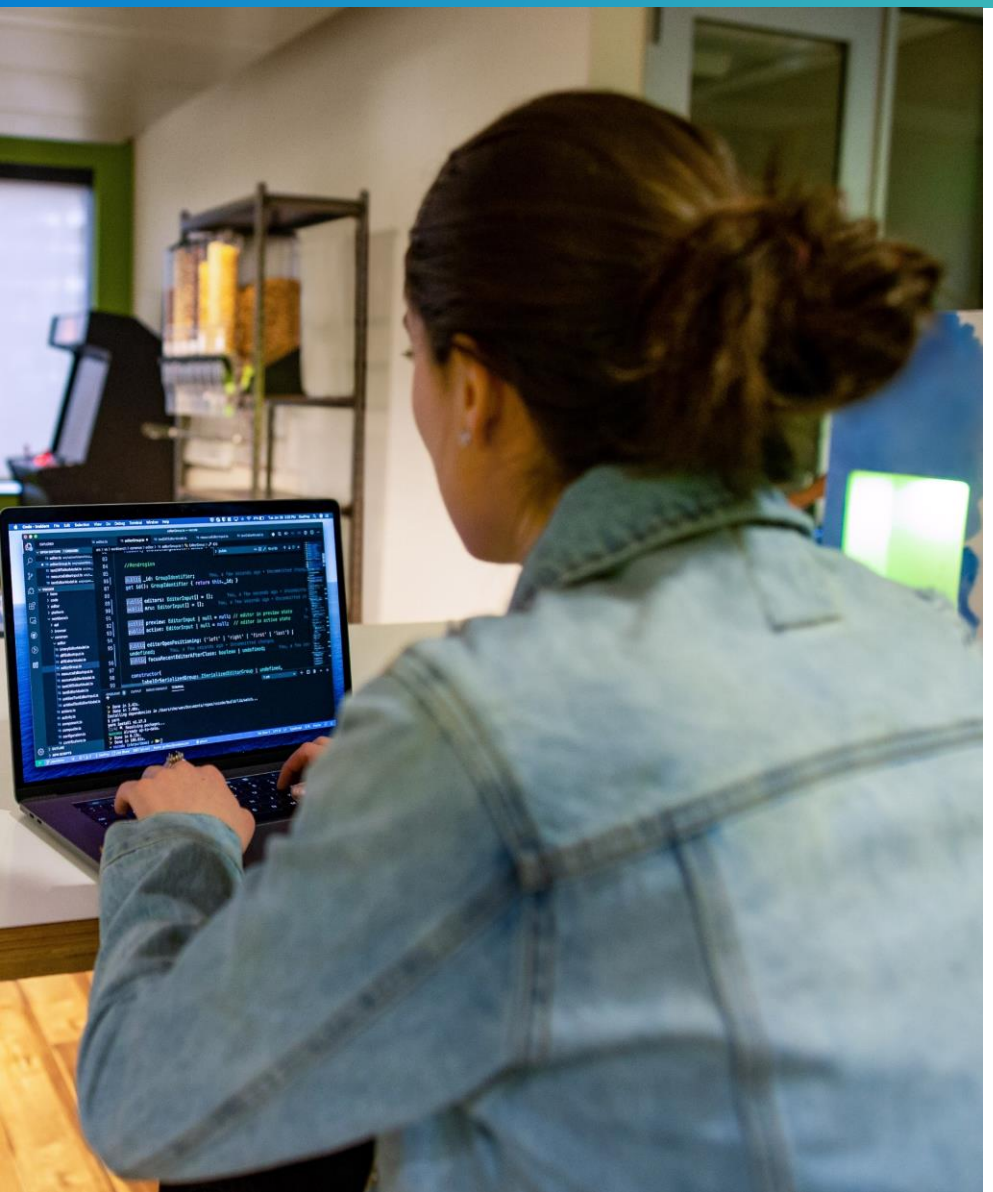
Azure Virtual Desktop for Azure Local

Introduction to Azure Virtual Desktop for Azure Local



- Designed for customers who need **secure on-premises virtualized apps and desktops**
- Combines the **benefits of Azure Virtual Desktop and Azure Local**
- Customers can **deploy in their datacenters** to **extend their on-premises infrastructure** to Azure
- All while enjoying many of the **key benefits of Azure Virtual Desktop on Azure**, such as **Azure portal, Windows 11 and Windows 10 multi-session**

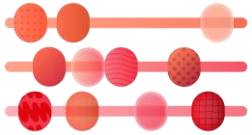
Azure Local provides a cloud native hybrid solution based on a modern subscription and an efficient hyper-converged infrastructure

