Business Continuity

March 11, 2020

Contributed by:

IN THIS ARTICLE

Contributors
Overview
Remote PC Access
Citrix Managed Desktops

Contributors

Author: Daniel Feller and Mayank Singh

Most organizations have defined business continuity plans. The success of a business continuity plan is based on how much it impacts the user experience, how well it scales to overcome global issues, and how well it maintains corporate security policies.

Overview

Business continuity allows organizations to enable seamless workforce productivity during any kind of planned or unplanned disruption. The success of a business continuity plan is often based on the following user and business requirements:

User Requirements

- Ability to access all apps and data to perform job
- User experience remains the same
- Ability to be productive with varying network conditions

Business Requirements

- Ability to rapidly scale to support unexpected need
- Protect corporate resources from untrusted endpoint devices
- Easy to integrate with current infrastructure
- Must not bypass security rules and policies

VPN Risks

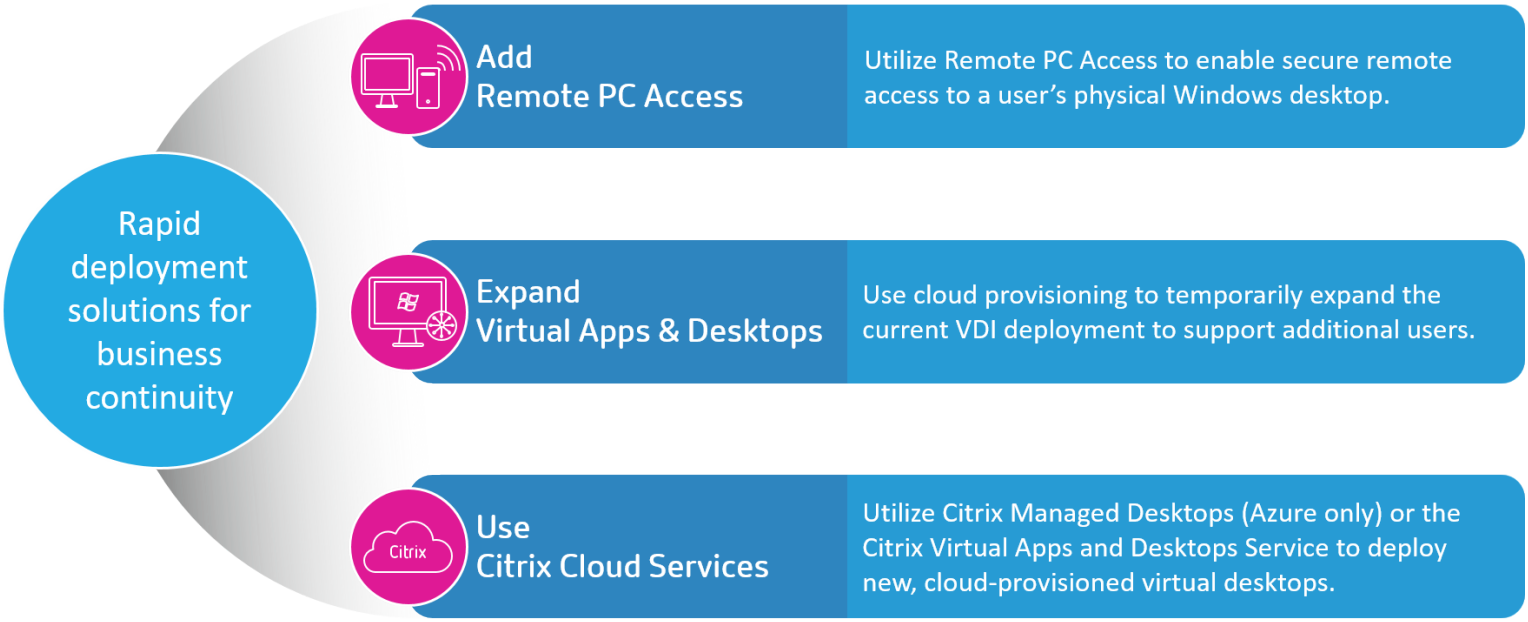
Most organizations need a way to provide users with secure remote access to corporate resources without relying on the deployment of VPN-based solutions. VPN-based of solutions are risky because they:

- VPN Risk 1: Are difficult to install and configure
- VPN Risk 2: Require users install VPN software on endpoint devices, which might utilize an unsupported operating system
- VPN Risk 3: Require the configuration of complex policies to prevent an untrusted endpoint device from having unrestricted access to the corporate network, resources, and data.

