## Table of Contents

- **Introduction** ................................................. 3
- **Comparing Citrix XenApp to VMware Horizon** .................. 4
  - Remote Desktop Services .................................................. 5
  - License Server ............................................................... 5
  - Database ........................................................................ 6
  - Connection Brokering and Session Monitoring ......................... 6
  - Web Portal ...................................................................... 6
  - Clients and Protocol ............................................................ 6
- **Preparing for the Migration** ....................................... 7
  - Business Requirements ....................................................... 7
  - Published Applications ......................................................... 7
  - XenApp Infrastructure ......................................................... 7
  - End-User Requirements ......................................................... 8
- **Four Approaches to XenApp Migration** ......................... 9
  - Integration ...................................................................... 9
  - Migration ....................................................................... 9
  - Replacement ................................................................... 9
  - Combination ................................................................... 10
- **Integrating XenApp with Horizon Using VMware Identity Manager** ................................................... 11
  - Deploy VMware Identity Manager ........................................ 11
  - Implement the Identity Manager Integration Broker ............... 11
  - Configure Identity Manager to Connect to XenApp .................. 12
  - Decommission Citrix Web Interface or StoreFront .................. 16
- **Migrating or Replacing XenApp with VMware Horizon** ...... 17
  - Deploy VMware Horizon ...................................................... 17
  - Deploy VMware Identity Manager (Optional) ......................... 18
  - Prepare the Microsoft RDSH Servers .................................... 18
  - Create RDSH Server Farms and Application Pools and Entitle Users ................................................. 19
    - Add an RDSH Server Farm .................................................. 19
    - Create Application Pools to Publish Applications .................. 23
    - Manually Create Application Pools ....................................... 26
    - Publish Shared Desktops .................................................... 28
    - Decommission Citrix XenApp ............................................... 31
- **Additional Documentation** .......................................... 33
- **About the Author** ...................................................... 34
Introduction

VMware Horizon® support for published applications provides exciting new opportunities for customers running Citrix XenApp. Tightly integrated with Microsoft Remote Desktop Services (RDS), VMware Horizon is a new option for delivering not just published applications and shared desktops, but also virtual desktops, software as a service (SaaS), and virtualized applications to the devices your end users want to use.

This white paper provides guidance for planning and undertaking a migration from Citrix XenApp to VMware Horizon. Four approaches to XenApp migration are detailed, including the major steps required for their implementation. Whether the goal is to migrate an existing XenApp infrastructure to Horizon, replace it with a new system, or simply integrate legacy Citrix infrastructure with your Horizon virtual desktop deployment, VMware has the innovative products and technology you need.
Comparing Citrix XenApp to VMware Horizon

Before preparing for the migration, it is useful to understand how the major components of Citrix XenApp correlate to VMware Horizon. The two platforms are similar: They both provide users access to published applications and shared desktops installed on Microsoft Remote Desktop Session Host (RDSH) servers using an advanced display protocol and client application. The following figure compares the major Citrix XenApp 6.x and 7.x components with their VMware Horizon counterparts.

<table>
<thead>
<tr>
<th>Component</th>
<th>Citrix XenApp 6.x</th>
<th>Citrix XenApp 7.x</th>
<th>VMware Horizon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Desktop Services</td>
<td>Microsoft RDSH</td>
<td>Microsoft RDSH</td>
<td>Microsoft RDSH</td>
</tr>
<tr>
<td></td>
<td>with XenApp 6.x</td>
<td>with Virtual Delivery Agent</td>
<td>with Horizon Agent</td>
</tr>
<tr>
<td>License Server</td>
<td>License Server</td>
<td>License Server</td>
<td>None</td>
</tr>
<tr>
<td>Database</td>
<td>Required</td>
<td>Required</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>XenApp Data Store</td>
<td>Site Configuration Database</td>
<td></td>
</tr>
</tbody>
</table>

*Figure 1: Comparing Citrix XenApp and VMware Horizon Components*
## Remote Desktop Services

Both Citrix XenApp and VMware Horizon are enhancements to Microsoft Remote Desktop Services. Microsoft RDS is a multi-user mode of the Microsoft Windows Server operating system. It enables multiple users to share a single Windows server, including its installed applications.

### License Server

Citrix XenApp requires installation and maintenance of a license server. Historically the Citrix License Server has been the cause of numerous system issues and support calls. Recognizing the benefits of reducing the number of system components that need to be supported, VMware does not require use of a license server.
Database

Like the license server, VMware does not require customers to deploy and maintain a database server to support published applications and shared desktops. As an option, a database can be used to store system events, but these system messages can also be sent to syslog or stored in files to be parsed by other tools.

