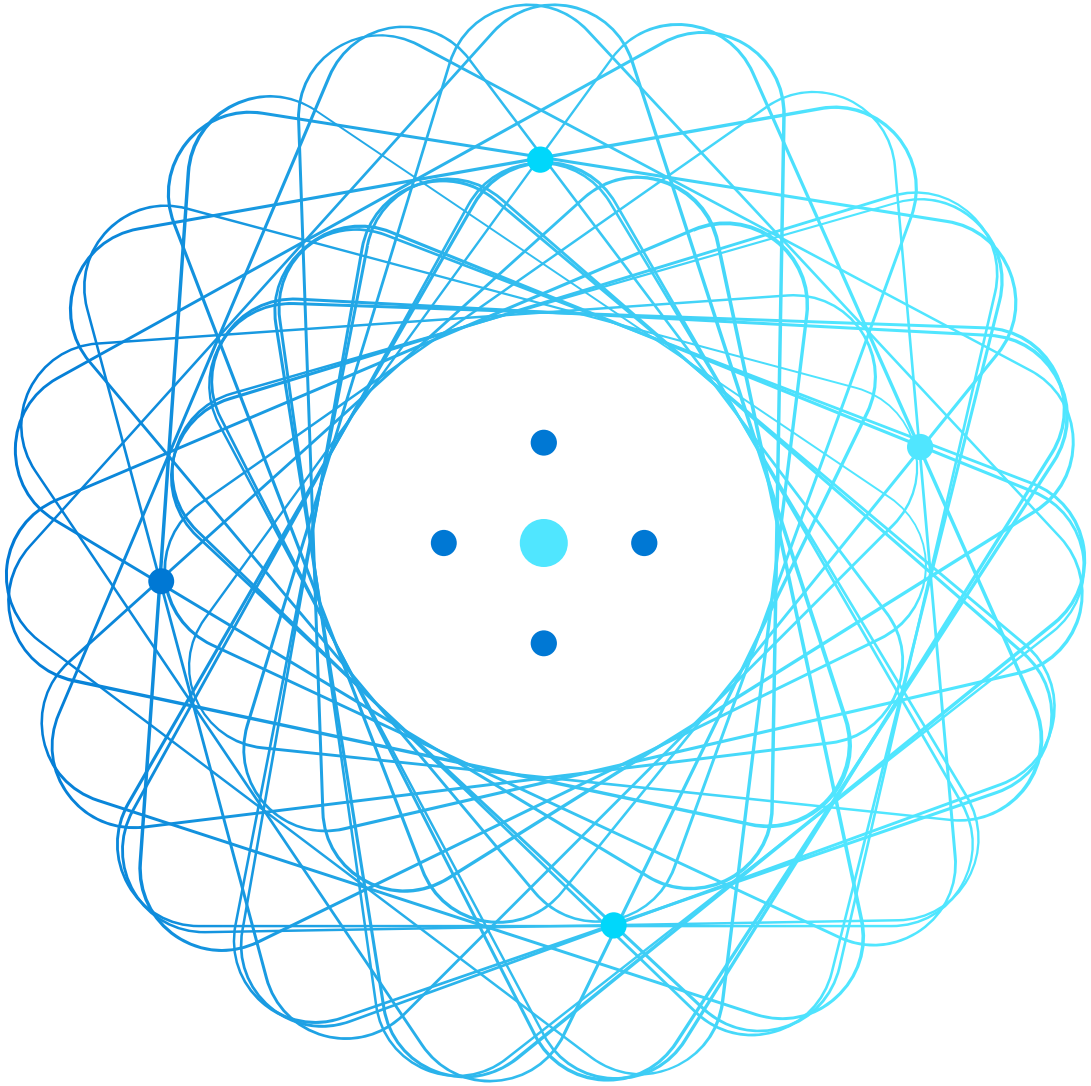
Microsoft Azure

AZ-140

Configuring and Operating Azure Virtual Desktop



AZ-140 Agenda

Learning Path 1

1. Azure Virtual Desktop Architecture
2. Design the Azure Virtual Desktop architecture
3. Design for user identities and profiles

