27 shows the infrastructure implemented in the lab to deploy Tenants 3-9, Private Delivery Group/Shared Delivery Site tenants of various sizes.

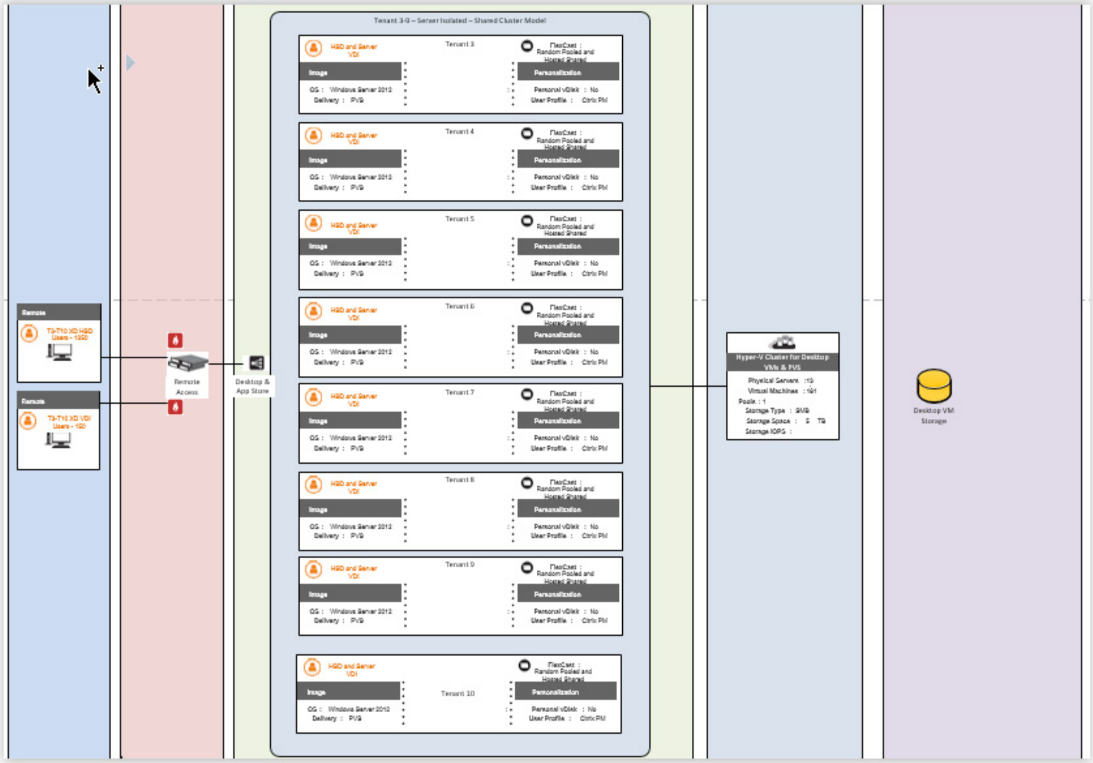


Figure 27: Implementation Detail for Private Delivery Group/Shared Delivery Site Tenant

Citrix Service Provider Control Layer

Figure 28 shows the infrastructure for the Citrix Service Provider Control layer.

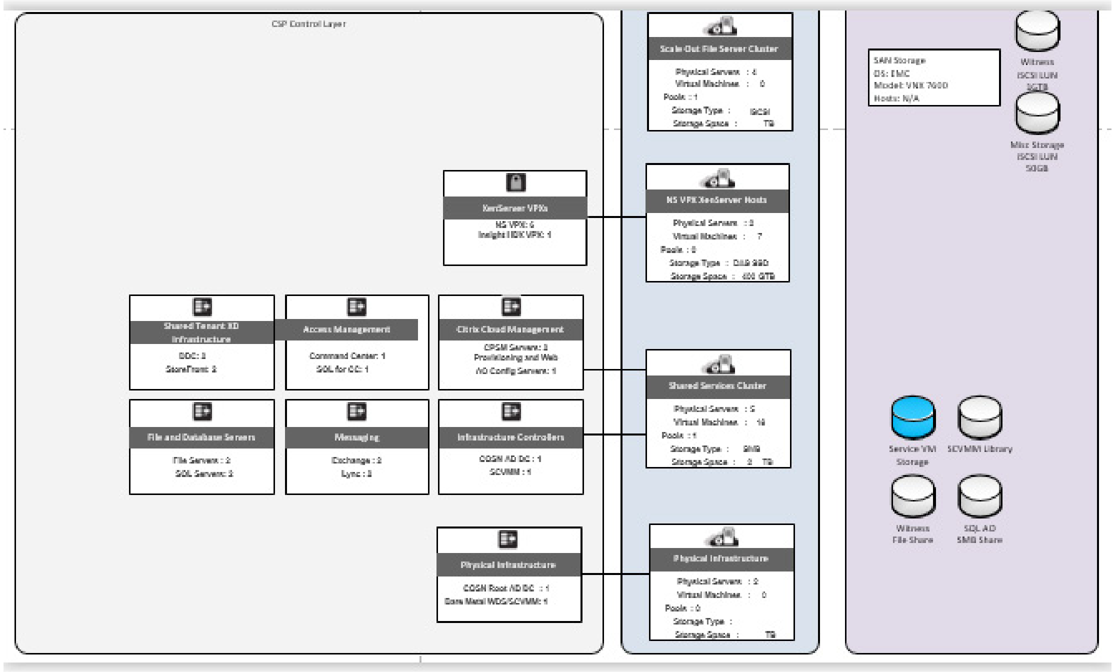


Figure 28: Implementation Detail for Citrix Service Provider Control Layer

Hyper-V Cluster Configurations

Clusters

Cluster Name	Function	Cluster IP	Witness
SOFS	Scale Out File Server	192.168.48.30	iSCSI Disk Witness
SharedServices	Shared Services	192.168.48.31	\\sofileserver\Misc\SharedServices_Witness
TS-DS	Tenant Shared	192.168.48.103	NA
SQLC-CSP	SQL Always-On	192.168.48.19	\\sofileserver\Misc\SQLC_Witness
Tenant1-DS	Tenant 1 Desktop and Services	192.168.48.76	NA
T1-SQLC	SQL Always-On	192.168.136.29	NA
Tenant2-D	Tenant 2 Desktop	192.168.48.77	NA
Tenant2-S	Tenant 2 Services	192.168.48.78	NA
T2-SQLC	SQL Always-On	192.168.137.29	NA
CLInfra	Client Launcher Services	192.168.50.171	NA
ClientLaunchers	Client Launcher Desktops	192.168.50.172	iSCSI Disk Witness

Tenant Desktop Clusters and VMs

Separate tenant clusters were deployed to host HDS and VDI workloads. The specific number and configuration of VM instances that a provider will need to deploy will vary according to desktop sizing and workload requirements. The tenant desktop cluster also includes Master-SVRVDI, Master-HSD, Template-HSD, and Template-SVRVDI VMs. Citrix Provisioning Services and SCVMM use these master and template VMs to deploy the HSD and VDI VMs for the tenant.

VM Name	Function	Qty.	CPU	RAM	GB	Master Image HDD
T1-HSD###	HSD	4	8	12-16	8	100
T1-VDI###	VDI	20	2	2	4	100
T2-HSD###	HSD	16	8	16	8	100
T2-VDI###	VDI	80	2	2	4	100
T3-HSD###	HSD	1	8	16	8	100
T3-VDI###	VDI	5	2	2	4	100
T4-HSD###	HSD	1	8	16	8	100
T4-VDI###	VDI	5	2	2	4	100
T5-HSD###	HSD	1	8	16	8	100
T5-VDI###	VDI	5	2	2	4	100
T6-HSD###	HSD	1	8	16	8	100
T6-VDI###	VDI	5	2	2	4	100
T7-HSD###	HSD	2	8	16	8	100
T7-VDI###	VDI	10	2	2	4	100
T8-HSD###	HSD	4	8	16	8	100
T8-VDI###	VDI	20	2	2	4	100
T9-HSD###	HSD	8	8	16	8	100
T9-VDI###	VDI	40	2	2	4	100
T10-HSD###	HSD	11	8	16	8	100
T10-VDI###	VDI	60	2	2	4	100

Tenant Infrastructure Cluster for Private Delivery Site Tenant

This tenant cluster is typical for the infrastructure needed to deploy a Private Delivery Site, although the number and configuration of VM instances may vary by function and sizing requirements. The table lists the VMs defined for the Tenant 2 infrastructure cluster in the lab implementation.

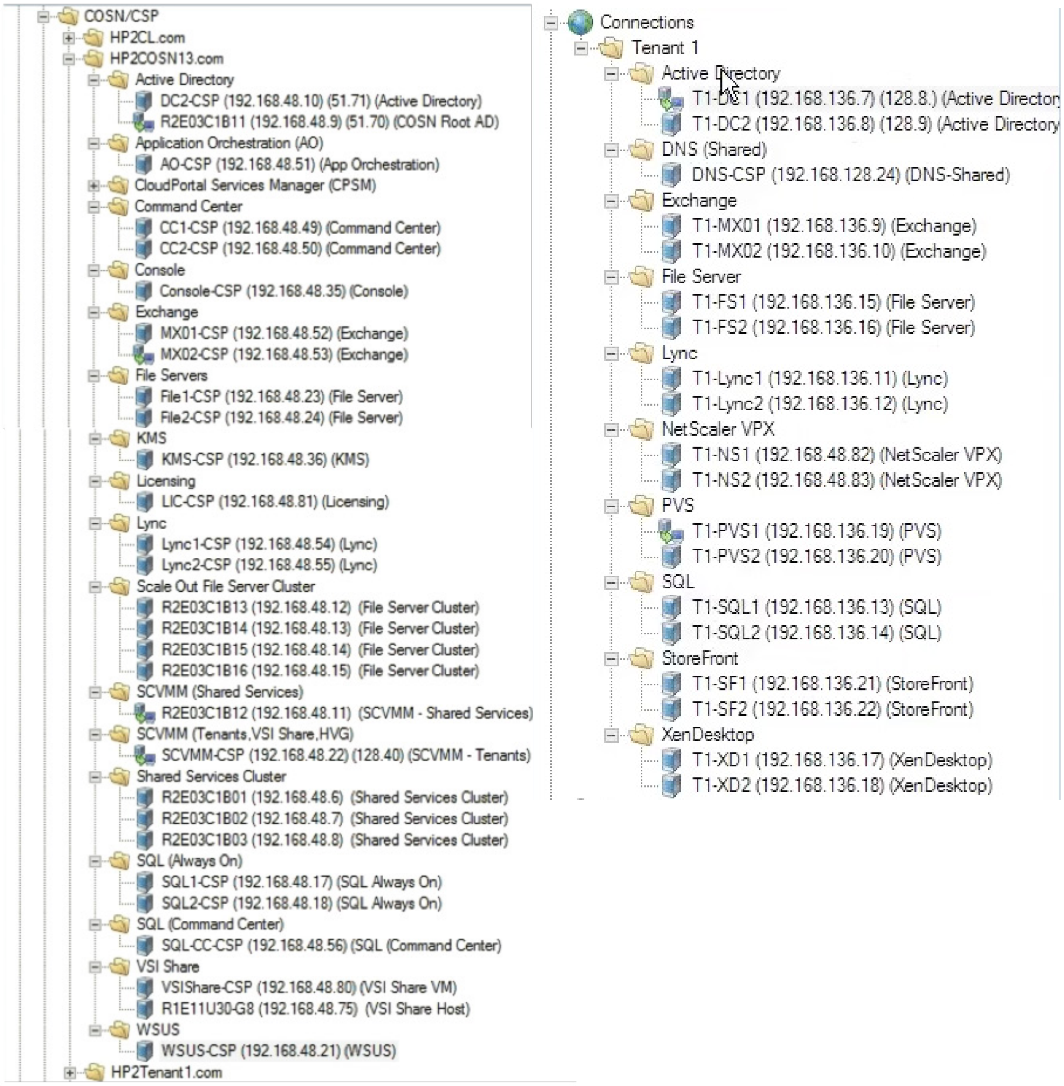
VM Name	Function	CPU	RAM	GB
T2-Console	Console	4	4	60
T2-DC1	Active Directory	2	4	60
T2-DC2	Active Directory	2	4	60
T2-MX1, MX2	Microsoft Exchange	2	4	60
T2-Lync1, Lync2	Microsoft Lync	2	8	100
T2-SQL1, SQL 2	SQL	1	32	100
T2-FS1, FS2	File Server	2	4	100
T2-XD1, XD2	XenDesktop	2	2	60
T2-PVS1, PVS2	PVS	2	4	60
T2-SF1, SF2	StoreFront	8	4	60
T2-NS1, NS2	NetScaler VPX for XS	2	4	20
T2-CPSM1	CPSM	4	4	100

