CITRIX

App Orchestration 2.0

Getting Started with Citrix App Orchestration 2.0

Prepared by: Jenny Berger

Commissioning Editor: Erin Smith

Version: 1.0

Last Updated: April 4, 2014

Contents

Welcome to App Orchestration 2.0 5
Additional resources 5
About App Orchestration 2.0 6
Configuration server 6
Delivery Sites 7
Session Machines 7
StoreFront 8
Compute resources 8
Tenant self-service 8
App Orchestration deployment overview 8
Step 1: Deploy the configuration server and configure global settings 9
Step 2: Add a Delivery Site and Delivery Controllers 11
Step 3: Create a Session Machine Catalog and add Session Machines 12
Step 4: Add StoreFront servers 15
Step 5: Create offerings 15
Step 6: Add tenants and users 16
Step 7: Subscribe tenants to offerings 17
Optional: Add self-service features with CloudPortal Services Manager 17
Prepare your environment 18
Prepare the deployment environment 18
Active Directory requirements 19
Create remote administration policies for App Orchestration 21
Installation and deployment administrator user account requirements 24
Create the Citrix Product Depot file share 26
Citrix Licensing requirements 28
Compute resource requirements 28
NetScaler Gateway requirements 29
Prepare the database server 29

Database server requirements 30
Support for mirrored databases 31
To configure a firewall exception for the App Orchestration database instance 31
Prepare the App Orchestration configuration server 32
App Orchestration configuration server requirements 32
SSL requirements 34
Sequence of preparation tasks for Windows Server 2008 R2 SP1 34
Client OS and browser support for the management console 35
Prepare Delivery Controllers and Session Machines 36
Machine requirements 36
Machine configuration requirements 38
Delivery Site administrator requirements 38
SSL recommendations for Delivery Controllers 39
SSL recommendations for Session Machines 39
Database and Delivery Site recommendations 40
Support for aggregating existing Delivery Sites 40
Requirements for cross-forest private Delivery Sites 40
Requirements for offerings with private delivery group isolation 40
Recommendations for updating Session Machine Catalogs 41
Prepare StoreFront servers 42
Machine requirements 42
Server group requirements 44
Certificate requirements 44
Security Considerations for App Orchestration 2.0 44
SMB security signatures 45
Machine hardening techniques 45
Restrict access for tenant user accounts 46
XenApp Session Machine isolation 46

Copyright and Trademarks

Welcome to App Orchestration 2.0

Thank you for choosing App Orchestration. This document includes information and instructions to help you learn more about deploying App Orchestration and getting the most out of your deployment. Before you begin deployment, review the following sections:

- **About App Orchestration** provides an overview of components and features.
- **App Orchestration Deployment Overview** provides a high-level description of each step in the deployment process.
- **Prepare Your Environment** helps you plan for deployment with system requirements, feature considerations, and preparation tasks. Use this section with the *App Orchestration Setup Checklist* to document your plan and track your progress.

Citrix recommends installing App Orchestration on servers containing fresh installations of supported Microsoft Windows Server operating systems. Do not attempt to upgrade to App Orchestration 2.0 from a previous release of App Orchestration.

Additional resources

The App Orchestration 2.0 web site is your primary source for information about the benefits, features, and components of App Orchestration 2.0. The web site includes a variety of videos, guides, and diagrams to help you progress smoothly through each stage of deployment.

To learn more about the Citrix products that work with App Orchestration 2.0, use the following links to review product documentation in Citrix eDocs:

- XenDesktop 7.1 documentation
- XenServer 6.2 documentation
- StoreFront 2.1 documentation
- CloudPortal Services Manager 11 documentation
- NetScaler Gateway 10.1 documentation

About App Orchestration 2.0

App Orchestration 2.0 works with the following Citrix products:

- XenDesktop 7.1
- XenServer 6.2
- StoreFront 2.1
- CloudPortal Services Manager 11.0.1
- NetScaler Gateway 10.1

App Orchestration provides simple unified management of Citrix application and desktop delivery technologies in a multi-tenant environment, using multiple datacenters across multiple domains. This topic describes the core components and shows how they work together to provision and manage hosted applications and desktops for tenants and users.

For additional information about the components described in this topic, use the following resources on the App Orchestration web site:

- The App Orchestration Architecture diagram illustrates where each component sits in a typical deployment.
- The App Orchestration Key Terms and Concepts guide explains the fundamental concepts and terminology of App Orchestration.

Configuration server

The App Orchestration configuration server hosts the App Orchestration engine and the web-based management console. These are stateless components that can be deployed on multiple servers to provide high availability and scalability. Additionally, an instance of Machine Creation Services (MCS) and an agent reside on the configuration server. MCS provides the functionality for creating and managing virtual machines (VMs) on the compute resources in the virtualization infrastructure.

When a change to the deployment occurs, such as creating a Delivery Site or adding a Session Machine to a catalog, the change is written to the configuration database and the App Orchestration engine issues all of the actions required to apply the change. These actions are called workflows which you can monitor from the web management console. The configuration server can apply these changes asynchronously, allowing multiple operations 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.

The agent that resides on the configuration server interacts with Active Directory for operations such as monitoring OUs. All Active Directory communication occurs through Active Directory Web Services. The agent also communicates with Session Machines that have not yet been allocated to host tenants' subscriptions. This occurs using PowerShell remoting (WinRM) and executing pre-installed scripts.

Delivery Sites

Delivery Sites are composed of identically configured Delivery Controllers and include the Session Machines, Delivery Groups, and other components that deliver hosted applications and desktops to tenants and their users at the appropriate isolation level.

Delivery Controllers are responsible for distributing and managing user access to hosted applications and desktops, power managing desktops, and reboot cycles for servers. Delivery Controllers can be provisioned to run XenApp 6.5 or XenDesktop 7.1. An App Orchestration deployment requires at least two Delivery Controllers (one primary Controller and one backup Controller).

When you deploy Delivery Controllers, an agent is installed on each machine to establish communication with the agent on the configuration server. The agent creates and manages Delivery Sites and manages the draining process for Session Machines. Additionally, the agent joins Session Machines to the Delivery Site using PowerShell remoting and executing pre-installed scripts.

Session Machines

Session Machines host applications and desktops for tenants' users to access through StoreFront. Like Delivery Controllers, Session Machines can be provisioned to run XenApp 6.5 or XenDesktop 7.1. An App Orchestration deployment requires at least one Session Machine. The capacity of your deployment to host user sessions is determined by the number of Session Machines you deploy.

Collections of Session Machines are contained in Session Machine Catalogs. All Session Machines in a catalog are identically configured, using the same physical hardware, the same operating system and configuration settings, and the same installed software. This ensures that users can access the applications and desktops associated with the catalog when needed, regardless of the machines App Orchestration selects to host the sessions. When a subscription is created, Session Machines from the catalog are added to a Delivery Group that is associated with the subscribing tenant. Delivery Groups can be dedicated to a single tenant's users or shared among the users of several tenants.

StoreFront

StoreFront authenticates users to sites hosting resources and manages stores of applications and desktops that users access using Receiver. An App Orchestration deployment requires at least two StoreFront servers. When you add tenants to your deployment, you can choose whether the tenant uses a shared or private StoreFront site to access subscriptions.

Compute resources

Compute resources are the hypervisors, hypervisor pools, and other components required to create and manage VMs. These resources enable you to create virtual networks, a key component in isolating tenants and ensuring shared and private resources are allocated appropriately. To deploy compute resources, App Orchestration supports the use of the following products:

- Citrix XenServer 6.2
- VMware vSphere 5.1
- Microsoft SCVMM 2012 SP1
- Microsoft SCVMM 2012 R2

Tenant self-service

After you deploy App Orchestration, you can choose to integrate with CloudPortal Services Manager 11.0.1. This deployment option enables you to make App Orchestration offerings available for self-service consumption through the Services Manager web-based control panel. Tenants can self-administer the offerings to which they have subscribed and their users can request access to subscribed offerings as needed.

