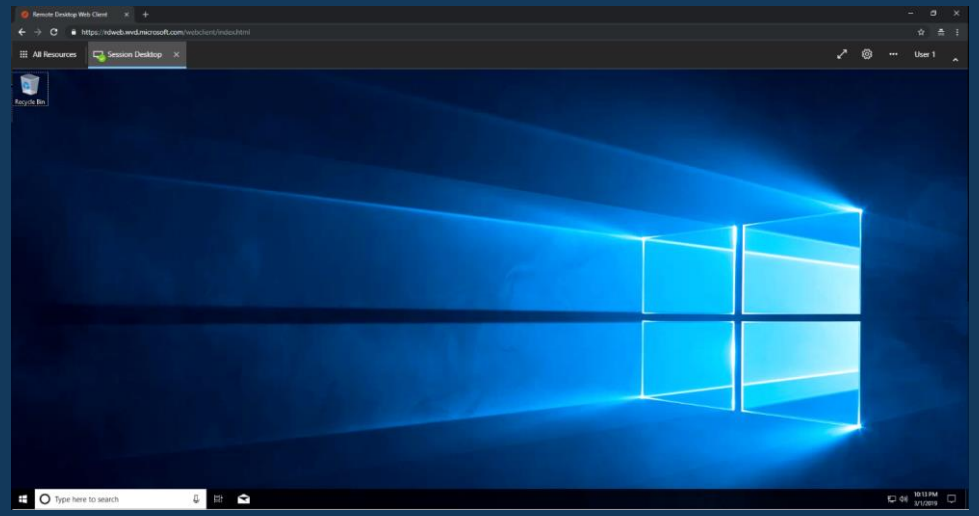
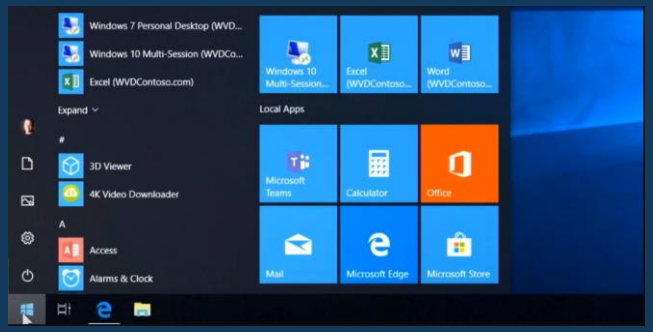
Windows Virtual Desktop