Unlike VMware, Citrix does require customers to deploy and maintain database servers. Database failure is another common cause of system issues and support calls.

Connection Brokering and Session Monitoring

In XenApp 6.5 and earlier versions, these critical system tasks are performed on the RDSH servers also tasked with delivering applications and shared desktops to users.

In contrast, VMware believes these critical functions should be performed at the management server level by the Horizon Connection Servers. This frees RDSH server resources to focus on their primary task of delivering applications and desktops to more users. It was not surprising when Citrix followed suit in XenApp 7.x, moving these critical tasks to the XenApp Delivery Controller servers.

Web Portal

Depending on the version(s) of XenApp in use, the Web portal may be provided by Citrix Web Interface, Citrix StoreFront, or in some cases both. These Web portals predominantly support just Citrix products. In comparison, the Web portal provided by VMware Identity Manager™ supports nearly every resource a user needs to access. This includes Horizon and XenDesktop virtual desktops, Horizon and XenApp published applications and shared desktops, SaaS applications like Salesforce, and applications virtualized by VMware ThinApp®.

Clients and Protocol

Both VMware Horizon and Citrix XenApp support the full spectrum of client devices including Android and Apple-based smartphones and tablets, Windows and Apple OS X-based personal computers, Google Chromebooks, specialized devices like thin clients and zero clients, and just about any Web browser that supports HTML5.

These clients communicate with the back-end system infrastructure using an advanced display protocol. Citrix markets their protocols under an umbrella name: HDX. This protocol family includes HDX Thinwire, HDX 3D Pro, ICA, and Framehawk. VMware also provides customers protocol choice and flexibility supporting PCoIP, Microsoft RDP, and the new VMware-developed Blast Extreme protocol.
Preparing for the Migration

Successful migrations require careful planning. It is essential to develop a comprehensive understanding of the business and technical requirements, the state of the XenApp infrastructure and its published applications, and the needs of the user community. This essential investigative work enables designing a solution that fits and selecting a migration approach that works.

The following examples illustrate the types of information to gather and questions to ask key stakeholders before undertaking a migration.

Business Requirements

It is important to have a solid understanding of the business objectives and other nontechnical requirements. Identify the business factors that could influence project requirements, system design, or the migration approach. For example:

• Is it a business priority to replace the Citrix infrastructure? Or is the organization considering integration of its Citrix infrastructure with VMware technologies?

• Is the goal to provide users a more versatile Web portal with access to XenApp published applications, Horizon virtual desktops, and other computing resources?

• Will the migration coincide with a major change to the business, such as the acquisition of another company or the launch of a new product or business initiative?

• Are there major changes to the number of office locations or users that need support?

Published Applications

Be sure to carefully inventory and assess the applications currently hosted by the XenApp infrastructure. Migrations can be a good opportunity to phase out applications that are no longer needed and to verify that user entitlements to applications are still correct. Questions to consider are:

• What are the application requirements and their performance characteristics?

• How many Remote Desktop Session Host servers currently host the applications?

• Who are the end users and which user communities are these applications for?

• Are all of the applications still in use or could any be decommissioned?

• Do any applications require significant changes, such as upgrades?

• Are you planning to replace an existing application with another?

XenApp Infrastructure

It is also critical to develop a thorough understanding of the XenApp infrastructure, identify the major Citrix components, and evaluate the health and specifications of the supporting systems.

• Which versions of Citrix XenApp and Microsoft RDS are in use?

• Are any servers running on Windows Server 2003 or earlier versions?

• Does the server operating system need to be upgraded as part of the project?

• Which XenApp features are in use and why?

• How many physical locations have XenApp infrastructure? How many XenApp farms are there?

• What sort of load balancing is in place?
• Is the XenApp infrastructure stable?
• Are there significant system stability or application issues?

End-User Requirements

Be sure to also carefully identify end-user requirements:
• Which devices do they use to access the system?
• Where do they need to access the system from? Will all access be from corporate LANs or WANs? Or is external access required?
• Which peripherals need to be supported?
• Which users should be migrated first?
• What will be the best approach to notifying and training end users about the new system?

These are examples of the questions to ask and information to gather. Taking care to properly understand project requirements and assess existing infrastructure enables you to identify the best approach to migration and design the Horizon infrastructure that meets your needs.
Four Approaches to XenApp Migration

After you have a solid understanding of the project requirements, consider whether the best approach is to integrate, migrate, replace, or a combined approach.