App Orchestration deployment overview

Deploying the components in App Orchestration typically occurs using the following sequence:

1. Deploy the configuration server and configure global settings.
2. Create a Delivery Site and add Delivery Controllers.
3. Create a Session Machine Catalog and add Session Machines.
4. Create a StoreFront server group and add StoreFront servers.

5. Create offerings.
6. Add tenants and users.
7. Subscribe tenants to offerings.

An overview of these steps is included here for your reference, to help you understand the deployment process and provide background for the tasks you will need to perform to prepare your environment. This topic assumes that you are deploying the minimum required components to the shared resource domain.

Step 1: Deploy the configuration server and configure global settings

This step consists of the following tasks:

1. Install the App Orchestration software on the server you have prepared as the configuration server. For more information about configuration server requirements, see “Prepare the App Orchestration configuration server” on page 32.
2. Configure the App Orchestration global settings.

Install App Orchestration

The App Orchestration software is installed using a wizard that prompts you for information about your deployment. During the installation you provide the following information:

- **Service deployment name:** This value becomes the name of the configuration database that App Orchestration creates. Additionally, App Orchestration creates a logging database for the deployment using the format “*ServiceDeploymentName*Logging.”
- **Database server:** The FDQN of the SQL Server that hosts the App Orchestration configuration and logging databases. For database server requirements, see “Prepare the database server” on page 29.
- **Administrators group:** This group contains non-privileged user accounts for administering your App Orchestration deployment. In App Orchestration's global settings, this group becomes the orchestration service group. This group must exist already in your environment; the installation process does not create it.
- **SSL certificate:** A server certificate signed by your domain certificate authority is required to secure connections with the configuration server.

Configure global settings

After the installation completes, you use the App Orchestration web console to configure the global settings for the deployment. This includes providing the following information:

- **Shared resource and default user domains:** The shared resource domain contains the root OU where the configuration server and all resources that will be shared among multiple tenants reside. The default user domain contains the OUs where user accounts for tenants using shared resources reside. You can specify different domains for shared resources and user accounts or you can use the same domain for both. These domains and the root OU must exist already in your environment; App Orchestration does not create them. For more information about these domains, see “Active Directory requirements” on page 19.

- **Orchestration service account:** This is the primary App Orchestration administrator. The orchestration service account is a non-privileged user account and must be a member of the administrators group you specified during installation. This account should not belong to the Domain Admins group. The orchestration service account must exist already in your environment; the installation process does not create it. For more information about this account, see “Installation and deployment administrator user account requirements” on page 24.

- **Product installation credentials:** These credentials enable App Orchestration to install the required software on the machines you deploy as Delivery Controllers, Session Machines, and StoreFront servers. This software is stored in the Citrix Product Depot, a network file share you create in your environment.

- **Default datacenter:** The default location for shared resources. In general, datacenters contain resources in the same geographic location. For more information about datacenters, see the *Multi-Datacenter Overview* guide on the App Orchestration web site.

- **Licensing:** The FQDN and port of the Citrix Licensing server in your environment.

- **Citrix Product Depot:** The FDQN or IP address of the network containing the software App Orchestration installs when you deploy machines and the credentials for accessing it. For more information about the Citrix Product Depot, see “Create the Citrix Product Depot file share” on page 26.

- **External DNS suffix:** The DNS suffix that is used to configure the NetScaler Gateway address.

- **Network isolation and NetScaler Gateway:** Select whether or not to enable network isolation and use with NetScaler Gateway. If you enable network isolation, enter the labels of the virtual networks you created on your compute resources. If you enable use with NetScaler Gateway, specify the correct address for the appliance.

Step 2: Add a Delivery Site and Delivery Controllers

To add a Delivery Site to your deployment, you perform one of the following tasks:

- Create a new Delivery Site using the Delivery Site wizard in the App Orchestration web console
- Aggregate an existing Delivery Site

Create a new Delivery Site

A Delivery Site consists of at least two Delivery Controllers. When you create a new Delivery Site, the Delivery Site wizard prompts you for the following information:

- Site name, licensing model, and Citrix product version to install on the machines you want to deploy as Delivery Controllers. You can select XenApp 6.5 or XenDesktop 7.1. A Delivery Site with one of these products installed will only work with Session Machines that are running the same product. For example, if the Controllers in a Delivery Site are running XenDesktop 7.1, only Session Machines running XenDesktop 7.1 can join the Delivery Site to deliver hosted applications and desktops.
- The servers you want to deploy as Delivery Controllers to the Site, including the resource domain and datacenter in which they should reside. App Orchestration requires at least two Controllers in a Delivery Site (a primary Controller and a backup Controller).
- The Delivery Site administrator group and Site administrator account for the Delivery Site. The Site administrator account is a non-privileged user account and must be a member of the Delivery Site administrator group. This account should not belong to the Domain Admins group. The Delivery Site administrator group and Site administrator account must exist already in your environment; App Orchestration does not create them. For more information about Delivery Site administrator privileges in the shared and tenant resource domains, refer to the Credentials Used in the App Orchestration Environment guide available on the App Orchestration web site.
- The database server, credentials, and names for the Site databases to be created (configuration, logging, and monitoring). For more information about the privileges required for the Delivery Site database user, refer to the Credentials Used in the App Orchestration Environment guide available on the App Orchestration web site.

When specifying the database details for the Delivery Site, Citrix recommends using separate databases for each database type. This enables you to create appropriate backup and recovery protocols for each database, and prevents outages due to a single point of failure. By default, App Orchestration creates separate databases for the Site's configuration, logging, and monitoring data. For example, for a Delivery Site named "Site1," App Orchestration creates the "Site1" configuration database, the "Site1Logging" logging database, and the "Site1Monitoring" monitoring database. Additionally, App Orchestration uses the same database server for all three databases by default. You can accept these defaults or specify different servers and names for each database.

After you complete the wizard, App Orchestration issues workflows that perform the following tasks:

- Install the App Orchestration agent on the Delivery Controllers.
- Evaluate the machine configuration of the controllers and create a profile. App Orchestration uses this profile to evaluate subsequent Delivery Controllers that you add to the Site. If new Delivery Controllers do not match the profile, App Orchestration does not add them to the Site. Therefore, all Delivery Controllers you add to a Site must be identically configured, including hardware configuration, operating system, and software updates.
- Install XenDesktop 7.1 or XenApp 6.5 on the Delivery Controllers, using the product software stored on the Citrix Product Depot file share. For more information about creating this file share, see “Create the Citrix Product Depot file share” on page 26.
- Create the Delivery Site and join the Delivery Controllers to it.

You can monitor these workflows using the Workflows tab in the web console.

Aggregate existing Delivery Sites

Aggregation is the means by which multiple instances of hosted applications or desktops from multiple Delivery Sites are presented to users with a single icon when they access their StoreFront site with Citrix Receiver. For example, if Microsoft Word is offered on multiple Delivery Sites, users see a single icon for Microsoft Word when they log on to their StoreFront site.

For more information about resource aggregation, see the topic StoreFront high availability and multi-site configuration in Citrix eDocs.

For more information about the versions of XenApp and XenDesktop that StoreFront supports for Delivery Site aggregation, see the topic Infrastructure requirements in Citrix eDocs.

Step 3: Create a Session Machine Catalog and add Session Machines

This step consists of the following tasks:

1. From the App Orchestration web console, create a Session Machine catalog.
2. Add the servers you have prepared as the first Session Machines to the catalog using integrated provisioning or external provisioning.

Catalog types

You can create two catalog types in App Orchestration: On-demand catalogs and catalogs for externally-provisioned machines.

On-demand catalogs use integrated provisioning to create Session Machines whenever more capacity is needed to host tenant subscriptions. Before you create an on-demand catalog, you must perform additional tasks to enable integrated provisioning in your deployment. For information about these tasks, refer to the Integrated Provisioning Deployment Guide, available from the App Orchestration web site.

Catalogs for externally provisioned machines allow you to use other means, such as Citrix Provisioning Services or PowerShell scripts, to provision servers and add them to the catalog. When additional capacity is needed in the catalog, App Orchestration notifies you to deploy more machines; additional machines are not deployed automatically.

OS types

When you create a new Session Machine Catalog, you must select an OS type which governs the operating system installed on each machine in the catalog.