- VPN Risk 4: Difficult to keep security policies synchronized between VPN infrastructure and on-premises infrastructure.

Business Continuity Options

Depending on the state of the current infrastructure, an organization can opt for one of the following solutions to provide secure remote access to users during a business continuity event:



Remote PC Access

For many users, the work environment centers on a physical Windows 10 PC sitting under their desk. Remote PC Access allows a remote user to log into their physical Windows office PC using virtually any device (tablets, phones, and laptops using iOS, Mac, Android, Linux, and Windows).

The following Remote PC Access Tech Insight video provides an overview of the solution.

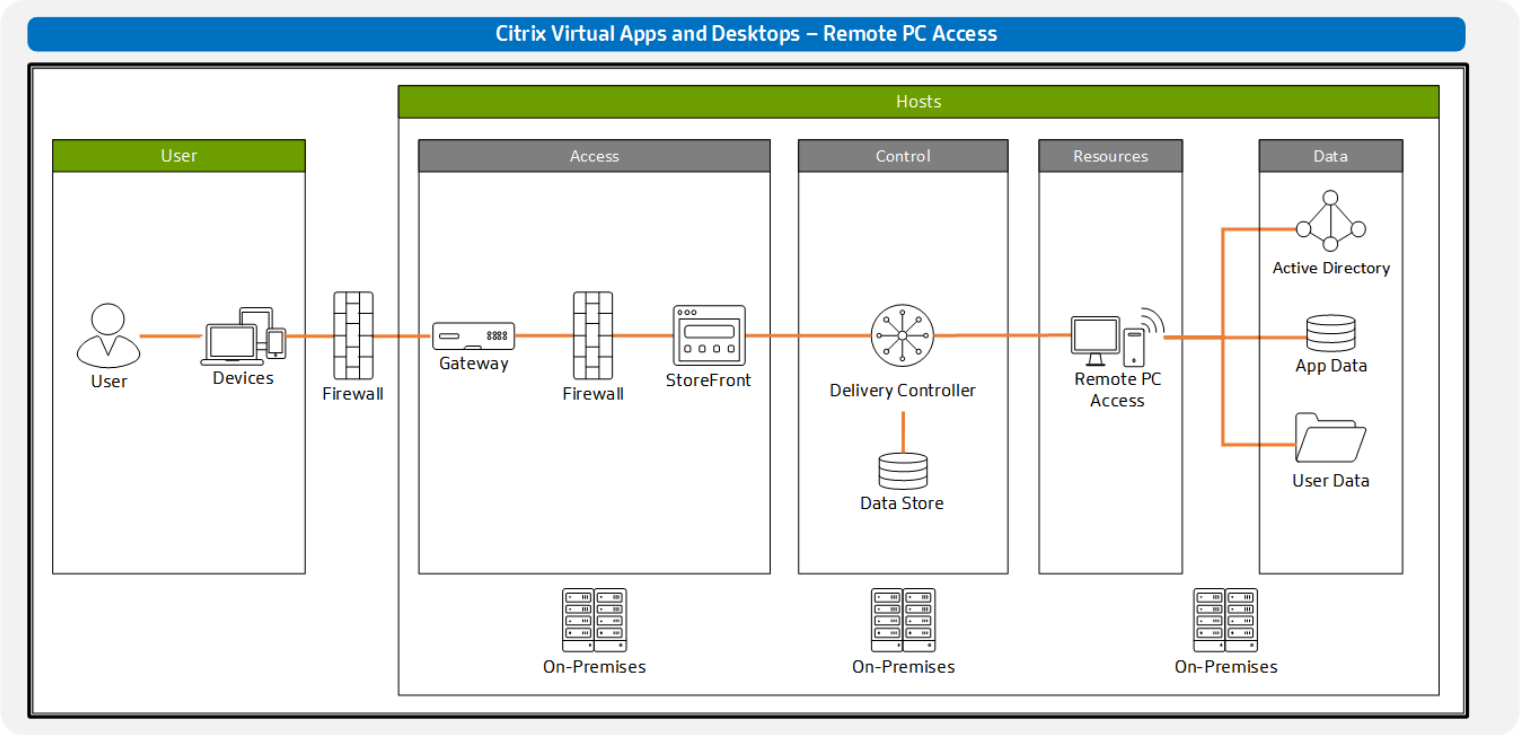
Adding Remote PC Access to the business continuity strategy assumes the following:

- A user's workspace is based on domain-joined Windows PCs
- User's authenticate with Active Directory
- There is minimal extra data center hardware capacity to accommodate a large virtual desktop (VDI) style deployment

When the user remotely accesses their work PC, the connection utilizes the ICA protocol, which dynamically adjusts to changing network conditions and content. The dynamic ICA protocol provides the best possible experience.

