Azure e-book series

Microsoft Azure

Migration Guide:
Citrix Cloud with Azure Virtual Desktop

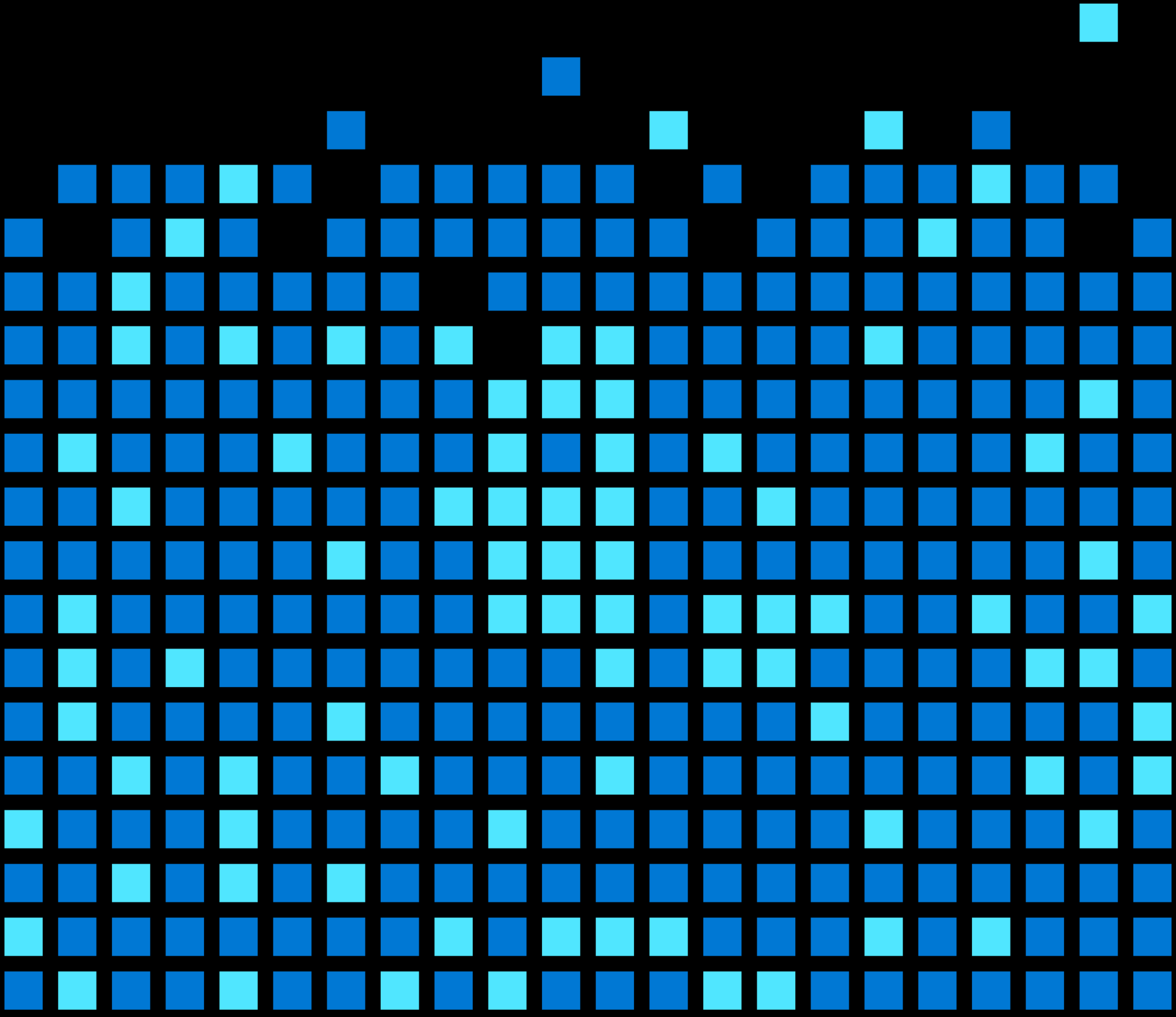


Table of contents

03 /
Introduction

03 Why consider cloud VDI on Azure?
03 Why migrate to the Citrix Virtual Apps and Desktops service with Azure Virtual Desktop?
05 Responsibilities and architecture

07 /
Preparing for your migration

07 Step 1: Prerequisites
07 Step 2: Azure Migrate step
08 Step 3: Discover VMs
09 Step 4: Review assessment

12 /
Preparing for a Citrix Virtual Apps and Desktops service environment with Azure Virtual Desktop

12 Azure Virtual Desktop prerequisites
14 Citrix Virtual Apps and Desktops service prerequisites
15 Methods of deployment for migration
16 Selecting an OS image

17 /
Creating the Citrix Virtual Apps and Desktops service environment

17 Deployment scope
18 Testing deployment

20 /
Post-deployment guidance

20 Considerations and planning
20 Optimizing Cost
21 Monitoring the Citrix Virtual Apps and Desktops service
23 Environment cleanup

24 /
Guidance on additional capabilities

24 Citrix App Layering
27 Microsoft Teams
28 Autoscale
30 Conditional Access
30 Profile Management
32 Monitoring and analytics

33 /
Conclusion and resources

Introduction

Today, many companies are considering new ways of working and assessing how to bring resilience to their organization, including the capabilities of providing a secure, remote desktop and app experience for employees to access from virtually anywhere.

Why consider cloud VDI on Azure?

Virtual desktop infrastructure (**VDI**) is often used by companies to deliver a remote desktop experience to internal and external employees, and is often delivered through **Remote Desktop Services** (**RDS**). However, as an on-premises solution, RDS does not realize the full value of the benefits and modernization that cloud desktop virtualization offers.

Azure Virtual Desktop is a flexible cloud VDI platform hosted on Microsoft Azure, giving you the full benefits of modernization, such as scalability and reduced infrastructure cost. In addition, you will receive the benefits of Azure, including integrated Microsoft security features and the unique Windows 10 Enterprise multi-session experience, which combines the Windows 10 experience with the ability to run multiple concurrent user sessions, which was only previously available on Windows Server operating systems.

Suppose you have an existing VDI solution hosted on RDS and managed through Citrix. In that case, you can quickly modernize by leveraging the Citrix Virtual Apps and Desktops service, a cloud software service from Citrix that enables the delivery and management of both on-premises and Microsoft Azure-based virtual desktops and applications by extending them to Azure Virtual Desktop, allowing you to keep your existing Citrix investment while modernizing your VDI.

Why migrate to the Citrix Virtual Apps and Desktops service with Azure Virtual Desktop?

There can be many reasons to migrate your VDI, and your company's needs determine the pace at which you do so. A typical scenario that would benefit from migration is when there is aging hardware that needs to be replaced. In this situation, rather than replacing the on-premises hardware, you can take full advantage of the economics of the Citrix Virtual Apps and Desktops service, including the built-in license, discounted consumption, and flexibility of deployment in terms of geographical region, shifting from a capital expenditure to an operating expenditure.

Besides the need to replace hardware, companies often migrate so they can realize the benefits of modernization, which helps enable secure remote work, simplify management, and reduce operating costs through an always-up-to-date software as a service model from Citrix, with the consumption-based infrastructure pricing and extensive global footprint of Azure. The Citrix Virtual Apps and Desktops service allows you to pair your Azure infrastructure capacity with the Citrix Cloud service without the need for third-party tools. It also provides additional capabilities such as power management, image management, adaptive protocol, Active Directory (AD) integration, and hybrid capabilities, which help enhance and further simplify management. Some additional benefits of migrating are detailed as follows.

Key benefits

By migrating your VDI, you can realize the benefits of modernization, including:

- Improved security posture through built-in and integrated security features with Azure Virtual Desktop
- Reduced hardware and infrastructure costs, lowering overall capital expenditure
- Simplified management that allows you to deploy and scale within minutes to meet your business needs
- A seamless experience optimized for Windows 10 and Microsoft 365 apps, including Microsoft Teams

Since Azure Virtual Desktop runs alongside the Citrix Virtual Apps and Desktops service, you'll also be able to take advantage of unified management across your entire hybrid environment.

Migration overview

When you migrate your VDI to the Citrix Virtual Apps and Desktops service and Azure Virtual Desktop, you need to consider the prerequisites to migrate your existing **virtual machines** (**VMs**) to Azure as well as those needed for the Citrix Virtual Apps and Desktops service, which extends to Azure Virtual Desktop. This enables you to connect the Azure instance to the Citrix control plane, deploy and manage virtual desktops and applications within Azure, and still embrace any existing on-premises resources.

The remainder of this guide is designed to walk you through the architecture and responsibilities for Azure Virtual Desktop with Citrix Virtual Apps and Desktops service, as well as the fundamentals you require to migrate to Citrix Cloud with Azure Virtual Desktop. We'll also walk you through the prerequisites, planning considerations, and steps to migrate successfully.

Responsibilities and architecture

In this section, we'll look at the responsibilities and architecture of both Azure Virtual Desktop and Citrix Virtual Apps and Desktops service.

Responsibilities

As you consider migration, it's important to understand the management responsibilities of each party. *Table 1* shows which areas of responsibility fall within the ownership scope of the customer/partner (**Yes**) or Citrix/Microsoft (**No**):

Responsibility	On-premises VDI	Citrix Virtual Apps and Desktops service with Azure
Identity	Yes	Yes
User devices (mobile and PCs)	Yes	Yes
Application security	Yes	Yes
Session host OS	Yes	Yes
Deployment configurations	Yes	Yes
Network controls	Yes	Yes
VDI control plane	Yes	No
Virtualization OS	Yes	No
Physical hosts	Yes	No
Physical network	Yes	No
Physical datacenter	Yes	No

Table 1: Distribution of management responsibilities

In short, when running the Citrix Virtual Apps and Desktops service, Citrix is responsible for all components within the cloud control plane, including updates, reducing management responsibilities, and allowing you to focus more on strategic imperatives. Learn more about the Citrix Virtual Apps and Desktops service here.

Architecture

Microsoft provides the underlining infrastructure, including compute, storage, and network, within Azure. Citrix Cloud adds a management layer (Citrix control plane) to Microsoft Azure. It is important to note that Citrix is responsible for core desktop virtualization management, including the broker, gateway, management, diagnostics, load balancing, and client. Like a native

Azure Virtual Desktop deployment, the customer is responsible for the desktop and remote apps, and management and policies.

The Citrix control plane enables the central management and orchestration of virtual desktops and apps in Microsoft Azure.