Multi User catalogs enable you to deploy a set of standard desktops and applications that are shared by a large number of users. Desktops and applications are allocated to users on a first-come, first-serve basis. Additionally, the desktop environment automatically resets to the default configuration when users log off. Session Machines in a catalog with this OS type run only supported versions of Windows Server. In XenDesktop, a Server OS catalog corresponds to a Multi User OS type in App Orchestration.

Single User catalogs enable you to deploy desktops and applications that are assigned to individual users. Users can personalize the desktop and install applications. Additionally, the desktop environment remains unchanged between sessions. Session Machines in a catalog with this OS type run only supported versions of Windows. In XenDesktop, a Desktop OS catalog corresponds to a Single User OS type in App Orchestration.

Create a catalog for externally-provisioned machines

As with Delivery Sites, you use the App Orchestration web console to complete a Session Machine Catalog wizard.

If you choose to create a catalog for externally-provisioned machines, the wizard prompts you for the following information:

- Catalog name and OS Type for the Session Machines it will contain.

- Type of Delivery Controllers that the machines will work with when hosting offerings for tenants (XenDesktop 7.1 or XenApp 6.5). The controller type you specify determines the Citrix product that is installed on the Session Machines you add to the catalog. For example, if you specify XenDesktop 7.1 as the controller type, App Orchestration will install XenDesktop 7.1 on Session Machines that are added to the catalog.

- Number of users allowed to access each machine before it is considered fully loaded. You can also allow App Orchestration to include CPU and memory in its calculations for determining server load.

Add Session Machines to the catalog

To add Session Machines to a catalog for externally-provisioned machines, you complete a separate wizard. This wizard prompts you for the name of the Session Machine Catalog, resource domain, and datacenter in which the Session Machine will reside. You also specify the names of the Session Machines you want to add to the catalog. App Orchestration requires at least one Session Machine be added to create offerings, but you can add up to 20 machines at one time. Deploying more than 20 machines places a heavy burden on the App Orchestration configuration server's resources, causing workflows to time out before the machines can complete the provisioning process.

After you complete the Add Session Machines wizard, App Orchestration issues a workflow that performs the following tasks:

- Evaluate the machine configuration of the Session Machine and create a profile. App Orchestration uses this profile to evaluate subsequent Session Machines that you add to the catalog. If new Session Machines do not match the profile, App Orchestration does not add them to the catalog. Therefore, all Session Machines you add to the catalog must be identically configured, including hardware configuration, operating system, system updates, and installed applications. If you want to add Session Machines that have, for example, different application installed, you must add them to a different catalog.

- Install XenDesktop or XenApp on the Session Machine, using the product software stored on the Citrix Product Depot file share. For more information about creating this file share, see “Create the Citrix Product Depot file share” on page 26.

- Add the Session Machine to the catalog.

You can monitor these workflows using the Workflows tab in the web console.

Step 4: Add StoreFront servers

In this step, you use the App Orchestration web console to create a StoreFront server group and specify the servers you want to add to it. A server group consists of at least two StoreFront servers (a primary server and a backup server). App Orchestration requires at least two StoreFront servers in the deployment for making offerings available to tenants' users.

As with Delivery Sites and Controllers, you add StoreFront servers to your deployment using a wizard. The wizard prompts you for the following information:

- Server group name, SSL certificate, and load balancer URL. StoreFront requires that each machine have an SSL certificate installed prior to deployment. For more information about StoreFront requirements, see “Prepare StoreFront servers” on page 42. When entering the load balancer URL, check to ensure the URL you enter is correct. Changing the URL later requires you to delete the entire server group and redeploy it with the new URL.
- Names of the StoreFront servers you want to add to the group.
- Resource domain and datacenter in which the servers will reside.

After you complete the wizard, App Orchestration issues workflows that perform the following tasks:

- Install the App Orchestration agent on the StoreFront servers.
- Evaluate the machine configuration of the servers and create a profile. App Orchestration uses this profile to evaluate subsequent StoreFront servers that you add to the group. If new StoreFront servers do not match the profile, App Orchestration does not add them to the Site. Therefore, all StoreFront server you add to a server group must be identically configured, including StoreFront version, operating system, and software updates.
- Install StoreFront on the servers, using the product software stored on the Citrix Product Depot file share. For more information about creating this file share, see “Create the Citrix Product Depot file share” on page 26.
- Create the server group and join the StoreFront servers to it.

You can monitor these workflows using the Workflows tab in the web console.

Step 5: Create offerings

This step consists of making applications and desktops (hosted on the Session Machines) available for subscription by tenants.

To create offerings, you use the App Orchestration web console to specify the applications and desktops you want to include and the isolation level at which you want to provide the offering to

tenants. The isolation level you select depends on whether you want to create an offering that uses shared machines or machines that are dedicated to an individual tenant. For more information about these isolation levels, see the App Orchestration Isolation guide on the App Orchestration web site.

Step 6: Add tenants and users

This step consists of adding tenants to the App Orchestration system and specifying the user groups that will be accessing offerings through StoreFront.

To add tenants, you use the App Orchestration web console to specify the tenant's resource and user domains, the default datacenter through which users will access offerings, the isolation level of the tenant's StoreFront site, and whether the tenant accesses a shared or private NetScaler Gateway (if NetScaler Gateway is enabled for the deployment). For more information about StoreFront isolation levels, see the App Orchestration Isolation guide on the App Orchestration web site.

To ensure the machines that are dedicated to tenants' exclusive use are adequately isolated, Citrix recommends using a private Active Directory forest for each tenant, a private management network, and offerings that employ Private Delivery Site isolation. This helps ensure that a tenant's resources are isolated from other tenants and other tenants' users.

Security considerations

As a security consideration when adding tenants, include user groups that contain only domain users. Users who belong to the Domain Admins group should not be added to these groups. This ensures that a tenant's users can access only the Session Machines in the resource management network (either shared or private). Additionally, keep the following considerations in mind:

- Do not grant tenant users or administrators Domain Admin permissions in any Active Directory domain included in the deployment.
- If administrator permissions are granted to a tenant, ensure the tenant has local machine administrator privileges only for privately allocated Session Machines. Tenants should not have administrator privileges on any other server or component in the deployment.
- Ensure that tenants do not have permissions to access any compute resources in the deployment.
- Ensure that tenants do not have permissions to log on to or administer shared components such as NetScaler Gateway appliances or StoreFront servers.

Step 7: Subscribe tenants to offerings

This step consists of creating a subscription for a tenant so that the tenant's users can access a specific offering through StoreFront.

To create a subscription, you use the App Orchestration web console to specify the offering, tenant, and user groups to include. The process of subscribing a tenant to an offering involves creating a Delivery Group according to the isolation level defined for the offering. This Delivery Group restricts access to the offering, ensuring only the specified users can access the offering through StoreFront. For more information about Delivery Group isolation levels, see the App Orchestration Isolation guide on the App Orchestration web site.

Optional: Add self-service features with CloudPortal Services Manager

After you deploy App Orchestration, you can choose to integrate CloudPortal Services Manager's self-service capabilities to enable tenants' users to select the offerings they want to use from among those that App Orchestration made available to the tenant.

This integration requires that you deploy the Hosted Apps and Desktops service according to the CloudPortal Services Manager 11 product documentation. CloudPortal Services Manager 11 comes with a version of the Hosted Apps and Desktops service that is not compatible with App Orchestration 2.0. To use Services Manager with App Orchestration 2.0, perform the following actions:

1. Download the latest version of the Hosted Apps and Desktops service from the Citrix web site.

2. Remove the existing Hosted Apps and Desktops service from your Services Manager deployment.

3. Import the downloaded service to the Services Manager control panel and configure as described in Deploy the Hosted Apps and Desktops service in Citrix eDocs.

When you enable this integration, the App Orchestration and Services Manager web consoles assume specific roles with regard to the administration tasks you perform in your deployment. You use the Services Manager control panel to manage tenant onboarding and subscribing users to offerings. You use the App Orchestration web console to create new offerings, add capacity to existing offerings, and manage the Delivery Sites, Session Machines, and StoreFront servers in your deployment.