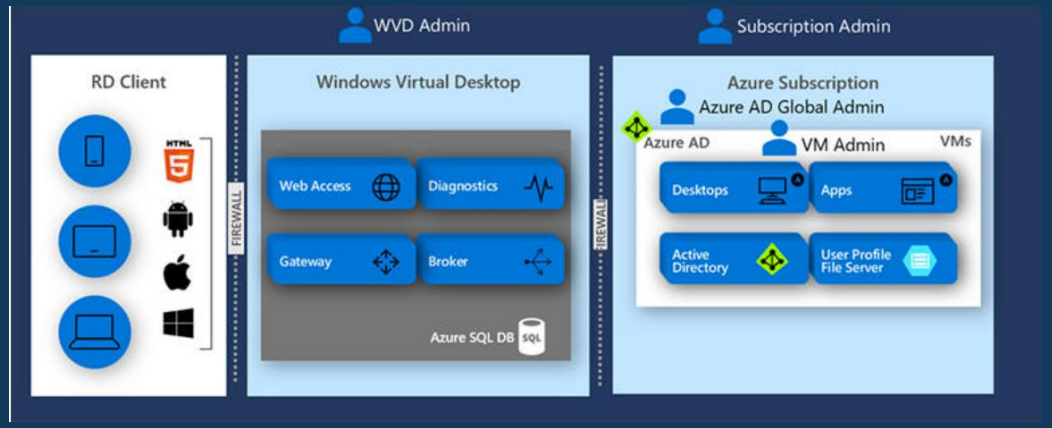
2 weeks setup Consultant Service

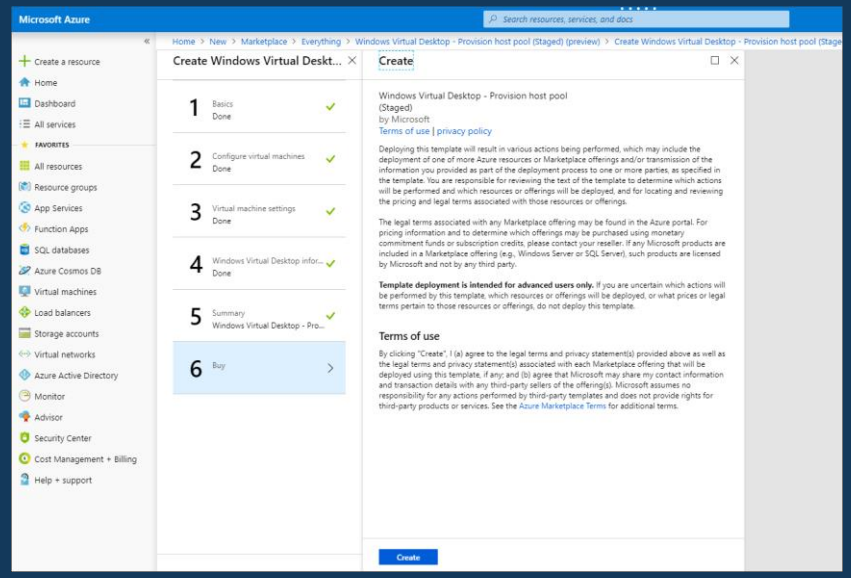
Asurgent 2 week WVD Setup Consultant Service

- Background
- What this 2 weeks Consultant Service contains and will deliver:
  - Prerequisites to be considered
  - AD Connection and Credentials
  - Setup of WVD – deploy of VMs
  - WVD access to AD
  - WVD Config
  - User test
  - Next step









What is WVD – short backgroud

Windows Virtual Desktop is a comprehensive desktop and app virtualization service that runs in the cloud. Here is a quick list of some of the key features and functionality:

•Infrastructure services like gateway, brokering, licensing, diagnostics are provided as a service in Azure. There's no need to deploy and maintain any on-premises infrastructure.

•Windows Virtual Desktop can leverage Azure Active Directory (Azure AD) as the identity provider, allowing you to leverage additional security controls like multi-factor authentication (MFA) or conditional access.

•Once a user is connected to Windows Virtual Desktop service, access to Active Directory joined virtual machines (VMs) will be provided using Azure AD identities. In environments where Active Directory Federation Services (AD FS) is implemented for single sign-on (SSO), the user won't be prompted for credentials when connecting to the VM, providing a seamless sign-on experience.

•Reverse connect technology means your destination VM doesn't need any inbound ports to be opened. Even the default RDP port, TCP/3389, doesn't have to be open. Instead, an agent creates an outbound connection using TCP/443 into the Windows Virtual Desktop management plane. Azure is your reverse proxy for RDP traffic.

•Virtual machines in Windows Virtual Desktop are not exposed to the Internet directly. They can run using a private IP address and run isolated from other workloads or even the Internet. (The reverse connect technology allows the VMs to be accessed.)

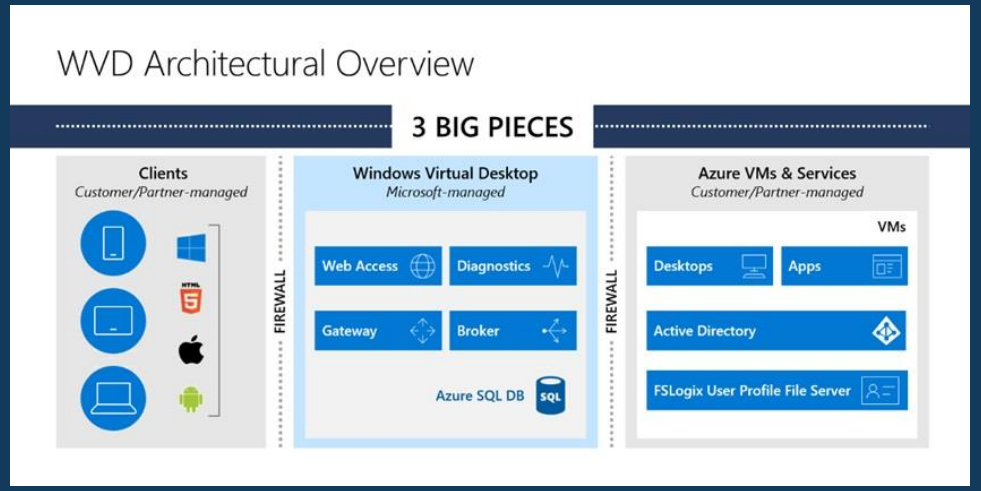
•Windows Virtual Desktop introduces Windows 10 multi-session, allowing you to offer a Windows 10 Enterprise experience where multiple users can log into the same Windows client VM simultaneously via RDP. (multi-session was historically only possible on Windows Server operating systems.)