Learning Path 2

4. Implement and manage networking for AVD
5. Implement and manage storage for AVD
6. Create and configure host pools and session hosts for AVD
7. Create and manage session host image for AVD

Learning Path 3

8. Manage access for AVD
9. Manage security for AVD

Learning Path 4

10. Implement and manage FSLogix
11. Configure user experience settings
12. Install and configure apps on a session host

Learning Path 5

13. Plan for disaster recovery
14. Automate Azure Virtual Desktop management tasks
15. Monitor and manage performance and health

Configure user experience settings

Introduction

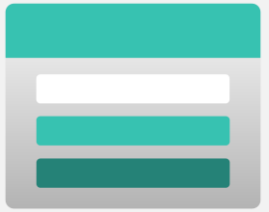
- Virtual desktop optimization principles
- Persistent virtual desktop environments
- Configure user settings through group policies
- Configure user settings through Endpoint Manager policies
- Configure session timeout properties
- Configure device redirections
- Configure Universal Print
- Troubleshoot user profile issues
- Troubleshoot Azure Virtual Desktop clients

AZ-140: Manage user environments and apps (20-25%)

Configure user experience settings

- Conceptual knowledge of Azure compute solutions.
- Working experience with virtual machines, virtual networks, and app service.

Virtual desktop optimization principles



Minimize graphic redraws, effects, and background activities that have no major benefit to the virtual desktop environment and reduce running processes to the bare minimum.

Use a "base" operating system image as the basis for the desktops:

- **Persistent:** preserves changes to the virtual desktop operating system from one session to the next.
- **Non-persistent:** does not preserve changes to the virtual desktop operating system from one session to the next.

Use a VM to build a VM:

- State can be saved
- Checkpoints can be set
- Backups can be performed
- A default OS installation is performed to the base VM
- VM is then optimized by removing unneeded apps
- Install Windows updates, delete temporary files, applying settings, etc...

Persistent virtual desktop environments

Persistent virtual desktop is a device that saves operating system state in between reboots.

- **Traditional VMs**, where the VM has its own virtual disk file, starts up normally, and saves changes from one session to the next.
- **Image-based persistent VMs**, a base/gold image on one or more host servers.
- **Master/gold image,** where updates are applied.

A **non-persistent virtual desktop** implementation is based on a base or "gold" image.

- The base image is read-only.
- When started, a copy of the base image is streamed to the VM.
- All activity until the next reboot is redirected to a temporary location.
- Users are provided network locations to store their data.