New Deployment

Organizations can easily deploy Citrix Virtual Apps and Desktops to provide Remote PC Access to their environment with a minimal deployment footprint, as seen in the following.



To add a new environment, the administrator must deploy the following components:

- Gateway: Secures connections between internal Windows PCs and untrusted end point devices via a reverse-proxy.
- StoreFront: Provides users an enterprise app store used to launch sessions to authorized resources.
- Delivery Controller: Authorizes and audits user sessions to Windows PCs.

It is recommended that three components be deployed with redundancy to overcome any single point of failure.

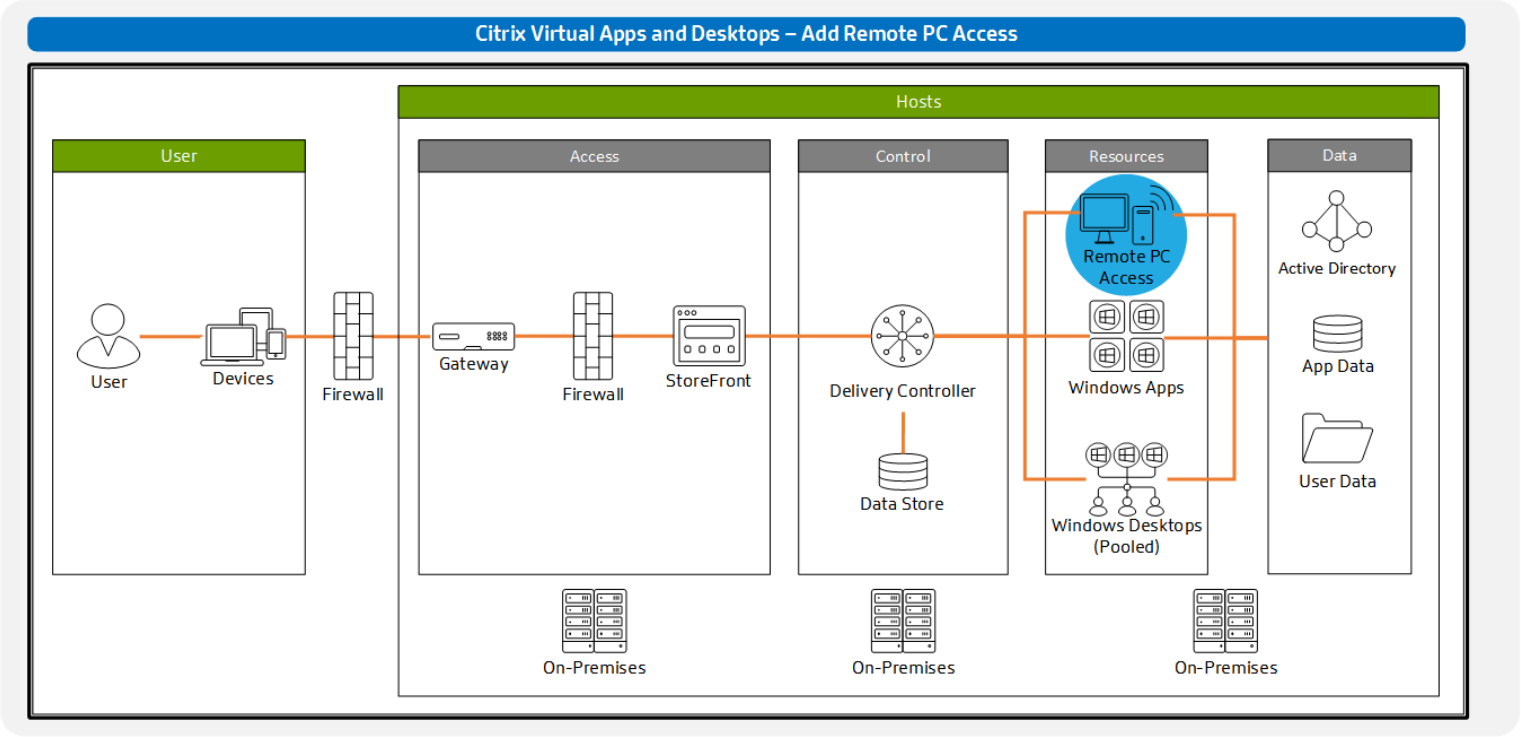
With a new infrastructure deployed, the administrator can perform the following to enable Remote PC Access:

- Deploys the Virtual Delivery Agent to physical Windows PCs (Automation Deployment Scripts)
- Creates a new Remote PC Access catalog
- Assigns users to PCs

Although the Virtual Delivery Agent can be installed on each physical PC manually, to simplify deployment of the Virtual Delivery Agent, it is recommended to use electronic software distribution such as Active Directory scripts and Microsoft System Center Configuration Manager.