Integration

Integrating XenApp with Horizon replaces the Citrix Web Interface or Citrix StoreFront with the Web portal provided by Identity Manager. An integration broker synchronizes the list of available XenApp published applications, shared desktops, and associated user entitlements with Horizon through Identity Manager. This solution provides end users access to XenApp published applications, Horizon virtual desktops, SaaS applications, and VMware ThinApp virtualized applications through a user-friendly Web portal without making major changes to the Citrix infrastructure.

Follow this approach when the business priority is a unified Web portal or coexistence between XenApp and Horizon virtual desktops. Also consider this approach if you have legacy XenApp RDSH servers with critical applications running on old operating systems that cannot easily be migrated to new systems. XenApp RDSH servers running on versions of Windows Server prior to 2008 R2 cannot be migrated to the newest versions of XenApp or VMware Horizon and must either be integrated or replaced with newer systems.

Integration is also a good option if niche XenApp features are still required to support critical applications; and when existing RDSH servers are simply too unhealthy to risk migrating.

This approach provides a flexible way to handle the legacy infrastructure while providing users a single Web portal with easy access to the application and desktop resources they need. Integration with XenApp can also be combined with migration or replacement to handle complex XenApp infrastructures or multiphase migrations.

Because integrating XenApp with Horizon leaves much of the Citrix infrastructure in place, it is not the recommended approach if the immediate goal is to replace XenApp.

Migration

Migrating the Citrix XenApp RDSH servers and their installed applications to VMware Horizon enables publishing the existing applications and shared desktops without deploying new servers. You can deploy Identity Manager to replace the Citrix Web Interface or StoreFront, providing users a single Web portal with access to Horizon hosted applications, shared desktops and virtual desktops, SaaS applications, ThinApp virtualized applications, and XenApp published applications if any legacy Citrix infrastructure remains. Users access the migrated infrastructure using the Horizon Client and compatible devices, replacing Citrix Receiver.

Select this approach if the existing RDSH servers are stable and do not require major changes to the server operating system or installed applications. This approach allows you to phase out and decommission the entire Citrix XenApp infrastructure and can be considerably faster than deploying new RDSH servers. To prevent bad system or application issues from spreading to the Horizon infrastructure, be certain the RDSH servers and applications are stable before selecting this option.

Replacement

Consider replacement when the existing RDSH servers are unstable, require substantial application changes, are running on legacy operating systems (pre-2008 R2), or need to be migrated to a new server operating system (2012 R2). Replacing old systems with new Horizon RDSH servers with freshly installed applications is the cleanest option and the one least likely to transfer problems from the legacy Citrix infrastructure.

Users access the new infrastructure using the Horizon Client and compatible devices, replacing Citrix Receiver. You can also deploy Identity Manager to replace the Citrix Web Interface or StoreFront, providing users a Web portal with access to Horizon hosted applications, shared desktops and virtual desktops, SaaS applications, and ThinApp virtual applications.
If you can replace all RDSH servers with new systems configured for Horizon, you can phase out and decommission the entire Citrix XenApp infrastructure.

**Combination**

If some legacy XenApp infrastructure must remain to support old operating systems, applications, or niche XenApp features, while some infrastructure has clean configurations and up-to-date operating systems that could be migrated to Horizon, a combination of two or all three of these options is often the best approach. In a combination scenario, you can migrate stable XenApp RDSH servers with their installed applications to Horizon; replace unstable RDSH servers with new systems and clean application installs; and integrate Identity Manager with any Citrix infrastructure that must remain to support legacy applications, old operating systems, or niche XenApp features.
Integrating XenApp with Horizon Using VMware Identity Manager

Integrating XenApp with Identity Manager involves the following steps.

1. Deploy Identity Manager
2. Implement the Identity Manager Integration Broker.
3. Configure Identity Manager to communicate with XenApp using the Integration Broker.
4. Decommission the Citrix Web Interface or StoreFront.

The following figure shows the major Microsoft, Citrix, and VMware components required.

![components](image)

**Figure 3:** Components Required to Integrate Citrix XenApp with VMware Horizon

**Deploy VMware Identity Manager**

The first step in the integration process is to deploy Identity Manager. Identity Manager is a purpose-built virtual appliance. One of its capabilities is providing Web-based access to Horizon published applications and shared desktops, Horizon virtual desktops, SaaS applications, ThinApp virtualized applications, and Citrix published resources from a Web portal.

For guidance on how to deploy Identity Manager, see Additional Documentation at the end of this guide. After Identity Manager has been deployed, the next step is to implement the Integration Broker.

