Citrix Virtual Apps and Desktops Service

Your pre-implementation checklist

Prepare for a textbook deployment and optimal user experience

Before you deploy Citrix Virtual Apps and Desktops service, you need to complete the essential preparations.

This checklist is designed to guide you through everything you need to consider at every layer of your architecture – including all the technical prerequisites – to ensure a smooth deployment and an outstanding end-user experience.

Ready? Then let’s get started.

Before you begin

Identifying barriers to implementation

○ Change management processes

Infrastructure change management processes for new resources often include specific schedules for component deployment.

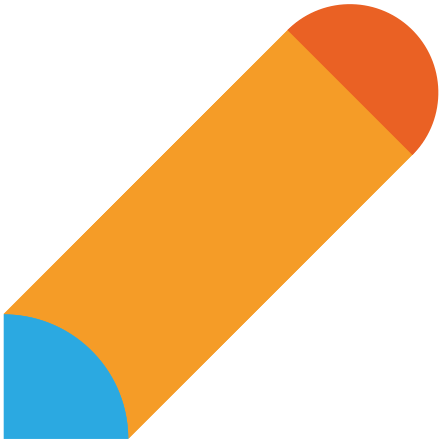
If your organization has an infrastructure change management process, review its component deployment schedules now and avoid unexpected delays during implementation.

○ Your implementation team's skillset

Whether you're handling your implementation in-house or engaging a Citrix Partner, your team should have experience implementing the Virtual Apps and Desktops service.

If your team only has experience implementing an on-premises Citrix environment – or has no Citrix experience at all – talk to our experts to identify the skills you need or visit training.citrix.com to view our Citrix cloud services curriculum.

Speak to an expert now



The control layer

Key considerations

○ Multi-forest configurations

Citrix Cloud Connectors cannot speak through forest trusts. This means if you have a multi-forest environment, and you have users coming from domains in two different forests, you'll need Cloud Connectors in both domains.

○ Active Directory security groups and organizational units

Even if you have an existing Citrix environment, we recommend creating new Active Directory security groups and organizational units for your new Citrix deployment. This will give you greater power to configure policies specifically for the new deployment.

Technical prerequisites

Active Directory

Availability

2 x domain controllers (for redundancy) with minimum Windows 2008 R2 functional domain level or higher

Configuration

Servers must be pre-configured prior to Citrix components being implemented

Citrix Cloud Connectors

Availability

2 x (for redundancy) domain joined physical or virtual Windows 2012 R2 or Windows 2016 servers

Connectivity

Port 443 opened outbound with access to the Internet

Installation proxy configuration, whitelist the following URLs:

- https://login.citrixonline.com
- https://*.citrixworkspacesapi.net
- https://cwsproduction.blob.core.windows.net/downloads

Connector firewall configuration, whitelist the following URLs:

- https://*.citrixworkspacesapi.net
- https://*.servicebus.windows.net
- https://cwsproduction.blob.core.windows.net/downloads
- https://*.cloud.com
- https://*.xendesktop.net

Hypervisor connection ports:

- XenServer Resource Pool Master TCP: 80/443
- Microsoft SCVMM TCP: 8100
- VMware vCenter TCP: 443

Sizing

Configure minimum VM specifications:

- vCPUs: 4
- RAM: 8GB
- Storage: 40GB
- OS: Windows Server 2012 R2 or Windows Server 2016

Configuration

- All Windows Security Updates have been applied
- Antivirus exclusions have been applied based on based on Citrix leading practices
- Machines are joined to the domain
- Date and time settings are correct
- Windows is licensed and activated

Optional

- VMWare: Add the self-signed certificate to the Citrix Cloud Connector
- Hyper-V: Console must be installed on the Citrix Cloud Connectors if MCS based provisioning will be used
- Secure XML: Named or wildcard certificates

The virtualization layer

Key considerations

○ Resources in multiple zones

If you're currently deploying resources at a single on-premises site, you may need to consider deploying them in multiple zones as your environment grows. This could be used to enable disaster recovery, keep resources closer to end-user locations, or both.

○ Hypervisors and public cloud environments

The Citrix Virtual Apps and Desktops service supports most common hypervisors, including vSphere, Hyper-V, and XenServer; it also supports public cloud environments including Microsoft Azure, AWS, and Google Cloud Platform.

If you use these environments, you'll be able to take advantage of automated machine provisioning with Machine Creation Services and Power Management; whereas in other environments, you will need to create machines manually.