Configure user settings through group policies

Configure user settings through group policies

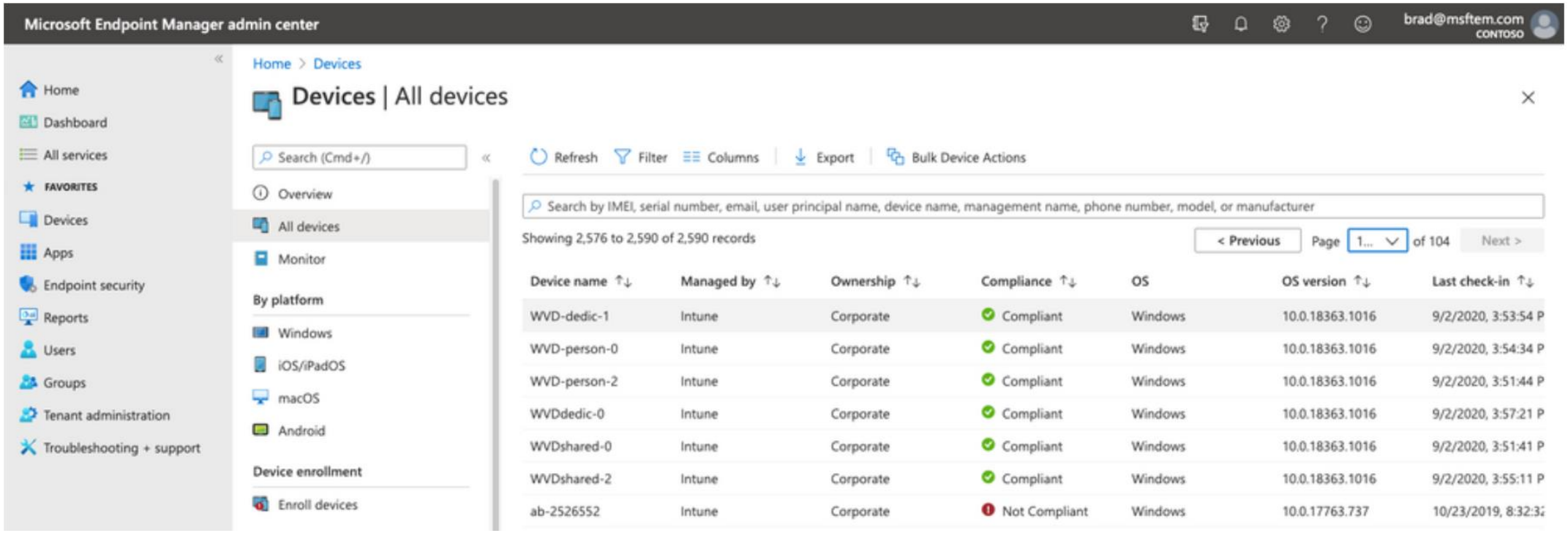
Setting area	Setting	Recommended value
Background Intelligent Transfer Service (BITS)		
	Do not allow the BITS client to use Windows Branch Cache	**Enabled**
	Do not allow the computer to act as a BITS Peercaching client	**Enabled**
	Do not allow the computer to act as a BITS Peercaching server	**Enabled**
	Allow BITS Peercaching	Disabled
BranchCache		
	Turn on BranchCache	Disabled
Hotspot Authentication		
	Enable Hotspot Authentication	Disabled
Microsoft Peer-to-Peer Networking Services		
	Turn off Microsoft Peer-to-Peer Networking Services	**Enabled**
Offline Files		
	Allow or Disallow use of the Offline Files feature	Disabled

Intune
MEM
Intune

Configure user settings through Endpoint Manager policies

Enroll Azure Virtual Desktop VMs that are hybrid Azure AD joined with Microsoft Intune and manage them in the Microsoft Endpoint Manager admin center as you would physical devices.

Endpoint Manager integration is available for Windows 10 Enterprise desktops.