**Implement the Identity Manager Integration Broker**

The Identity Manager Integration Broker communicates with Citrix XenApp farms to synchronize and support single sign-on (SSO) to the published applications and shared desktops that each user is entitled to access. Identity Manager does not make changes to the XenApp infrastructure; it simply copies the information it requires from XenApp to display each user’s XenApp published resources in their Web portal. Installing VMware software on XenApp servers is not required.

Install the Integration Broker on a Windows 2008 R2, 2012, or 2012 R2 server running Microsoft Internet Information Server (IIS) 7 or 8 with the IIS 6 Management Tools and the .NET Framework v3.5. The Integration Broker supports XenApp versions 5.0, 6.0, 6.5, and 7.x. For more information, see Preparing and Installing Integration Broker in Setting Up Resources in VMware Identity Manager. (Note: Use the drop-down menu to select an on-premises version of Identity Manager.)
Citrix PowerShell Remoting, which enables communication with Identity Manager using the XenApp software development kit, must also be installed on each XenApp RDSH server that communicates with Identity Manager. Only one RDSH server needs to be configured per XenApp farm. For information on how to obtain and deploy Citrix PowerShell Remoting, see Enabling Citrix PowerShell Remoting on Citrix Server Farm in Setting Up Resources in VMware Identity Manager. (Note: Use the drop-down menu to select an on-premises version of Identity Manager.)

Configure Identity Manager to Connect to XenApp

After the Integration Broker has been deployed, configure Identity Manager to synchronize with the XenApp infrastructure.

1. Log in to Identity Manager as an administrator and select the Catalog tab.
2. Under Manage Desktop Applications, click Citrix Published Applications to begin the configuration.

Figure 4: Identity Manager Configuration
The following configuration menu will be displayed:

3. Check the **Enable Citrix-based Applications** check box and enter the appropriate settings to configure the Integration Broker. The settings are detailed in Table 1.

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Citrix-based Applications</td>
<td>Select to enable XenApp published applications and shared desktops.</td>
</tr>
<tr>
<td>Sync Integration Broker</td>
<td>Fully qualified domain name (FQDN) of the system running the Citrix Integration Broker used for synchronizing XenApp published applications, shared desktops, and user entitlements.</td>
</tr>
<tr>
<td>Server Port</td>
<td>TCP/IP port that the Integration Broker uses. Typically, 80 or 443 (for SSL).</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select if the Integration Broker uses SSL to secure the synchronization.</td>
</tr>
<tr>
<td>SSO Integration Broker</td>
<td>FQDN of the system running the Integration Broker that is responsible for single sign-on to the XenApp system. If the same Integration Broker provides both synchronization and XenApp SSO integration, click <strong>Use same as Sync Integration Broker</strong> to populate this field, Server Port, and Use SSL.</td>
</tr>
<tr>
<td>Server Port</td>
<td>TCP/IP port that the Integration Broker uses for SSO. Typically, 80 or 443 (for SSL).</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select if the Integration Broker uses SSL to secure the SSO integration.</td>
</tr>
</tbody>
</table>

Table 1: Integration Broker Configuration Settings
4. Next, specify the XenApp RDSH servers and their failover order for each server farm, as detailed in Table 2. Then click **Add Server Farm**.

*(Note: Multiple farms are supported.)*

![Figure 6: Configuring Identity Manager to Synchronize with XenApp]
### Table 2: Configure Identity Manager with XenApp Server Farms

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>XenApp version installed on the RDSH server. XenApp 5.0, 6.0, 6.5, and 7.x are supported.</td>
</tr>
<tr>
<td>Server name</td>
<td>FQDN of the XenApp RDSH server. Click Add to List to add it to the Servers list. Multiple servers can be added, one at a time.</td>
</tr>
<tr>
<td>Servers (failover order)</td>
<td>XenApp RDSH servers in the server farm listed in preferred failover order. If multiple RDSH servers are listed, use the Move up and Move down buttons to select the order. Click Delete to remove an RDSH server from the list.</td>
</tr>
<tr>
<td>Transport type</td>
<td>Specifies whether to use HTTP or HTTPS (SSL) to connect the RDSH servers.</td>
</tr>
<tr>
<td>Port</td>
<td>TCP/IP port that the RDSH servers use. Typically, 80 for HTTP and 443 for HTTPS.</td>
</tr>
<tr>
<td>Deployment Type</td>
<td>User-Activated or Automatic. Select Automatic to have icons for all applications appear in the user’s Web portal automatically. Select User-Activated if users should be permitted to control their workspace and choose which icons appear.</td>
</tr>
<tr>
<td>Sync categories from server farms</td>
<td>Select this option to synchronize categories in addition to XenApp published applications, shared desktops, and user entitlements.</td>
</tr>
<tr>
<td>Do not sync duplicate applications</td>
<td>Prevents synchronizing duplicate applications from multiple XenApp servers.</td>
</tr>
<tr>
<td>Choose Frequency</td>
<td>How often the system synchronizes with XenApp. The default is every hour.</td>
</tr>
<tr>
<td>Choose the time</td>
<td>Specify the time for synchronization.</td>
</tr>
</tbody>
</table>