Tenant Infrastructure within XD Cluster for Private Delivery Group/Shared Delivery Site Tenant

VM Name	Function	CPU	RAM	GB
TS-PVS1, PVS2	PVS	2	4	60
DC2-CSP	Active Directory	2	4	60
SQL1-CSP, SQL2-CSP	SQL (Always On)	1	4	100
WSUS-CSP	WSUS	2	6	100
File1-CSP, File2-CSP	File Server	4	4	60
SCVMM-CSP	SCVMM	4	4	60
CC1-CSP	NetScaler Command Center (Win2012R2)	2	2	60
AO-CSP	App Orchestration	2	4	60
MX1-CSP, MX2-CSP	Exchange	2	8	100
Lync1-CSP, Lync2-CSP	Lync	2	32	100
SQL-CC-CSP	SQL (Command Center) (WS2012R2/SQL2008R2)	1	4	100
CPSM1-CSP, CPSM2-CSP	CloudPortal Service Manager	2	2	100
LIC-CSP	Citrix License / RDS Server	2	4	60
KMS-CSP	KMS Router for licensing	2	2	60
TS-XD1	XenDesktop	2	4	60
TS-XD2	XenDesktop	2	4	60
TS-SF1	StoreFront	2	4	60
TS-SF2	StoreFront	2	4	60
TS-NS1	NetScaler VPX (Pair 1)	6	12	20
TS-NS2	NetScaler VPX (Pair 1)	6	12	20

Active Directory Configuration

Figure 29 shows the Active Directory configuration for the Citrix Service Provider root and Tenant1 domains in the lab implementation.



```
COSN/CSP
  HP2CL.com
  HP2COSN13.com
    Active Directory
      DC2-CSP (192.168.48.10) (51.71) (Active Directory)
      R2E03C1B11 (192.168.48.9) (51.70) (COSN Root AD)
    Application Orchestration (AO)
      AO-CSP (192.168.48.51) (App Orchestration)
    CloudPortal Services Manager (CPSM)
    Command Center
      CC1-CSP (192.168.48.49) (Command Center)
      CC2-CSP (192.168.48.50) (Command Center)
    Console
      Console-CSP (192.168.48.35) (Console)
    Exchange
      MX01-CSP (192.168.48.52) (Exchange)
      MX02-CSP (192.168.48.53) (Exchange)
    File Servers
      File1-CSP (192.168.48.23) (File Server)
      File2-CSP (192.168.48.24) (File Server)
    KMS
      KMS-CSP (192.168.48.36) (KMS)
    Licensing
      LIC-CSP (192.168.48.81) (Licensing)
    Lync
      Lync1-CSP (192.168.48.54) (Lync)
      Lync2-CSP (192.168.48.55) (Lync)
    Scale Out File Server Cluster
      R2E03C1B13 (192.168.48.12)  (File Server Cluster)
      R2E03C1B14 (192.168.48.13)  (File Server Cluster)
      R2E03C1B15 (192.168.48.14)  (File Server Cluster)
      R2E03C1B16 (192.168.48.15)  (File Server Cluster)
    SCVMM (Shared Services)
      R2E03C1B12 (192.168.48.11)  (SCVMM - Shared Services)
    SCVMM (Tenants,VSI Share,HVG)
      SCVMM-CSP (192.168.48.22) (128.40) (SCVMM - Tenants)
    Shared Services Cluster
      R2E03C1B01 (192.168.48.6)  (Shared Services Cluster)
      R2E03C1B02 (192.168.48.7)  (Shared Services Cluster)
      R2E03C1B03 (192.168.48.8)  (Shared Services Cluster)
    SQL (Always On)
      SQL1-CSP (192.168.48.17) (SQL Always On)
      SQL2-CSP (192.168.48.18) (SQL Always On)
    SQL (Command Center)
      SQL-CC-CSP (192.168.48.56) (SQL (Command Center)
    VSI Share
      VSIShare-CSP (192.168.48.80) (VSI Share VM)
      R1E11U30-G8 (192.168.48.75)  (VSI Share Host)
    WSUS
      WSUS-CSP (192.168.48.21) (WSUS)
  HP2Tenant1.com
```

```
Connections
  Tenant 1
    Active Directory
      T1-DC1 (192.168.136.7) (128.8.) (Active Director
      T1-DC2 (192.168.136.8) (128.9) (Active Directory
    DNS (Shared)
      DNS-CSP (192.168.128.24) (DNS-Shared)
    Exchange
      T1-MX01 (192.168.136.9) (Exchange)
      T1-MX02 (192.168.136.10) (Exchange)
    File Server
      T1-FS1 (192.168.136.15) (File Server)
      T1-FS2 (192.168.136.16) (File Server)
    Lync
      T1-Lync1 (192.168.136.11) (Lync)
      T1-Lync2 (192.168.136.12) (Lync)
    NetScaler VPX
      T1-NS1 (192.168.48.82) (NetScaler VPX)
      T1-NS2 (192.168.48.83) (NetScaler VPX)
    PVS
      T1-PVS1 (192.168.136.19) (PVS)
      T1-PVS2 (192.168.136.20) (PVS)
    SQL
      T1-SQL1 (192.168.136.13) (SQL)
      T1-SQL2 (192.168.136.14) (SQL)
    StoreFront
      T1-SF1 (192.168.136.21) (StoreFront)
      T1-SF2 (192.168.136.22) (StoreFront)
    XenDesktop
      T1-XD1 (192.168.136.17) (XenDesktop)
      T1-XD2 (192.168.136.18) (XenDesktop)
```

Figure 29: Active Directory Root OUs for Citrix Service Provider Domain HP2COSN13.com (left) and Tenant 1 Domain (right).

Virtual Machine Configurations

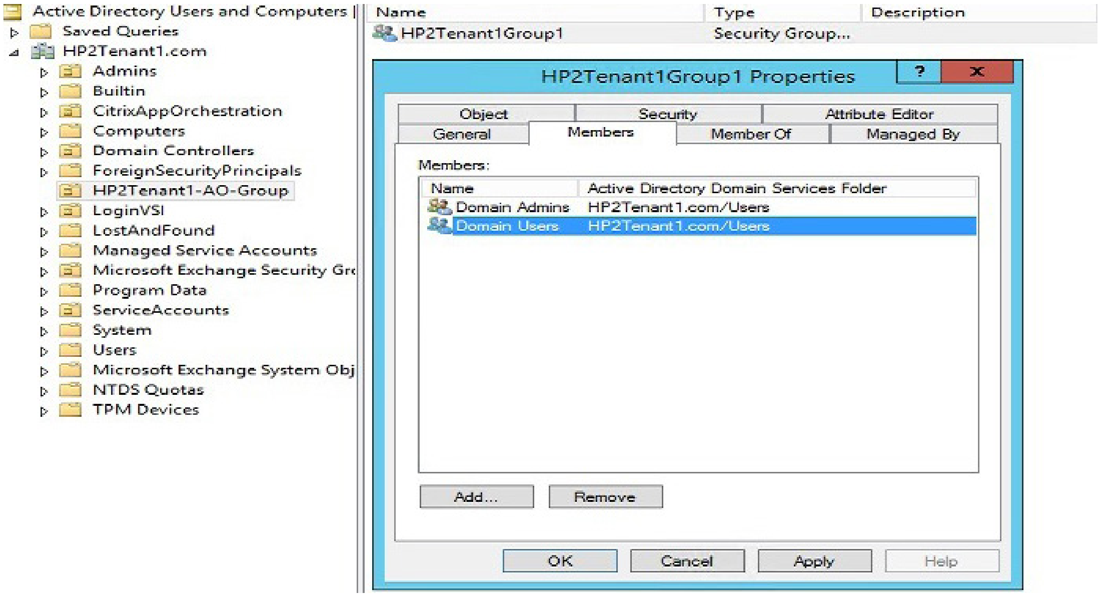
Purpose	Description
Active Directory domain controllers	• OS: Microsoft Windows Server 2012 R2 • Installed roles: Active Directory Services • Additional software: None
XenDesktop SQL Database servers	• OS: Microsoft Windows Server 2012 R2 • Installed roles: Microsoft .NET Framework 4.0 • Additional software: Microsoft SQL Server 2012 SP1
XenDesktop Delivery Controllers	• OS: Microsoft Windows Server 2012 R2 • Installed roles: Automatically deployed with XenDesktop installation wizard • Additional software: XenDesktop 7.1
Citrix License Server	• OS: Microsoft Windows Server 2012 R2 • Installed roles: None • Additional software: Citrix License Server 11.11.1
Citrix Studio	• OS: Microsoft Windows 7, Windows 8, Windows Server 2012, or Windows Server 2008 R2 SP1 • Installed roles: Microsoft Management Console 3.0 • Additional software: installed with XenDesktop • Hypervisor: Microsoft 2012 R2 with Hyper-V
NetScaler Gateway VPX servers	• OS: NetScaler VPX • Installed roles: None • Additional software: None • Hypervisor: XenServer 6.2
CloudPortal Services Manager front-end servers	• OS: Microsoft Windows Server 2012 R2 SP1 • Hypervisor: Microsoft 2012 R2 with Hyper-V • Virtual server configuration: 4 vCPU, 8GB RAM • Virtual NIC: 1x NIC
CloudPortal Services Manager Provisioning Engine servers	• OS: Microsoft Windows Server 2012 R2 SP1 • Hypervisor: Microsoft 2012 R2 with Hyper-V • Virtual NICs: 1x NIC Zone 2 Network, 1x NIC heartbeat network
CloudPortal Services Manager database server	• OS: Microsoft Windows Server 2012 R2 • Additional software: Microsoft SQL 2012 R2 • Hypervisor: Microsoft 2012 R2 with Hyper-V

Group Policy Object Management

This section describes GPO configuration required to support the reference architecture implementation in the Citrix Solutions Lab.

The advantage of cascading Group Policy Objects (GPOs) in Active Directory is that they enable significant tenant and SLA customization with minimal administrative effort. This is largely because a child Organizational Unit (OU) inherits properties from the parent OU, allowing properties to be easily propagated.

Many GPO properties and settings have critical implications in a multi-tenant environment. As shown below, the ForeignSecurityPrincipals property defines security members and administrative group access for each tenant domain. For domains across this reference architecture, it’s crucial that GPO settings are precisely configured to facilitate centralized tenant administration and meet tenant isolation requirements.



- Active Directory Users and Computers
  - Saved Queries
  - HP2Tenant1.com
    - Admins
    - Builtin
    - CitrixAppOrchestration
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - HP2Tenant1-AO-Group
    - LoginVSI
    - LostAndFound
    - Managed Service Accounts
    - Microsoft Exchange Security Gr
    - Program Data
    - ServiceAccounts
    - System
    - Users
    - Microsoft Exchange System Obj
    - NTDS Quotas
    - TPM Devices

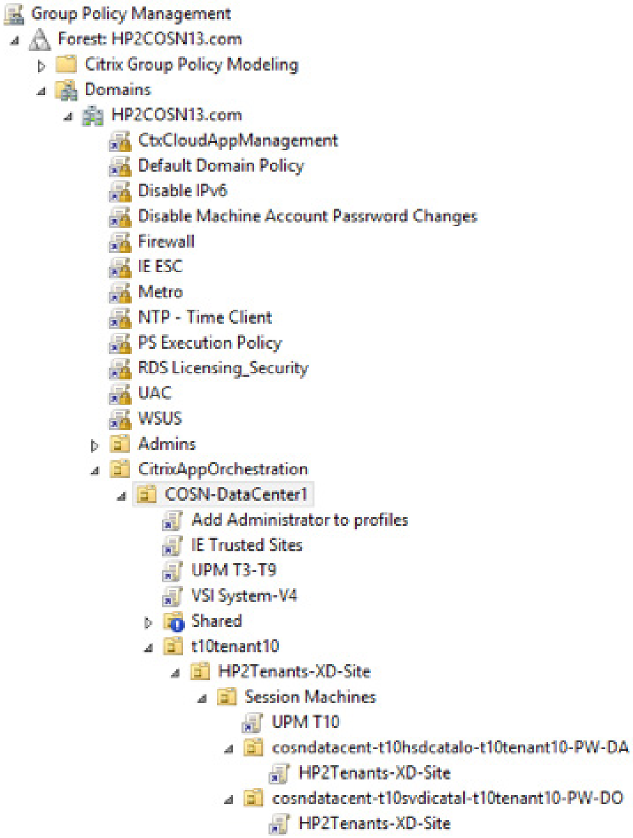
Name	Type	Description
HP2Tenant1Group1	Security Group...	