Prepare your environment

Before you install App Orchestration, some planning is required to prepare your environment and ensure deployment activities run smoothly.

This section provides an overview of the tasks you will need to perform during deployment, information you will need to consider as you prepare your environment for specific features, and the requirements for each component in the deployment. Additionally, this section includes instructions for preparing your environment prior to installation.

To ensure all preparation tasks have been completed, use the App Orchestration Setup Checklist available for download from the App Orchestration web site. This printable checklist provides a complete list of tasks for each component and helps you document and track your planning and preparation efforts.

Prepare the deployment environment

Before you deploy App Orchestration components, perform the following tasks to prepare your network environment:

- Create the shared resource and default user domains and the root OU for the deployment. See “Active Directory requirements” on page 19.
- Create a policy for all machines in the deployment that sets the PowerShell execution policy, enables PowerShell remoting, and enables remote administration with WMI. See “Create remote administration policies for App Orchestration” on page 21.
- Create the non-privileged user accounts that you will use to install App Orchestration and designate as the orchestration service account for the deployment. See “Installation and deployment administrator user account requirements” on page 24.
- Create a network file share where the App Orchestration agent software and Citrix product software reside. See “Create the Citrix Product Depot file share” on page 26.
- Set up Citrix Licensing. See “Citrix Licensing requirements” on page 28.
- If you intend to offer certain tenants private access to hosted applications and desktops, create virtual networks that isolate these private resources from those shared among multiple tenants. See “Compute resource requirements” on page 28.

- Consider whether or not you want to use NetScaler Gateway to provide secure remote access and load balancing for the StoreFront servers in your deployment. See “NetScaler Gateway requirements” on page 29.

Active Directory requirements

To deploy App Orchestration, you must have at least one domain controller in your environment. App Orchestration supports deployment in multi-forest and multi-domain Active Directory environments.

App Orchestration supports the following domain functional levels:

Resource Domain Functional Levels	User Domain Functional Levels
• Windows Server 2012 • Windows Server 2008 R2	• Windows Server 2012 • Windows Server 2008 R2 • Windows Server 2003

Required domains

App Orchestration requires that you prepare the following domains:

- **Shared resource domain:** The domain where the App Orchestration configuration server resides. This domain contains all components that are shared with multiple tenants. This is also where the App Orchestration root OU is created.

- **Default user domain:** The domain where App Orchestration user accounts reside (for example, the user account designated as the orchestration service account). You can create a separate domain for these accounts or you can designate the shared resource domain for this purpose.

You will need to specify these domains when you configure App Orchestration's global settings.

Required organizational units

Prior to installing and configuring the App Orchestration configuration server, create a root OU for the deployment in the shared resource domain. When you configure App Orchestration's global settings, you will need to specify this OU. After you configure the global settings, App Orchestration creates the DecommissionedServers OU automatically within the root OU. This OU is for machines that been removed from the deployment.

Required tenant domains and organizational units

Before you add tenants to the deployment, determine the tenants who will require shared or private access to offerings. When you import tenants, you will need to specify the resource and user domains that belong to the tenant so that, when subscriptions are created later, App Orchestration can allocate the machines hosting the tenant's offerings appropriately. These domains must exist in Active Directory before you import the tenant.

Tenants with private offerings

For each tenant who needs private access to offerings, perform the following tasks:

1. Create a resource domain and resource OU. This is where App Orchestration will allocate machines for hosting private offerings.

2. Create a user domain for the tenant's user accounts. Alternatively, you can use the tenant's resource domain for this purpose.

3. In the user domain, create a user OU and add the appropriate user groups. Finally, add user accounts to these groups.

Tenants with shared offerings

For each tenant who needs shared access to offerings, perform the following tasks:

1. Create a resource OU for the tenant within the App Orchestration root OU in the shared resource domain.

2. Create a user domain for the tenant's user accounts. Alternatively, you can use App Orchestration's default user domain for this purpose.

3. In the user domain, create a user OU and add the appropriate user groups. Finally, add user accounts to these groups.

Required domain trusts for private offerings

When you create If you intend to deploy private machines to tenants' resource domains, you must create a two-way trust between App Orchestration's shared resource domain and the tenant's private resource domain. App Orchestration does not verify that this trust exists when you import the tenant or create subscriptions to a private offering. If this trust does not exist, subscriptions to private offerings cannot be created.

Create remote administration policies for App Orchestration

To facilitate remote administration, create a policy that apply to all machines in your App Orchestration environment and include the following:

- PowerShell execution policy is set to AllSigned or RemoteSigned
- PowerShell remoting is enabled, including auto-configuration of listeners, trusted hosts, and Windows Remote Shell
- Allow inbound remote administration in Windows Firewall

> **Note:** By default, WinRM 2.0 uses the ports 5985 for HTTP traffic and 5986 for HTTPS traffic. If you are using firewalls between the App Orchestration configuration server and the other servers in your deployment, ensure these ports are enabled.

You can create this policy using one of the following methods:

- Manually configure policy settings using the Group Policy Management Console. Use this topic to configure these settings.
- Automatically configure policy settings using the New-CamGPO.ps1 script.

The New-CamGPO script creates a Group Policy Object (GPO) and configures all the required policy settings described in this topic. You can run this script after you prepare the server you want to use as the App Orchestration configuration server, join it to the shared resource domain, and add it to the App Orchestration root OU. This script is located in the %Program Files%\Citrix\CloudAppManagement\InfrastructureTools directory on the App Orchestration configuration server.

After you create this policy, link the GPO to the following objects:

- App Orchestration root OU in the shared resource domain
- All resource OUs in the tenant resource domains that you create

> **Important:** When you deploy machines that reside in these OUs (for example, adding a Delivery Site), App Orchestration issues workflows to complete the deployment tasks. For these workflows to complete successfully, the machines on which they run must have these policy settings applied. App Orchestration does not verify these policy settings are applied before issuing the workflows.

To set the PowerShell execution policy

1. On a server joined to the domain, open the Group Policy Management Console (gpmc.msc) and create a new GPO or edit an existing one.
2. From the Group Policy Management Editor, navigate to **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows Components** > **Windows PowerShell**.
3. Right-click **Turn on Script Execution** and select **Edit**.
4. Select **Enabled** and then, under **Options**, select **Allow local scripts and remote signed scripts**.

To configure PowerShell remoting

To configure PowerShell remoting using Group Policy, use the Group Policy Management Console to enable the WinRM service, configure listeners, set the amount of session memory available, and provide a list of trusted hosts. You will also need to configure the WinRM service to start automatically and ensure Windows Firewall allows traffic through the ports assigned to WinRM.

1. On a server joined to the domain, open the Group Policy Management Console (gpmc.msc) and create a new Group Policy Object (GPO) or edit an existing one.
2. From the Group Policy Management Editor, navigate to **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows Components**.
3. Use the following table to configure the required policy settings:

Setting Location & Name	Policy Setting	Setting Values
Windows Remote Management (WinRM) > WinRM Service	Allow automatic configuration of listeners	• Enabled. • To configure WinRM to listen on all addresses, type an asterisk (*) in the **IPv4 Filter** and **IPv6 Filter** fields.
Windows Remote Management (WinRM) > WinRM Client	Trusted Hosts	• Enabled. • In **TrustedHostsList**, type an asterisk (*) to indicate all hosts are trusted.

Windows Remote Shell	Specify maximum amount of memory in MB per Shell	• Enabled. • In **MaxMemoryPerShellMB**, type 1024.
	Specify maximum number of remote shells per user	• Enabled. • In **MaxShellsPerUser**, typing 0 indicates an unlimited number of shells.

4. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > System Services**.
5. Double-click the **Windows Remote Management** service and select the following options:
   - **Define this policy setting**
   - **Automatic**
6. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security > Inbound Rules**.
7. Right-click **Inbound Rules** and select **New Rule**.
8. In the **New Inbound Rule Wizard**, on the **Rule Type** page, select **Predefined** and then select the **Windows Remote Management** rule. Click **Next**.
9. On the **Predefined Rules** page, accept the defaults and click **Next**.
10. On the **Action** page, ensure **Allow the connection** is selected and click **Finish**.
11. To apply the settings, on each server, open a PowerShell command window and run **gpupdate**.