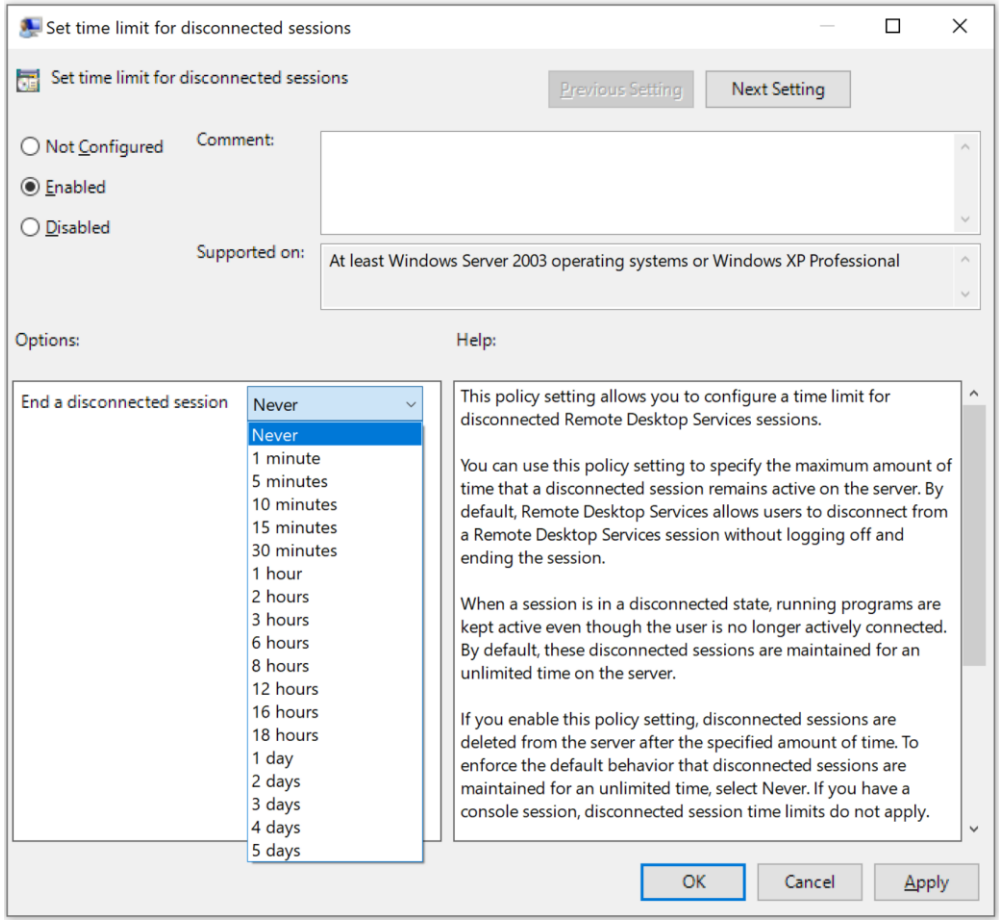
Configure session timeout properties

Configure session timeout properties

Signing users out when they're inactive preserves resources and prevents access by unauthorized users.

The timeout options for RDP is set on the servers in the Local Group Policy:

- Set time limit for disconnected sessions
- Set time limit for active but idle Remote Desktop Services sessions
- Set time limit for active Remote Desktop Services sessions
- End Session when time limits are reached