HP2Tenant1Group1 Properties

Members:

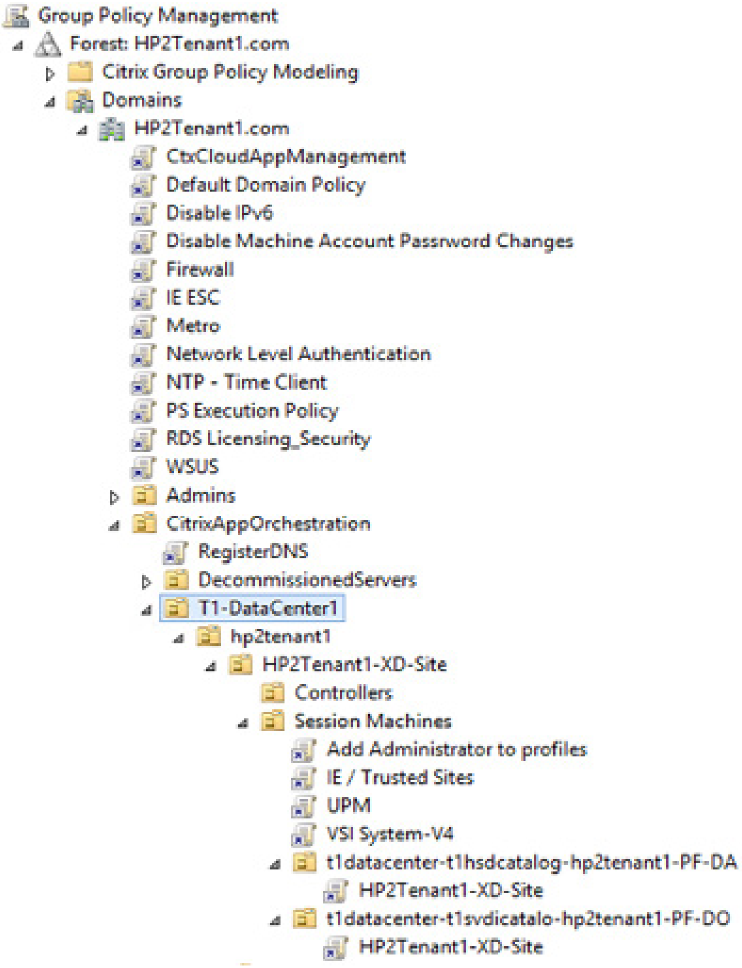
Name	Active Directory Domain Services Folder
Domain Admins	HP2Tenant1.com/Users
Domain Users	HP2Tenant1.com/Users

The screenshot excerpt below represents the GPOs created in the root Citrix Service Provider Management domain HP2COSN13.com.



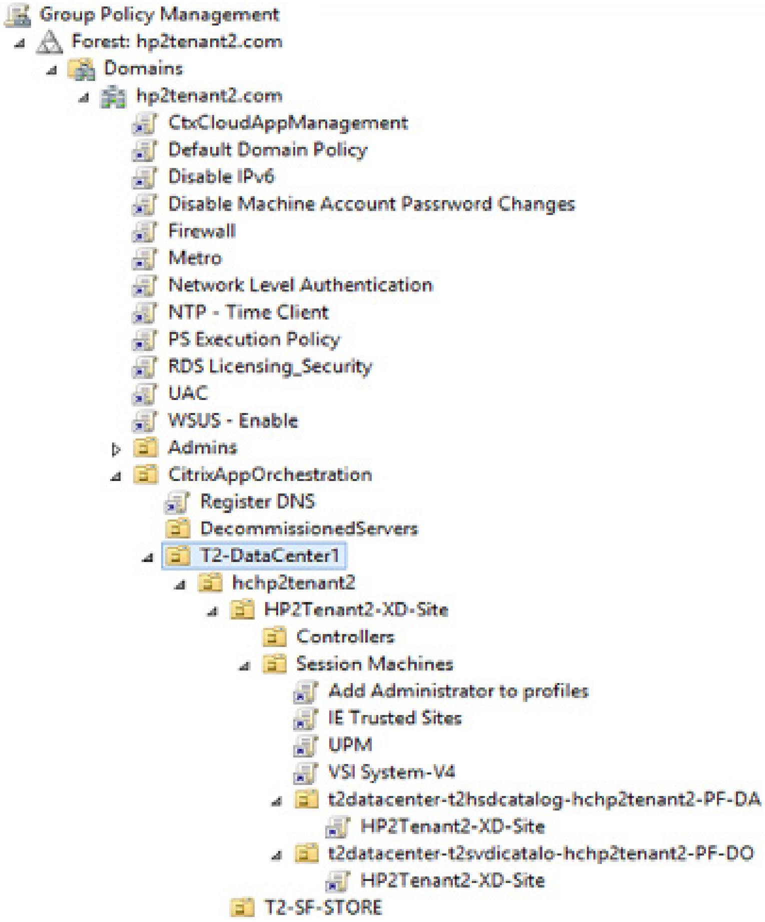
- Group Policy Management
  - Forest: HP2COSN13.com
    - Citrix Group Policy Modeling
    - Domains
      - HP2COSN13.com
        - CtxCloudAppManagement
        - Default Domain Policy
        - Disable IPv6
        - Disable Machine Account Passrword Changes
        - Firewall
        - IE ESC
        - Metro
        - NTP - Time Client
        - PS Execution Policy
        - RDS Licensing_Security
        - UAC
        - WSUS
        - Admins
        - CitrixAppOrchestration
          - COSN-DataCenter1
            - Add Administrator to profiles
            - IE Trusted Sites
            - UPM T3-T9
            - VSI System-V4
            - Shared
            - t10tenant10
              - HP2Tenants-XD-Site
                - Session Machines
                  - UPM T10
                  - cosndatacent-t10hsdcatalo-t10tenant10-PW-DA
                    - HP2Tenants-XD-Site
                  - cosndatacent-t10svdicatal-t10tenant10-PW-DO
                    - HP2Tenants-XD-Site

The screenshot below lists GPOs for HPTenant1.com, which is the root domain for Tenant 1, a Private Delivery Site tenant.



```
Group Policy Management
  Forest: HP2Tenant1.com
    Citrix Group Policy Modeling
    Domains
      HP2Tenant1.com
        CtxCloudAppManagement
        Default Domain Policy
        Disable IPv6
        Disable Machine Account Passrword Changes
        Firewall
        IE ESC
        Metro
        Network Level Authentication
        NTP - Time Client
        PS Execution Policy
        RDS Licensing_Security
        WSUS
        Admins
        CitrixAppOrchestration
          RegisterDNS
          DecommissionedServers
          T1-DataCenter1
            hp2tenant1
              HP2Tenant1-XD-Site
                Controllers
                Session Machines
                  Add Administrator to profiles
                  IE / Trusted Sites
                  UPM
                  VSI System-V4
                  t1datacenter-t1hsdcatalog-hp2tenant1-PF-DA
                    HP2Tenant1-XD-Site
                  t1datacenter-t1svdicatalo-hp2tenant1-PF-DO
                    HP2Tenant1-XD-Site
```

The screenshot below lists GPOs for HPTenant2.com, which is the root domain for Tenant 2, a Private Delivery Site tenant.



```
Group Policy Management
  Forest: hp2tenant2.com
    Domains
      hp2tenant2.com
        CtxCloudAppManagement
        Default Domain Policy
        Disable IPv6
        Disable Machine Account Passrword Changes
        Firewall
        Metro
        Network Level Authentication
        NTP - Time Client
        PS Execution Policy
        RDS Licensing_Security
        UAC
        WSUS - Enable
        Admins
        CitrixAppOrchestration
          Register DNS
          DecommissionedServers
          T2-DataCenter1
            hchp2tenant2
              HP2Tenant2-XD-Site
                Controllers
                Session Machines
                  Add Administrator to profiles
                  IE Trusted Sites
                  UPM
                  VSI System-V4
                  t2datacenter-t2hsdcatalog-hchp2tenant2-PF-DA
                    HP2Tenant2-XD-Site
                  t2datacenter-t2svdicatalo-hchp2tenant2-PF-DO
                    HP2Tenant2-XD-Site
              T2-SF-STORE
```

GPO Properties for Root Citrix Service Provider Domain

GPO properties for the root Citrix Service Provider domain HP2COSN13.com are set at the Domain Control Level (for the NTP server) and the Domain Level. In the lab implementation, GPO properties were configured as shown below.

GPO	Policy	Setting
NTP Time Server (Domain Control Level)	Configure Windows NTP Client	Enabled NtpServer: 192.168.51.70,0x9 Type: NTP CrossSiteSyncFlags: 2 ResolvePeerBackoffMinutes: 15 ResolvePeerBackoffMaxTimes: 7 SpecialPollInterval: 3600 EventLogFlags: 0
Add Administrator to profiles	Delegation	HP2COSN13\Domain Admins: Edit settings, delete, modify security; Inherited: No HP2COSN13\Enterprise Admins: Edit settings, delete, modify security; Inherited: No NT AUTHORITY\Authenticated Users Read (from Security Filtering); Inherited: No NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS Read; Inherited: No NT AUTHORITY\SYSTEM: Edit settings, delete, modify security; Inherited: No
	Add the Administrators security group to roaming user profiles	Enabled
Disable IPv6	Registry item: DisabledComponents	
Disable Machine Account Password Changes	Domain member: Disable machine account password changes	Enabled
Firewall	Global Settings	Policy version 2.10 Other settings not configured
	Domain, Private, & Public Profile Settings	Firewall state off Other settings not configured
	Prohibit use of Internet Connection Sharing on your DNS domain network	Enabled
	Windows Firewall: Protect all network connections	Disabled
	Enhance Internet Explorer Security for Admin & User accounts on the machine	Both Disabled
IE ESC	Enhance Internet Explorer Security for Admin & User accounts on the machine	Both Disabled
NTP - Time Client	Global Configuration Settings	Enabled
	Enable Windows NTP Client	Enabled
PS Execution Policy	Registry item: ExecutionPolicy	Action: Update Hive: HKEY_LOCAL_MACHINE Key path: SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell Value name: ExecutionPolicy Value type: REG_SZ Value data: Bypass
RDS Licensing Security	Allow users to connect remotely by using Remote Desktop Services	Enabled

	Set the Remote Desktop licensing mode	Enabled. Specify the licensing mode for the RD Session Host server: Per device
	Use the specified Remote Desktop license servers	Enabled. License servers to use: 192.168.48.81
	Require user authentication for remote connections by using Network Level Authentication	Disabled
User Account Control (UAC)	Behavior of the elevation prompt for administrators in Admin Approval Mode	Elevate without prompting
	Detect app installations and prompt for elevation	Disabled
	Run all administrators in Admin Approval Mode	Disabled
WSUS	Allow Automatic Updates immediate installation	Enabled
	Allow signed updates from an intranet Microsoft update service location	Enabled
	Configure Automatic Updates	Configure automatic updating - Enabled: 4 - Auto download and schedule the install Install during automatic maintenance: Disabled Scheduled install day: 0 - Every day Scheduled install time: 12:00
	Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box	Enabled
	Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Enabled
	No auto-restart with logged on users for scheduled automatic updates installations	Enabled
	Specify intranet Microsoft update service location	Enabled Set the intranet update service for detecting updates: http://192.168.48.21:8530 Set the intranet statistics server: http://192.168.48.21:8530 (example: http://IntranetUpd01)

GPO Properties for Tenant Domains

GPO properties for each tenant domain must be set at the Domain Control Level (for the NTP server) and the Domain Level. In the lab implementation, GPO properties were configured for the HP2Tenant 1.com domain as shown below.