Technical prerequisites

General

- Hypervisor credentials are available
- DHCP server with sufficient scope for provisioned Citrix Virtual Apps servers and Citrix Virtual Desktops machines
- Hypervisor access URL or IP
- DNS Server exists and is functional
- Network infrastructure and configuration is in place

Azure

Full Scope Service Principal

- Subscription ID needs to be available
- Subscription admin credentials are required

Narrow Scope Service Principal

- Subscription ID needs to be available
- Active Directory ID needs to be available
- Application needs to be created in Azure and proper permissions need to be granted, based on based on Citrix recommendations
- Application ID needs to be available
- Application secret needs to be available

VMWare vCenter

Create a user account with proper permissions, based on based on Citrix documentation

Nutanix

Install additional vendor provided plugins in the Cloud Connectors for Nutanix to be available as a hosting connection option in Cloud Studio.

The resource layer

Key considerations

Applications, desktops, or both

The choice between deploying applications or desktops will determine not only the user experience, but also the amount of control you have over it.

Publishing apps will give you greater, more granular control, but often publishing full desktops is the more natural solution – especially if you're using thin clients. Depending on your use case, you may also want to take both approaches.

Operating systems and VDI models

Your choice of OS will influence the VDI models you can adopt. Deploying VDIs in Windows Server environments will allow you to support multiple concurrent users on the same machine, but keep in mind that you'll need additional Microsoft Remote Desktop Services licenses with this VDI model.

If you're deploying on a Windows Desktop OS, you can't create multi-user environments. Instead, you can choose between a pooled/random model, dedicated, non-persistent desktops, or personal, persistent desktops. An alternative option, which can be useful in some cases, is to deploy Windows Server in a Windows Desktop-like environment, called server VDI.

Profile Management and folder redirection

If you're deploying non-persistent desktops, Profile Management ensures that user data and settings persist across sessions, giving users the same experience regardless of which server or desktop in the pool they access.

Using folder redirection alongside Profile Management helps minimize profile footprints and increase access speeds for users.

Policies for environment and session management

There's a broad range of Citrix policies available to help you control user experience. You can configure these for your unique use cases or apply our set of recommended baseline policies that are use-case agnostic.

Integrating your Citrix policies with the Microsoft Group Policy Management Console will give you a single point of control for all your policies.

If you would prefer to keep your Citrix policies separate, you can configure them in Studio – but remember they'll still need to take their place in the GPMC precedence chain.

Provisioning methods for Citrix VDAs

As we saw earlier, if you're using a supported hypervisor and public cloud, you can use Machine Creation Services to automatically provision machines. If not, you'll need to manually provision every machine – a viable approach for small, server-based environments.

For additional scalability in very large environments that aren't on public clouds, consider using Citrix Provisioning, which uses streaming technology to deploy machines from a master image captured on a vDisk.

Master images for machine catalogs

While you'll want to keep the number of master images as low as possible to minimize the administrative burden, you'll likely need multiple master images to accommodate different use cases.

The resource layer

Technical prerequisites

VDAs

Connectivity

Required connection ports:

- ICA (Inbound)
  - TCP: 1494, 2598, 8008
  - UDP: 1494, 2598, 3224 – 3324, 16500 – 16509
- Cloud Connector Registration
  - TCP: 80
- RDS Licensing (XenApp)
  - TCP: 135, 139, 445, Dynamic Range
  - UDP: 137, 138
- Profiles
  - TCP: 445

Sizing

Citrix Virtual Apps minimum VM specifications:

- vCPUs: Numa or ½ Numa
- RAM: 320 MB - 1280 MB per user (depending on workload)
- Storage: Depending on workload
- OS: Windows Server 2012 R2 or Windows Server 2016

Citrix Virtual Desktops minimum VM specifications:

- vCPUs: 2 - 4 vCPUs (depending on workload)
- RAM: 2 GB - 8 GB (depending on workload)
- Storage: Depending on workload
- OS: Windows 8.1 or Windows 10

Configuration

- All Windows Security Updates have been applied
- Antivirus exclusions have been applied based on Citrix leading practices
- Machines are joined to the domain
- Date and time settings are correct
- Powerplan is set to High Performance
- Required applications are installed
- Citrix VDA software is available for install
- Windows is licensed and activated

Azure:

- Machine is in Stopped - Deallocated state
- RDS Licensing Server is available (XenApp)

Citrix Policies

Citrix Profile Management

- Server is available with sufficient capacity to store user profiles
- GPO central store exists to import admx templates
- Access to a machine with GPMC

Folder Redirection

Server is available with sufficient capacity to store redirected folders

The user layer

Key considerations

○ End-user devices and operating systems

It's vital to make sure that end-user devices are running operating systems supported by Citrix. If users have thin clients, check that their devices support Citrix Workspace Experience and Citrix Gateway Service in the access layer.