To enable remote administration with WMI

As part of maintaining your App Orchestration environment, you might need to update Session Machine Catalogs to deploy patches, upgrade installed applications, or take advantage of new hardware on Session Machines. To ensure the update process occurs smoothly, a firewall

exception is required to enable inbound remote administrative connections on TCP ports 135 and 445. If this exception is not present, the update process might fail.

1. On a server joined to the domain, open the Group Policy Management Console (gpmc.msc) and create a new Group Policy Object (GPO) or edit an existing one. This GPO should be associated with all servers in the App Orchestration environment.

2. From the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile**.

3. Double-click the **Windows Firewall: Allow inbound remote administration exception** setting and select **Enabled**.

4. Under **Options**, in **Allow unsolicited incoming messages from these IP addresses**, type an asterisk (*****).

5. Click **OK** to save your selection.

Installation and deployment administrator user account requirements

To install and manage components in your App Orchestration deployment, create the following objects:

- A user group for the user accounts for installing and administering the deployment. This group is known as the orchestration service group.

- A user account for installing the App Orchestration configuration server.

- A user account for performing administrative tasks using the App Orchestration web management console, known as the orchestration service account.

Orchestration service group

The orchestration service group contains the administrator user accounts for the App Orchestration deployment, conferring full rights on member accounts. User accounts that are added to this group should be non-privileged users with no administrator rights to the machines in the deployment. Accounts in this group should not be members of the Domain Admins group. You will need to supply this group name when you install the App Orchestration configuration server. After you supply this group name, it cannot be changed later.

Installation user account

The user account you use to install the App Orchestration configuration server must meet the following requirements:

- Be a local administrator on the server you prepare as the App Orchestration configuration server
- Have permission to create databases on the database server and connect using PowerShell remoting
- Be a member of the orchestration service group

Orchestration service account

The orchestration service account is the primary administrator account for the App Orchestration deployment. It is a non-privileged user account that has permission to access all App Orchestration functions and add and modify objects. This account should not be part of the Domain Admins group. This account need not be the same account used to install the App Orchestration configuration server.

The orchestration service account must meet the following requirements:

- Be a member of the orchestration service group.
- Be a local administrator on the App Orchestration configuration server.
- Have permission to connect to machines in the domain using PowerShell remoting.
- Be a local administrator on all XenDesktop and XenApp servers.
- Have Full Control permission for the App Orchestration root OU. This enables the account to deploy machines in the shared resource domain, create directory objects, enumerate compute resource configurations, and manage virtual machines.

For more information on the permissions required for the installer and orchestration service accounts, refer to the Credentials Used in the App Orchestration Environment guide available from the App Orchestration web site.

Create the Citrix Product Depot file share

The Citrix Product Depot is a network file share that hosts the software for the following Citrix products:

- App Orchestration 2.0
- XenDesktop 7.1
- XenApp 6.5
- StoreFront 2.1

When you deploy Delivery Sites, Session Machines, or StoreFront server groups, App Orchestration uses this file share to install the required agents and software on the servers you specify.

Requirements

You can create this file share on a machine joined to any domain in your environment. Trusts are not required to access the file share. App Orchestration requires a user account that can access the file share with Read permission. Additionally, the DNS server in the shared resource domain and, if applicable, in tenants' resource domains must be able to resolve the FQDN of the server hosting the file share. Access to the file share created on a machine joined to a workgroup is not supported.

> **Note:** When configuring the location of the Citrix Product Depot network file share in App Orchestration's web console, ensure the file share you specify is a Windows (SMB) file share. If the file share you specify is a Distributed File System (DFS) share, App Orchestration cannot access the location and, therefore, cannot provision Delivery Sites, Session Machines, or StoreFront server groups successfully.

You will need to specify the network path to this file share and the user account for accessing it when you configure App Orchestration's global settings. You can specify the network path using IPv4 addressing or IPv6 addressing. If using IPv6, specify a literal IPv6 address. For more information, see "IPv6 Address Nomenclature Used for a UNC Path" available on the Microsoft web site.

Folder structure

When creating the file share, use the following folder structure:

- \\ServerName
  - \CitrixProductDepot
  - \CloudAppManagementAgents
  - \CitrixStoreFront
  - \XenDesktop
  - \XenApp
    - \XenAppHRP

CloudAppManagementAgents folder

The contents for the CloudAppManagementAgents folder are located in the **Packages** folder of the App Orchestration installation media. Copy all the files in the Packages folder to the CloudAppManagementAgents folder in the file share.

CitrixStoreFront and XenDesktop folders

Copy the entire contents of the StoreFront and XenDesktop installation media to their respective folders in the file share.

XenApp and XenAppHRP folders

Copy the entire contents of the XenApp 6.5 installation media to the **XenApp** folder in the file share. Additionally, copy the entire contents of the latest Hotfix Rollup Pack to the **\XenApp\XenAppHRP** folder.

To enable App Orchestration to deploy XenApp controllers without requiring PowerShell remoting on the XenApp configuration database, the following SQL Server tools are installed on the controllers when XenApp 6.5 FP2 is installed:

- PowerShellTools.msi
- SharedManagementObjects.msi
- SQLSysClrTypes.msi

These tools are included on the App Orchestration installation media, in the **\Support\SQLServer2012** folder. To add these tools to the Citrix Product Depot, copy the **SQLServer2012** folder to the **\XenApp\Support** folder on the network file share.

For more information about these tools, see the Microsoft SQL Server 2012 Feature Pack download page, located at http://www.microsoft.com/en-us/download/details.aspx?id=29065 on the Microsoft web site.

Citrix Licensing requirements

Citrix Licensing 11.11.1 is required for configuring the App Orchestration configuration server as well as configuring the Delivery Controllers, Session Machines, and StoreFront servers you want to deploy. If you use an older version of Citrix Licensing, App Orchestration cannot validate the server during configuration of global settings.

For Delivery Sites that use Controllers running XenApp 6.5 Feature Pack 2, specify the Licensing Server using the FQDN or an IPv4 address. If you use an IPv6 address, App Orchestration cannot validate the server and create the Delivery Site.

For more information about deployment steps, obtaining license files, and managing your Licensing server, see Citrix Licensing 11.11.1 in Citrix eDocs.

Compute resource requirements

Compute resources include the hypervisors and virtual networks and machines that form the foundation for your App Orchestration deployment. These resources enable you to deploy Session Machines on demand using integrated provisioning and use network isolation to provide tenants with private resources.

App Orchestration supports using the following products to create the virtual networks and machines you need for your deployment:

- Citrix XenServer 6.2
- Microsoft System Center Virtual Machine Manager 2012 SP1
- VMware vSphere 5.1

If you intend to use network isolation in your deployment, you create at least two networks when you set up your compute resources: a shared Controller management network and a shared Delivery Group management network. If you intend to offer tenants private access to hosted applications and desktops, create a private management network for each tenant. Additionally, these networks must be labeled.

> **Important:** You will need to supply these labels when you configure App Orchestration's global settings. In App Orchestration, network labels are case-sensitive. When configuring the global settings, enter the labels exactly as they are configured for your compute resources.

For more information about these networks and instructions for creating and labeling them, review the document App Orchestration Isolation on the App Orchestration web site.

NetScaler Gateway requirements

App Orchestration supports the use of NetScaler Gateway 10.1 to provide secure remote access and load balancing for the StoreFront servers in your App Orchestration deployment. If you intend to use NetScaler Gateway in your deployment, review the following information prior to deployment:

Review the document Configuring NetScaler Load Balancing and NetScaler Gateway for App Orchestration on the App Orchestration web site. This document provides detailed requirements and instructions for integrating NetScaler Gateway with App Orchestration.

Review the security considerations as described in the Planning for Security with NetScaler Gateway section of Citrix eDocs.

LDAP authentication for NetScaler Gateway

When configuring LDAP authentication for NetScaler Gateway to verify user accounts in Active Directory, a user account is entered in the Administrator Bind DN setting to bind NetScaler Gateway to the LDAP server and search for the user. Citrix strongly recommends using a non-privileged user account that has bind DN permission in Active Directory. Do not use an administrator account for this setting.