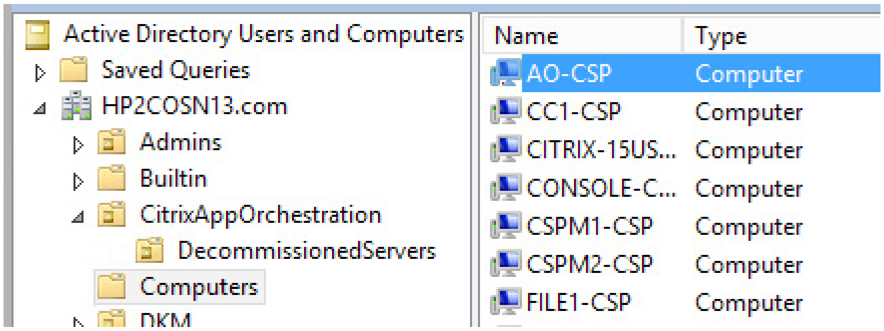
GPO	Policy	Setting
NTP Time Server (Domain Control Level)	Configure Windows NTP Client	Enabled NtpServer: 192.168.51.70,0x9 Type: NTP CrossSiteSyncFlags: 2 ResolvePeerBackoffMinutes: 15 ResolvePeerBackoffMaxTimes: 7 SpecialPollInterval: 3600 EventLogFlags: 0
Add Administrator to profiles	Delegation	HP2COSN13\Domain Admins: Edit settings, delete, modify security; Inherited: No HP2COSN13\Enterprise Admins: Edit settings, delete, modify security; Inherited: No NT AUTHORITY\Authenticated Users Read (from Security Filtering); Inherited: No NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS Read; Inherited: No NT AUTHORITY\SYSTEM: Edit settings, delete, modify security; Inherited: No
	Add the Administrators security group to roaming user profiles	Enabled
Disable IPv6	Registry item: DisabledComponents	
Disable Machine Account Password Changes	Domain member: Disable machine account password changes	Enabled
Firewall	Global Settings	Policy version 2.10 Other settings not configured
	Domain, Private, & Public Profile Settings	Firewall state off Other settings not configured
	Prohibit use of Internet Connection Sharing on your DNS domain network	Enabled
	Windows Firewall: Protect all network connections	Disabled
	Enhance Internet Explorer Security for Admin & User accounts on the machine	Both Disabled
Metro	Start Menu and Taskbar: Go to the desktop instead of Start when signing in or when all the apps on a screen are closed	Enabled
Network Level Authentication	Require user authentication for remote connections by using Network Level Authentication	Disabled
NTP - Time Client	Global Configuration Settings	Enabled
	Configure Windows NTP Client	Enabled
	Enable Windows NTP Client	Enabled

PS Execution Policy	Registry item: ExecutionPolicy	Action: Update Hive: HKEY_LOCAL_MACHINE Key path: SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell Value name: ExecutionPolicy Value type: REG_SZ Value data: Bypass
RDS Licensing Security	Allow users to connect remotely by using Remote Desktop Services	Enabled
	Set the Remote Desktop licensing mode	Enabled. Specify the licensing mode for the RD Session Host server: Per device
	Use the specified Remote Desktop license servers	Enabled. License servers to use: 192.168.128.36
	Require user authentication for remote connections by using Network Level Authentication	Disabled
User Account Control (UAC)	Behavior of the elevation prompt for administrators in Admin Approval Mode	Elevate without prompting
	Detect app installations and prompt for elevation	Disabled
	Run all administrators in Admin Approval Mode	Disabled
WSUS	Allow Automatic Updates immediate installation	Enabled
	Allow signed updates from an intranet Microsoft update service location	Enabled
	Configure Automatic Updates	Configure automatic updating - Enabled: 4 - Auto download and schedule the install Configure automatic updating: 4 - Auto download and schedule the install Install during automatic maintenance: Disabled Install during automatic maintenance: Disabled Scheduled install day: 0 - Every day Scheduled install day: 0 - Every day Scheduled install time: 12:00 Scheduled install time: 12:00
	Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box	Enabled
	Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Enabled
	No auto-restart with logged on users for scheduled automatic updates installations	Enabled
	Specify intranet Microsoft update service location	Enabled Set the intranet update service for detecting updates: http://192.168.128.37:8530 Set the intranet statistics server: http://192.168.128.37:8530 (example: http://IntranetUpd01)

GPO Properties for App Orchestration

Citrix App Orchestration provides a script ("New-CamGPO.ps1") that creates a GPO called “CtxCloudAppManagement” and configures the required policy settings for App Orchestration. After running the script, the GPO is linked to OUs in the Citrix Service Provider Management domain, Shared Resources domain, and tenant domains.

As shown below, the Citrix Service Provider Management domain must contain an empty “CitrixAppOrchestration” OU for the initial configuration of App Orchestration.



Name	Type
AO-CSP	Computer
CC1-CSP	Computer
CITRIX-15US...	Computer
CONSOLE-C...	Computer
CSPM1-CSP	Computer
CSPM2-CSP	Computer
FILE1-CSP	Computer

Appendix C: Configuring Hyper-V Extended ACLs

Microsoft Windows Server 2012 R2 with Hyper-V introduces support for Hyper-V Virtual Switch Extended Port Access Control Lists (ACLs). Administrators can configure ACLs on the Hyper-V virtual switch rather than within the VMs, making it easier to manage security policies for tenants in a multi-tenant environment.

Using Windows PowerShell, you can configure firewall rules. When you create rules for Windows Server 2012 R2, you can specify the port number in addition to the source and destination MAC and IP addresses. General information about Hyper-V Extended ACLs is available at http://technet.microsoft.com/en-us/library/dn343757.aspx#bkmk_acl. Configuration guidelines are available at http://technet.microsoft.com/en-us/library/dn375962.aspx. Engineers in the Citrix Solutions Lab developed a PowerShell script to set the appropriate firewall rules for the lab implementation, and this appendix describes the approach taken in designing those rules.

Extended ACLs in the Citrix Service Provider Reference Architecture

In the Citrix Service Provider reference architecture, Hyper-V ACLs were used to isolate and secure different tenant VMs while permitting communication with the shared Citrix Service Provider environment. ACLs were applied only to the VM network adapters of the tenant VMs. ACLs were configured to allow all traffic between the specific tenant VMs and with Citrix Service Provider shared systems. At the same time the baseline ACLs prevent communication with any systems from other tenants for private tenant network isolation.

The approach was to start out with baseline ACLs with a respective weight starting at 1 (both inbound and outbound), and then add additional ACLs based on the IP address and port number, increasing the weight for each one.

Baseline ACLs

In the process of researching how these new ACLs work, it became apparent that the best approach was to lock down all inbound and outbound connections and then "poke" holes for each inbound connection with which we wanted to connect.

After locking down a system, however, we were unable to perform any outbound connections, such as reaching a website or performing a DNS look-up. This problem was resolved by adding two additional ACLs to allow outbound stateful connections for TCP and UDP. Although UDP connections are not inherently stateful, turning on the stateful option allowed responses to be processed and not blocked by the inbound deny ACL.

Another issue centered on the ability to ping machines successfully. Since ICMP is a Layer 3 protocol, ping does not use a TCP port. ICMP connectivity was resolved by adding 2 ACLs to allow inbound and outbound ICMP traffic. The PowerShell cmdlet did not accept ICMP as a protocol nickname, but using the IP protocol ID of 1 was an effective workaround.

In summary, there were a total of six baseline ACLs:

- Inbound Deny on all connections (weight 1)
- Inbound Allow ICMP protocol traffic on all connections (weight 2)
- Outbound Deny on all connections (weight 1)
- Outbound Allow TCP protocol stateful traffic on all connections (weight 2)
- Outbound Allow UDP protocol stateful traffic on all connections (weight 3)
- Outbound Allow ICMP protocol traffic on all connections (weight 4)

PowerShell Cmdlets Used

For SCVMM, the following PowerShell cmdlets were used:

- Get-SCVirtualMachine
- Get-SCVMHost
- Get-SCVirtualNetworkAdapter

For Hyper-V, the following PowerShell cmdlets were used:

- Get-VMNetworkAdapter
- Get- VMNetworkAdapterExtendedAcl
- Remove-VMNetworkAdapterExtendedAcl
- Add-VMNetworkAdapterExtendedAcl

Hyper-V ACL Configuration

ACLs were applied in the Hyper-V environment using a custom written PowerShell module that allows Hyper-V ACL changes based on tenant-specific XML "answer" files.

ACL PowerShell Module

The ACL actions using the imported module CspTenantNetworkAcls.psm1 allow for two commands:

- *Add-CspTenantNetworkAcls -AclXmlFile C:\CspTenantNetworkAcls.xml*. This command adds the specified ACLs to Network Adapters for the tenant VMs defined in the XML file.
- *Remove-CspTenantNetworkAcls -AclXmlFile C:\CspTenantNetworkAcls.xml.* This command removes the specified ACLs from Network Adapters for the tenant VMs defined in the XML file.

Tenant-Specific ACL XML Files

A tenant-specific XML file drives the PowerShell Add and Remove functions and is split into two sections (environment node and configuration node). There is a concept of machine roles in which the machines are mapped from environment to configuration and vice versa. This reduces the amount of ACL configuration but allows us to expand the explicit ACLs that are applied to each VM network adapter.

The environment node contains information about all the machines for the tenant configuration (and relevant Citrix Service Provider infrastructure). This node includes all of the role nodes that comprise the tenant and Citrix Service Provider environment to which the ACLs are applied. This includes each VM and related IP address in each VM network type (service/trust). Also, in the environment node, information about the SCVMM environment was included, such as the FQDN of the SCVMM servers that manage the Hyper-V hosts and the actual names of the service and trust management VM networks. A "noacls" XML attribute can be set to "true" for an environment role element in the case where such a role will only be used as a remote role reference for the ACLs and will not have any ACLs added to it. This is expected for Citrix Service Provider infrastructure roles.

The configuration node contains the information about the ACLs. Similar to the environment node, this node is also broken down by roles that include all of the ACLs with VM network and remote role references. The script uses these references to generate a complete list of ACLs that are applied to each VM network adapter for each VM. The configuration node acts essentially as a comprehensive library of ACL settings meant to work for any Citrix Service Provider reference architecture tenant type and configuration.

By default, the PowerShell script removes all existing ACLs on the VM network adapter and adds the baseline ACLs followed by the ACLs prescribed in the configuration node. The connections are handled via PowerShell remoting. At the end of the script's execution, a list of all the applied ACLs is written out to a summary file containing the ACLs and additional metadata.

Appendix D: Implementation Details for Citrix App Orchestration and CPSM

Citrix CloudPortal Services Manager (CPSM) provides an easy-to-use interface for managing customers, users, and application delivery. This appendix gives details on the implementation and operation of App Orchestration and CPSM.

Prerequisites for Deploying App Orchestration

Refer to Citrix App Orchestration 2.0 documentation at http://www.citrix.com/edocs for detailed requirements and installation steps. In addition to obtaining the software, the servers below (at a minimum) should be available to the installation of App Orchestration:

- Domain controller (and an Active Directory domain)
- App Orchestration configuration server
- Database server (Microsoft SQL Server 2012 or 2008 R2)
- Citrix Licensing Server (new or existing) with appropriate licenses
- Two XenDesktop Delivery Controllers
- Two StoreFront servers
- One or more Session Machines
- One hypervisor server (in this reference architecture Microsoft Hyper-V was used)
- One server for Citrix Product Depot

App Orchestration provides a script ("New-CamGPO.ps1") that creates a GPO called “CtxCloudAppManagement” and configures the required policy settings for App Orchestration. After running the script in the Citrix Service Provider Management domain, the Shared Tenant Resource domain, and each tenant domain, the GPO is linked to the App Orchestration root OU in the Citrix Service Provider Management domain.

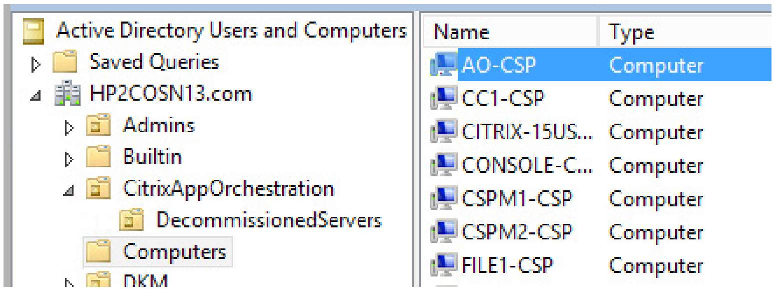
Important: When an administrator deploys machines (for example, adding a Delivery Site), App Orchestration issues workflows to complete deployment tasks. For workflows to complete successfully, the machines on which they run must have policy settings applied. App Orchestration does not verify that policy settings are applied before issuing workflows.

The App Orchestration and StoreFront servers must have an IIS security certificate signed by the Citrix Service Provider’s domain Certificate Authority (CA) to protect web server SSL communications. StoreFront servers require the IIS security certificates as well as bindings on port 443 to be available. On the App Orchestration server, place the certificate into the Personal certificate store.