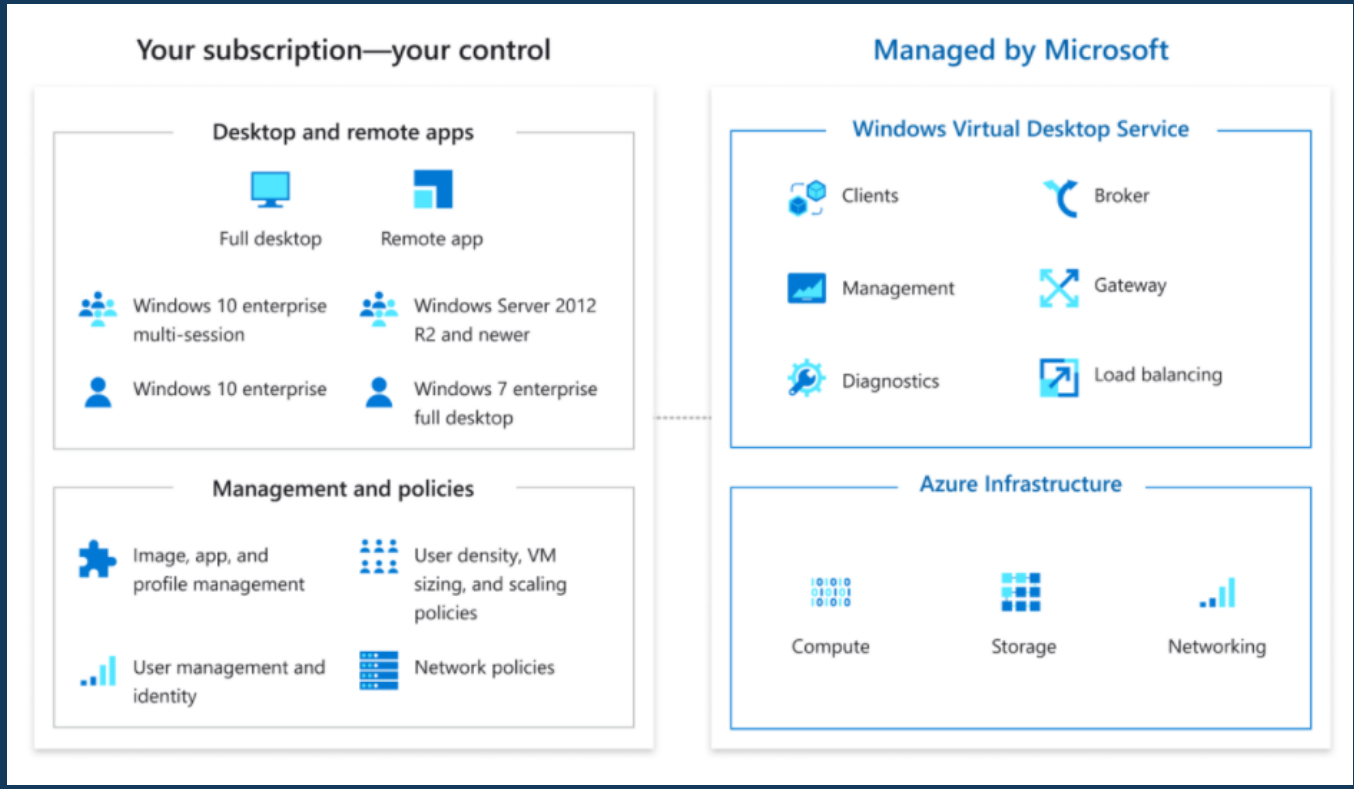
•Access to FSLogix technology, making your Office experience in a non-persistent environment feel like you are using a traditional PC.