Prepare the database server

In an App Orchestration deployment, the database server hosts the App Orchestration configuration and logging databases. If you choose, it can also host the databases for the Delivery Sites you deploy. Prepare the database server before you install App Orchestration. You will need to supply information about this server when you install the App Orchestration configuration server and deploy Delivery Sites, Session Machines, and StoreFront server groups.

Database server requirements

App Orchestration supports using the following database servers:

- Microsoft SQL Server 2012 Express, Standard, and Enterprise editions
- Microsoft SQL Server 2008 R2 Express, Standard, Enterprise, and Datacenter editions

When you install the App Orchestration configuration server, you are prompted to provide a service deployment name. This name is used for the configuration database. If you want to use an existing database for your App Orchestration deployment, you specify that database name as the service deployment name. If you enter a database name that does not exist on the database server, the database is automatically created.

The service deployment name is also used to create the logging database for the deployment, using the format "*ServiceDeploymenName*Logging." To ensure the configuration database is created smoothly and can communicate with the other servers in your deployment, the following items are required:

Authentication Mode	Windows authentication is enabled.
TCP	Enabled, along with all appropriate IP addresses, in SQL Server Configuration Manager.
SQL PowerShell Provider	Installed. This provider is included with SQL Management Studio.
SQL Server Browser service	Enabled, and set to run automatically.
SQL Server instance	Enabled, and set to run automatically
Firewall	Allow inbound connections to the database server from the other servers in your App Orchestration deployment. Additionally, enable firewall exceptions for the SQL Server Browser and SQL Server instance. See “To configure a firewall exception for the App Orchestration database instance” on page 31.

User account permissions	The user account with which App Orchestration is installed must have the **Sysadmin** role to create the required accounts and databases during App Orchestration configuration server setup. For more information about required user accounts and permissions, refer to the Credentials Used in the App Orchestration Environment guide available from the App Orchestration web site.

Support for mirrored databases

For the configuration database, App Orchestration supports the use of mirrored and non-mirrored databases.

If you want to use a mirrored database in your deployment, consider the following:

- If you specify a database that does not yet exist when installing the App Orchestration configuration server, the resulting database cannot be mirrored. The installer does not perform any mirroring configuration or create a database that supports mirroring by default.
- To use a mirrored database with the deployment, create the mirrored database before you deploy the App Orchestration configuration server, and ensure the database is empty. When you are prompted for the service deployment name during installation of the configuration server, enter the name of this database.

For more information about using mirrored databases with App Orchestration, refer to the Configure SQL database mirroring guide available on the App Orchestration web site.

To configure a firewall exception for the App Orchestration database instance

To ensure the database server can communicate as required with the other servers in your App Orchestration deployment, create a Windows Firewall exception on the database server that allows connections with other servers.

1. On the database server, click **Start > Administrative Tools > Windows Firewall with Advanced Security**.
2. In the left pane, click **Inbound Rules**.
3. Right-click **Inbound Rules** and then select **New Rule**. The New Inbound Rule Wizard appears.

4. On the **Rule Type** page, select **Program** and then click **Next**.
5. On the **Program** page, select **This program path** and then click **Browse**.
6. Locate and select the SQL Server executable and then click **Open**. Typically, the SQL Server executable is located at C:\Program Files\Microsoft SQL Server\MSSQL10_50.*instancename*\MSSQL\Binn\sqlservr.exe.
7. On the **Action** page, select **Allow the connection** and then click **Next**.
8. On the **Profile** page, select **Domain, Private,** and **Public**.
9. On the **Name** page, enter a name for the rule and click **Finish**.

Prepare the App Orchestration configuration server

The App Orchestration configuration server hosts the App Orchestration configuration engine and the web management console.

App Orchestration configuration server requirements

The server you prepare to be the App Orchestration configuration server must meet the following requirements:

Hardware	• Dual core processors, 2.6 GHz or higher • Minimum 3 GB RAM • Minimum 50 GB free disk space
Operating System	One of the following: • Windows Server 2008 R2 SP1 • Windows Server 2012 R2 (Standard, Enterprise, or Datacenter edition)
Domain Functional Level	Windows Server 2008 R2
Windows Management Framework and PowerShell versions	Version 3.0. The Windows Management Framework is available for download from the Microsoft web site at http://www.microsoft.com/en-us/download/details.aspx?id=34595.

.NET Framework version	• Windows Server 2008 R2 SP1: .NET Framework 4.5. This executable is located in the Support folder of the App Orchestration installation media. • Windows Server 2012: .NET Framework 3.5. For information on enabling this feature, see the article "Install or Uninstall Roles, Role Services, or Features" on the Microsoft web site.
PowerShell remoting	Enabled. See “Create remote administration policies for App Orchestration” on page 21.
Windows Update Service	Enabled.
SSL certificates	A server certificate signed by your domain certificate authority is required for deploying the configuration server.
System Temp folder	Must be writable by the Network Service account.
Internet Access	Enabled. Setup accesses Windows Update to verify the full version of the .NET Framework 4.5 is installed and to install .NET updates, if required.
Citrix Product Depot access	The Citrix Product Depot is a network file share containing the App Orchestration agents and Citrix products required to set up the other servers in your deployment using PowerShell remoting. All servers in the deployment and the user account performing the installations must have permission to access this file share. See “Create the Citrix Product Depot file share” on page 26.
Web browser (for accessing the web management console)	Internet Explorer 10 or 11

Important: When preparing the configuration server for App Orchestration installation, ensure the server operating system and anti-virus software have all appropriate updates and patches, and that the server is free of untrusted software.

SSL requirements

Deploying the configuration server requires that you use SSL to secure traffic between the configuration server and the other servers in your deployment. Before you begin deployment, you will need to acquire a server certificate signed by your domain certificate authority and install it on the server you prepare as the configuration server. When you install the configuration server, the installer prompts you to specify the server certificate you want to use. For proof-of-concept deployments, you can use a wildcard certificate.

Additionally, Citrix strongly recommends using SSL to secure connections with the other components in your App Orchestration deployment, including API calls, connections to and from the configuration database, and the web management console.

Sequence of preparation tasks for Windows Server 2008 R2 SP1

If you are preparing a server running Windows Server 2008 R2 SP1 as the configuration server, use the following sequence of tasks to ensure the configuration server is deployed smoothly:

1. Install the operating system and apply all required updates and patches.
2. Install .NET Framework version 4.5.
3. Install Windows Management Framework 3.0, which includes Windows PowerShell 3.0.
4. Install the server certificate required for installation of the configuration server.
5. Join the server to the shared resource domain.
6. Verify the Group Policy settings described in “Create remote administration policies for App Orchestration” on page 21 have been applied to the App Orchestration root OU of the shared resource domain for your deployment. For more information about required OUs, see “Active Directory requirements” on page 19.

> **Note:** If you join the configuration server to the shared resource domain and enable PowerShell remoting before you install the Windows Management Framework 3.0 and upgrade to PowerShell 3.0, installing App Orchestration might fail. If this happens, execute the command `winrm delete http://schemas.microsoft.com/wbem/wsman/1/config/plugin?Name=Microsoft.ServerManager` and retry the installation.

Client OS and browser support for the management console

To manage your deployment, App Orchestration includes a web-based management console. The console is hosted, by default, on the configuration server, but you can also run the console on other computers in your environment. To run the console, App Orchestration supports the following web browsers and operating systems:

Windows Operating Systems

Web Browser	Windows 7 SP1 (32-bit and 64-bit)	Windows 8 (32-bit and 64-bit)	Windows 8.1 (32-bit and 64-bit)	Windows Server 2008 R2 SP1	Windows Server 2012 R2
Internet Explorer 10	X	X		X	
Internet Explorer 11			X	X	X
Mozilla Firefox 24	X	X			
Google Chrome 30	X	X			

Important: In Internet Explorer 11, AutoComplete is enabled by default. In addition to remembering previous entries for forms and URLs, AutoComplete remembers entries for usernames and passwords. To prevent unauthorized access to the App Orchestration web console due to remembered credentials, Citrix recommends disabling AutoComplete on all machines on which Internet Explorer 11 is used to access the web console. To do this, perform the following actions:

1. From the **Start** screen, click **Settings > Control Panel > Internet Options**.
2. Click the **Content** tab and then click **AutoComplete**.
3. Clear the **User names and passwords on forms** check box and then click **OK**.