Installing and Configuring App Orchestration 2.0

Deploying App Orchestration 2.0 in the reference architecture follows the general sequence of steps below. To install App Orchestration 2.5, refer to the installation documentation for that version:

1. Install the App Orchestration 2.0 software and create a new deployment. The installation wizard creates the required database on the SQL server. Select the IIS Web certificate to secure SSL communications and configure the App Orchestration server.
2. Launch the App Orchestration console. Begin to configure global settings, specifying an empty App Orchestration OU (e.g., “CitrixAppOrchestration”) in the Citrix Service Provider Management domain.



Active Directory Users and Computers
- Saved Queries
- HP2COSN13.com
  - Admins
  - Builtin
  - CitrixAppOrchestration
    - DecommissionedServers
  - Computers
  - DKM

Name	Type
AO-CSP	Computer
CC1-CSP	Computer
CITRIX-15US...	Computer
CONSOLE-C...	Computer
CSPM1-CSP	Computer
CSPM2-CSP	Computer
FILE1-CSP	Computer

The default resource and user domain for Private Delivery Site tenants will be the tenant domain where the StoreFront, XenDesktop, and VDA/VDI servers reside.

3. Define a global geo-based datacenter and point to valid Citrix license server. Define the Product Depot location, specifying the external Citrix Service Provider DNS suffix (this can be changed later on a per-tenant basis). The network share for the depot must be visible to App Orchestration, StoreFront, XenDesktop, and VDA/VDI servers. Defaults for Advanced Settings can be accepted and changed later on a per-tenant basis.
4. For each tenant define a new domain to App Orchestration. Trust validation is performed using .Net Directory Services libraries.
5. Configure the basic settings (name, resource domain, and user domain) for the tenant to be imported. For Private Delivery Site tenants, specify the tenant-specific resource and user domain (e.g., HP2Tenant1.com). For Private Delivery Group/Shared Delivery Site tenants, specify the global shared resource domain (e.g., HPCOSN13.com) and tenant-specific user domain (e.g., HP2Tenant3.com).
6. On the tenant, add an OU in Active Directory. In the “ForeignSecurityPrincipals” GPO, create a new security group (e.g., HP2Tenant1-AO-Group) and insert the appropriate domain administrators and users into that group. In the App Orchestration console, specify the location group for the tenant to be imported.
7. Also specify StoreFront isolation, Netscaler Gateway (which can be changed later), and the private management network. The network must exactly match the name of the Citrix Service Provider Shared Services Management VLAN listed in SCVMM where the StoreFront, XenDesktop, and VDA/VDI servers reside. Before continuing, test connections to these servers using the domain credentials where the resources reside. It is recommended to test connections using a PowerShell command (e.g., “Invoke-Command {0} –computername T1-XD1 –Credential hp2tenant1.com\administrator”) and to ping the FQDN of these servers. (Note: For ping to work properly, the correct subnets must be added to the Active Directory Sites and Service for these systems.)
8. Before creating a XenDesktop Delivery Site, place the trusted root certificate for the Citrix Service Provider management domain and the domain where the XenDesktop server will reside on the XenDesktop servers. Specify Delivery Site location and database settings.
9. Create the StoreFront server group and add StoreFront servers, specifying the SSL certificate friendly name and location settings. If there are multiple StoreFront servers, the SSL certificate friendly name must match between systems. Once the StoreFront server group has been deployed, if NetScaler is used, specify the Authentication method of “Pass-through from NetScaler Gateway” and verify NetScaler settings in the StoreFront console.

10. Import externally created Session Machines, which are PVS-based images. Make sure to follow the guidelines in "Provisioning Services in App Orchestration 2.0" in the App Orchestration 2.0 documentation at http://www.citrix.com/edocs. Important: In an App Orchestration environment, administrators must use the Streamed VM Setup Wizard in PVS for creating target devices in App Orchestration — not the XenDesktop Setup Wizard. Verify that systems are placed into the proper App Orchestration OU in the tenant domain. The destination OU should be the same as the App Orchestration root OU when running the Streamed VM Setup Wizard for App Orchestration.
11. Create a new Session Machine catalog. For HSD workloads, specify the Session Machine name, XenDesktop 7.1 as the Delivery Controller type, and the number of users per machine. For VDI workloads, specify the Session Machine name, "Single User" as the OS type, and the type of desktop (e.g., "Random"). In SCVMM, refresh the properties for the PVS vDisk VM (e.g., T1-HSD001") to update the computer name. It's recommended to disable IPv6 on vNICs within the PVS vDisk VM.
12. Create new HSD and VDI desktop offerings to which users can subscribe, specifying the isolation mode (Shared Delivery Group, Private Delivery Group, or Private Delivery Site).
13. Verify that the StoreFront, XenDesktop, and VDA/VDI servers can establish connections from the CitrixCamAgent back to the App Orchestration server. To do this, run the Powershell script Get-CamAgentConfiguration and ping the /cam/api page of the App Orchestration server (e.g., "ping AO-CSP.HP2COSN13.com"). If the ping fails, export the CA Trusted Root certificate from the App Orchestration server and import it into the Trusted Root certificate of the StoreFront, XenDesktop, or VDA/VDI systems.
14. Subscribe tenants to offerings. This is the point at which App Orchestration creates workflow jobs that are passed to its orchestration engine.
15. Once these steps have been completed and verified, the Session Machine catalog can be expanded with additional HSD and VDI Session Machines like the initial HSD and VDI machines created above. Select "Add Machines" to increase the machine quantities in the catalog. To import larger quantities, Citrix PowerShell cmdlets can be used. Capacity limits can also be adjusted.

After you deploy App Orchestration, CloudPortal Services Manager can be integrated to enable tenant self-service capabilities. This allows tenant users to select and deploy offerings from among those that App Orchestration has made available to the tenant. When you enable this integration, the App Orchestration and CloudPortal Services Manager consoles assume specific roles with regard to deployment administration tasks. The administrator uses the CloudPortal Services Manager control panel to manage tenant onboarding and user subscriptions for offerings. The App Orchestration web console can create new offerings, add capacity to existing offerings, and manage Delivery Sites, Session Machines, and StoreFront servers in the deployment.

CloudPortal Service Manager 11.0 configuration and integration with App Orchestration

The CloudPortal Services Manager (CPSM) cloud platform has four primary server components (shown with their DNS aliases):

- CPSM Web/User Interface (CortexWeb)
- Provisioning Engine (CortexProvisioning)
- Database (CortexSQL)
- Reporting Services (CortexReports)

A typical CPSM deployment process includes three phases:

1. Installing and configuring the CPSM platform. The Services Manager platform comprises a series of servers that perform provisioning tasks, authenticate and manage users, host the control panel interface and API services, store and process data from the main database, and manage billing and usage. These servers must be fully configured before services are deployed.
2. Deploying services. Deploying services includes installing and configuring services for resources such as Microsoft Exchange, Citrix Apps and Desktops, and Microsoft SharePoint. Before deploying any service, you must ensure the resources supporting the service are fully deployed in your network environment. For example, to deploy the Hosted Exchange service, Services Manager requires you have a working Exchange deployment in your environment. **This reference architecture includes CPSM integration with App Orchestration to deploy Hosted Apps and Desktop services, which required some additional configuration steps described in this document.**
3. Provisioning customers and users. Provisioning customers and users represents a series of tasks for enabling resellers to sell specific services, making services available to end-customers, enabling customers' users to access services, and assigning security roles.

Customers are provisioned into a location (the main unit of isolation between tenants), which corresponds to an Active Directory domain or forest. A XML configuration file maintains context across the CPSM deployment. As you configure server roles, information is read and written to the configuration file. For example, the Provisioning Engine writes its own configuration information and reads where to reach the database. When you configure the primary location, the configuration file will already have information needed about the Provisioning Server.

There is one configuration file per location, although all locations can share a single database server. You configure the primary location first, then optionally, remote locations. For example, a new Private Delivery Site tenant with an existing infrastructure and domain might be integrated as a remote location in the control panel. When you configure remote locations, you specify connection details that generate a new configuration file. In the lab implementation of this reference architecture, the primary site resides in the Citrix Service Provider domain and remote locations were created in the Shared Resource and Private Delivery Site tenant domains.

The following pages provide an overview of the CPSM deployment process. The overview includes:

- A summary of steps to deploy a primary CPSM location
- A summary of steps to deploy a secondary or remote location.
- A summary of steps that deploy primary and remote locations that integrate CPSM and App Orchestration, as in this reference architecture.

Deployment summary for a CPSM primary location

The following list gives an overview of the required tasks for deploying the platform servers and creating the primary location. Depending on your requirements, your deployment might include additional tasks.

1. **Prepare the deployment environment.** This includes the following tasks:

   - Provision the platform servers that will be designated as the domain controller, database server, reporting server, Provisioning server, and web server.
   - Extend the Active Directory schema using the Exchange installation media (use the Setup.exe script from the Exchange media).
   - Create DNS aliases for the Provisioning, database, reporting, and web servers.
   - Open the required firewall ports on all platform servers.
   - Install .NET Framework on all platform servers. If this component is not present, the Setup Tool installs it automatically, prior to installing the server roles.
   - Obtain a valid IIS Web certificate, which will be needed on the Directory Web Service system with bindings on port 443 for the “CortexServices” site.

Other system requirements are listed in the CPSM 11.0 documentation at http://support.citrix.com/proddocs/topic/ccps-11/ccps-sys-reqs.html.

2. **Perform environment readiness checks.** You can verify the extended Active Directory schema and DNS aliases. This procedure is available in the Setup Tool graphical interface; you can also perform the verifications manually.
3. **Create system databases.** Run this task on the server where Microsoft SQL Server is installed and use Windows “Integrated” authentication for the primary CPSM location. The account must be added to Security Logins within the SQL database and be a local admin on the operating system of the CPSM deployment server. Using the Configuration Tool's graphical interface, you specify database information before you install server roles.
4. **Install and configure server roles.** Using the Setup Tool, you install the platform server roles on the servers you designate. Initially you must install the Provisioning, Directory Web Service, and Web servers. (Reporting and Report Mailer services can be installed at a later time.) With the Configuration Tool, you specify the configuration settings for the installed roles.
5. **Create the primary location.** Use the Configuration Tool to specify the settings for the primary location. You configure the location from the server hosting the Provisioning engine or the web server.

Deployment summary for remote locations

Configuring a remote location is similar to configuring a primary location. The following steps describe the required tasks for deploying the platform servers that comprise a remote location.

1. **Prepare the deployment environment.** This includes tasks similar to the steps to prepare the primary location:

   - Provision the domain controller and Provisioning Servers. The remote location uses the web server and database server in the primary location for control panel administration and reporting, respectively.
   - Extend the Active Directory schema using the Exchange installation media.
   - Create DNS aliases for the Provisioning, database, and web servers.

- Define the required firewall ports on all servers to enable communication with the database server and web server in the primary location.
- Install .NET Framework on the platform servers, to avoid interruption when installing server roles. When installing the server roles, the Setup Tool also installs this component automatically if it is not present.

2. **Perform environment readiness checks.** Verify the extended Active Directory schema and DNS aliases.
3. **Install and configure server roles.** Using the Setup Tool, you select the server roles to be installed on each server. As with the primary location, you specify the configuration settings for the installed roles with the Configuration Tool.
4. **Create the remote location.** Use the Configuration Tool to define the settings for the primary location. You configure the location from the server hosting the Provisioning Engine or the web server. Afterward, continue configuring the remote location using the Services Manager control panel in the primary location.

CPSM and App Orchestration integration

The summaries above outline the general CPSM configuration process for primary and remote locations. The integration of CPSM and App Orchestration in this reference architecture required slight variations to the procedures above. The following steps were used in the Citrix Solutions Lab implementation:

1. **Prepare the deployment environment.** Follow the general procedures to prepare servers, AD schema, DNS aliases, and network communications. Obtain an IIS web certificate for SSL connections on the Web server.

   - Create an initial deployment configuration file on a share that all CPSM systems can access. For the primary location, install the Provisioning, Directory Web Service, and Web servers. Install the .NET framework as required.
   - Configure the Web Server, specifying the IIS web certificate for SSL connections. Enter the Active Directory Organizational Unit as the primary location — for the Citrix Solutions Lab implementation the primary location is the Citrix Service Provider management domain HP2COSN13.COM. After CPSM is installed, you can verify the AD OU structure and the accounts created.
   - Citrix provides an App Orchestration agent that supports integration with CPSM. (Citrix Service Providers can obtain this agent by downloading the Hosted Apps and Desktops 11.2 package from the Cloud Provider Pack on the partner site.) Install the agent on the App Orchestration server. From the CPSM DVD image, install the “App Orchestration Configuration Tool.” This tool requires details for the App Orchestration configuration server and the address of SQL server where the CPSM database is installed.