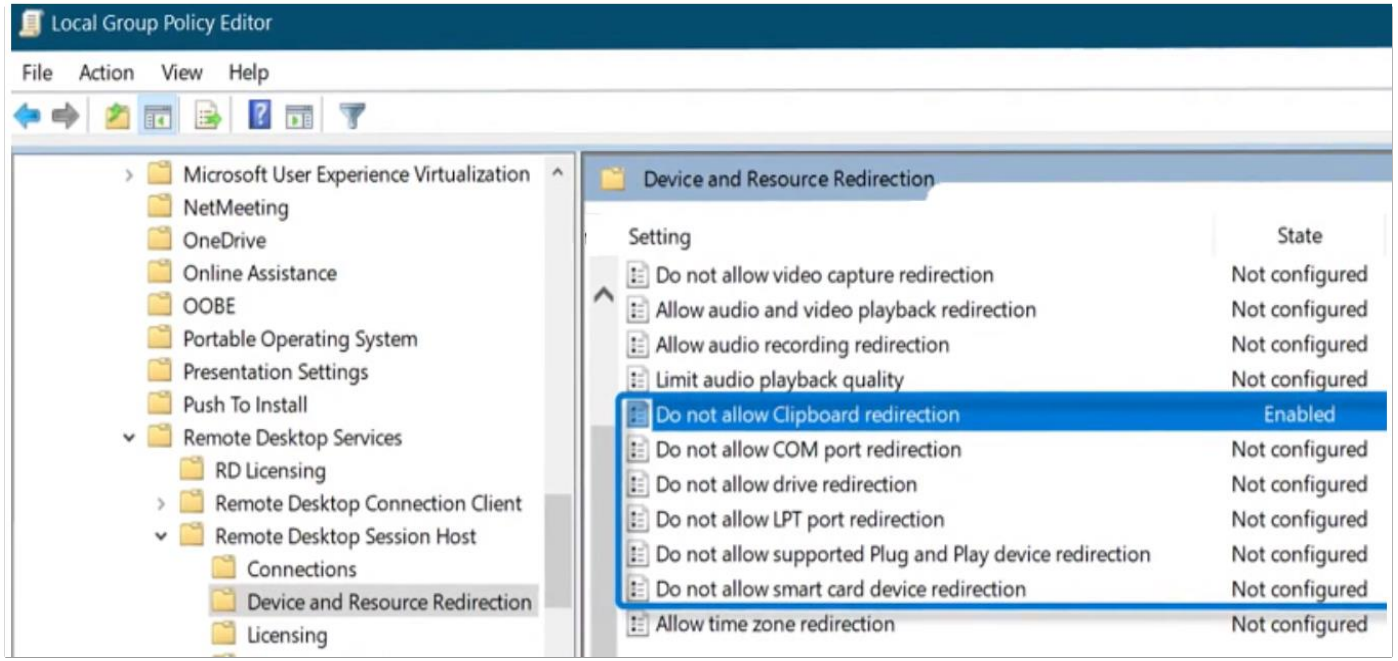
Configure device redirections

Configuring device redirections for your Azure Virtual Desktop environment allows you to use printers, USB devices, microphones and other peripheral devices in the remote session.

Clipboard redirection
`redirectclipboard:i:1` enables clipboard redirection