•Windows Virtual Desktop supports full desktop, RemoteApp, and persistent or non-persistent, dedicated or multi-session experiences.

•Organizations with "Windows 10 Enterprise E3 Per User" licenses or better (e.g. Windows 10 Enterprise E5 or Microsoft 365 E3, E5, F1, or Business) or RDS CALs can use Windows Virtual Desktop for no additional charge apart from Azure compute/storage and network usage billing. Reserved instances can be used to reduce Azure costs up to 80%.

What is WVD – short background





Prerequisites – we will help you with these

To set up Windows Virtual Desktop, we will need a few resources and to complete a few initial setup steps:

•An Azure subscription with sufficient credit (needed to host resources).

•Download and install the Windows Virtual Desktop cmdlets for Windows PowerShell on a device.

•Make sure your virtual network in Azure is configured in such a way that new VMs have your Domain Controller or Azure AD Domain Services (Azure AD DS) set as the DNS (otherwise the domain join step will likely fail). For guidance on how to configure DNS when using Azure AD DS, see Enable Azure Active Director Domain Services. For guidance for using a Domain Controller, see Name resolution for resources in Azure virtual networks.

•Make sure all Azure resources are in the same region.

•If you require seamless SSO (HTML5 client excluded), you will need AD FS or users will have to authenticate when gaining access to the VM. (Steps on how to enable this with AD FS will follow at a later stage.)

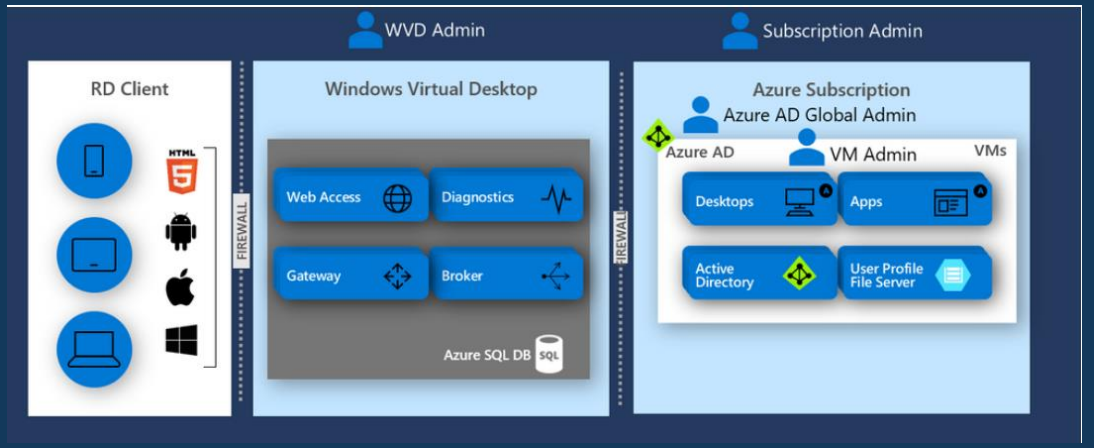
AD Connection and Credentials

- An Active Directory to which we can join your VMs.

  For this, we have three options and we will adapt to your needs:

Option	Pros	Cons
Use Azure AD DS.	Great for test or isolated environments that do not need connectivity to on-premises resources. Azure AD will be your leading source for identities.	AD DS will always be running, resulting in a fixed charge per month.
Spin up a DC in your Azure subscription.	Can sync with on-premises DCs if VPN or ExpressRoute is configured. All familiar AD Group Policies can be used. Virtual machines can be paused or stopped when needed to reduce costs.	Adds additional management of a VM and Active Directory in Azure.
Use VPN or ExpressRoute and make sure your on-premises DCs can be found in Azure.	No AD DS or Domain Controller required in Azure.	Latency could be increased adding delays during user authentication to VMs. This assumes you have an on-premises environment, not suitable for cloud only tests.