Figure 1 depicts the responsibilities for all three parties, the customer, Citrix, and Microsoft:

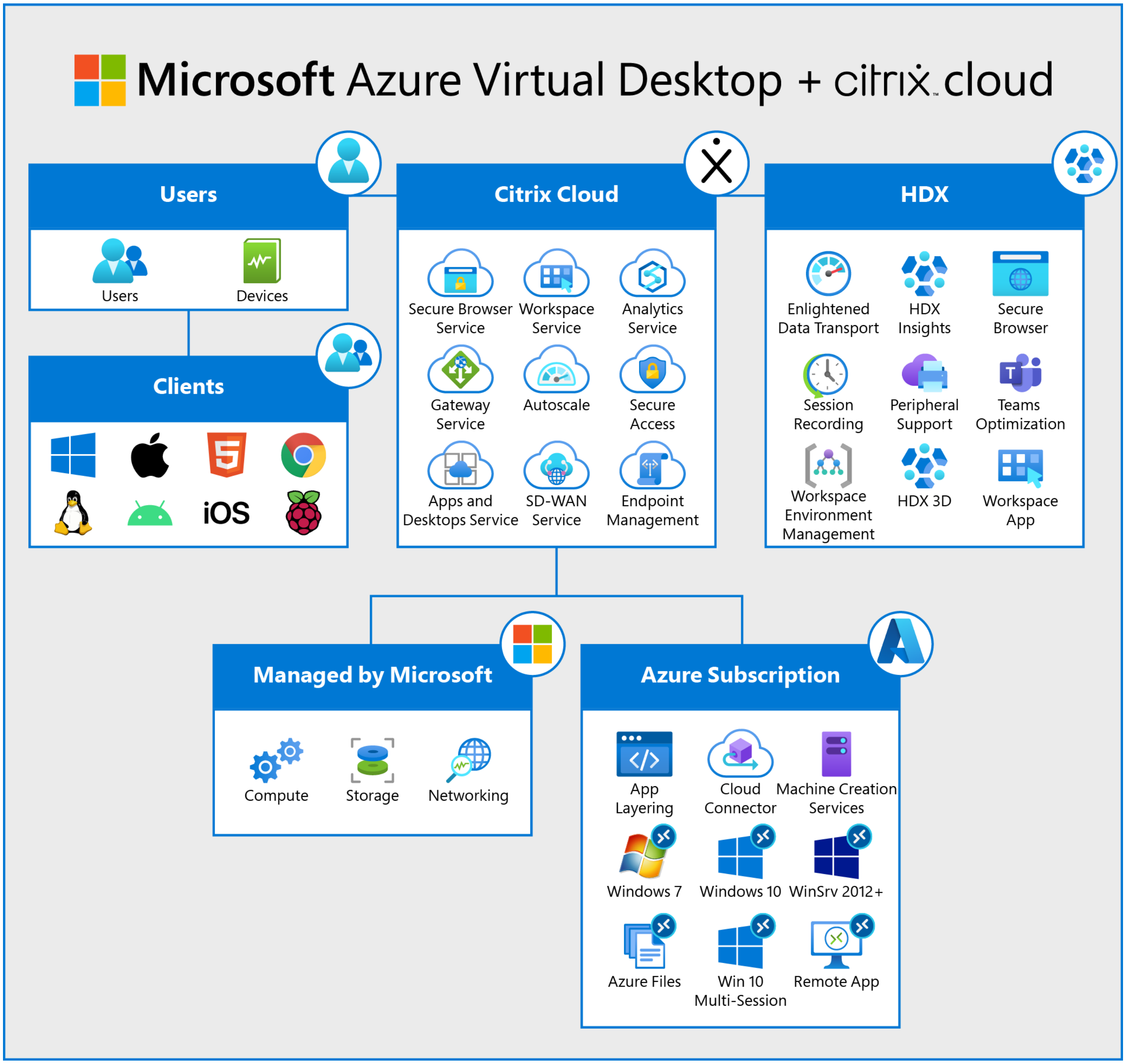


Figure 1: Responsibilities of the customer, Citrix, and Microsoft

Now that you understand the architecture, let's move on to the migration plan, where we look at the prerequisites and assess your environment requirements.

Preparing for your migration

This first part of your migration focuses on ensuring that you have the right prerequisites and covers the key steps to migrate existing on-premises resources such as VMs to Azure. Later, we'll cover the prerequisites for Citrix Virtual Apps and Desktops service.

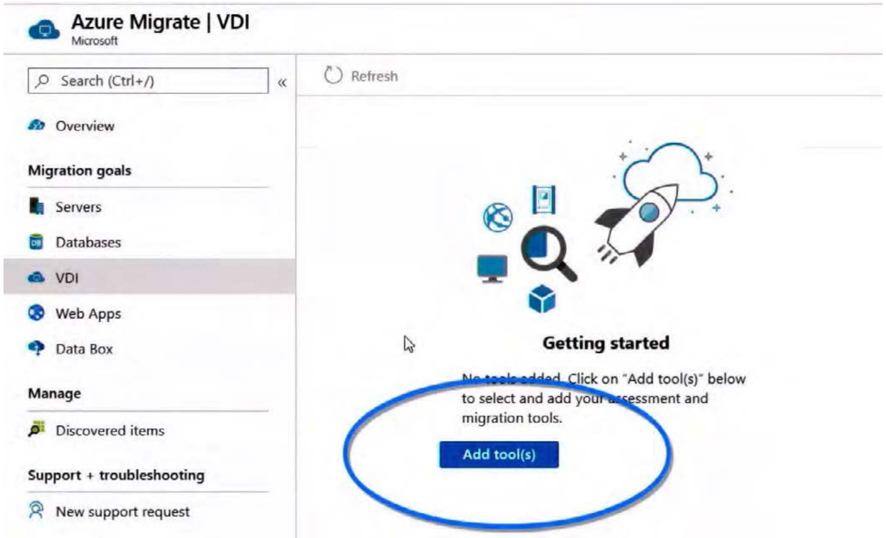
Step 1: Prerequisites

First, an Azure subscription is required. You also need to ensure you have the correct permissions to work with storage, networking components, and VMs. Ensure that domain services, either AD or Azure AD Domain Services, are pre-configured and available. Also, make sure that the domain service is accessible from the Azure subscription and virtual network available for the Citrix Virtual Apps and Desktops service. Follow the Azure AD Connect guide to synchronizing AD on-premises with Azure AD.

Note: *For the latest guidance on setting up Azure AD based on the newest product capabilities, please refer to Azure Virtual Desktop documentation here.*

Step 2: Azure Migrate step

There is a dedicated wizard within the Azure portal, allowing you to set up Azure Migrate for VDI. This can be found in the section called **VDI**, as shown in *Figure 2*:



No tools added. Click on "Add tool(s)" below to select and add your assessment and migration tools.

Figure 2: The Azure Migrate wizard

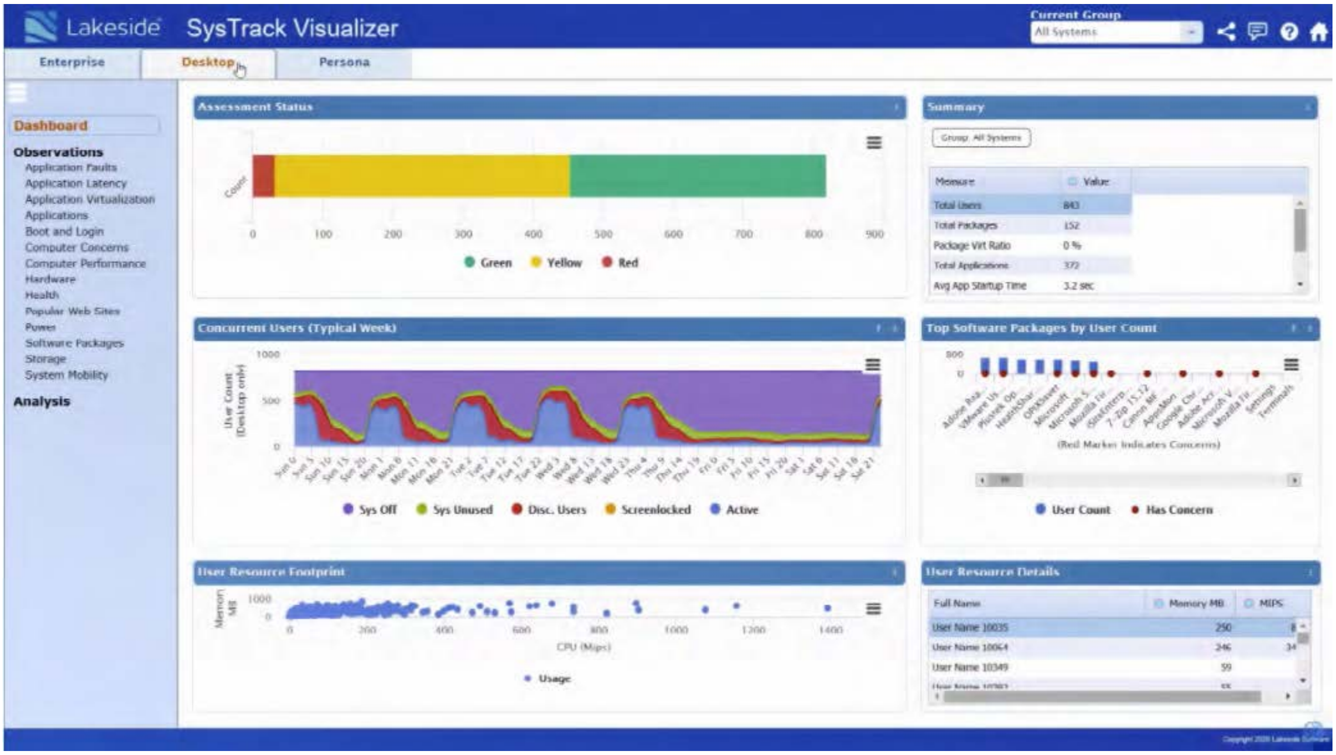
In this wizard, you set your subscription, resource group, project name, and geography. You start the assessment of the current VDI environment by selecting **Register**. During this step, you create a new Azure Migrate project in the destination Azure subscription. This subscription needs to match the prerequisites outlined in Step 1. You then select the option to assess and migrate servers, select **VDI**, and add a tool. After configuring basic parameters, such as the subscription, resource group, and location, make sure you choose **Azure Migrate: Server Migration** as the migration tool.

The setup wizard also allows you to select optional ecosystem partner tools that provide additional benefits on top of the server migration. As per the example, you can choose Lakeside SysTrack as your assessment tool on top of Azure Migrate as your migration tool. Lakeside is an ecosystem partner that specializes in assessing VDI environments. Lakeside SysTrack provides in-depth knowledge about your current workload to help you determine sizing and usage. Lakeside SysTrack does support Citrix environments to help you assess your environment for migration to Azure. After connecting Azure Migrate and optional ecosystem partner tools and accepting any requested permissions, the discovery process starts.