2. **Set up the secondary or remote CPSM site.** Start by confirming that the remote server can ping the CPSM database system using the DNS alias “CortexSQL.” The remote CPSM site will also need to the IIS web certificate from the App Orchestration server. Add the remote location and load the XML configuration file created earlier. Provide details so that

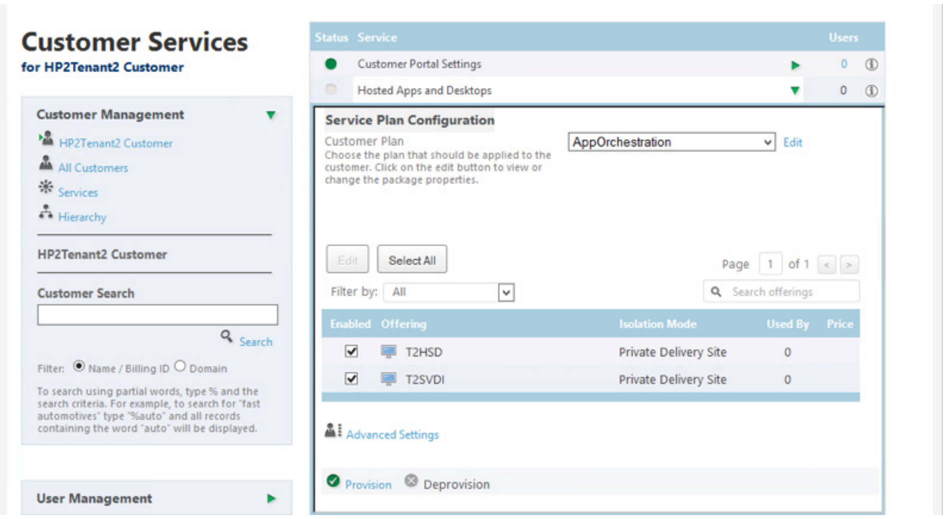
the remote server can connect to the primary location database. Install the Directory Web Server and Provisioning Engine components and configure the secondary location. To support email to administrators and users (including usage reporting), you must provide the SMTP address of the remote domain Exchange server. Configure Directory Web Services (including the Queue Monitor Service and Directory Monitoring Services). Lastly, provision the remote location in Active Directory and the database.

3. **Configure CPSM to provision hosted desktops and applications** using App Orchestration using the CPSM web console. Note that the CPSM 11.0 release, however, does not fully support the Internet Explorer 11 browser. Either use an alternate browser (e.g., Firefox) or configure the IE11 browser in IE10 mode. Run the CPSM web console as “cspadmin,” which should have the service schema administrator role assigned.

    - Remove the current Hosted Apps and Desktops (HAAD) role and import the Hosted Apps and Desktops 11.2 package for App Orchestration 2.0. After importing the HAAD 11.2 service, restart the Citrix Queue Monitor Service. Before configuring this role, verify that the Session Machine Catalog for App Orchestration has machines ready to be allocated to a delivery Site and that the offerings have no currently defined subscriptions.
    - Enable the HAAD service as a Top Environment Service. Specify the Active Directory Resources Path for the service. For the remote CPSM site, configure the AD Location Services and select the correct Location Filter. For the Citrix Service Provider Management domain, configure the App Orchestration server as the server to provision Hosted Apps and Desktops and specify the credentials for connections. Verify the server setup, specify an SSL connection, and confirm that the remote connection to the App Orchestration server is successful.

4. **Configure Customer Services.** Set up a new customer (or “reseller”) for the remote CPSM location. Define the new customer by specifying the remote CPSM location and server role — in this case the role is delivering Hosted Apps and Desktops to users. In the lab implementation, a Private Delivery Site tenant (Tenant 2) was defined as a remote CPSM location with provisioning capabilities; the Tenant 2 AD domain “HP2Tenant2.com” is given for the remote location. The CPSM console provides an easy way of testing the connection to the App Orchestration server. On the Service Deployment screen, the administrator defines the App Orchestration Datacenter in which subscriptions for the customer will be created.

Provision the Hosted Apps and Desktops service. At this point, the CPSM configuration is ready to provision Hosted Apps and Desktops service for the Private Delivery Site tenant. If during the provisioning process there is a “Model state is invalid” error on an ImportTenantModel API, you may need to apply an App Orchestration 2.0 Hotfix to resolve it. Please check the Citrix knowledgebase for the latest information regarding hotfixes.



Filter: ● Name / Billing ID ○ Domain

To search using partial words, type % and the search criteria. For example, to search for "fast automotives" type "%auto" and all records containing the word "auto" will be displayed.

Status	Service		Users
●	Customer Portal Settings	▶	0
○	Hosted Apps and Desktops	▼	0

Customer Plan: AppOrchestration

Choose the plan that should be applied to the customer. Click on the edit button to view or change the package properties.

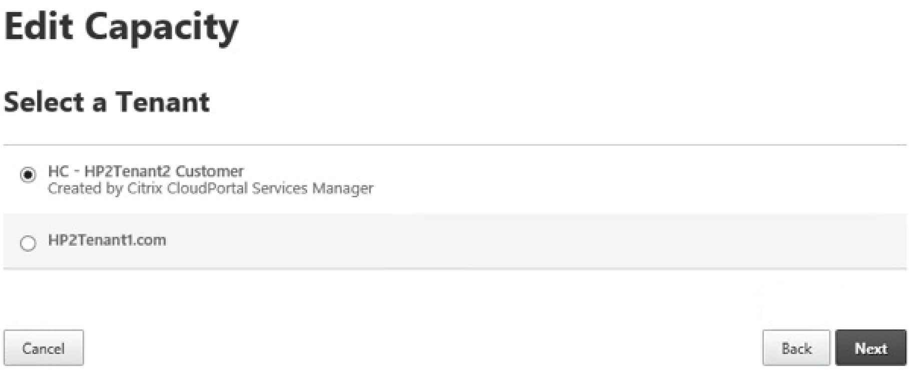
Filter by: All

Enabled	Offering	Isolation Mode	Used By	Price
☑	T2HSD	Private Delivery Site	0	
☑	T2SVDI	Private Delivery Site	0	

Add the "csm_haad_selfsvc" account into "CortexAdmins" on the Citrix Service Provider Management Active Directory domain to enable administration of Hosted Apps and Desktops on the site-isolated tenant. The provisioned services should be visible in the Customer Services console and the administrator should be able to monitor App Orchestration workflows.

5. **Configure the AD Sync service on the remote location.** Add the AD Sync Service into the AD location of the remote site. Using the Customer Services interface, add the AD Sync service to the remote site, apply the change, and provision the service. The AD Sync setup utility requires the .NET 2.0 Framework, so add this if it was not previously configured. Install the AD Sync client on all remote Domain Controllers. (Log onto the CPSM management control panel as the remote administrator and select AD Sync Download under the AD Sync option. Only one of the Domain Controllers should be configured to watch for changes.) After installation, restart the Domain Controllers and verify that the AD Sync service is running. (Note: The AD Sync service may not start automatically.) Confirm that AD logins are set correctly in the firstName.lastName format. (A PowerShell script can be used to correct entries.)
6. **Test the AD Sync service.** After restarting services on all AD Sync servers, then log on to CPSM control panel on the remote location and click Users to view the user list. Synchronized users have a small green arrow next to the user icon. To validate that synchronization works for new accounts, create a new user account in the external domain, add it to a user group included in AD Sync operations, change an account attribute, and verify that the account appears on the Users screen. Once the user has been provisioned to the HAAD role, the User count should increment.

7. **Modify App Orchestration capacity and select the CPSM tenant.** Notifications in App Orchestration should show that you need to edit catalog capacity. Edit the capacity for the tenant created by CPSM, adjusting the number of HSD and VDI offerings.



Edit Capacity

Select a Tenant

● HC - HP2Tenant2 Customer
Created by Citrix CloudPortal Services Manager

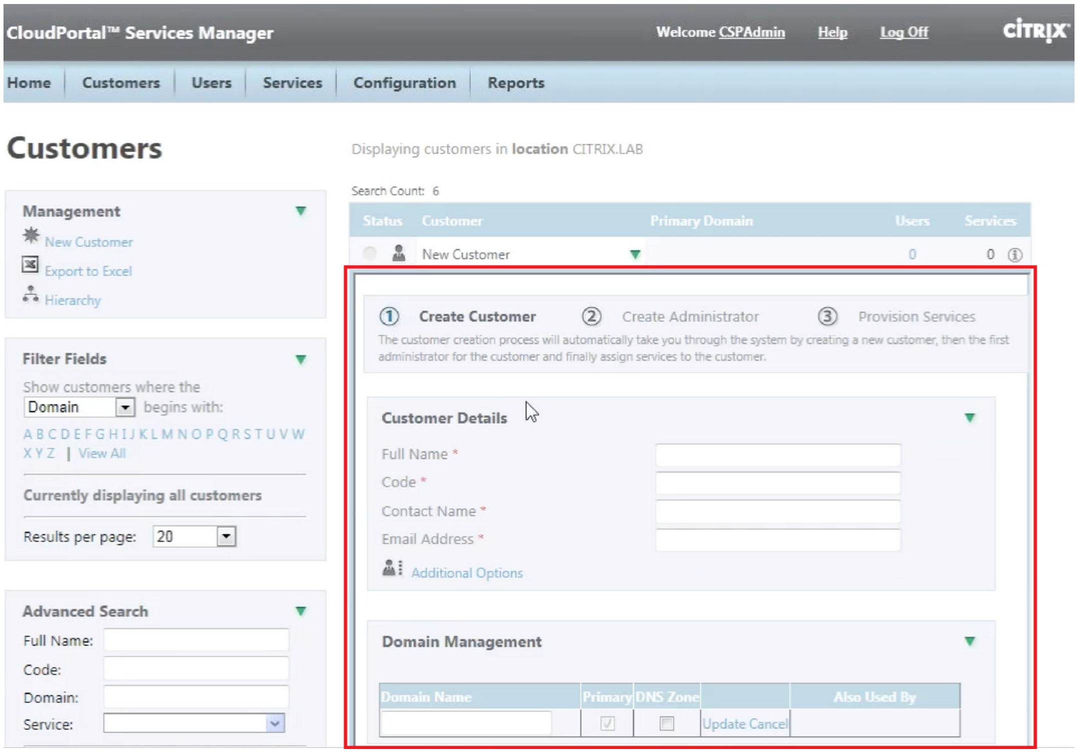
○ HP2Tenant1.com

CPSM customer onboarding example

Through CPSM, you can drive App Orchestration to create and manage the customer/tenant hierarchy. The CPSM menu bar, shown below, allows you to navigate the CPSM interface.

The following steps show the process for on-boarding a new customer into CPSM:

1. Log on to CPSM.
2. From the Home screen, select Customer > New Customer from the menu bar to bring up the New Customer pane.
3. Fill out the customer information fields in the New Customer pane. The Code field is filled out automatically once a Customer Name is entered, and enables faster lookups.
4. Additional AD properties can be filled out by clicking on Additional Options at the bottom of the Customer Details pane.
5. The Domain Management pane, below the Customer Details pane, allows you to set up domain properties for the new customer.
6. You can set up passwords, email, and allows security roles using the Advanced Properties section.



CloudPortal™ Services Manager

Welcome CSPAdmin Help Log Off

Home | Customers | Users | Services | Configuration | Reports

Customers

Displaying customers in **location** CITRIX.LAB

Search Count: 6

Status	Customer	Primary Domain	Users	Services
	New Customer		0	0

① Create Customer ② Create Administrator ③ Provision Services

The customer creation process will automatically take you through the system by creating a new customer, then the first administrator for the customer and finally assign services to the customer.