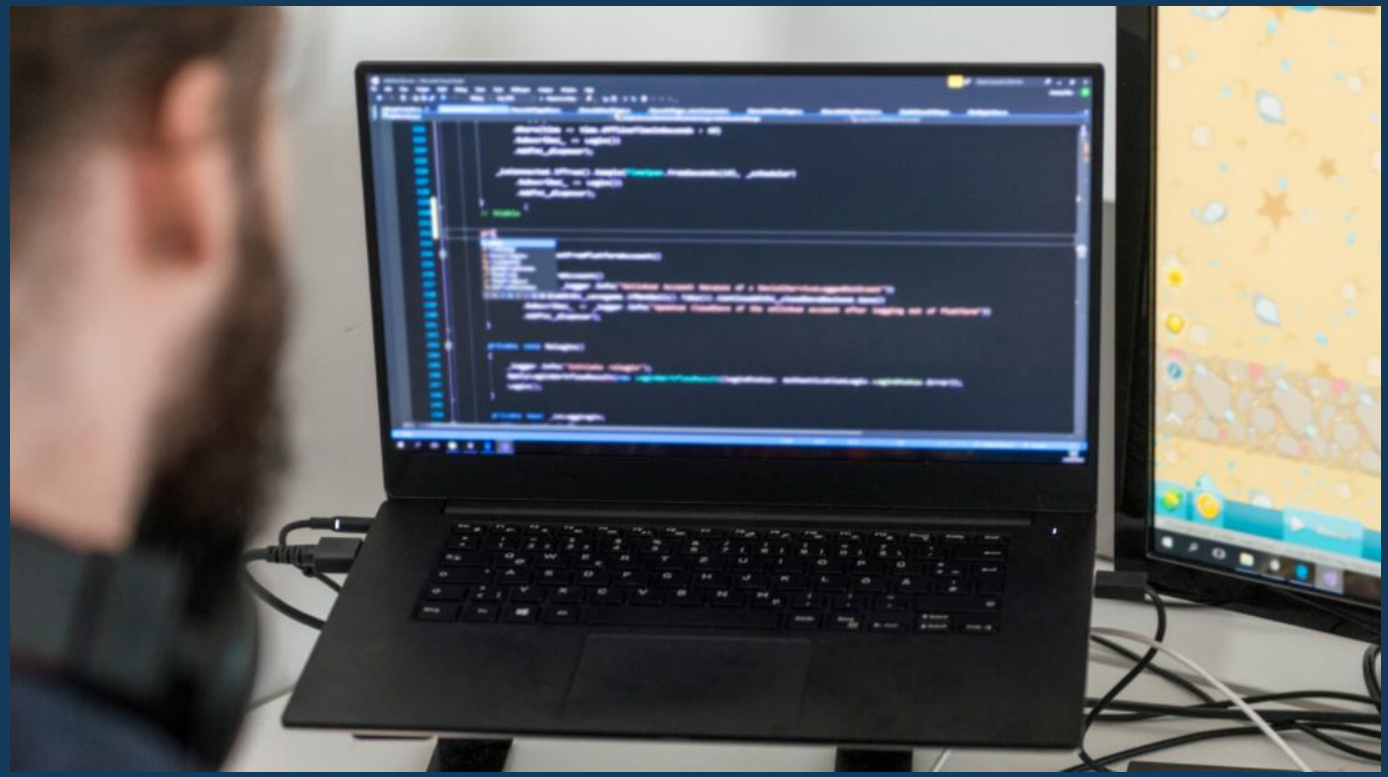
- We will also need to make sure we have the right credentials. Here's an overview of the accounts being used throughout the deployment process:



Setup of WVD – deploy initial VMs

We will now move on to the initial setup of Windows Virtual Desktop. Once these steps have been completed, we will be ready to deploy your initial VMs:

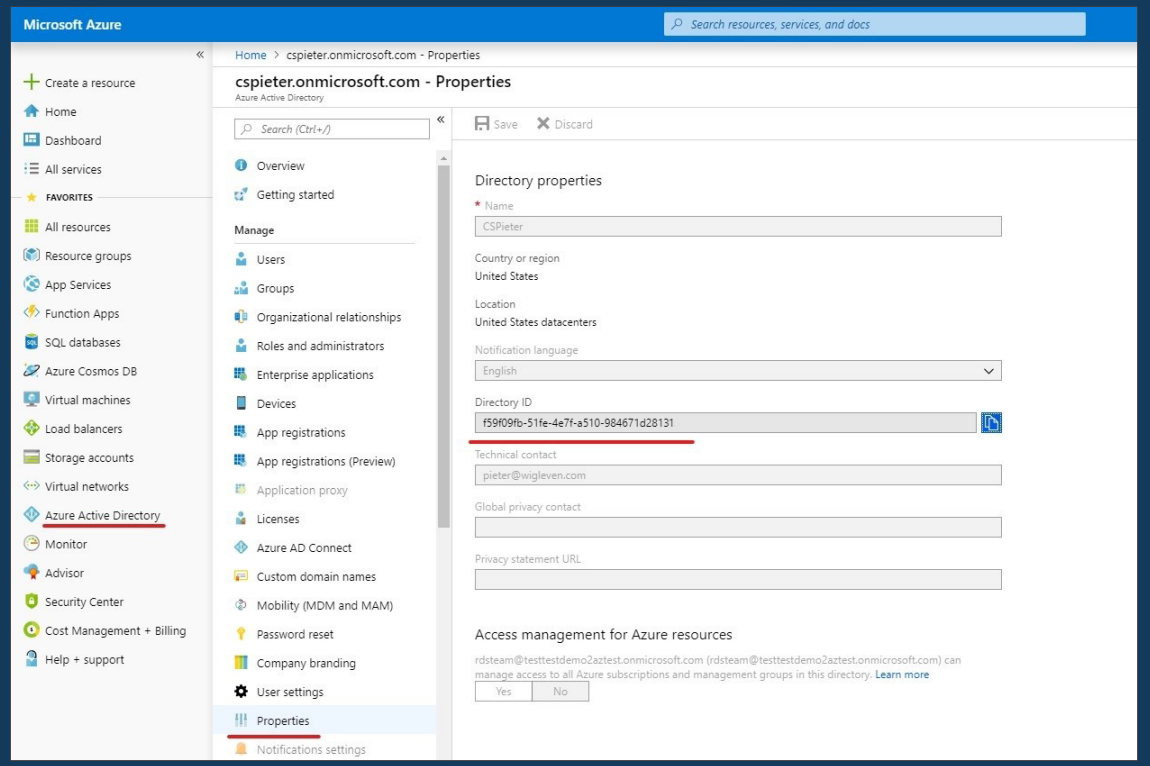
1. Allow the Windows Virtual Desktop service to access Azure AD.
2. Assign the "TenantCreator" role to a user account.
3. Create a Windows Virtual Desktop tenant.
4. Deploy your first Windows Virtual Desktop host pool.
5. Test if a user can access a full desktop session.

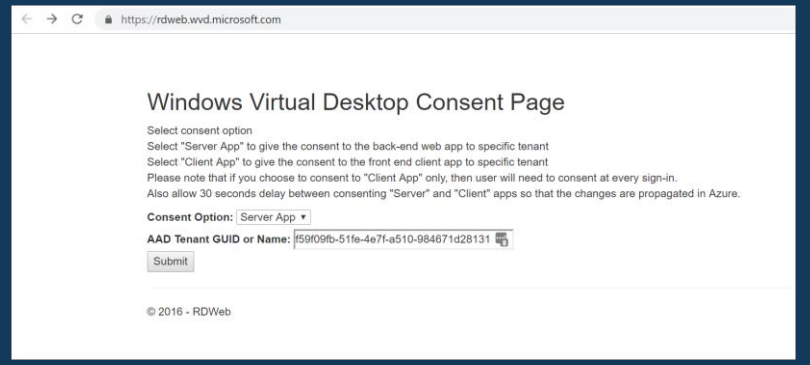


WVD access to AD

Before we can create a Windows Virtual Desktop tenant, yweou must allow Windows Virtual Desktop services to access your Azure AD tenant. The way Windows Virtual Desktop is designed requires explicit Azure AD consent. The process is much like how Azure requires you to enable non-standard resource providers before being able to use them.