Expanded Deployment

An organization can also easily add Remote PC Access to a current Citrix Virtual Apps and Desktops environment. This process effectively expands the conceptual architecture as follows:



To add Remote PC Access to a current Citrix Virtual Apps and Desktops environment, the administrator simply does the following:

- Deploys the Virtual Delivery Agent to physical Windows PCs
- Creates a new Remote PC Access catalog
- Assigns users to PCs

Because users simply access their physical work PC, the organization only needs to consider additional hardware for the access and control layers. These components must be able to accommodate the influx of new users' requests during a business continuity event.

Identity

Users continue to authenticate with Active Directory, but this authentication happens when the user initiates a connection to the organization's public fully qualified domain name for Citrix Gateway. Because the site is external, organizations require stronger authentication than a simple Active Directory user name and password. Incorporating multifactor authentication, like a time-based one-time password token, can greatly improve authentication security.

Citrix Gateway provides organizations with numerous multifactor authentication options, which include:

- One Time Password
- RAIUS
- TACACS+
- SAML

Session Security

Users are able to remotely access the work PC with an untrusted, personal device. Organizations can use integrated Citrix Virtual Apps and Desktops policies to protect against:

- Endpoint Risks: Key loggers secretly installed on the endpoint device can easily capture a user's username and password. Anti-keylogging capabilities protect the organization from stolen credentials by obfuscating keystrokes.

- Inbound Risks: Untrusted endpoints can contain malware, spyware, and other dangerous content. Denying access to the endpoint device's drives prevents transmission of dangerous content to the corporate network.
- Outbound Risks: Organizations must maintain control over content. Allowing users to copy content to local, untrusted endpoint devices places additional risks on the organization. These capabilities can be denied by blocking access to the endpoint's drives, printers, clipboard, and anti-screen-capturing policies.

Results

Because Remote PC Access allows users to connect to their standard Windows PC during a business continuity event, organizations are able to:

- Provide users access to all apps and data to perform their job. Everything on the user's Windows PC is accessible with Remote PC Access.
- Maintain the user experience between normal operations and business continuity events. Users continue to use the same Windows PC in all situations.
- Remain productive, regardless of location and network conditions. The ICA protocol connecting the user's end point device to the Windows PC dynamically adjusts based on network conditions to provide the most responsive experience possible.
- Rapidly scale to support unexpected need. Once the agent gets deployed to the Windows PCs, the administrator can simply enable the Remote PC Access capability.
- Protect corporate resources from untrusted endpoint devices. Gateway creates a reverse proxy between the end point and work PC. With session policies, administrators can block users from transferring data to/from the work PC and corporate network.
- Easily integrate with the current infrastructure. Remote PC Access is simply a different type of virtual desktop within the Citrix Virtual Apps and Desktops solution.
- Maintain the same security profile during a business continuity event. Remote PC Access connects users to their office-based Windows PC. Users have the ability to access the same resources, the same way as they were physically in the office.

Citrix Managed Desktops

Customers who want to use cloud to host their business continuity environment can use Citrix Managed Desktops, a Desktop-as-a-Service (DaaS) offering. This deployment option also works when an administrator does not have time to setup or does not want to manage an on-premises Citrix Virtual Apps and Desktops environment.

The entire Citrix Managed Desktops environment is hosted in Microsoft Azure. The Citrix Managed Desktops service can be spun up quickly when the business continuity event occurs. With the monthly pay-as-you-go billing (which includes Azure consumption), the environment can be shut down when no longer needed.

Identity

To maintain a user experience similar to the traditional, on-premises model, the user's identity continues to use Active Directory. Domain-joined, Active-Directory based deployments of Citrix Managed Desktops allow users to use either of the following options:

- Option 1: Users authenticate to the organization's Azure Active Directory, which is synchronized from the organization's on-premises Active Directory domain.
- Option 2: Users authenticate to the on-premises Active Directory domain by using an Azure-to-Data Center tunnel created with Citrix SD-WAN.