5. Click **Save** to save the settings.
6. Click **Sync Now** to synchronize Identity Manager with XenApp. To display synchronization alerts, click **Check Alerts**.

When the synchronization has successfully completed, each user’s XenApp published applications and shared desktops will be available for them to access from the Identity Manager Web portal.

![Identity Manager Web Portal with XenApp Published Resources](image)

**Figure 7:** Identity Manager Web Portal with XenApp Published Resources

7. When a user clicks an icon in their Web portal, the Citrix Receiver client application will launch and connect to the desired XenApp published application or shared desktop using the HDX display protocol.

**Decommission Citrix Web Interface or StoreFront**

After Identity Manager has been successfully integrated with the Citrix XenApp infrastructure, you can notify users to begin accessing their XenApp published applications and shared desktops from Identity Manager. You can also deliver Horizon virtual desktops, SaaS applications, and ThinApp packages from the same Web portal.

Citrix Web Interface or StoreFront may be decommissioned once all users have switched to Identity Manager. Do not decommission any other Citrix components, including the License Server and Citrix Receiver. They are required to support the XenApp published applications and shared desktops that are still hosted by the Citrix infrastructure when integrated with Identity Manager.

If you are building a combination system with some XenApp resources integrated with Identity Manager and others migrated to Horizon, continue to **Migrating or Replacing XenApp with VMware Horizon**.
Migrating or Replacing XenApp with VMware Horizon

If decommissioning the Citrix infrastructure is your goal, you can migrate the XenApp infrastructure to Horizon or replace it. Migrating entails moving stable and up-to-date XenApp RDSH servers with their installed applications to Horizon. Replacing requires deploying new Horizon RDSH servers with clean application installs.

Replacing XenApp with Horizon is typically the option to choose when the existing XenApp RDSH servers are unstable or outdated, when the applications installed on the XenApp RDSH servers require significant changes, or when a project goal is to implement a newer version of Windows Server.

As an option, Identity Manager can be deployed when migrating or replacing XenApp to provide a Web portal with access to Horizon hosted applications, shared desktops, virtual desktops, SaaS apps, and ThinApp virtualized applications.

Migrating or replacing XenApp with Horizon entails the following steps:

1. Deploy VMware Horizon 7.01 (or upgrade if running earlier version).
2. (Optional) Deploy Identity Manager.
3. Prepare Microsoft RDSH servers.
4. Create RDSH server farms and application pools; then entitle users.

The following figure shows the major Microsoft and VMware components required. No Citrix components are necessary when migrating or replacing the XenApp infrastructure since the goal is to decommission the Citrix infrastructure.

![Figure 8: Components Required for Migrating or Replacing XenApp](image)

**Deploy VMware Horizon**

Published applications and shared desktops are core capabilities of VMware Horizon. Before migrating Citrix XenApp, the Horizon system must be deployed. The main system component, Horizon Connection Servers, handle connection brokering, application publishing, and virtual desktop deployment. Connection Servers also provide the Web-based administration console that administrators use to manage the system. Another component, VMware Access Point, enables secure access to published applications and shared desktops from untrusted networks like the Internet and does not require a VPN. Users connect to their applications and desktops with the Horizon Client and compatible devices including Chromebooks, Android and Apple tablets and smartphones, thin clients, zero clients, and HTML5 Web browsers.
At least one Connection Server is required, although at least two are commonly deployed with load balancing to provide system scalability and redundancy. The same Horizon design and deployment best practices developed for virtual desktop infrastructure apply to published applications and shared desktops. For detailed guidance on Horizon infrastructure design and deployment, see Additional Documentation.

**Deploy VMware Identity Manager (Optional)**

As an option, Identity Manager can be deployed. Identity Manager is a purpose-built virtual appliance providing Web-based access to Horizon published applications and shared desktops, Horizon virtual desktops, SaaS applications, ThinApp virtualized applications, and XenApp published resources.