`redirectclipboard:i:0` disables clipboard redirection

COM port redirections
`redirectcomports:i:1` enables COM port redirection
`redirectcomports:i:0` disables COM port redirection

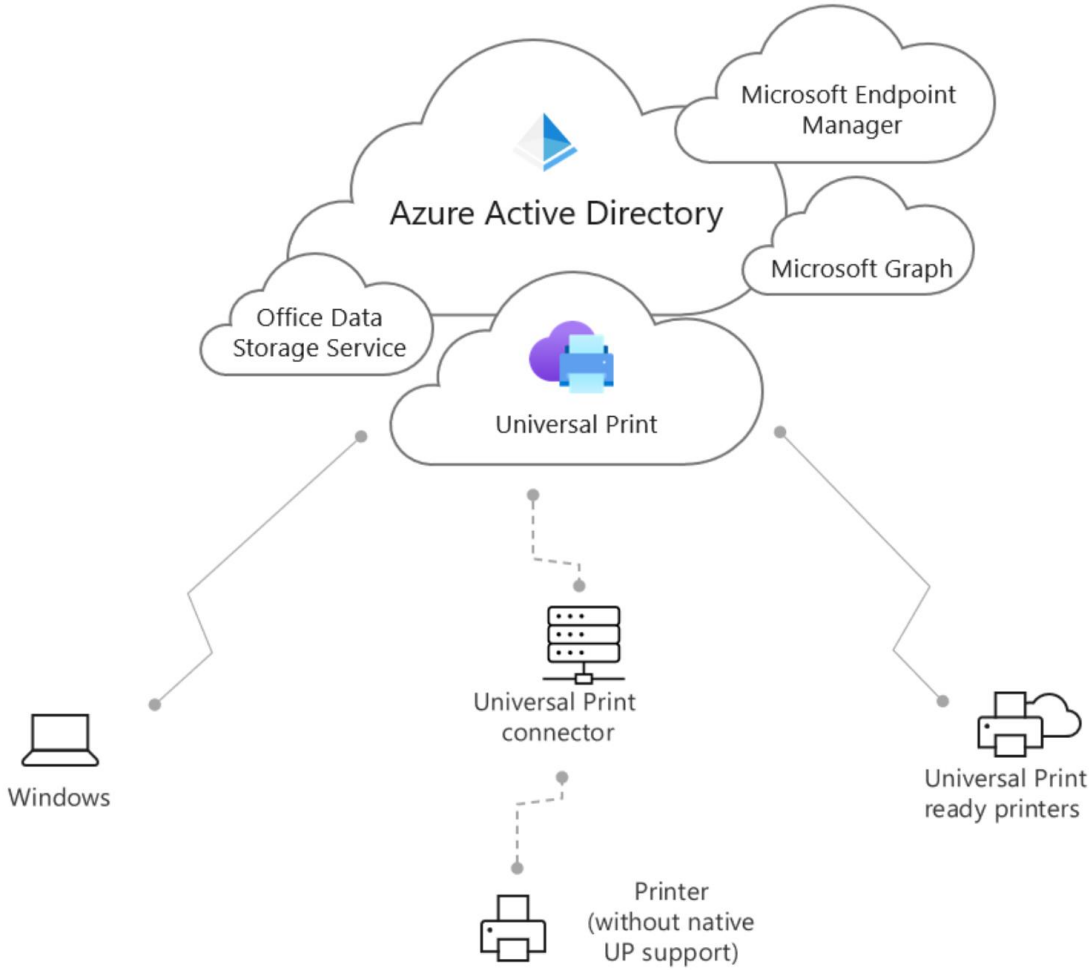
USB redirection
`usbdevicestoredirect:s:*` enables USB device redirection
`usbdevicestoredirect:s:` disables USB device redirection