Mac OS and Apple iOS

Web Browser	Mac OS X (10.8)	Apple iOS 7 (iPad only)
Mozilla Firefox 24	X	
Google Chrome 30	X	
Apple Safari for iOS		X

Prepare Delivery Controllers and Session Machines

App Orchestration supports using XenApp 6.5 Feature Pack 2 and XenDesktop 7.1 to provision the Delivery Controllers and Session Machines that are required for creating Delivery Sites and hosting the applications and desktops that tenants' users access. Each Delivery Site consists of at least two identically-configured Controllers. Session Machine Catalogs consist of one or more identically-configured Session Machines.

Machine requirements

Servers prepared as Delivery Controllers and Session Machines have the following requirements:

Hardware	• Dual core processors, 2.6 GHz or higher • Minimum 3.0 GB RAM • Minimum 50 GB free disk space

Operating System (XenDesktop 7.1)	**Delivery Controllers:** • Windows Server 2008 R2 SP1, with PowerShell 3.0 • Windows Server 2012 R2 (Standard, Enterprise, or Datacenter edition) **Session Machines:** • Windows XP SP3 (32-bit only), with PowerShell 2.0 • Windows 7 SP1 (32-bit and 64-bit), with PowerShell 3.0 • Windows 8 (32-bit and 64-bit) • Windows 8.1 (32-bit and 64-bit) • Windows Server 2008 R2 SP1, with PowerShell 3.0 • Windows Server 2012 • Windows Server 2012 R2
Operating System (XenApp 6.5 FP2)	Windows Server 2008 R2 SP1, with PowerShell 3.0
Domain Functional Level	• Windows Server 2008 R2 • Windows Server 2012
.NET Framework version	Windows Server 2008 R2 SP1: .NET Framework 4.5. This executable is located in the Support folder of the App Orchestration installation media. Windows Server 2012: .NET Framework 3.5. For information on enabling this feature, see the article "Install or Uninstall Roles, Role Services, or Features" on the Microsoft web site.
Windows Management Framework and PowerShell version	For most supported operating systems, Version 3.0 is required unless otherwise specified. For Windows 7 SP1 and Windows Server 2008 R2 SP1, the Windows Management Framework 3.0 is available for download from the Microsoft web site at http://www.microsoft.com/en-us/download/details.aspx?id=34595.
PowerShell remoting	Enabled. See “Create remote administration policies for App Orchestration” on page 21.

Windows Update Service	Enabled.
Automatic updates	Disabled on all servers designated as Session Machines.
Windows Server Roles	.NET Framework 3.5.1.
Citrix Product Depot access	The Citrix Product Depot is a network file share containing the App Orchestration agents and Citrix products required to set up the other servers in your deployment using PowerShell remoting. All servers in the deployment and the user account performing the installations must have permission to access this file share. See “Create the Citrix Product Depot file share” on page 26.
Database server	• Microsoft SQL Server 2012 Express, Standard, and Enterprise editions • Microsoft SQL Server 2008 R2 Express, Standard, Enterprise, and Datacenter editions
Citrix software	None installed. If any Citrix products are installed when you add Delivery Controllers or Session Machines to the deployment, App Orchestration might remove or overwrite these files. To ensure these machines are deployed successfully, completely remove all Citrix software beforehand.

Machine configuration requirements

When you add the initial Controllers to a Delivery Site or Session Machines to a catalog, App Orchestration uses these machines to construct machine profiles that are used to evaluate subsequent machines that are added to the Site or catalog. If these machines do not match the profile for the Site or catalog, they are not added to the deployment. Therefore, each machine you add to a Site or catalog must have the same machine configuration, operating system and updates, Citrix product version, and installed applications as the first machines you deployed. To add machines with differing configurations, create a new Delivery Site or Session Machine Catalog as appropriate.

Delivery Site administrator requirements

When you provision a Delivery Site in App Orchestration, you must specify an administrator account for the Delivery Site. This account has limited privileges in tenants’ resource domains when integrated provisioning is used in App Orchestration. If integrated provisioning is enabled in App Orchestration's global settings, this administrator account has only the ability to create machine accounts in the tenant's resource domain. The account has no other rights or privileges in the

tenant's resource or user domains. If integrated provisioning is not enabled, this account has no rights or privileges in the tenant's resource or user domains.

For more information about the user accounts required for deploying Delivery Sites and Session Machines, refer to the Credentials Used in the App Orchestration Environment guide available from the App Orchestration web site.

SSL recommendations for Delivery Controllers

To avoid security risks, Citrix recommends that you use SSL to secure communications between the Delivery Controllers and StoreFront servers in your deployment. By default, App Orchestration requires StoreFront servers to be configured to use SSL. For the machines you prepare as Delivery Controllers, in addition to configuring SSL, you also add a registry key that enables SSL for the Citrix XML Service. This registry key is added to both the App Orchestration configuration server and to Delivery Controllers before they are deployed to Delivery Sites.

By default, App Orchestration does not automatically configure SSL for the XML Service when adding Delivery Controllers to Delivery Sites. By adding this registry key, App Orchestration can verify that the Controllers have SSL enabled and workflows issued to the Controllers can complete successfully.

Use the following information to add this registry key to the App Orchestration configuration server and to Delivery Controllers before they are deployed to Delivery Sites:

- Registry location: HKEY_LOCAL_MACHINE\Software\Citrix\CloudAppManagement\Configuration
- Name: XmlSslEnabled
- Type: REG_DWORD
- Value: 1

SSL recommendations for Session Machines

To avoid security risks, Citrix recommends that you use SSL to secure communications between the Session Machines and NetScaler Gateway appliances in your deployment. As part of deploying NetScaler Gateway in your environment, a signed SSL certificate and, if applicable, a trusted root certificate are required. For Session Machines running XenDesktop 7.1 or XenApp 6.5 FP2, manually configure SSL and install a signed SSL certificate on each machine. If you use App Orchestration to aggregate Delivery Sites running XenDesktop 5.6, ensure the Session Machines and Delivery Controllers in those Sites have the latest public hotfix applied.

Database and Delivery Site recommendations

When you create a Delivery Site through the App Orchestration web console, you are prompted for the names of the configuration, logging, and monitoring databases that are created automatically when the Delivery Site is deployed. Citrix recommends using separate databases for each database type. For example, "Site1" for the configuration database, "Site1Logging" for the logging database, and "Site1Monitoring" for the monitoring database. This enables you to create appropriate backup and recovery protocols for each database, and prevents outages due to a single point of failure.

Support for aggregating existing Delivery Sites

Aggregating applications and desktops enables users to access offerings that are available in multiple StoreFront stores from a single point of access. Using aggregation, you can add Delivery Sites that already exist in your environment to your App Orchestration deployment.

App Orchestration supports aggregating existing Delivery Sites that run the following versions of XenApp or XenDesktop:

- XenApp 5.0, 6.0, and 6.5
- XenDesktop 5.5, 5.6, 7.0, and 7.1

Aggregation of Delivery Sites running versions of XenApp or XenDesktop that are older than specified in this section (such as Citrix Presentation Server 4.5) is not supported. For a complete list of all XenApp and XenDesktop versions that are supported for Delivery Site aggregation, refer to the StoreFront topic Infrastructure requirements on Citrix eDocs.

Requirements for cross-forest private Delivery Sites

To create Delivery Sites in a tenant's private resource domain in a different forest, the root certificates from the shared resource domain must be imported to the Delivery Controllers comprising the Delivery Site you want to create. This enables the App Orchestration agent installed on the Controllers during Site creation to establish a trust relationship with the shared resource domain.