1. Navigate to https://rdweb.wvd.microsoft.com.
2. Add Azure AD tenant ID, also referred to as the Directory ID, and hit Submit. (Your Azure AD tenant ID can be found by visiting the Microsoft Azure Portal and navigating to Azure Active Directory > Properties > Directory ID, or by using whatismytenantid.com.)
3. Wait a moment for the consent options to refresh, then change Consent Option to Client App and enter the same Azure AD tenant ID to the field for AAD Tenant GUID or Name. Click Submit to continue.

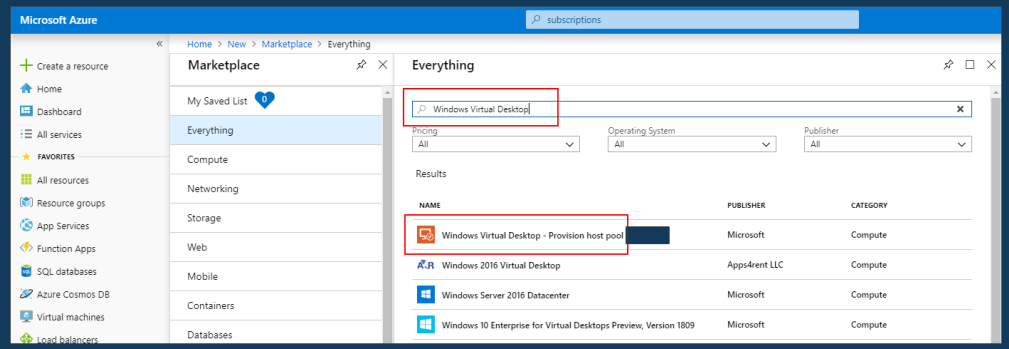


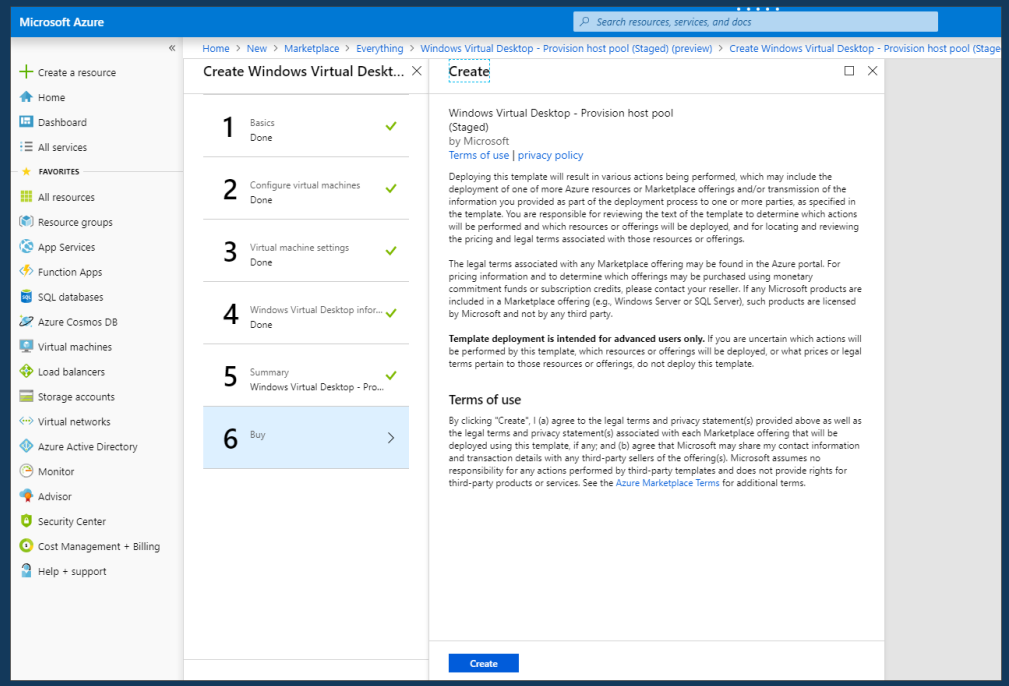


WVD Config

We will:

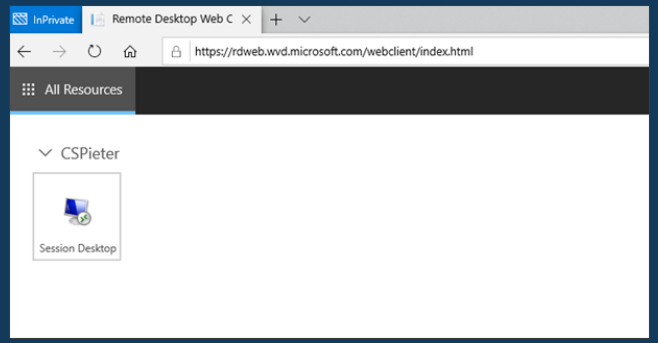
- Assign the “TenantCreator” role to a user account
- Create a Windows Virtual Desktop tenant
- Deploy your first Windows Virtual Desktop host pool
    1. Basic Settings
    2. Configure VMs
    3. Configure VM settings
    4. Authentication details
    5. Check Summary
    6. Finalize Creation

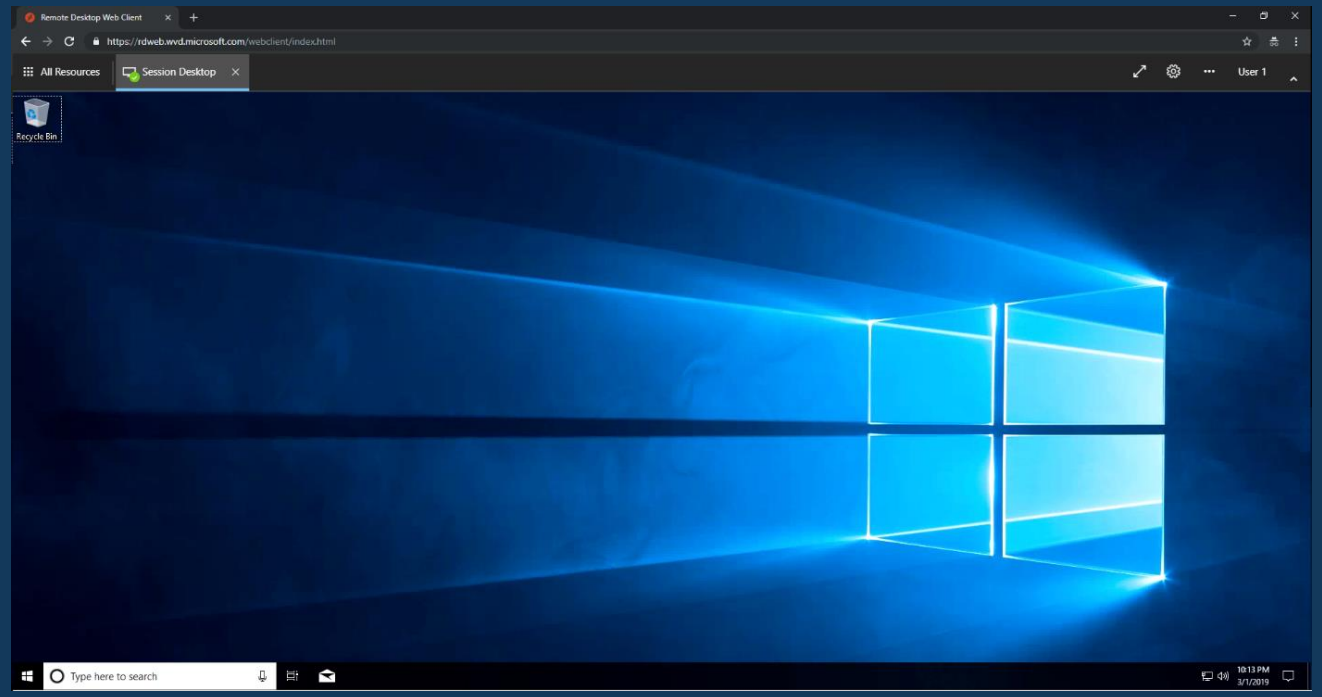




User test

- Test if a user can access a full desktop session. This is how it will look like when we are ready:





What's next?

- Once you have completed your setup of Windows Virtual Desktop, you can assign other users to your host pool using the following PowerShell command, replacing <WVDTENANTNAME> with the name of your tenant, <HOSTPOOLNAME> with the name of your host pool, and leveraging the appropriate user principal name:

Windows Virtual Desktop

2 weeks setup Consultant Service