Configure Universal Print

Universal Print manages print infrastructure through cloud services from Microsoft.

- Universal Print runs entirely on Microsoft Azure.
- With Universal Print–compatible printers, it doesn't require on-premises infrastructure.
- A Microsoft 365 subscription-based service that centralizes print management through the Universal Print portal.
- Integrated with Azure Active Directory and supports single sign-on scenarios.
- Can be deployed with non-compatible printers by using Universal Print connector software.



Implement the Start Virtual Machine on Connect feature

Start VM On Connect reduces costs by enabling end users to turn on their session host VMs only when they need them.

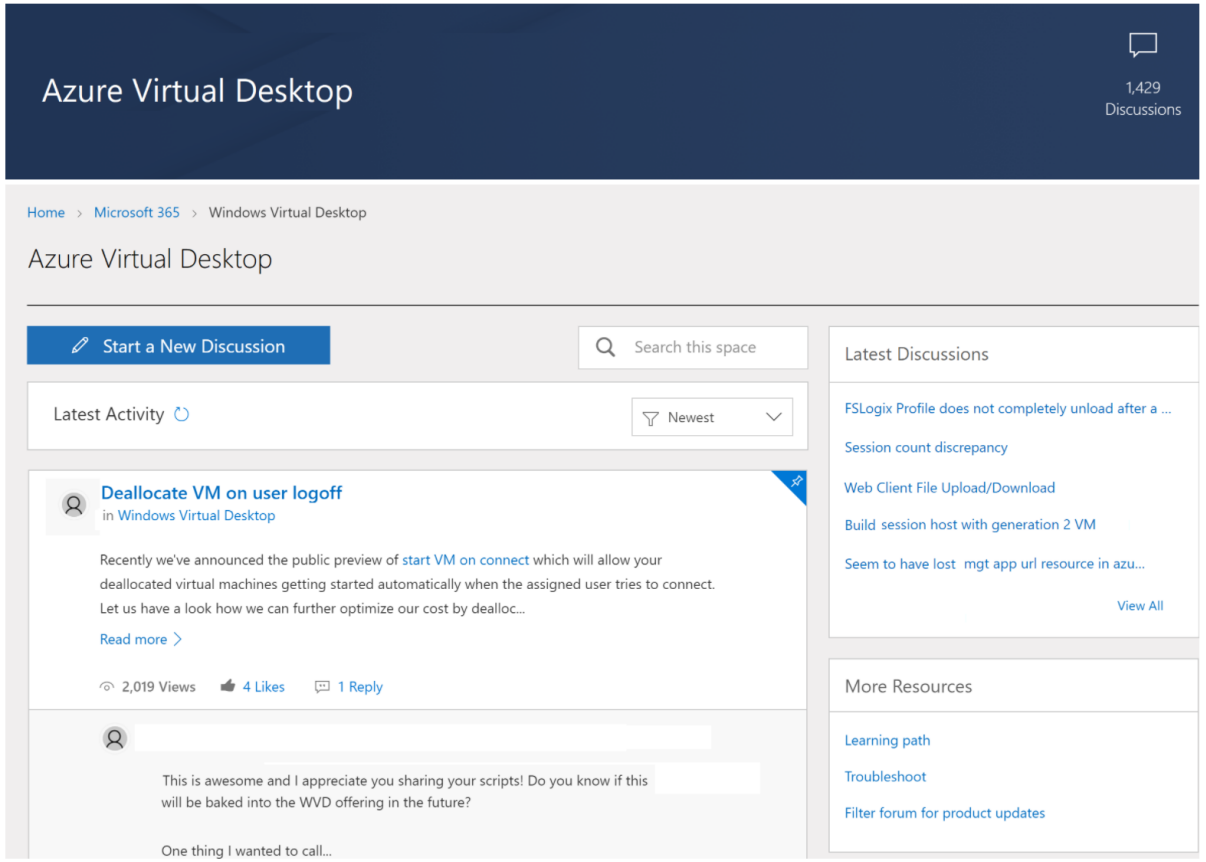
- You can them turn off VMs when they're not needed.
- You can configure Start VM on Connect for personal or pooled host pools using the Azure portal or PowerShell. Start VM on Connect is a host pool setting.
- For personal host pools, Start VM On Connect will only turn on an existing session host VM that has already been assigned or will be assigned to a user.
    - For pooled host pools, Start VM On Connect will only turn on a session host VM when none are turned on.
    - More VMs will only be turned on when the first VM reaches the session limit.
- You can only configure Start VM on Connect on existing host pools. You can't enable it at the same time you create a new host pool.

Troubleshoot user profile issues

Troubleshoot user profile issues

To report issues or suggest features for Azure Virtual Desktop with Azure Resource Manager integration, visit the [Azure Virtual Desktop Tech Community](#).

- Use the Tech Community to discuss best practices or suggest and vote for new features.
- When you make a post asking for help or propose a new feature, make sure you describe your topic in as much detail as possible.



Troubleshoot Azure Virtual Desktop clients

Troubleshoot Azure Virtual Desktop clients

Remote Desktop client for Windows 10 stops responding or cannot be opened

You can reset the user data from the About page or using a command.
Use the following command to remove your user data, restore default settings and unsubscribe from all Workspaces.

```
msrdcw.exe /reset [/f]
```

Web client won't open

First, test your internet connection by opening another website in your browser.
Use **nslookup** to confirm DNS can resolve the FQDN:

```
nslookup rdweb.WVD.microsoft.com
```

Try connecting with another client (eg, Remote Desktop client for Windows 10) to see if you can open the web client.

Web client keeps prompting for credentials

If the Web client keeps prompting for credentials, follow these instructions:

1. Confirm the web client URL is correct.
2. Confirm that the credentials you're using are for the Azure Virtual Desktop environment tied to the URL.
3. Clear browser cookies.
4. Clear browser cache.
5. Open your browser in Private mode.

Knowledge check and Summary

Check your knowledge

What you learned:

- Configure user settings through group policies for Azure Virtual Desktop.
- Configure user settings through Endpoint Manager policies for Azure Virtual Desktop.
- Configure session timeout properties for Azure Virtual Desktop.
- Configure device redirections for Azure Virtual Desktop.
- Configure Universal Print.
- Troubleshoot user profile issues.

End of presentation