Note: *You can also use Citrix's Automated Configuration tool for the Citrix Virtual Apps and Desktops service to help migrate from on-premises to Citrix Cloud; read more here.*

Step 3: Discover VMs

During this phase, the virtual desktops of your current environment are discovered and assessed. During this step, we are going to gather a lot of information about your existing infrastructure. If you selected Lakeside SysTrack as your assessment tool in the previous step, this will help you collect even more information about your current VDI workload. Lakeside SysTrack requires an agent that you can easily install using your existing deployment tools. *Figure 3* shows the Lakeside SysTrack visualizer, which makes current usage, consumption, and application inventories easy to digest and helps you determine the sizing of your Citrix Cloud VMs and much more:



Measure	Value
Total Users	843
Total Packages	152
Package Virt Ratio	0 %
Total Applications	372
Avg App Startup Time	3.2 sec

Full Name	Memory MB	MIPS
User Name 10035	250	8
User Name 10064	246	34
User Name 10349	59	

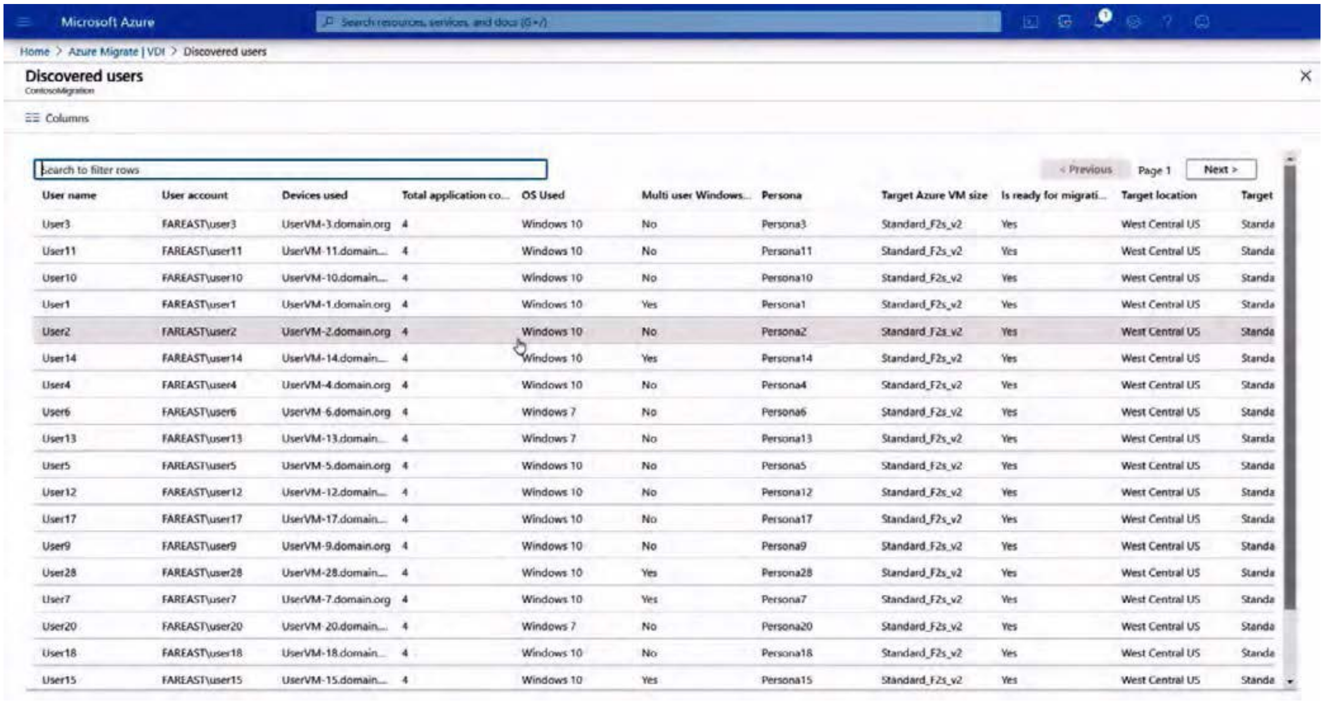
Figure 3: Lakeside SysTrack Visualizer

As part of this step, you also gather insights on any application back-end workloads you may or may not want to move to Azure. Typically, moving those application back ends to Azure ensures the best performance. In that scenario, the client side of the Citrix Virtual Apps and Desktops service application will be closer to the application back end. Azure Migrate can assist you with moving these workloads to Azure as well. If you decide not to move some of these back-end resources, ensure you configure connectivity with your on-premises environment using either ExpressRoute or a site-to-site VPN. Detailed steps about the discovery of Hyper-V VMs can be found here.

Step 4: Review assessment

Once an adequate amount of data is captured, you can review the assessment data to determine the best migration path for you. This assessment data includes the raw assessment data from the desktop and the data broken down into different user personas. As you analyze the data, you can determine the most cost-effective use of both pooled Virtual Desktop resources and personal Virtual Desktop resources. The information gathered as part of *Step 3* is visible in your Azure portal.

Figure 4 shows an example containing information that is collected:


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Azure Migrate | VDI > Discovered users
Columns
Search to filter rows
< Previous
Page 1
Next >

Discovered users
ContosoMigration

User name	User account	Devices used	Total application co...	OS Used	Multi user Windows...	Persona	Target Azure VM size	Is ready for migrati...	Target location	Target
User3	FAREAST\user3	UserVM-3.domain.org	4	Windows 10	No	Persona3	Standard_F2s_v2	Yes	West Central US	Standa
User11	FAREAST\user11	UserVM-11.domain....	4	Windows 10	No	Persona11	Standard_F2s_v2	Yes	West Central US	Standa
User10	FAREAST\user10	UserVM-10.domain....	4	Windows 10	No	Persona10	Standard_F2s_v2	Yes	West Central US	Standa
User1	FAREAST\user1	UserVM-1.domain.org	4	Windows 10	Yes	Persona1	Standard_F2s_v2	Yes	West Central US	Standa
User2	FAREAST\user2	UserVM-2.domain.org	4	Windows 10	No	Persona2	Standard_F2s_v2	Yes	West Central US	Standa
User14	FAREAST\user14	UserVM-14.domain....	4	Windows 10	Yes	Persona14	Standard_F2s_v2	Yes	West Central US	Standa
User4	FAREAST\user4	UserVM-4.domain.org	4	Windows 10	No	Persona4	Standard_F2s_v2	Yes	West Central US	Standa
User6	FAREAST\user6	UserVM-6.domain.org	4	Windows 7	No	Persona6	Standard_F2s_v2	Yes	West Central US	Standa
User13	FAREAST\user13	UserVM-13.domain....	4	Windows 7	No	Persona13	Standard_F2s_v2	Yes	West Central US	Standa
User5	FAREAST\user5	UserVM-5.domain.org	4	Windows 10	No	Persona5	Standard_F2s_v2	Yes	West Central US	Standa
User12	FAREAST\user12	UserVM-12.domain....	4	Windows 10	No	Persona12	Standard_F2s_v2	Yes	West Central US	Standa
User17	FAREAST\user17	UserVM-17.domain....	4	Windows 10	No	Persona17	Standard_F2s_v2	Yes	West Central US	Standa
User9	FAREAST\user9	UserVM-9.domain.org	4	Windows 10	No	Persona9	Standard_F2s_v2	Yes	West Central US	Standa
User28	FAREAST\user28	UserVM-28.domain....	4	Windows 10	Yes	Persona28	Standard_F2s_v2	Yes	West Central US	Standa
User7	FAREAST\user7	UserVM-7.domain.org	4	Windows 10	Yes	Persona7	Standard_F2s_v2	Yes	West Central US	Standa
User20	FAREAST\user20	UserVM-20.domain....	4	Windows 7	No	Persona20	Standard_F2s_v2	Yes	West Central US	Standa
User18	FAREAST\user18	UserVM-18.domain....	4	Windows 10	No	Persona18	Standard_F2s_v2	Yes	West Central US	Standa
User15	FAREAST\user15	UserVM-15.domain....	4	Windows 10	Yes	Persona15	Standard_F2s_v2	Yes	West Central US	Standa

Figure 4: Information from the assessment data

This includes information such as the following:

- The number of users in each persona
- Applications in use by users
- Resource consumption by a user
- Resource utilization averages by user persona
- VDI server performance data
- Concurrent user reports
- Top software packages in use

Detailed steps about the assessment can be found here.

Depending on the results you analyzed as part of the assessment and depending on whether you want to benefit from Windows 10 multi-session or keep on using Windows Server or Windows 10 Enterprise, you have two options.

Option 1: Create a new image template

The most common approach is to create a new template. One of the benefits of doing so is that it can deploy Windows 10 multi-session to make use of all the latest OS features and benefits.

Windows 10 Enterprise multi-session is available in the Azure Shared Image Gallery. To create a template image using the Citrix Virtual Apps and Desktops service, consult this guide.

For a full step-by-step guide on preparing, creating, and deploying custom template images for the Citrix Virtual Apps and Desktops service, consult this guide.

Remember, once uploaded to Azure, you need to import your custom template into Citrix Virtual Apps and Desktops service, and you need to ensure the Citrix **Virtual Delivery Agent** (**VDA**) software is installed.

Option 2: Migrate and transform

With the second option, you can migrate the existing VDI to Azure and transform it into a Citrix Virtual Apps and Desktops service session host server. This migration, or "lift-and-shift" approach, is suitable for scenarios such as moving on-premises resources in their current state. In that case, you will be using the **Discover** option in the **Azure Migrate: Server Migration** tools. This allows you to convert an appliance in its environment, which manages the machines' replication, to Microsoft Azure. The replication provider is downloaded, installed, and registered to the Azure Migrate project to replicate Azure. As the replication of the hosts into Azure Blob Storage is now started, you can continue to let the replication occur until it's ready to test the VMs and then migrate them into production.

As the machines start running in Azure, you will need to ensure that the Citrix VDA is installed on each VM you have migrated for use. Check this resource on installation guidance for Windows 10 Enterprise and Windows Server Citrix VDA.

Next, we look at the specific requirements for the Citrix Virtual Apps and Desktops service environment with Azure Virtual Desktop.

Preparing for a Citrix Virtual Apps and Desktops service environment with Azure Virtual Desktop

Previously, we covered the key steps to migrate existing on-premises resources such as VMs to Azure. Now, we'll look at the Azure Virtual Desktop requirements and the steps to prepare for your Citrix Virtual Apps and Desktops service deployment.

Azure Virtual Desktop prerequisites

In this section, we'll take a look at the specific Azure Virtual Desktop prerequisites, such as licensing requirements and naming conventions, that you need to consider before you start with the migration.

License requirements

Depending on the OS you select, appropriate licenses for users connecting to the desktops and applications are also required. Ensure all users who are allowed access to these resources within the Citrix Virtual Apps and Desktops service have the required license. *Table 2* shows the needed Microsoft licenses per OS. You can read more about the required licenses here.