For guidance on how to deploy Identity Manager, see Additional Documentation. Follow the steps necessary to configure the Connection Server for virtual desktops. The same configuration is required to provide access to Horizon published applications and shared desktops.

After Identity Manager has been configured it will synchronize the published applications, shared desktops, and virtual desktops and make them available to each entitled user within the Web portal.

**Prepare the Microsoft RDSH Servers**

After the Horizon infrastructure and optional Identity Manager have been deployed, the Microsoft RDSH servers can be prepared. If existing XenApp RDSH servers are to be migrated, preparing a host for Horizon simply requires installing the Horizon Agent. However, if XenApp servers need to be replaced, be sure to deploy a sufficient number of new RDSH servers with fully installed and configured applications in addition to the Horizon Agent.

The Horizon Agent supports RDSH servers running Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. If the XenApp RDSH servers to be migrated are running earlier versions of Windows Server, you must first upgrade the operating system. However, it is better to replace these old systems with new RDSH servers with clean application installs whenever possible. Upgrading legacy infrastructure tends to preserve legacy problems.

1. Back up or snapshot any systems that will be migrated before installing the Horizon Agent.
2. During installation you will be prompted to specify a Connection Server and provide an account with administrative rights to the Horizon system to register the new RDSH server.

![Horizon Agent Installation](image)

Figure 9: Installing the Horizon Agent

3. Once the Connection Server and administrator credentials have been entered, click Next and wait for the installation to finish.

To complete the installation, each RDSH server must be rebooted. Be sure to schedule appropriate downtime to avoid interrupting active XenApp or native Remote Desktop Service users. The Horizon Agent can also be silently installed to support automated deployment during IT service windows.

After the Horizon Agent has been installed on each RDSH server, Horizon can be configured to provide users published applications and shared desktops.

### Create RDSH Server Farms and Application Pools and Entitle Users

In both XenApp and Horizon, groups of RDSH servers are known as *farms*. You can use farms to group servers that provide the same applications, typically to the same user communities. Before applications can be published you must create at least one farm.

### Add an RDSH Server Farm

Creating a farm is simple. After the Horizon Agent has been installed on the RDSH servers, it can be accessed from the Horizon Administration console.

1. In the Horizon Administration console, go to View Configuration > Registered Machines and select the RDS Hosts tab.
2. Verify that each RDSH server is enabled and the status for all servers is Available.

![Registered RDS Hosts in Horizon Administration Console](image1)

3. Next, from the left pane of the Administration console select **Resources > Farms**, then click **Add** to create a farm.

4. Enter the information on the Identification and Settings page, as detailed in Table 3, then click **Next**.

![Adding an RDSH Server Farm in Horizon: Identification and Settings](image2)
<table>
<thead>
<tr>
<th><strong>OPTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Alphanumeric identifier for the farm. Do not include spaces or special characters.</td>
</tr>
<tr>
<td>Description</td>
<td>Add a description to help identify the farm. Spaces and special characters are allowed.</td>
</tr>
<tr>
<td>Access group</td>
<td>(Optional) Access groups help organize and restrict access to the Horizon Administrator console using roles. Specify one here if an access group will be used.</td>
</tr>
<tr>
<td>Default display protocol</td>
<td>Select the default display protocol. VMware Blast is recommended.</td>
</tr>
<tr>
<td>Allow users to choose protocol</td>
<td>Choose whether to allow users to choose between Blast, PCoIP, or RDP. Only Blast and PCoIP are supported for hosted applications.</td>
</tr>
<tr>
<td>Empty session timeout (applications only)</td>
<td>Amount of time after which an empty session is timed out. An empty session is an open connection to an RDSH in which the user has closed all applications. The default is 1 minute.</td>
</tr>
<tr>
<td>When timeout occurs</td>
<td>Choose how to handle an empty session that has timed out. Disconnect closes all open connections. Log off logs out the user. The default is Disconnect.</td>
</tr>
<tr>
<td>Log off disconnected sessions</td>
<td>Choose whether disconnected user sessions are logged out and when. By default, disconnected sessions are never logged out, enabling users to reconnect to applications they left running on the RDSH servers. If you select After, specify the number of minutes before the user is logged out. Immediate logs disconnected users out immediately.</td>
</tr>
<tr>
<td>Allow HTML Access to desktops and applications on this farm</td>
<td>Enables or disables HTML5-based access to this farm. This provides a way for users to access desktops and applications using just an HTML5-compliant Web-browser.</td>
</tr>
</tbody>
</table>

*Table 3: Adding an RDSH Server Farm: Identifications and Settings*
5. On the Select RDS Hosts page, select which hosts to add to the farm and then click **Next**.