Requirements for offerings with private delivery group isolation

App Orchestration enables you to create offerings for tenants at varying levels of isolation. With Private Delivery Group isolation, the offering you create uses a Delivery Site that is shared with other tenants but the Session Machines that host the offering are dedicated to a specific tenant. If you intend to create offerings for tenants using the Private Delivery Group isolation level, consider the following requirements:

- A two-way trust must exist between App Orchestration's shared resource domain, where the Delivery Site resides, and the tenant's private resource domain, where the Session Machines hosting the offering reside.

- The Delivery Site administrator account must be a local administrator on each Session Machine in the tenant's private resource domain.

- If the Delivery Sites and Session Machines are running XenDesktop 7.1 and reside in domains in different forests, the Session Machines included in the private delivery group must have the **SupportMultipleForest** registry key configured. This ensures that subscription to the offering hosted on the Session Machines is successful and that Citrix Studio registers the Session Machines in a delivery group. Use the following information to add this registry key:

    - Registry location: HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest

    - Name: SupportMultipleForest

    - Type: REG_DWORD

    - Value: 1

For more information about support for multiple forests in XenDesktop 7.1, see Deploy XenDesktop in a multiple forest Active Directory environment in Citrix eDocs.

Recommendations for updating Session Machine Catalogs

During the life of your deployment, you might need to update the Session Machines in a catalog by applying hotfixes, adding new applications, or upgrading to more efficient hardware. To do this, you typically perform the following tasks:

1. Prepare new servers with the updates you want to introduce to your App Orchestration deployment. For example, create a new VM template or prepare a server with the updated software or hardware you want to add to the deployment.

2. Create a new version of the catalog.

3. Provision the machines to the new catalog.

When updating Session Machine Catalogs, consider the following:

- When using a new VM template to deploy updated Session Machines, ensure the template includes no snapshots. To successfully deploy updated Session Machines using integrated provisioning, App Orchestration must create the first snapshot of the template. If snapshots exist when the VM template is added, subsequent machine provisioning fails.
- When updating multiple machines through a scripted or otherwise automated process, ensure that no administrator credentials are sent to updated Session Machines. This includes using Basic authentication for PowerShell remoting.
- If CredSSP is enabled in your environment, do not use PowerShell remoting to connect to Session Machines using implicit authentication in the context of an administrator.
- Do not encode credentials in any updating scripts.

Prepare StoreFront servers

StoreFront authenticates users to sites hosting resources and manages stores of applications and desktops that users access with Citrix Receiver.

Machine requirements

Servers prepared as StoreFront servers have the following requirements:

Hardware	• Dual core processors, 2.6 GHz or higher • Minimum 3.0 GB RAM • Minimum 50 GB free disk space
Operating System	• Windows Server 2008 R2 SP1, with PowerShell 3.0 • Windows Server 2012 R2 (Standard, Enterprise, or Datacenter Edition)
Windows Management Framework and PowerShell version	Version 3.0. For Windows Server 2008 R2 SP1, the Windows Management Framework 3.0 is available for download from the Microsoft web site at http://www.microsoft.com/en-us/download/details.aspx?id=34595.

Domain Functional Level	• Windows Server 2008 R2 • Windows Server 2012
.NET Framework version	• Windows Server 2008 R2 SP1: .NET Framework 4.5. This executable is located in the Support folder of the App Orchestration installation media. • Windows Server 2012: .NET Framework 3.5. For information on enabling this feature, see the article "Install or Uninstall Roles, Role Services, or Features" on the Microsoft web site.
PowerShell remoting	Enabled. See “Create remote administration policies for App Orchestration” on page 21.
Windows Update Service	Enabled.
Windows Server Roles	• .NET Framework 3.5.1 • Web Server (IIS), with all default role services
Citrix Product Depot access	The Citrix Product Depot is a network file share containing the App Orchestration agents and Citrix products required to set up the other servers in your deployment using PowerShell remoting. All servers in the deployment and the user account performing the installations must have permission to access this file share. See “Create the Citrix Product Depot file share” on page 26.
Database server	• Microsoft SQL Server 2012 Express, Standard, and Enterprise editions • Microsoft SQL Server 2008 R2 Express, Standard, Enterprise, and Datacenter editions
Citrix software	None installed. If any Citrix products are installed when you add StoreFront servers to the deployment, App Orchestration might remove or overwrite these files. To ensure these machines are deployed successfully, completely remove all Citrix software beforehand.

Server group requirements

In App Orchestration, you add StoreFront servers to a deployment by creating server groups. A server group is a collection of two or more StoreFront servers. When adding StoreFront servers to your deployment, consider the following requirements:

- To import tenants, App Orchestration requires at least two StoreFront servers in the deployment. You can deploy multiple StoreFront server groups to provide high availability and scalability.
- The StoreFront servers that are included in the server group must have the same version of StoreFront installed. Including servers of differing StoreFront versions in the same server group is not supported.

Certificate requirements

App Orchestration requires a server certificate signed by your domain certificate authority to be installed on each StoreFront server you deploy. For proof-of-concept deployments, you can use a wildcard certificate.

Security Considerations for App Orchestration 2.0

When planning to deploy machines in your App Orchestration environment, be sure to review the security best practices and recommendations for the Citrix products that are used with App Orchestration. Refer to the following topics in Citrix eDocs:

- XenDesktop 7.1: Security
- XenApp 6.5: Security Standards and Deployment Scenarios
- StoreFront 2.1: Secure your StoreFront deployment
- NetScaler Gateway: Planning for Security with NetScaler Gateway

Additionally, for up-to-date information about security standards and Citrix products, visit http://www.citrix.com/security.

SMB security signatures

Citrix recommends requiring client-side and server-side SMB security signatures for all servers in your deployment. This helps ensure that SMB packets are not modified in transit among the servers in your deployment. To require SMB security signatures, configure the following Group Policy settings:

Setting Location	Policy Setting	Setting Value
Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options	Microsoft network client: Digitally sign communications (always)	Enabled
Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options	Microsoft network server: Digitally sign communications (always)	Enabled

Machine hardening techniques

To mitigate security risks such as "pass-the-hash" attacks, Citrix recommends the following techniques for reducing the attack surface of the machines in your App Orchestration deployment:

- **Use unique local account passwords.** When deploying machines from an image or template, ensure that each machine you deploy has unique local administrator credentials. This helps prevent a malicious user from reusing credentials gained elsewhere to compromise additional machines.

- **Restrict remote access for local administrator accounts.** Consider removing network and remote interactive logon privileges from local non-service accounts, such as local administrator accounts. This technique forces machines to be physically administered or remotely administered using a domain account. When remotely administering machines in your deployment, use tools and methods that do not leave reusable credentials in memory, such as using an MMC snap-in or initiating a PowerShell remoting session (for example, Enter-PSSession *ServerName*). Additionally, the domain accounts you use to administer machines should possess only the privileges required to perform the tasks needed. Do not use highly trusted domain accounts to administer lower trusted machines (for example, using a Domain Admin account to administer a client workstation).

Restrict access for tenant user accounts

To mitigate security risks to the machines in the shared resource domain, Citrix recommends that only members of the orchestration service group have permission to access these machines. Tenants' users should not have Domain Admin or local administrator privileges on any machines or components in the App Orchestration deployment. Tenants' users should be able to access only the applications and desktops that are hosted on these machines.

To limit tenants' access only to the machines that are privately allocated to them, Citrix recommends using private Active Directory forests for each tenant, creating offerings that employ Private Delivery Site isolation, and using Private server groups to deliver offerings to tenants' users. These isolation levels help ensure that tenants' private machines are kept separate from the machines in the shared resource domain, thus limiting the opportunity for a malicious user to gain access to other tenants' machines or data in the deployment.

XenApp Session Machine isolation

To ensure Session Machines running XenApp 6.5 FP2 are adequately isolated in your App Orchestration deployment, Citrix recommends creating offerings that employ Private Delivery Site isolation. By using this isolation level, the Session Machines and the Delivery Site with which they are associated are connected to a specific tenant's private management network and the desktops and applications that are hosted on the machines are accessible only by the tenant's users. Because these machines are privately allocated, not shared, this isolation level helps prevent a malicious user from gaining elevated privileges on the XenApp Delivery Site by way of the associated Session Machines.