Operating system	Required license
Windows Server 2012 R2, 2016, 2019	RDS Client Access License (CAL) with Software Assurance
Windows 7 Enterprise	Microsoft 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5
Windows 10 Enterprise multi-session or Windows 10 Enterprise	Microsoft 365 E3, E5, A3, A5, F3, Business Premium Windows E3, E5, A3, A5

Table 2: Required licenses for different operating systems

Furthermore, your core infrastructure needs the following to be able to support the Citrix Virtual Apps and Desktops service:

- An Azure AD instance
- A Windows Server AD instance that is in sync with Azure AD. You can choose to implement this based on Azure AD Connect (ideal for hybrid organizations) or based on Azure AD Domain Services (suitable for hybrid or cloud organizations). In terms of identifying sources and domain membership of the Citrix Virtual Apps and Desktops service session desktops/ host servers, you can select from the following options:
    - You can use Windows Server AD in sync with Azure AD, and the user accounts are sourced from Windows Server AD. The Virtual Desktop/session host VM is joined to the Windows Server AD domain.
    - You can use Windows Server AD in sync with Azure AD, and the user accounts are sourced from Windows Server AD. The Virtual Desktop/session host VM is joined to Azure AD Domain Services.
    - An Azure subscription is required, which needs to be parented to the same Azure AD tenant that contains the virtual network. The virtual network needs to have access to the Windows Server AD or Azure AD Domain Services instance.

The user connecting to the Citrix Virtual Apps and Desktops service must meet the following requirements:

- The user must be sourced from the same AD that is connected to Azure AD.
- The Virtual Desktop/session host VMs you create as part of your pod must be Standard domain-joined or Hybrid AD-joined. VMs cannot be Azure AD-joined.

For Citrix Cloud's Citrix Virtual Apps and Desktop service system requirements, check this documentation.

Naming conventions

With an Azure subscription, it is crucial to have a reliable naming convention. This also applies to Citrix Virtual Apps and Desktops service. The following list contains considerations regarding naming conventions:

- A useful naming convention assembles resource names using important resource information as part of a resource's name. When you construct your naming convention, identify the critical pieces of information you want to reflect in a resource name.
- Each workload can consist of many individual resources and services. Incorporating resource type prefixes into your resource names makes it easier to identify application or service components visually.
- When you apply metadata tags to your cloud resources, you can include information about those assets that couldn't be included in the resource name. If you do not have an existing naming convention for your subscription, please follow the guidance at this link to maintain a consistent naming convention across your resources.

Find out more about Citrix naming convention best practices here.

The next section summarizes some of the key requirements for Citrix Virtual Apps and Desktops service.

Citrix Virtual Apps and Desktops service prerequisites

This section summarizes the key requirements needed to deploy the Citrix Virtual Apps and Desktops service with Microsoft Azure. You need to ensure that you have taken care of the prerequisites detailed in *Step 1* of the Preparing for your migration section. You will need to have:

- An Azure subscription
- The correct permissions to work with storage, networking components, and VMs
- Domain services, either AD or Azure AD Domain Services, pre-configured and available
- Domain services accessible from the Azure subscription and virtual network available for the Citrix Virtual Apps and Desktops service

Before you get started with migrating, you should check out these resources on system requirements and proof of concept.

In the next section, we look at the deployment methods for your migration and which option may be best suited for your needs.

Methods of deployment for migration

There are two methods of deployment, **Quick Deploy** and **Full Configuration/Web Studio**. The Quick Deploy console provides the fast deployment of apps and desktops or remote PC access, which connects to corporate-managed devices such as PCs and laptops.

This deployment method offers basic configuration without the configuration of advanced features. The Full Configuration option provides a comprehensive deployment process, including advanced features.

Table 3 details the differences:

Feature	Quick Deploy	Full Configuration/Web Studio
Deploy using Azure	Yes	Yes
Deploy using other cloud services	No	Yes
Deploy using on-premises hypervisors	No	Yes
Citrix-managed images available	Yes	No
Deliver Windows apps and desktops	Yes	Yes
Deliver Linux apps and desktops	Yes	Yes
Remote PC Access	Yes	Yes
Simplified user experience	Yes	No

Table 3: Comparison between the deployment methods for migration

To find out more about the Quick Deploy feature, see the guide here.

The next section details the benefits of using Windows 10 multi-session as the OS of choice for migration.

Selecting an OS image

When choosing an operating system (OS) image, there are a couple of considerations. Suppose you have an on-premises session-based VDI deployment that you want to migrate to Azure. You may also be using the Windows Server version as your hosting OS. This is because Windows 10 multi-session is not supported outside of Microsoft Azure.

As part of your Citrix Virtual Apps and Desktops service migration, you have two options you can consider:

- You migrate your existing session host servers and virtual desktops to Azure to be managed by Citrix Cloud.
- You create new Windows 10 multi-session VMs using Citrix's **Machine Creation Services** (**MCS**) technology.

It's important to note that Windows Server 2012 R2 and any later version are supported in the Citrix Virtual Apps and Desktops service.

However, for multiple reasons, as outlined in the *Introduction*, using Windows 10 multi-session provides several additional benefits, including a cost-saving as the traditional RDS CALs are no longer required. To fully optimize Azure Virtual Desktop and the Azure cloud experience, we advise rebuilding your images to use Windows 10 multi-session.

This article provides guidance on preparing a master **virtual hard disk** (**VHD**) image to upload to Azure, including creating VMs and installing software on them. We suggest following this article to take advantage of the capabilities of Azure Virtual Desktop fully.

Read more on:

- Creating machine catalogs
- Windows 10 compatibility with Citrix virtual desktops

Next, we'll consider a high-level walkthrough of a basic deployment to get started with your migration, and use the services on the new Citrix Cloud with the Azure Virtual Desktop platform.

Creating the Citrix Virtual Apps and Desktops service environment

The following steps provide a high-level description of the process for deploying a Citrix Virtual Apps and Desktops service environment that will extend to Azure Virtual Desktop. Before you start a deployment, you need to make sure you have met all the requirements as set out in *Preparing for your migration* and *Preparing for a Citrix Virtual Apps and Desktops service environment with Azure Virtual Desktop*. This link details things you need to know before and during the use of the Citrix Virtual Apps and Desktops service.

Deployment scope

This section summarizes the steps to deploy the Citrix Virtual Apps and Desktops service. The service will automatically extend to Azure Virtual Desktop upon deployment.

The following steps will guide you in setting up and deploying the Citrix Virtual Apps and Desktops service:

Step 1: Create a Citrix Cloud account.

Step 2: Request a Citrix Virtual Apps and Desktops service trial.

Step 3: Create a resource location and install the Citrix Cloud Connector.

Step 4: Install Citrix VDA on the VMs.

Step 5: Create a machine catalog in the Citrix Virtual Apps and Desktops service.

Step 6: Create a delivery group.

Step 7: Launch a session from Citrix Workspace.

> **Tip:** *You can also follow the proof of concept guide, which guides you through the getting started phase of the Citrix Virtual Apps and Desktop service.*

Once the seven steps have been completed, you are ready to move on to the next section.

Figure 5 shows the Citrix workspace after proof of concept deployment:

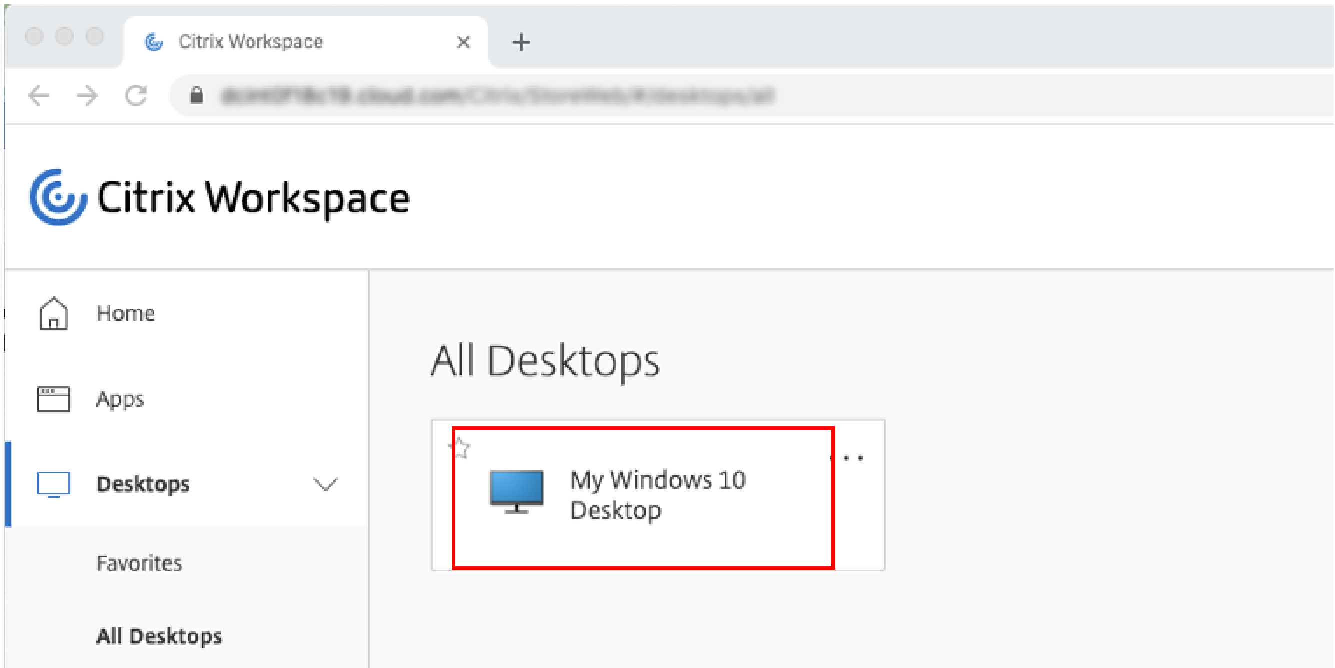


Figure 5: The Citrix workspace after proof of concept deployment

This concludes the deployment of Citrix Virtual Apps and Desktops service with Azure. Follow the guidance in the next section for best practices on testing.

Testing deployment

Once you have completed all the steps and the environment has been deployed, you need to confirm your Citrix Virtual Apps and Desktops service environment's health. Once you have tested and confirmed the health, you can then proceed with testing the deployment.

You can access Citrix Virtual Apps and Desktops service resources on Windows endpoints with the Citrix Workspace app. Besides the Windows platform, you can also use Android, iOS, macOS, Linux, Chrome, and web clients, among other operating systems. The following link contains a list of the various clients with guides on installing, configuring, and using the client Citrix Workspace app.