Customer Details

Full Name *

Code *

Contact Name *

Email Address *

Additional Options

Domain Management

Domain Name	Primary	DNS Zone		Also Used By
	☑	□	Update Cancel	

Management

New Customer

Export to Excel

Hierarchy

Filter Fields

Show customers where the Domain begins with:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z | View All

Currently displaying all customers

Results per page: 20

Advanced Search

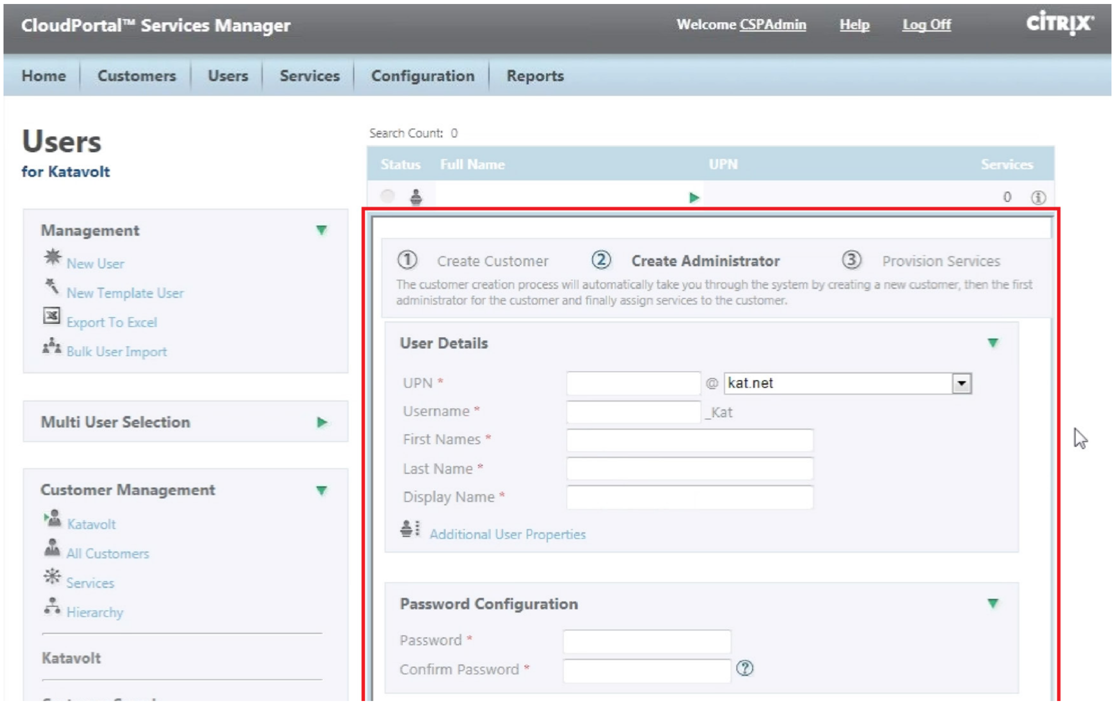
Full Name:

Code:

Domain:

Service:

7. Click Provision at the bottom of the New Customer pane to create the new customer profile and begin provisioning resources and services.
8. Next, you'll set up the administrator for your new customer. Fill out the administrator information in the Create Administrator pane.
9. Clicking Additional Properties at the bottom of the User Details pane allows you to enter additional details.
10. The Password Configuration pane is used to set up password properties for the administrator.
11. The Account Settings pane allows you to disable, lock, and set the account to expire on a specified date.
12. You can enter in a specific email user name at the bottom of the Create Administrator pane, or leave the field blank to let CPSM set up the email address according to the UPN address entered at the top of the User Detail pane.

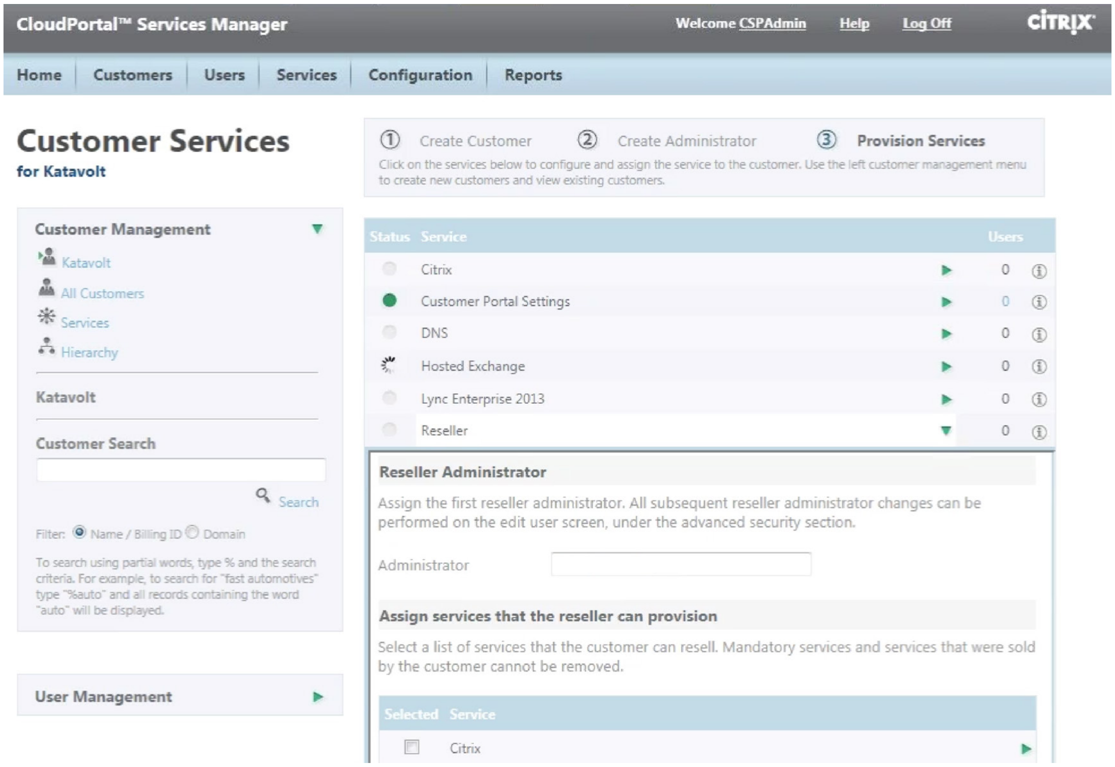


① Create Customer ② Create Administrator ③ Provision Services

The customer creation process will automatically take you through the system by creating a new customer, then the first administrator for the customer and finally assign services to the customer.

UPN * @ kat.net
Username * _Kat
First Names *
Last Name *
Display Name *
Password *
Confirm Password *

13. Click Provision to create the administrator profile.
14. The Provision Services pane allows you to set up and enable services for the new customer. Available services are listed, and the Status indicator to the left of each one shows whether the service is active (green), currently being provisioned (orange or spinning), or inactive (grey). Because CPSM operates asynchronously, each service can be set up in parallel without waiting first for the previous service to be fully provisioned within the system.
15. To set up Hosted Exchange properties, click the green arrow to the right of Hosted Exchange. Fill out the Hosted Exchange settings for the new customer and click Provision. In the main Provision Services pane, the status indicator next to Hosted Exchange will turn orange as the service is being set up in the infrastructure.
16. To set up Citrix-enabled services and applications, such as Microsoft Office and Windows Desktop VDA, click on the green arrow to the right of Citrix in the services list. Check the checkboxes next to the applications and services you wish to enable and click Provision.



Customer Services
for Katavolt

① Create Customer ② Create Administrator ③ Provision Services

Click on the services below to configure and assign the service to the customer. Use the left customer management menu to create new customers and view existing customers.

Filter: ◉ Name / Billing ID ○ Domain

To search using partial words, type % and the search criteria. For example, to search for "fast automotives" type "%auto" and all records containing the word "auto" will be displayed.

Status	Service		Users	
○	Citrix	▶	0	ⓘ
●	Customer Portal Settings	▶	0	ⓘ
○	DNS	▶	0	ⓘ
	Hosted Exchange	▶	0	ⓘ
○	Lync Enterprise 2013	▶	0	ⓘ
○	Reseller	▼	0	ⓘ

Reseller Administrator

Assign the first reseller administrator. All subsequent reseller administrator changes can be performed on the edit user screen, under the advanced security section.

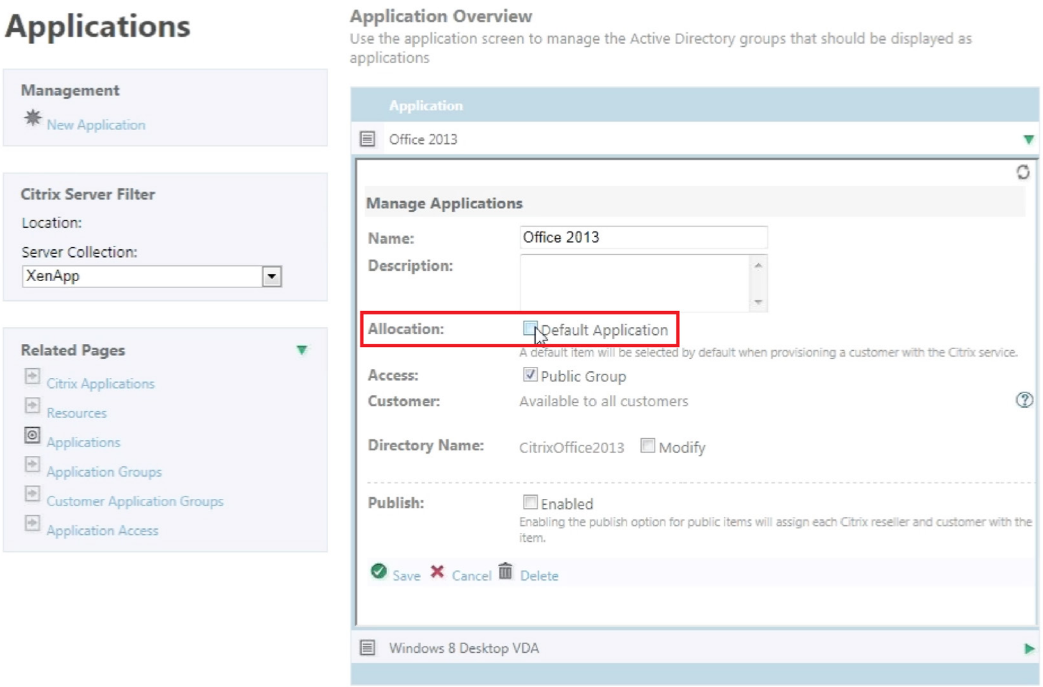
Administrator

Assign services that the reseller can provision

Select a list of services that the customer can resell. Mandatory services and services that were sold by the customer cannot be removed.

Selected	Service	
□	Citrix	▶

17. You can also set up reseller administrator privileges to allow the new customer to provision services to sub-customers and manage their own services through CPSM. To enable reseller privileges, click the green arrow next to the Reseller service. Check the boxes for the services you wish to allow the new customer to resell. Click Provision.



Applications

Management

New Application

Citrix Server Filter

Location:

Server Collection: XenApp

Related Pages

- Citrix Applications
- Resources
- Applications
- Application Groups
- Customer Application Groups
- Application Access

Application Overview

Use the application screen to manage the Active Directory groups that should be displayed as applications

Application

Office 2013

Manage Applications

Name: Office 2013

Description:

Allocation: ☐ Default Application

A default item will be selected by default when provisioning a customer with the Citrix service.

Access: ☑ Public Group

Customer: Available to all customers

Directory Name: CitrixOffice2013 ☐ Modify

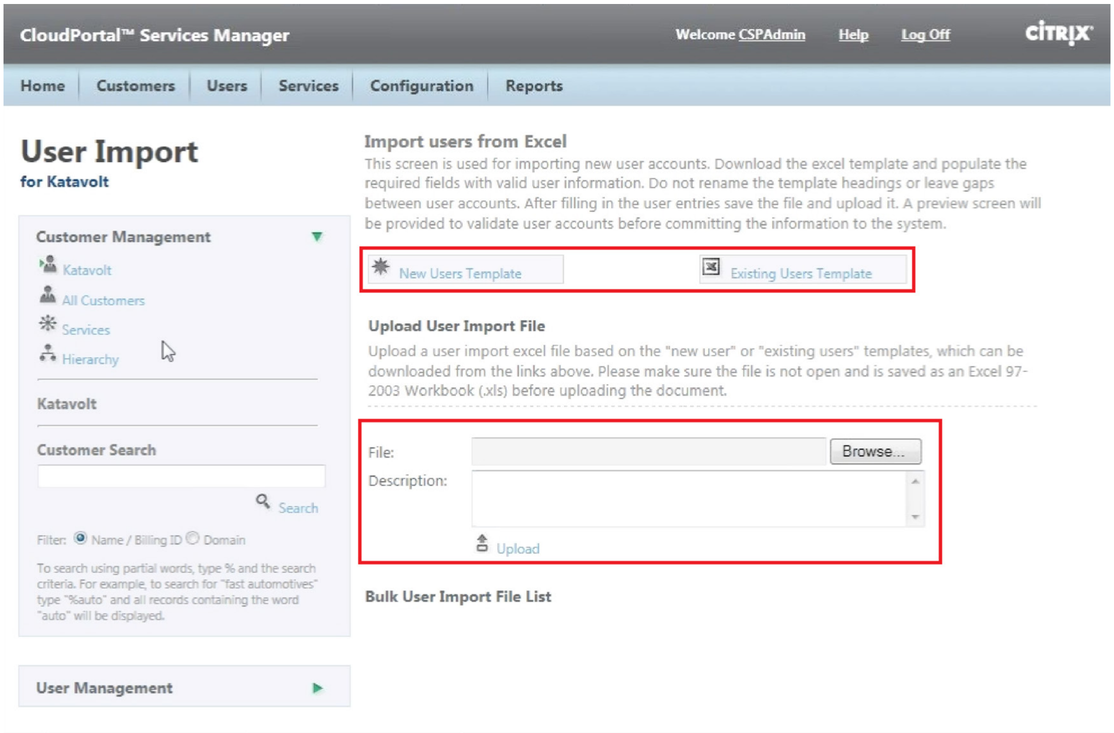
Publish: ☐ Enabled

Enabling the publish option for public items will assign each Citrix reseller and customer with the item.