![Figure 12: Adding an RDSH Server Farm in Horizon: Select RDS Hosts](image12)

6. Review the configuration, then click **Finish**.

![Figure 13: Adding an RDSH Server Farm in Horizon: Ready to Complete](image13)
After the farm has been created, verify it is listed on the Farms page under Resources in the Horizon Administration console.

![Figure 14: Newly Created RDSH Server Farm in Horizon Administration Console](image)

**Create Application Pools to Publish Applications**

After a farm has been created, create application pools to publish the XenApp applications that are to be migrated.

1. In the Horizon Administration console, go to **Catalog > Application Pools**, then click **Add**.

   The Add Application Pools window appears listing the applications installed on the RDSH servers in the farm.

2. Select the appropriate farm and the applications to migrate, then click **Next**.

![Figure 15: Select Applications to Publish Through Application Pools](image)
3. Review the application pools to be created and change their system-generated alphanumeric IDs and display names if necessary.

(Note: Application Pool IDs do not support special characters or spaces.)

<table>
<thead>
<tr>
<th>ID</th>
<th>Display Name</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calculator</td>
<td>Calculator</td>
<td>C:\ProgramData\Microsoft\Windows\Start Menu\Programs</td>
</tr>
<tr>
<td>Access_2013</td>
<td>Access 2013</td>
<td>C:\ProgramData\Microsoft\Windows\Start Menu\Programs</td>
</tr>
<tr>
<td>Excel_2013</td>
<td>Excel 2013</td>
<td>C:\ProgramData\Microsoft\Windows\Start Menu\Programs</td>
</tr>
<tr>
<td>OneNote_2013</td>
<td>OneNote 2013</td>
<td>C:\ProgramData\Microsoft\Windows\Start Menu\Programs</td>
</tr>
<tr>
<td>PowerPoint_2013</td>
<td>PowerPoint 2013</td>
<td>C:\ProgramData\Microsoft\Windows\Start Menu\Programs</td>
</tr>
<tr>
<td>Project_2013</td>
<td>Project 2013</td>
<td>C:\ProgramData\Microsoft\Windows\Start Menu\Programs</td>
</tr>
<tr>
<td>Publisher_2013</td>
<td>Publisher 2013</td>
<td>C:\ProgramData\Microsoft\Windows\Start Menu\Programs</td>
</tr>
<tr>
<td>Word_2013</td>
<td>Word 2013</td>
<td>C:\ProgramData\Microsoft\Windows\Start Menu\Programs</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>Internet Explorer</td>
<td>C:\Program Files\Internet Explorer\explore.exe</td>
</tr>
</tbody>
</table>

![Figure 16: Edit Application Pool IDs and Display Name](image)

4. Verify the **Entitle users after this wizard finishes** box is checked, then click **Finish** to create the application pools and publish the applications.
5. On the Add Entitlements page, add or remove the users and/or groups who should be granted access to these applications, then click **OK**.

![Figure 17: Entitle Users and Groups](image)

6. To view and manage the newly created application pools, navigate to **Catalog > Application Pools**.

![Figure 18: Application Pools in the Horizon Administration Console](image)
Users can now access their published applications via VMware Horizon.

![Horizon Client Displaying Newly Published Applications](image1)

Users can also access their published applications from the Web portal within Identity Manager if this optional component was deployed.

![Identity Manager Web Portal Displaying Newly Published Applications](image2)

**Manually Create Application Pools**

If any XenApp published applications to be migrated were not found when Horizon scanned the RDSH servers, or if any applications require special parameters when started, they can be published manually.

1. In the Horizon Administration console, go to **Catalog > Application Pools** and click **Add**.
2. In the Add Application Pools window, select the farm that contains the RDSH servers hosting the application.
3. To select the users who are entitled to access this application pool, select **Entitle users after this wizard finishes**.

4. Select **Add application pool manually**.

5. Then, specify the configuration for the application to be manually published, as detailed in Table 4, and click **Finish** when completed.