Important: *From the beginning of August 2018, Citrix Receiver was replaced with the Citrix Workspace app.*

Figure 6 shows an example of the Citrix Workspace app, which contains published desktops and applications:

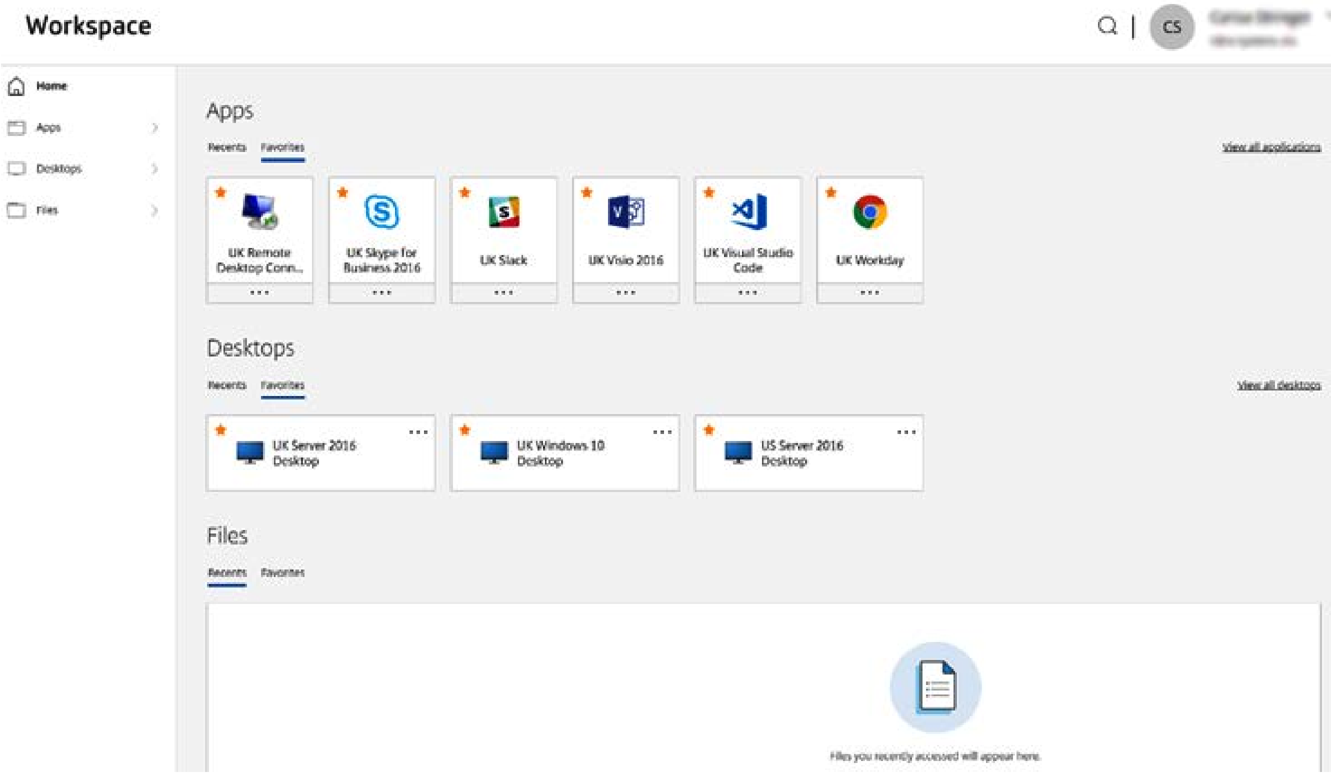


Figure 6: An example of the Citrix Workspace client

To find more information about the Citrix Workspace app, please see this link.

Post-deployment guidance

In this chapter, we'll look at some of the considerations for going live and post-deployment steps.

Considerations and planning

After taking your Citrix Virtual Apps and Desktops service into production, it is a good practice to consider and plan post-deployments steps. In the previous step, you confirmed your Citrix Virtual Apps and Desktops service deployment's health and usage, but it is advised to monitor that health on an ongoing basis. Consider implementing monitoring based on Azure Monitor, Log Analytics, and Monitor within your Citrix Virtual Apps and Desktops service. You can also use security as an important part of your Azure environment. You might have used multi-factor authentication (MFA) in your previous Virtual Desktop environment; read more here.

Now is a good time to consider adding Conditional Access to your deployment. We outline this task in the Conditional Access section later. As you start leveraging Citrix Virtual Apps and Desktops service, consider other scenarios that can benefit from this deployment. For example, you might allow your administrators remote access to your environment to perform maintenance tasks. You might currently be using a VPN solution for that.

Optimizing Cost

To make full use of Azure environments managed by Citrix Cloud, we advise you to consider the different ways to realize cost savings. The following list contains six ways to save costs on your Azure Virtual Desktop deployment:

- Use Windows 10 multi-session as the OS of your Azure Virtual Desktop session host servers. By using a multi-session desktop experience for users with identical compute requirements, you can let more users sign in to a single VM at once. This results in considerable Azure consumption cost savings for the VMs that are running. If you want additional guidance, the Windows 10 Enterprise multi-session FAQ contains more detailed information.
- Leverage Azure Hybrid Benefit. If your organization has Microsoft Software Assurance, you can use Azure Hybrid Benefit for Windows Server to save on your Azure infrastructure costs. For more information, visit this link.

- Azure VM Reserved Instances (RI) can significantly reduce costs by up to about 72% compared to pay-as-you-go prices, with a one-year or three-year commitment on Windows and Linux VMs. With Azure RI, you prepay for your VM usage. Optimally, combine Azure RI with Azure Hybrid Benefit (as outlined previously) to save up to 80% on list prices.
- You can reduce your total Citrix Cloud deployment cost by scaling your VMs by using Autoscale. This means shutting down and deallocating session host VMs during off-peak usage hours, then turning them back on and reallocating them during peak hours. Read more on Autoscale here.
- When setting up session host VMs, consider the different load balancing options. There are two key options available to you when it comes to Autoscale: schedule-based scaling, which allows you to set options for the Autoscale schedule for peak and off-peak times, and load-based scaling, focusing on scaling up or down based on server load. You can also consider dynamic machine provisioning, which helps reduce storage costs and more efficiently handle the load on your machines. Read more here.

Monitoring the Citrix Virtual Apps and Desktops service

Once you have migrated to Citrix Cloud, you can then investigate your environment's usage and health. The Monitor feature is built into the Citrix Virtual Apps and Desktop service, providing real-time data from the broker agent. It provides metrics on health, capacity, and historical data to assist the prevention of repeat incidents such as bottlenecks.

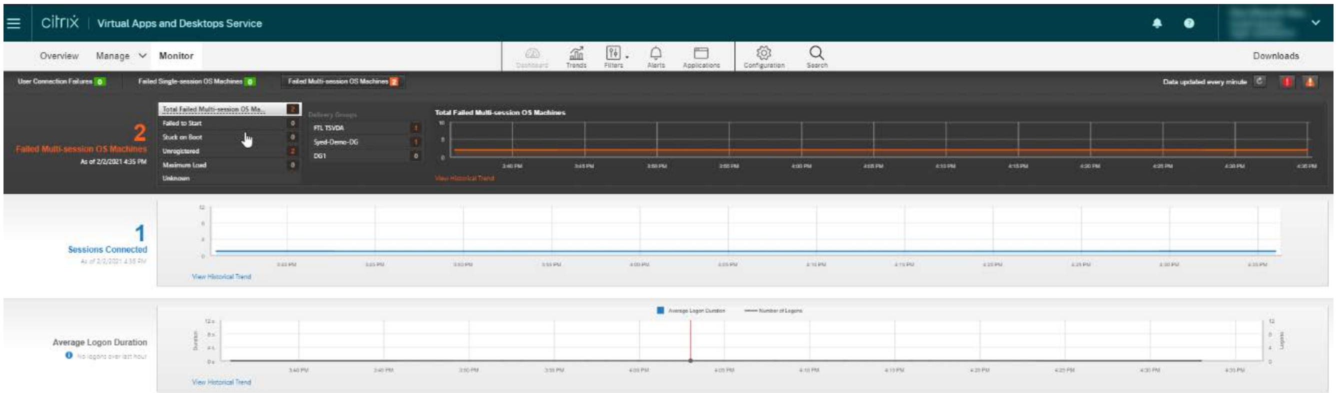
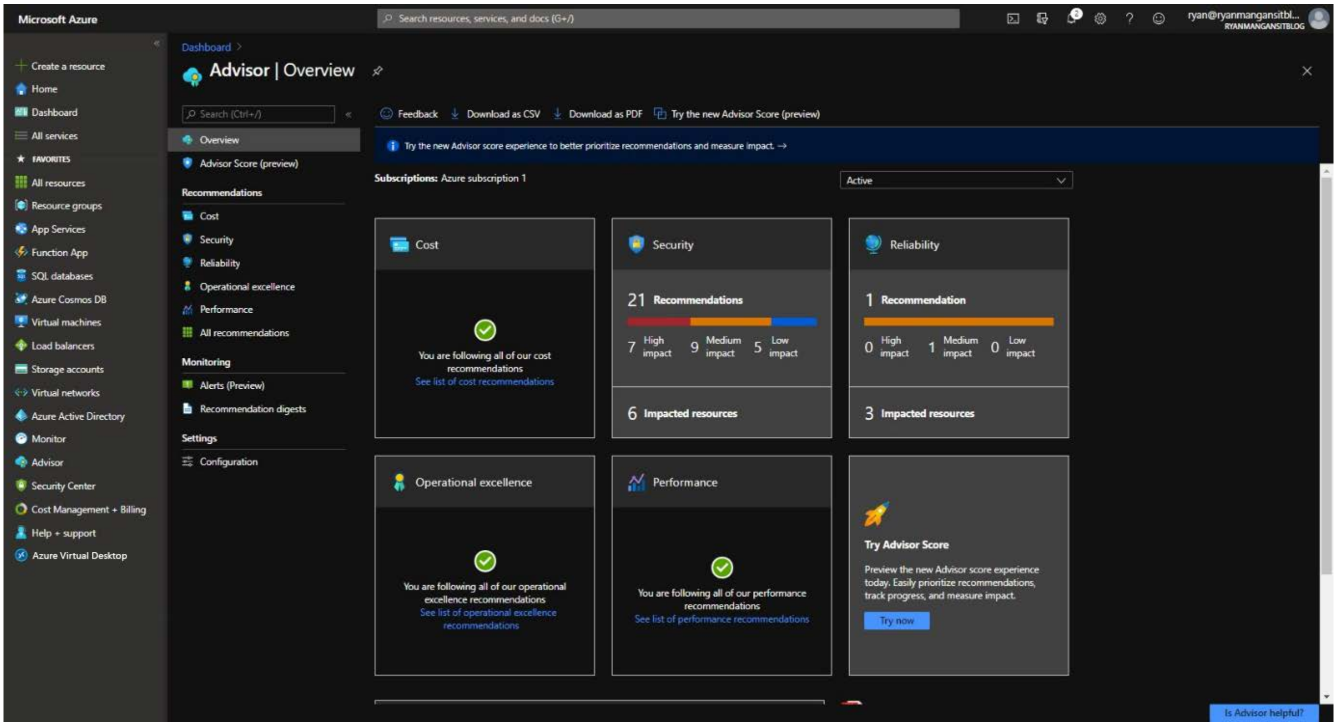


Figure 7: Citrix Virtual Apps and Desktops Service Monitor dashboard

You can read more on Monitor here.