In most instances, an organization synchronizes the on-premises Active Directory with Azure Active Directory by using the Azure Active Directory Connect utility.

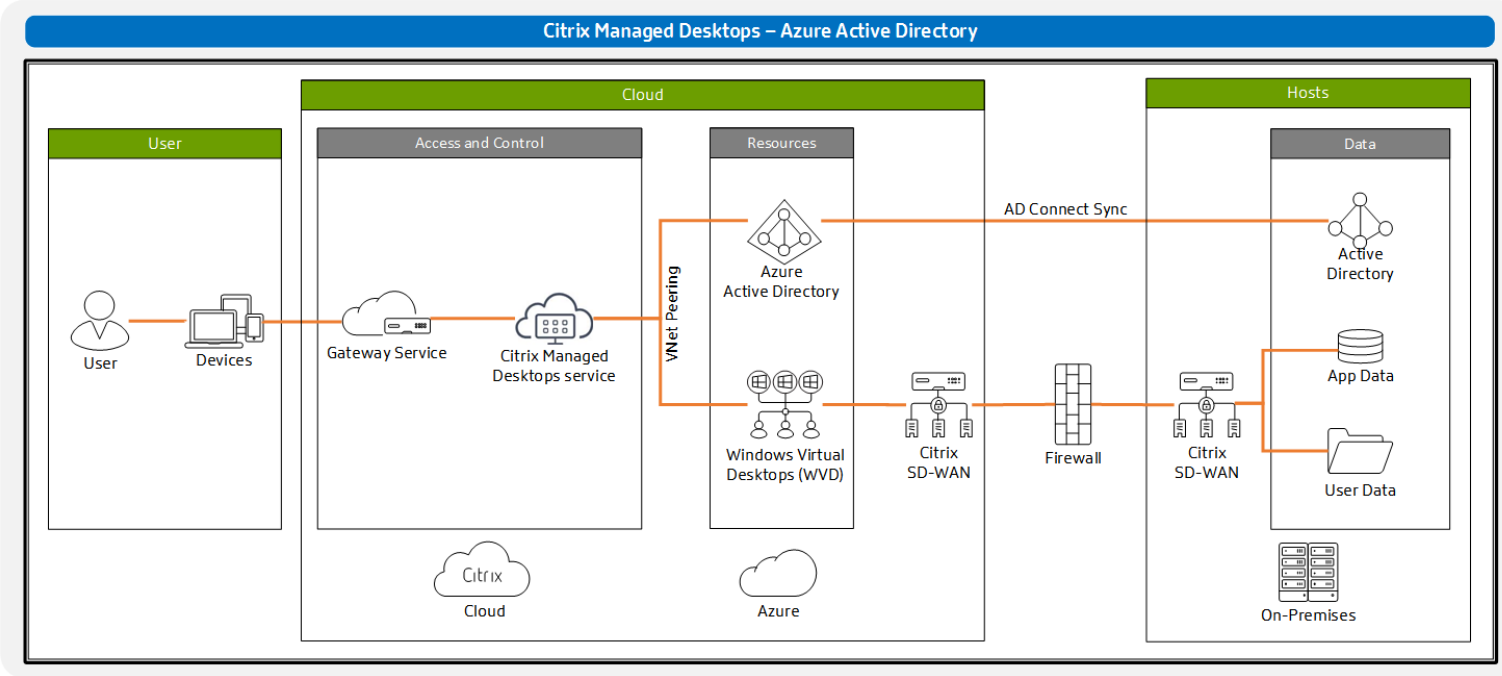
Data Center Connectivity

To be effective, users need to access files and back end resources from their Citrix Managed Desktop. Unless these items are transitioned to Azure, connectivity between Azure and the data center must be established.