○ User groups

Your user groups will be determined by the use cases you identified in the Success Plan that you completed in the Citrix Cloud Success Center. You will need to understand what your user groups are going to be so you can relate those groups to master images, machine catalogs, and delivery groups.

○ Workload types

Understanding your workload types will help you correctly size your environments. This is especially important in Citrix Virtual Apps environments where calculating scalability and user density is crucial.

The access layer

Key considerations

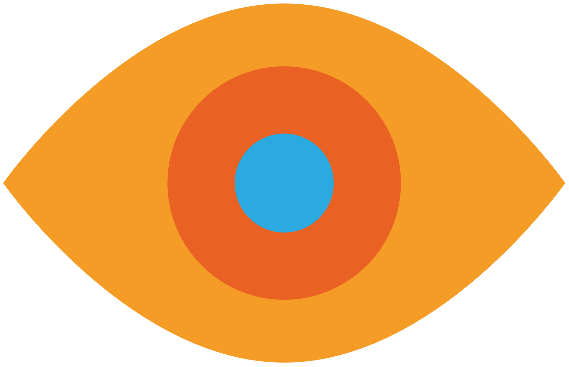
○ StoreFront and Citrix Gateway implementation options

When you're thinking about on-premises and Citrix-hosted options for StoreFront and Citrix Gateway, remember that hosted deployments don't support custom URLs, custom multi-factor authentication, or offline user access.

○ Internal and external access

In on-premises deployments, internal users have direct access to StoreFront, while external users must go through Citrix Gateway.

In Citrix-hosted deployments, all traffic is handled as if it was external – so all user access to Workspace Experience goes through Citrix Gateway.



The access layer

Technical prerequisites

StoreFront

Availability

2 x (for redundancy) domain joined physical or virtual Windows 2012 R2 or Windows 2016 servers

Connectivity

Required connection ports:

- App Enumeration
  - TCP: 80, 443
- User Connections
  - TCP: 80, 443 (Recommended)
- Citrix ADC Monitors (Inbound)
  - TCP: 80, 443, 8000

Sizing

Storefront minimum VM specifications:

- vCPUs: 4
- RAM: 4 GBs
- Storage: 60 GBS
- OS: Windows Server 2012 R2 or Windows Server 2016

Configuration

- All Windows Security Updates have been applied
- Antivirus exclusions have been applied based on Citrix leading practices
- Machines are joined to the domain
- Date and time settings are correct
- Powerplan is set to High performance
- Required applications are installed
- Citrix StoreFront software is available for install
- Windows is licensed and activated
- Base URL has been determined
- A Server Certificate is available for the Base URL (Needs to be installed on both StoreFront Servers and Citrix ADC LB vServer)

Load Balancing

- An internal static private IP is available to be assigned to the Load Balancer
- DNS A-Record has been created pointing the base URL FQDN to the LB VIP
- Citrix ADC admin credentials
- SSL Certificate for Load Balanced vServer
- CA Root and Intermediate Certificates to be linked with Load Balancing vServer
- A decision has been taken between SSL Offload or full end to end SSL
- Citrix ADC Load Balancing feature is enabled
- Citrix ADC SSL Offloading feature is enabled

Citrix Gateway

Availability

2 x Citrix ADCs (for redundancy) located in DMZ

Connectivity

Required connection ports:

- User Connections
  - TCP: 443
- STA (Cloud Connectors)
  - TCP: 80, 443
- LDAP (Domain Controllers)
  - TCP: 389/636
- ICA/HDX (VDAs)
  - TCP: 1494/2598
  - UDP: 1494/2598/3224-3324/16500-16509
- StoreFront
  - TCP: 80, 443, 8000

Configuration

- Citrix ADC admin credentials
- Citrix Gateway public URL has been determined
- Public IP Address is available for Citrix Gateway URL
- Public DNS A-record has been created pointing the Citrix Gateway URL to the Public IP Address
- NAT IP address is available in the DMZ (recommended)
- NSIP and SNIPs are properly configured
- SSL Certificate for Citrix Gateway vServer
- CA Root and Intermediate Certificates to be linked with Load Balancing vServer
- Authentication policies/servers configured in Citrix ADC
- Citrix Gateway Feature is Enabled

Your next step:
Build the solution

Now that you've considered all the layers of your architecture and have all the technical prerequisites in place, you're all set to start building your Citrix cloud solution.

Visit the Citrix Cloud Success Center for click-by-click guidance and expert tips.

For additional information, please see the
Virtual App and Desktops product documentation.