You can also use Azure Advisor to provide you with information about your Virtual Desktop environment and guide you with the best practices you might have missed during your deployment. Closely investigate the recommendations that Azure Advisor contains and implement the suggested best practices shown there.

Figure 8 shows an example of Azure Advisor:



Try the new Advisor score experience to better prioritize recommendations and measure impact. →

Subscriptions: Azure subscription 1

Active

Cost: You are following all of our cost recommendations
See list of cost recommendations

Security: 21 Recommendations
7 High impact 9 Medium impact 5 Low impact
6 Impacted resources

Reliability: 1 Recommendation
0 High impact 1 Medium impact 0 Low impact
3 Impacted resources

Operational excellence: You are following all of our operational excellence recommendations
See list of operational excellence recommendations

Performance: You are following all of our performance recommendations
See list of performance recommendations

Try Advisor Score: Preview the new Advisor score experience today. Easily prioritize recommendations, track progress, and measure impact.

Figure 8: Azure Advisor

Environment cleanup

Once you have successfully migrated your VDI deployment to the Citrix Virtual Apps and Desktops service, it is also advised to clean up your VDI deployment. It's important to thoroughly investigate, plan, and execute this cleanup to ensure no components or configurations are left behind. There are a couple of areas where cleanup of the VDI environment is advised:

- The VMs of your VDI deployment can be removed. The VMs running your VDI infrastructure roles, such as connection brokers, web access, and gateways, are not needed anymore. The remote desktop session host VMs are migrated to Azure as part of the migration to the Citrix Virtual Apps and Desktops service and can also be removed. It might also be a good idea to snapshot/back up one of your session host servers in case you experience unexpected behavior with applications or settings inside the session host servers as part of the Citrix Virtual Apps and Desktops service at a later stage, and you want to compare settings with the previous VDI deployment.
- Your VDI deployment will have also used various DNS records and, most likely, these records were created in public and private DNS services. DNS type A records were used for the previous VDI deployment.
  These DNS records can now be safely removed as they are not needed anymore for the Citrix Virtual Apps and Desktops service.
- The infrastructure components of the VDI deployment, including the session host servers, are all members of your internal AD Domain Services. Since we have removed the infrastructure VMs, the corresponding AD computer objects, including their DNS entries, can now also be removed. Whether or not you can also remove the session host server computer object depends on how you migrated those workloads. If you migrated the VMs themselves, you are reusing those computer objects, and you should not remove them. If you migrated based on a new set of VMs in Azure, for example, as part of your move from Windows Server to Windows 10 multi-session, you are most likely also using new names and computer objects, which means you can remove the old objects.

Guidance on additional capabilities

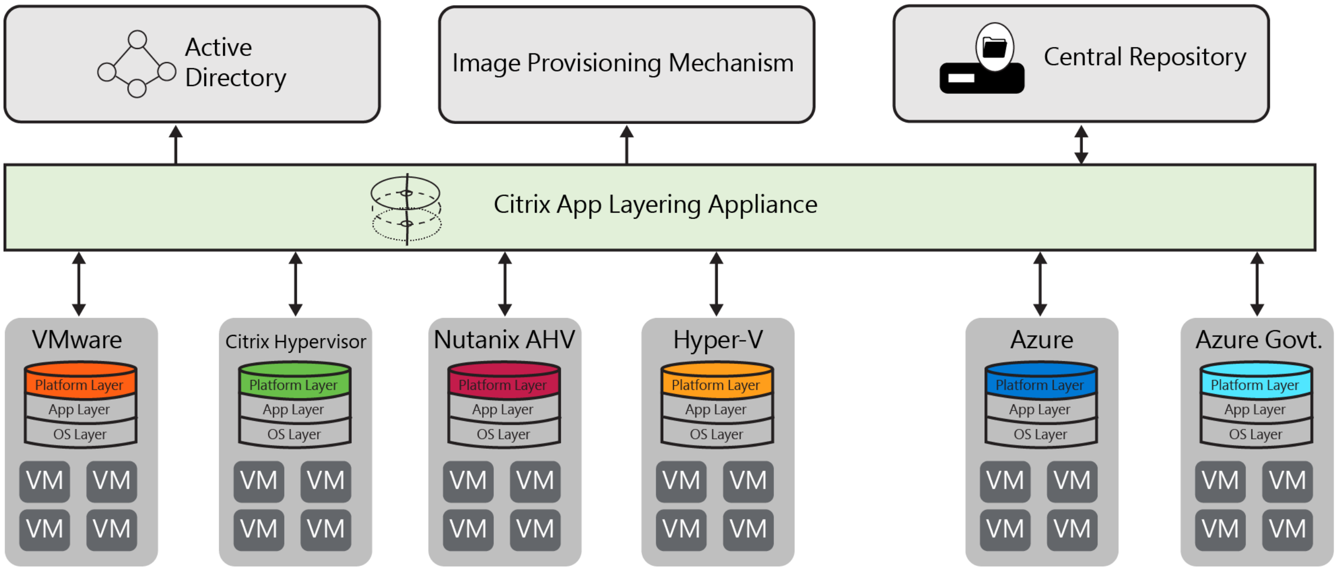
This chapter summarizes some of the additional capabilities you can implement during or after your migration.

Citrix App Layering

Citrix App Layering reduces the time it takes to manage Windows applications and images. On Microsoft Azure, the App Layering service lets you:

- Install the OS, platform tools, and apps in separate layers.
- Maintain a single OS layer for each major OS version. For an OS update, you can add a version to the layer. You can then select a specific version of the layer for each image template, as needed. The existing app and platform layers continue to run on each OS update.
- Create image templates for each unique combination of layers required by your users.
- Use templates to provision as many VMs as you need.
- Elastically assign specific app layers for on-demand delivery to users when they sign in.

Using layers and templates, you can significantly reduce the number of images you maintain. The App Layering solution works for both pooled desktops and session hosts:



Supports multiple hypervisors and cloud plaforms

Figure 9: Architectural representation of Citrix App Layering

Provision servers and desktops in any environment

App Layering allows you to package any Windows app as a virtual disk. You can deliver those apps to pooled desktops and session hosts. With App Layering, you can:

- Install the Windows OS on one layer and use it in as many images as you would like to generate. The same goes for your apps, and your hypervisor, and other platform software.
- Select any combination of layers to create layered images that are deployable as desktops or session hosts.
- Deploy those layered images to VM desktops and session hosts, making the applications available to users.

You can deliver an app update or an OS patch to an entire server farm or desktop silo with one image update.

Deliver applications based on need

You can deliver applications based on need, where:

- You include applications that everyone needs in your base images.
- You deliver individual app layers "on-demand" using the elastic layering feature.

Base image: The base image is one that you generate from a barebones image template. It includes only the software that you want *all* users to receive. You can deliver more specialized apps using *elastic layers*, which are "layers on demand."

Elastic layers, "layers on demand": With elastic layering enabled on an image, you can assign app layers not included in the base image to users on that machine. Users receive apps when they sign in. The more generic your base image, the fewer unique images there are to maintain.

User (personalization) data and settings

The *user (personalization) layer* is a writable layer that includes users':

- Locally saved data and profile changes
- Locally installed apps and plugins

Give users a persistent experience by enabling **User layers** on non-persistent, pooled desktop images. Users receive a layer for local data and settings. You can then size your infrastructure based on the maximum number of *concurrent* users.

A simple addition to your infrastructure

At the heart of Citrix App Layering deployment is the **Enterprise Layer Manager** (**ELM**) technology that runs on the App Layering appliance. The appliance hosts the App Layering management console.

The management console lets you:

- Create and manage layers.
- Create image templates and publish images.
- Assign layers to users as part of the base image or using the elastic layers feature.

You can layer virtually any app that is compatible with your OS. Each app layer can include one or more apps, preferably on the same upgrade schedule. To upgrade the apps, you:

- Install the updates on a new version of the app layer.
- Update the applicable image templates with the new layer version.
- Republish the images and reprovision your systems.

Platform layers isolate your hypervisor, provisioning, and connection broker software. Deliver the same OS and app layers with a unique platform layer for each platform.

Connector configurations

The appliance uses connector configurations to access specific locations in your virtual environment. App Layering uses the defined locations to:

- Import the OS for the OS layer.
- Package layers during layer creation.
- Publish layered images to a specific location.

Read more on Citrix App Layering here.

Microsoft Teams

Citrix supports media optimizations for the Citrix Virtual Apps and Desktops service for Microsoft Azure.

Making audio and video calls from within a virtual desktop has always been a difficult nut to crack. Citrix and Microsoft have worked closely to release optimization for desktop-based Microsoft Teams (1.2.00.31357 or higher) using the Citrix Virtual Apps and Desktops service and the Citrix Workspace app. This feature allows the endpoint (physical device) to do the voice and video processing as opposed to the virtual desktop. This improves performance and scalability while keeping sensitive data, such as logs, files, and SIP authentication, secure within Azure.

Figure 10 shows the Microsoft Teams optimization flow, detailing how audio and video are offloaded to the endpoint client:

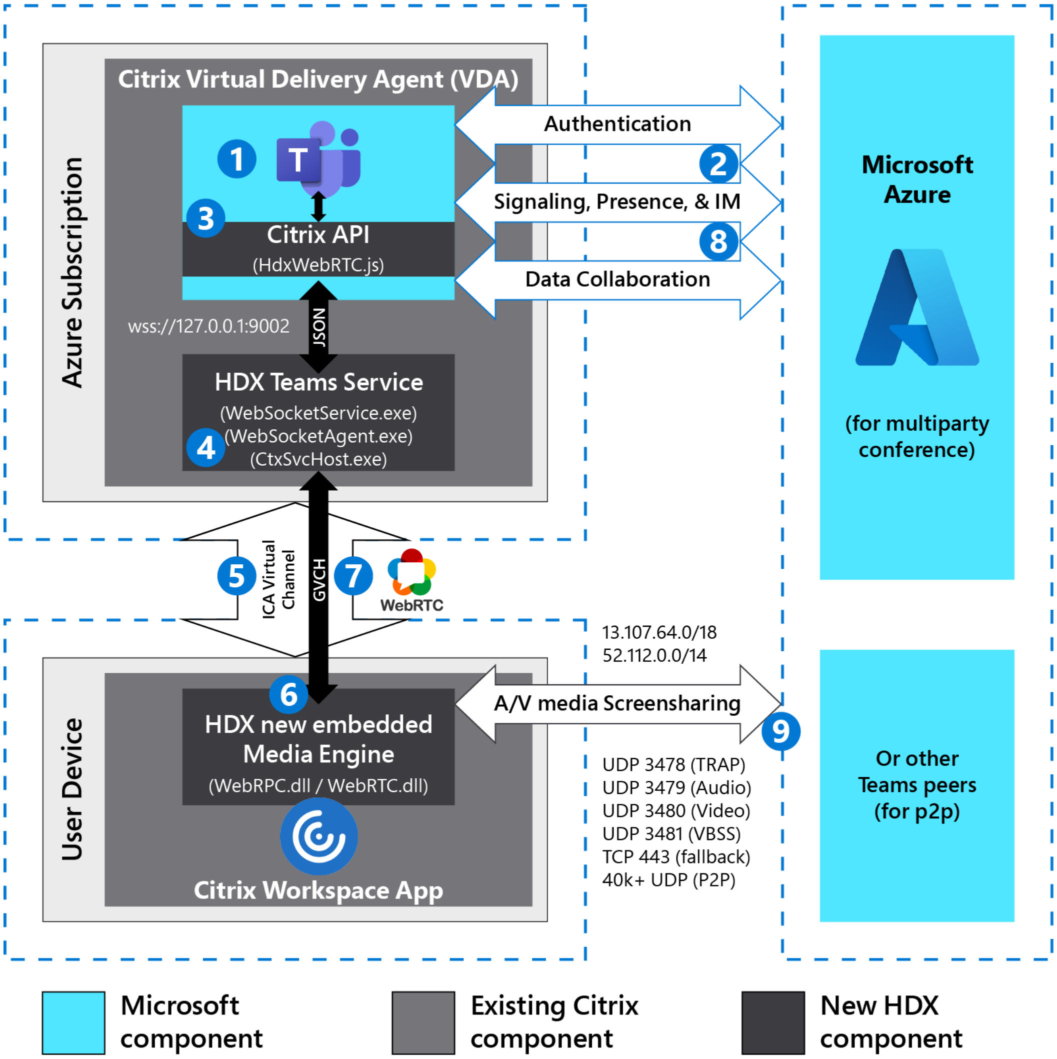


Figure 10: The Microsoft Teams optimization flow

This resolves the previous challenges of unoptimized Teams meetings, which require data packets to traverse from the endpoints back to the session hosts and then back to the other party in the conversation and vice versa. This phenomenon is called hair pinning. With media optimization, this reduces resource consumption as Microsoft Teams audio and video connections are offloaded to the endpoint. Read more about optimization for Microsoft Teams here.

Autoscale

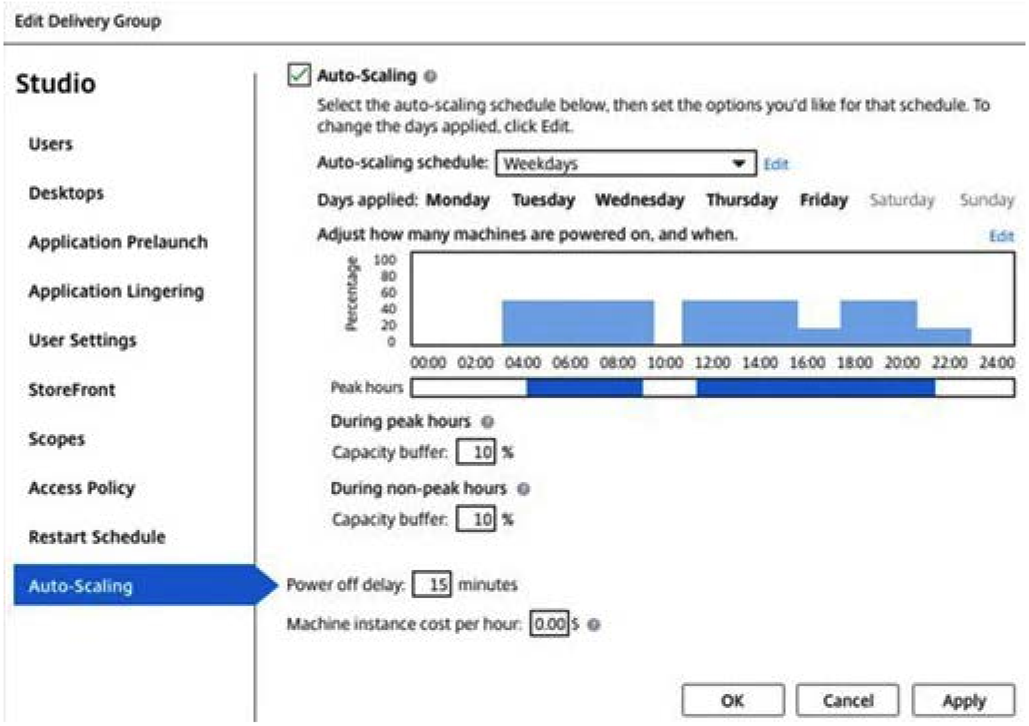
Autoscale is a feature exclusive to the Citrix Virtual Apps and Desktops service that provides a solution to proactively power manage your cloud VMs to control costs. It aims to balance cloud cost with resource availability and is fully configurable. It is directly integrated within the management console of Citrix Cloud.

Autoscale enables proactive power management of all registered single-session and multi-session OS machines in a delivery group. Autoscale works with both RDS and VDI. There are three user interfaces to be aware of:

- Autoscale user interface for RDS delivery groups
- Autoscale user interface for pooled VDI delivery groups
- Autoscale user interface for static VDI delivery groups

For more information about the user interfaces for different delivery groups, see Three types of Autoscale user interfaces.

Figure 11 shows the Autoscale user interface for static VDI delivery groups:



Edit Delivery Group

☑ Auto-Scaling

Select the auto-scaling schedule below, then set the options you'd like for that schedule. To change the days applied, click Edit.

Auto-scaling schedule: Weekdays

Days applied: Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Adjust how many machines are powered on, and when.

During peak hours

Capacity buffer: 10 %

During non-peak hours

Capacity buffer: 10 %

Power off delay: 15 minutes

Machine instance cost per hour: 0.00 $

Figure 11: The Autoscale user interface

Conditional Access

In most production environments, we advise configuring the Conditional Access policy to Citrix Virtual Apps and Desktops service. This allows you to define additional security requirements that a user's session needs to meet before accessing the published desktops and applications.

A typical Conditional Access example is Azure MFA. After configuring Azure MFA, when a user signs in, the client asks for their username and password, followed by an Azure MFA prompt. If they select Remember me, your users can sign in after restarting the client without needing to re-enter their credentials. These credentials are stored on the local credential manager. While remembering credentials is convenient, it can also make deployments for enterprise scenarios or personal devices less secure. To protect your users, you'll need to make sure the client always asks for Azure MFA credentials. More information on setting up and configuring Azure MFA for the Citrix Virtual Apps and Desktops service is provided here. For single sign-on and how to configure your IDP to work with cloud App security, read this documentation.

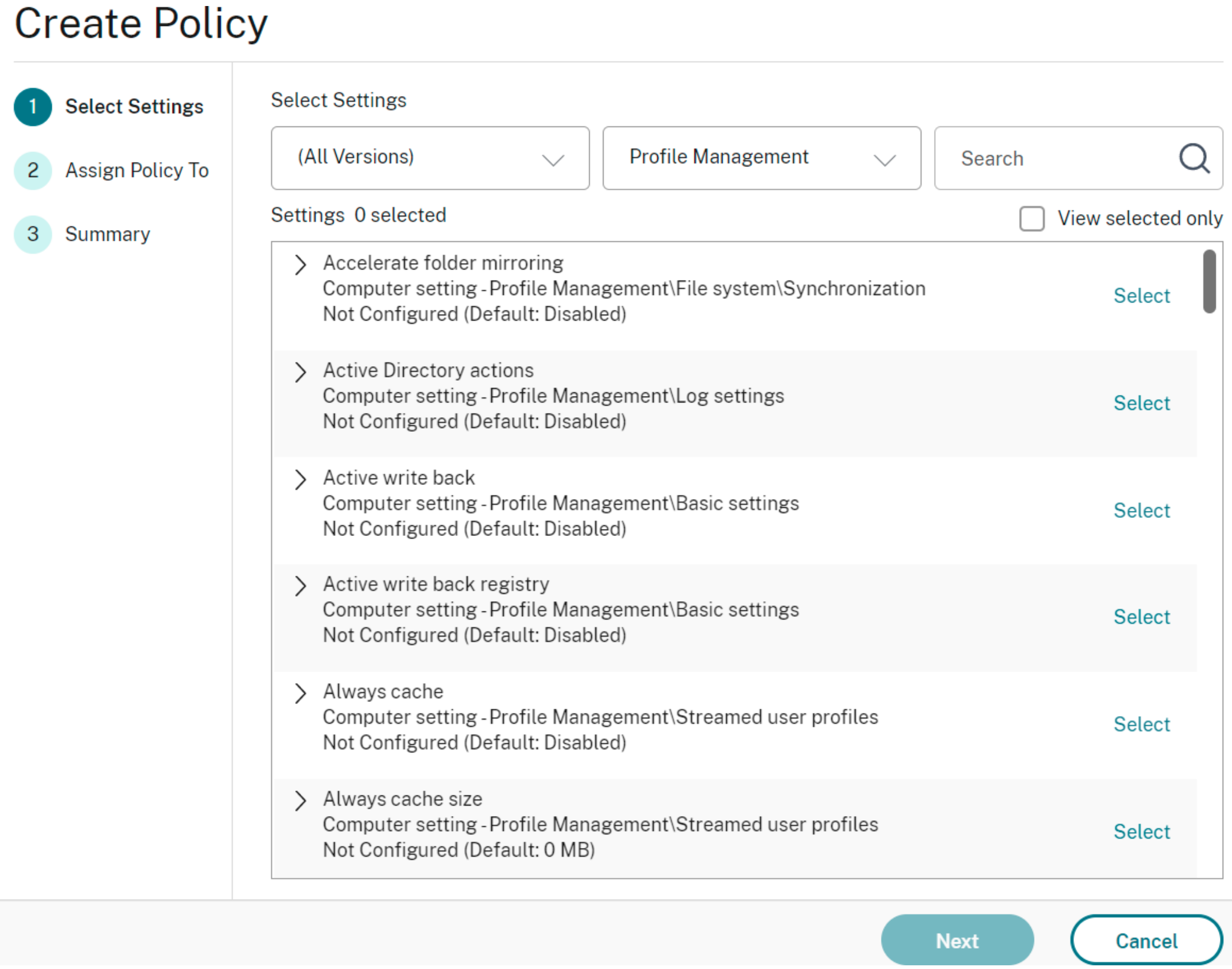
Profile Management

Profile Management addresses user profile deficiencies in environments where the same user's simultaneous domain sign-ins introduce complexities and consistency issues to the profile. For example, if a user starts sessions to two different virtual resources based on a roaming profile, the session's profile that terminates last overrides the profile of the first session. This problem, known as "last write wins," discards any personalization settings that the user makes in the first session.

Profile Management optimizes profiles efficiently and reliably. At interim stages and signing out, registry changes and the files and folders in the profile are saved to each user's user store. If, as is typical, a file exists, it is overwritten if it has an earlier timestamp.