Save Cancel Delete

Windows 8 Desktop VDA

18. You can set up which applications and services are provisioned by default for new users to speed the process of adding new users. Select Services > service class (e.g. Citrix) > Configuration > Applications to display the available applications. Expand the application properties by clicking on the green arrow to the right of the application name. Check the Default Application checkbox next to Allocation to provision the application to new users by default. Repeat for the remaining applications and service classes as required.
19. Now that your new customer profile and administrator are set up and services have been enabled and provisioned, you can import the remaining users in bulk. From the Customer Services screen, click the green arrow next to User Management in the lower left corner of the screen. In the User Management pane, click on Bulk User Import. Users are imported through a Microsoft Excel spreadsheet. You can download the template for this file by clicking on one of the template links at the top of the pane.



User Import

for Katavolt

To search using partial words, type % and the search criteria. For example, to search for "fast automotives" type "%auto" and all records containing the word "auto" will be displayed.

Import users from Excel

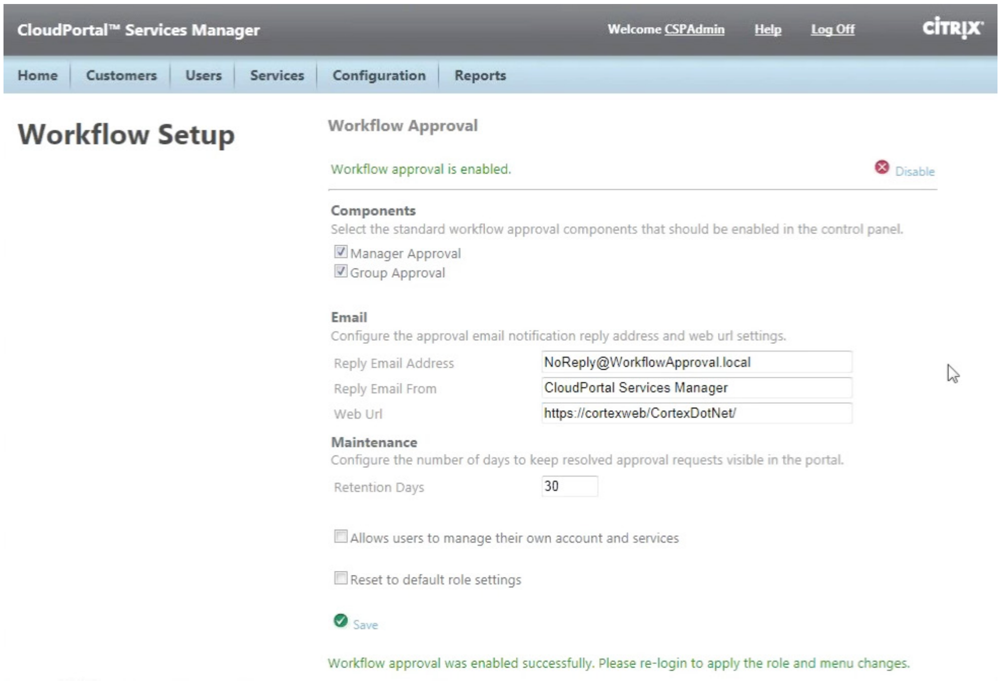
This screen is used for importing new user accounts. Download the excel template and populate the required fields with valid user information. Do not rename the template headings or leave gaps between user accounts. After filling in the user entries save the file and upload it. A preview screen will be provided to validate user accounts before committing the information to the system.

Upload User Import File

Upload a user import excel file based on the "new user" or "existing users" templates, which can be downloaded from the links above. Please make sure the file is not open and is saved as an Excel 97-2003 Workbook (.xls) before uploading the document.

Bulk User Import File List

20. Once you have filled out the template with your user information, upload the file using the fields in the center of the pane. All users are granted default services and applications for the parent customer.



Workflow Setup

Workflow Approval

Workflow approval is enabled.

Components
Select the standard workflow approval components that should be enabled in the control panel.
☑ Manager Approval
☑ Group Approval

Email
Configure the approval email notification reply address and web url settings.

Reply Email Address	NoReply@WorkflowApproval.local
Reply Email From	CloudPortal Services Manager
Web Url	https://cortexweb/CortexDotNet/

Maintenance
Configure the number of days to keep resolved approval requests visible in the portal.

Retention Days	30

□ Allows users to manage their own account and services

□ Reset to default role settings

Workflow approval was enabled successfully. Please re-login to apply the role and menu changes.

21. To set up approval workflows, select Configuration > System Manager > Workflow Setup from the menu bar to open the Workflows screen. Click Enable to activate workflows and open the Workflow Approval pane. Fill out the workflow information fields to set up approval email addresses and routing. Click Save.
22. CPSM allows you to create reports based on usage, billing, and licensing data to monitor your infrastructure and customers. Select Reports > View Reports from the menu bar to open the View Reports screen.

    Expand the service class and click on the application or service to generate a report on that service or application. Reports can be customized by date range and other properties. Click on Parameters in the upper left corner of the screen to show these options.

Appendix E: Glossary

This appendix clarifies terminology used in this reference architecture. For additional terms and definitions, see the following Citrix documentation:

- App Orchestration 2.0 Key Concepts & Terms (see the App Orchestration documentation at http://www.citrix.com/edocs)
- CloudPortal Services Manager Terminology and Concepts
- http://support.citrix.com/proddocs/topic/ccps-11/ccps-plan-deploy-terminology.html
- NetScaler 10.0 Glossary, http://support.citrix.com/servlet/KbServlet/download/30560-102-681707/NS-Glossary.pdf

Isolation models are a key architectural concept and require careful definition and comparison. For this reason, they are defined first, and are followed by a listing of other glossary terms and definitions.

Isolation Models

There are three multi-tenancy isolation models: Shared Delivery Group, Private Delivery Group/Shared Delivery Site, and Private Delivery Site. The type of isolation refers to whether the Delivery Controllers and Session Machines are shared with other tenants or private to the subscribing tenant. Two of these three models, Private Delivery Group/Shared Delivery Site and Private Delivery Site, are implemented in this reference architecture.

- **Shared Delivery Group/Shared Delivery Site isolation.** Shared Delivery Group/Shared Delivery Site isolation (similar to XenApp "Session Isolation") describes a multi-tenancy approach in which tenant isolation is achieved through session isolation — that is, each tenant's applications and desktops run within separate sessions executing on a shared Session Machine (a shared virtual server that hosts desktop and application sessions). The Shared Delivery Group/Shared Delivery Site model is most appropriate for tenants who do not require strict isolation.
- **Private Delivery Group/Shared Delivery Site isolation.** The Private Delivery Group/Shared Delivery Site isolation model (similar to XenApp "Server Isolation") uses dedicated Session Machines to host application and desktop sessions. However, the XenDesktop Delivery Controllers in this group are shared with other tenants (e.g., tenants share the XenDesktop site but have private servers to host desktops and applications).
- **Private Delivery Site isolation.** Private Delivery Site isolation (similar to XenApp "Farm/Network" Isolation) is implemented by dedicating a Delivery Site exclusively to a single tenant. Hosted applications and desktops run on machines accessible only to a single tenant's users. This configuration is appropriate for tenants that require the highest level of data and infrastructure isolation.

Other Glossary Terms

Active Directory Location Services ("location level")
The level at which CloudPortal Services configures settings. By default, services deployed within a location inherit the settings configured at the top environment level. However, these settings can be overridden at the location level.

App Orchestration
App Orchestration provides unified management of Citrix application and desktop delivery technologies in a multi-tenant environment. It can coordinate application and desktop delivery across multiple datacenters and multiple domains.

Delivery Controller
A Delivery Controller is a server-side component responsible for distributing desktops and applications to users, managing user access through policies, and managing desktops and reboot cycles for servers.

Delivery Group
A Delivery Group is a container for one or more virtual machines that are used to deliver applications and desktops to a specific group of users. A Delivery Group is associated with a specific Delivery Site. It can be shared among tenants or dedicated to a specific tenant, according to the isolation level of the subscriptions it is hosting.

Delivery Site (XenDesktop site)
Delivery Sites provision desktops and applications to users through App Orchestration. In the XenDesktop 7.1 release, XenApp "farms" are now known as "sites." A Delivery Site is the core environment that contains the XenDesktop Delivery Controllers and the SQL Database used to deploy both XenApp and XenDesktop services. A Site must reside within a single datacenter.

FlexCast Management Architecture (FMA)
FlexCast Management Architecture is the underpinning of the Citrix XenDesktop 7 release. It enables provisioning of Windows apps and desktops on hosted-shared RDS servers or VDI-based virtual machines using the same tools and common policies.

Location
Corresponds with an Active Directory domain and used to create associations between specific services, customers, and users. For example, a service can be deployed to a specific location and provisioned only to customers and users in that location.

Offering
An offering is a specific type of service that a service provider supplies to tenants. Typically an offering is a hosted application or desktop.

Provisioning Services
Provisioning Services is a software service that allows providers to create virtual or physical instances of desktop or server machines.

Session Machine
A Session Machine is a virtual or physical machine that hosts desktop and application sessions. It is the machine to which the user connects.

StoreFront
StoreFront is used to manage stores of desktops and applications, and to authenticate users to sites that host resources. App Orchestration defines both private and shared StoreFront services.

Subscription
A subscription is an association between an offering, a group of users (in a tenant organization), and a collection of machines that host a specific desktop or application.

Tenant
A tenant is the service provider’s customer. A tenant contracts services from the service provider organization, such as hosted desktops and applications, as well as cloud infrastructure.

Citrix Insight Services: Formerly known as Tools-as-a-Service (TaaS)
Tools-as-a-Service, or TaaS, is now known as Citrix Insight Services. Citrix Insight Services enables predictive diagnostic and troubleshooting by connecting directly to the desktop virtualization environment. It reads log files from XenDesktop, XenServer, XenApp and NetScaler, profiles the virtualization environment, and scans for known issues. See http://www.citrix.com/static/services/support-ninja-secrets.pdf for more information.

Top Environment Services ("top environment level")
The level at which default settings are configured for the CloudPortal Services Manager deployment. Settings configured at this level are inherited by all locations in the deployment. These settings can be overridden at the Active Directory Location Services level. Services must be enabled at the top environment level before they can be enabled and configured at the location level.

Appendix F: Additional Online Resources

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

Citrix App Orchestration 2.0 Documentation
Available at http://www.citrix.com/edocs

Citrix XenDesktop 7.1 Documentation
http://support.citrix.com/proddocs/topic/xendesktop/cds-xendesktop-71-landing-page.html

CloudPortal Services Manager Documentation
http://support.citrix.com/proddocs/topic/cloudportal/ccps-services-manager.html

Citrix NetScaler Documentation
http://support.citrix.com/proddocs/topic/netscaler/ns-gen-netscaler-wrapper-con.html

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

XenDesktop 7 Reference Architectures
http://www.citrix.com/products/xendesktop/tech-info.html

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

HDX Insight
http://support.citrix.com/proddocs/topic/ni-10-1-map/ni-hdxinsight-overview-con.html

Citrix Service Providers Guide to using Citrix EdgeSight
https://citrix.gosavo.com/Document/Document.aspx?id=31046972&view=&srlid=25782731&srisprm=False&sritidx=0&srpgidx=0&srpgsz=25

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

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix
Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.