![Add Application Pools](image)

**Figure 21**: Manually Add an Application Pool

<table>
<thead>
<tr>
<th>OPTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Alphanumeric identifier for the farm. Do not include spaces or special characters.</td>
</tr>
<tr>
<td>Display name</td>
<td>Name of the application pool displayed in the Horizon Client, Identity Manager, and Horizon Administration console.</td>
</tr>
<tr>
<td>Version</td>
<td>(Optional) Version identifier for the application.</td>
</tr>
<tr>
<td>Publisher</td>
<td>(Optional) Publisher of the application can be specified if desired.</td>
</tr>
<tr>
<td>Path</td>
<td>(Optional) Complete path to the installed application on the RDSH, including Windows drive letter.</td>
</tr>
<tr>
<td>Start Folder</td>
<td>Specify which folder the application starts in, if required.</td>
</tr>
<tr>
<td>Parameters</td>
<td>(Optional) Launch time parameters for the application.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Description of the application pool. Spaces and special characters are allowed.</td>
</tr>
</tbody>
</table>

**Table 4**: Add Application Pools Specifications

Next, the Add Entitlements window appears.
6. Add or remove the users and groups who are entitled to access the application pool, then click OK.

![Figure 22: Entitle Users and Groups to Manual Application Pool](image)

**Publish Shared Desktops**

VMware Horizon can also publish shared desktops, enabling you to migrate XenApp users who require a full RDS desktop. In Horizon, published RDS desktops are referred to as RDS desktop pools.

1. In the Horizon Administration console, go to Catalog > Desktop Pools, then click Add.

   The Add Desktop Pools wizard will start.

2. Select RDS Desktop Pool, then click Next.

![Figure 23: Add an RDS Desktop Pool](image)
3. Under Desktop Pool Identification, specify the alphanumeric ID, display name, and optional description for the RDS desktop pool, then click **Next**.

![Figure 24: Desktop Pool Identification](image)

4. Configure the desktop pool settings, then click **Next**.

![Figure 25: Configure the Desktop Pool Settings](image)
5. Select an RDS farm for the new desktop pool, then click **Next**.

![Select an RDS Farm for the New Desktop Pool](image1)

6. On the Ready to Complete page, verify the RDS desktop pool settings, check the **Entitle users after this wizard finishes** check box, then click **Finish**.

![Add RDS Desktop Pool: Ready to Complete](image2)
7. On the Entitlements page, add the users and/or groups who are entitled to access the new desktop pool, then click **Close**.

![Entitlements table](image)

**Figure 28**: Entitle Users and Groups to Access the New Desktop Pool

The RDS desktop pool is now created and can be viewed and managed from the Horizon Administration console’s Desktop Pools page.

![Desktop Pools](image)

**Figure 29**: Horizon Administration Console Desktop Pools Page Showing Newly Created Pool

### Decommission Citrix XenApp

Once all of the XenApp published applications and shared desktops to be migrated have been published in Horizon, the appropriate users and groups entitled, the desktops and applications successfully passed any required QA or user acceptance testing, and users are happily using the new infrastructure, Citrix XenApp can be safely decommissioned. Because Horizon does not use the Citrix License Server, Web Interface, or StoreFront, you can dismantle these components immediately, taking care not to disrupt any applications and systems that might still use the same servers. If these components are VMware vSphere® virtual machines, you can re-task the vSphere capacity for new purposes. You can also uninstall the Citrix Receiver client software from all client machines.
If XenApp RDSH servers were migrated to the Horizon infrastructure, you can now uninstall their XenApp components. Be sure to back up each RDSH server before performing these changes. Since the RDSH servers are now part of an active Horizon farm it is best to uninstall XenApp when the systems are not in use, formally scheduling downtime as necessary.

When rebooting RDSH servers, be sure to temporarily disable them in Horizon so they do not accept new connections. (Note: This action does not disconnect any active connections.)

1. In the Horizon Administration console, go to View Configuration > Registered Machines and select the RDS Hosts tab.

2. Click an RDSH server with the secondary mouse-button (right-click) and select Disable from the menu that appears.

![Registered Machines and RDS Hosts](image_url)

Figure 30: Temporarily Disabling RDSH Servers

After the servers have been disabled and all active users have logged out, the XenApp components can be safely uninstalled. Once this has been completed the server can be rebooted then re-enabled to return it to service, Citrix free.
Additional Documentation

VMware Horizon 7 product page
VMware Horizon 7 Documentation
View Architecture Planning
Setting up Desktop and Application Pools in View
VMware Horizon View Large-Scale Reference Architecture
VMware Identity Manager product page
VMware Identity Manager Documentation and Release Notes
Providing Access to Citrix-Published Resources
Preparing and Installing Integration Broker
About the Author

Mark Ewert is the Lead Technologist on the VMware End-User Computing Marketing Team. Over his 25+ year career Mark has designed and implemented hundreds of successful solutions, including numerous Citrix XenApp and VMware Horizon infrastructures. Mark is also the author or coauthor of several other VMware technical resources, a frequent VMworld speaker, and developer of the View Controlled Recompose Script, a VMware Fling.