When signing in, users' registry entries and files are copied from the user store. If a locally cached profile exists, the two sets are synchronized. As a result, all settings for all applications and silos are available during the session and it is no longer necessary to maintain a separate user profile for each silo. Citrix streamed user profiles can further enhance signing-in times.

You can configure the desired settings and apply the policies, with the **Select Settings** option:



Create Policy

1 Select Settings
2 Assign Policy To
3 Summary

Select Settings

(All Versions) | Profile Management | Search

Settings 0 selected   □ View selected only

Accelerate folder mirroring
Computer setting - Profile Management\File system\Synchronization
Not Configured (Default: Disabled)   Select

Active Directory actions
Computer setting - Profile Management\Log settings
Not Configured (Default: Disabled)   Select

Active write back
Computer setting - Profile Management\Basic settings
Not Configured (Default: Disabled)   Select

Active write back registry
Computer setting - Profile Management\Basic settings
Not Configured (Default: Disabled)   Select

Always cache
Computer setting - Profile Management\Streamed user profiles
Not Configured (Default: Disabled)   Select

Always cache size
Computer setting - Profile Management\Streamed user profiles
Not Configured (Default: 0 MB)   Select

Figure 12: Configuring the desired settings and applying the policy

Profile Management helps to safeguard application settings for mobile users who experience network disruption (if the offline profiles features are configured) and users who access resources from different operating systems (if the cross-platform settings feature is configured).

To find out more about Citrix Profile Management, click here.

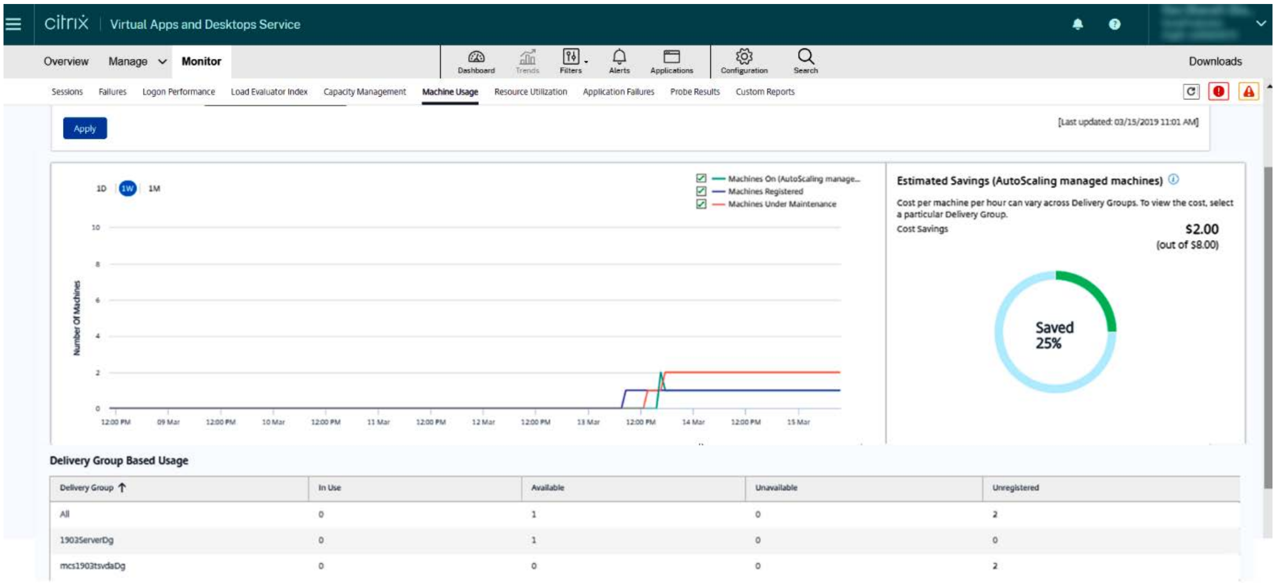
Note: The Workspace Environment Management service uses intelligent resource management and Profile Management technologies to deliver the best possible performance, desktop logon, and application response times for Citrix Virtual Apps and Desktops deployments—service and on-premises. It is a software-only, driver-free solution.

Monitoring and analytics

The Citrix Virtual Apps and Desktops service provides monitoring and reporting functionality. This includes dashboards, activity monitoring, and reporting features with the following benefits:

- Real-time data from the broker agent using a unified console integrated with analytics and performance management tools.
- Analytics tools that include performance management for health and capacity assurance, and historical trending to identify bottlenecks in your Citrix Virtual Apps or Desktops service environment.
- Historical data stored in the Monitor database to access the Configuration Logging database.
- Visibility into the user experience for virtual applications, desktops, and users for the Citrix Virtual Apps or Desktops service.
- A Monitor dashboard for troubleshooting that provides real-time and historical health monitoring of the Citrix Virtual Apps and Desktops service. This feature allows you to see failures in real time, providing a better idea of what the users are experiencing.

Figure 13 shows the Citrix Virtual Apps and Desktops Service Monitor dashboard, highlighting machines powered on, machines registered, and machines under maintenance:



[Last updated: 03/15/2019 11:01 AM]

Estimated Savings (AutoScaling managed machines)

Cost per machine per hour can vary across Delivery Groups. To view the cost, select a particular Delivery Group.

Cost Savings $2.00 (out of $8.00)

Delivery Group Based Usage

Delivery Group ↑	In Use	Available	Unavailable	Unregistered
All	0	1	0	2
1903ServerDg	0	1	0	0
mcs1903tsvdaDg	0	0	0	2

Figure 13: The Citrix Virtual Apps and Desktops Service Monitor dashboard

You can read more on Citrix Virtual Apps and Desktops service monitoring capabilities here.

Conclusion and resources

With an ever-increasing infrastructure and technological demand to enable remote work, it is becoming more important to modernize and realize the benefits of the cloud for your virtual desktop and apps. On the other hand, remote work for a hybrid workspace can also add security concerns. Migrating your VDI to Azure Virtual Desktop can help improve performance efficiency, optimized use of resources, and your overall security posture through the integrated security features of Microsoft Azure. For a smooth migration, it is essential to have an understanding of the process and considerations to design a successful plan.

This guide highlighted some of the key benefits of modernizing your current workloads and how Azure Virtual Desktop is integrated with the Citrix Virtual Apps and Desktops service. It covered the prerequisites for Microsoft Azure that you need to check before you start with your migration journey, and how to assess your existing environment using Azure Migrate and Lakeside SysTrack.

After pre-requisites, the guide provided a walk through for setting up the Citrix Virtual Apps and Desktop environment with Azure Virtual Desktop. The final stages covered post-deployment and optimization, enabling you to check performance and optimize cost.

There are additional resources available to help along the way listed in the next section.

You can get started with an Azure free account or get in touch with an Azure sales specialist to get advice and guidance on how to quickly deploy and scale Azure Virtual Desktop.

Further reading

There are a lot of other resources and support to help you get started—here are a few:

- Learn more about Citrix Virtual Apps and Desktops service with Azure.
- Sign up for a free Azure account to try deploying your virtualized Windows desktops and apps.
- Join the Azure Migration and Modernization Program to get curated guidance and expert help.
- Download the free Total Economic Impact™ of Microsoft Azure Virtual Desktop to get a detailed analysis of the return on investment and other outcomes experienced by real customers who migrated.

We’re here to help

Learn more about how to migrate your VDI to Azure Virtual Desktop by connecting with an Azure sales specialist.

Get in touch

If needed, use the following resources for more in-depth information on specific topics mentioned in this e-book:

Azure Reserved VM Instances

Azure Virtual Desktop partner integrations

What is Azure Virtual Desktop?

Windows 10 computer specifications and systems requirements

SLA for VMs

RDS – GPU acceleration

GPU optimized VM sizes

VM series

About Azure Migrate

Prepare and customize a master VHD image

FSLogix Migration Preview Module

Azure Virtual Desktop pricing

Supported VM OS images

Safe URL list

Windows 10 Enterprise multi-session FAQ

Host pool load-balancing methods

Recommended naming and tagging conventions

What are ARM templates?

RDS/Azure Virtual Desktop ARM templates

Azure Virtual Desktop and Citrix—modernize your environment

Glossary

Whether you are new to desktop virtualization or an expert at desktop virtualization, there may be some terms you are not familiar with. Here is an explanation of some additional terms that were introduced in this guide.

Term	Description
Active Directory Domain Services (AD DS)	A directory is a hierarchical structure that stores information about objects on the network. A directory service such as AD DS provides methods for storing directory data and making this data available to network users and administrators.
Azure Active Directory (Azure AD)	Azure AD is Microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources.
Azure Virtual Desktop	A desktop and app virtualization service that runs on Microsoft Azure.
Citrix Cloud	Citrix Cloud is a cloud-based platform for managing and deploying Citrix products and desktops and applications to end users using any type of cloud, whether public, private, or hybrid, or on-premises hardware. The product supports cloud-based versions of every major Citrix product.
Citrix Virtual Apps and Desktops service	Citrix Virtual Apps and Desktops service provides virtualization solutions that give IT control of VMs, applications, and security while providing anywhere access for any device. You maintain complete control over applications, policies, and users while delivering the best user experience on any device.

Term	Description
Citrix Workspace	Citrix Workspace is a complete digital workspace solution that delivers secure access to the information, apps, and other content that is relevant to a person's role in your organization. Users subscribe to the services you make available and can access them from anywhere, on any device.
Cloud Connector	The Connector serves as a channel that authenticates and encrypts all communication between Citrix Cloud and your resources.
Multi-factor authentication (MFA)	MFA is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan.
Remote Desktop Services (RDS)	RDS is the Infrastructure as a Service (IaaS) platform building virtualization solutions.
Resource location	Resource locations contain the resources you manage to deliver cloud services to your users.
Windows 10 Enterprise multi-session	Windows 10 Enterprise multi-session, formerly known as Windows 10 Enterprise for Virtual Desktops (EVD), is a new Remote Desktop session host that allows multiple concurrent interactive sessions.

About the author

Ryan Mangan is an end-user computing (EUC) specialist. A speaker and presenter, he has helped customers and technical communities with EUC solutions—ranging from small to global, 30,000-user enterprise deployments—in various fields.

Ryan is the owner and author of ryanmangansitblog.com, which has over 3 million visitors and over 70 articles on RDS and Azure Virtual Desktop. His GitHub repository is available at https://github.com/RMITBLOG.

Some of Ryan's community and technical awards include:

- Author of:
  - *A Quickstart Guide to Azure Virtual Desktop*
  - *An Introduction to MSIX App Attach*
- Parallels RAS VIPP – three consecutive years
- LoginVSI Technology Advocate – two consecutive years
- Technical person of the year 2017 KEMP Technologies
- Parallels RAS EMEA Technical Champion 2018
- Microsoft Community Speaker
- Top 50 IT Blogs 2020 – Feedspot
- Top 50 Azure Blogs 2020 – Feedspot

This document is provided "as is." Information and views expressed in this document, including URL and other internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.