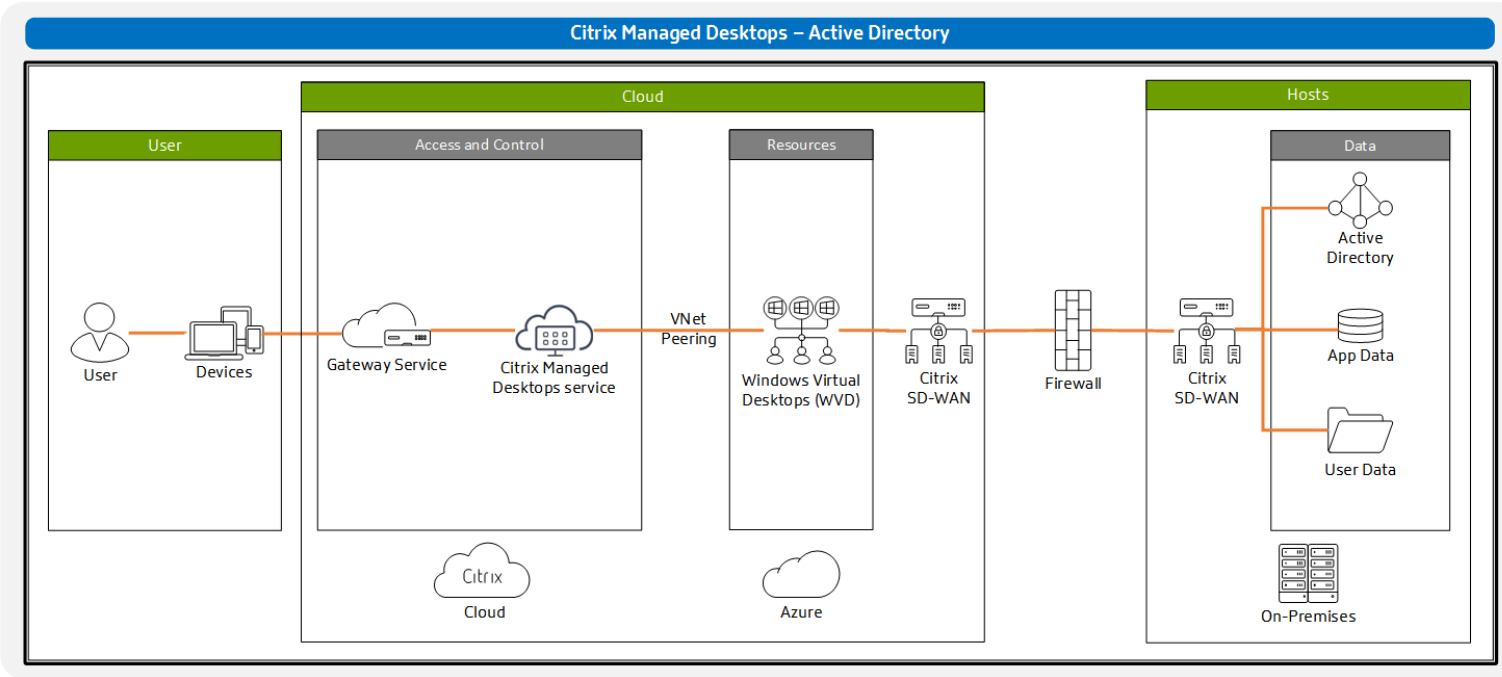
Using Citrix SD-WAN, organizations create a secure tunnel between Azure and the data center. SD-WAN understands the data traversing the tunnel and can properly optimize the traffic to improve application response time and user experience.

Deployment

Organizations can easily deploy Citrix Managed Desktops with a minimal deployment footprint, as seen in the following conceptual diagrams. The first diagram shows Citrix Managed Desktops using Azure Active Directory for user authentication:



The second diagram shows how Citrix Managed Desktops can use the SD-WAN tunnel to authenticate users to an on-premises Active Directory domain.



To add a new deployment, the admin performs the following steps:

- Sets up VNet peering between the Azure subscription where the machines would be hosted and the organization's Azure Active Directory (if the machines are not already in the same subscription)
- Creates and uploads a master Windows image, which contains the required apps
- Deploys a machine catalog based on the master image
- Assigns users to the machine catalog

Once deployed, users authenticate to the environment and receive a cloud-hosted managed virtual desktop available from any location and from any device.

Results

- Easily deployed in an environment where no existing Citrix infrastructure is present.
- Citrix updates and manages the setup with best practices. Only the desktop hosts are managed by the admin.
- Can bring up an environment in just a few hours and accessible to users from anywhere in the world.
- With the cloud scale of Azure, admins can bring up as many machines as needed in very short time.
- The monthly subscription model keeps the cost down by having the machines in the secondary location up and running only when needed.
- The session is connected on over the super-fast Azure back bone
- The user connects to the session over the internet for the last mile (from the nearest Citrix Gateway PoP), the ICA protocol adjusts based on network conditions to provide the most responsive experience possible.
- Citrix session policies secure the environment by blocking untrusted endpoints from transferring data to and from the managed desktop.