Modern infrastructure to deploy cloud native solutions anywhere

Cloud native anywhere

Secured to run all workloads from cloud to edge

Familiar management and operations



Flexible options at the right price and performance point

Azure Virtual Desktop for Azure Local extends the benefits of cloud VDI to on-premises

Secure anywhere

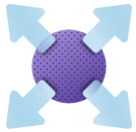
- Run virtualized desktops and apps securely with Entra ID, conditional access, and MFA
- Simplify VDI deployment
- No need to manage brokers, gateways, or underlying servers and storage

Windows 10 and 11 multi-session

- Windows 10 & 11 multi-session or single-session support
- Achieve high utilization & lower operation costs

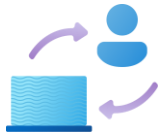
Prime performance

- Enjoy optimized Microsoft 365/Teams/Windows App experiences
- Run graphic-intensive workloads with GPU support
- Built for sensitive low-latency workloads



Full control

- Satisfy data locality requirements
- On-premises storage and data residency



Scale cloud and on-premises

- Manage and scale deployments across both Azure and Azure Local through a single management experience
- Use the familiar Azure portal and admin experience

Optimize for cost

- Use existing eligible Windows licenses
- No need to manage overhead licenses for Remote Desktop Services (RDS)
- Save with Windows 10 & 11 multi-session support

Azure Virtual Desktop for Azure Local use cases

Security and compliance

Secure, high performance cloud platform for financial institutions that meets compliance requirements

Data sovereignty

Cloud functionality that can meet the data sovereignty and data gravity requirements for public sector entities

Low latency workloads

High performance and low latency cloud capabilities that can meet the compute requirements for the most demanding workloads

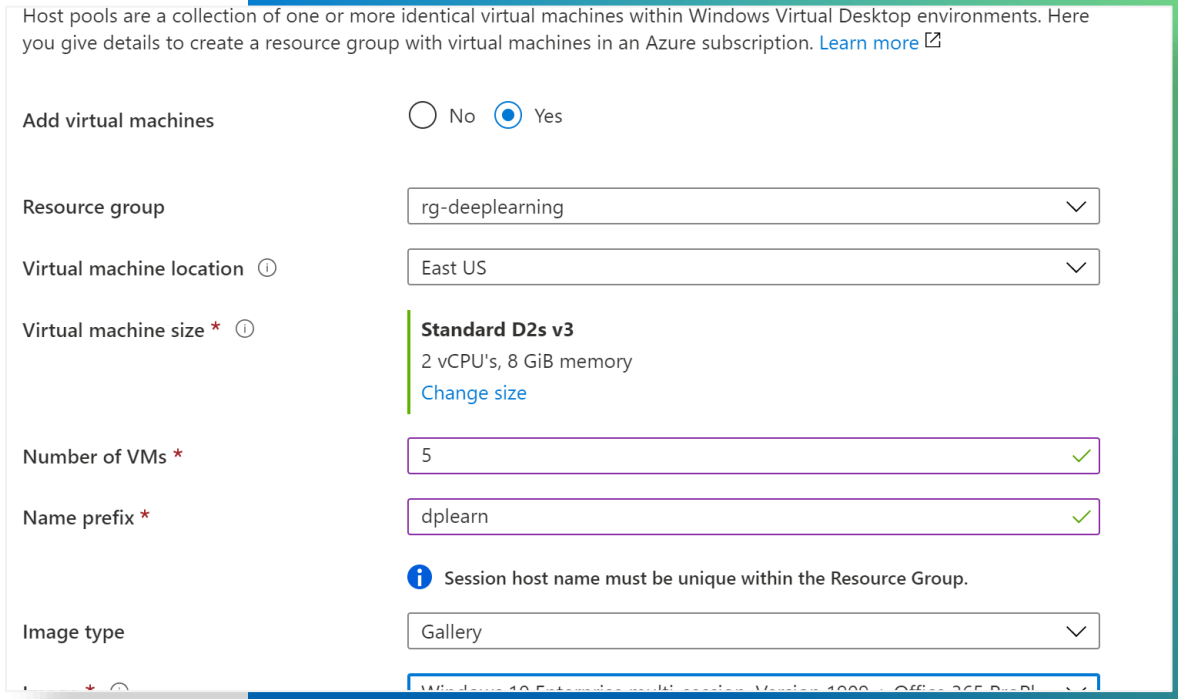
Virtual Desktop Infrastructure (VDI) modernization

Migrate existing VDI workloads to Azure using Azure Local

Azure Virtual Desktop Feature details

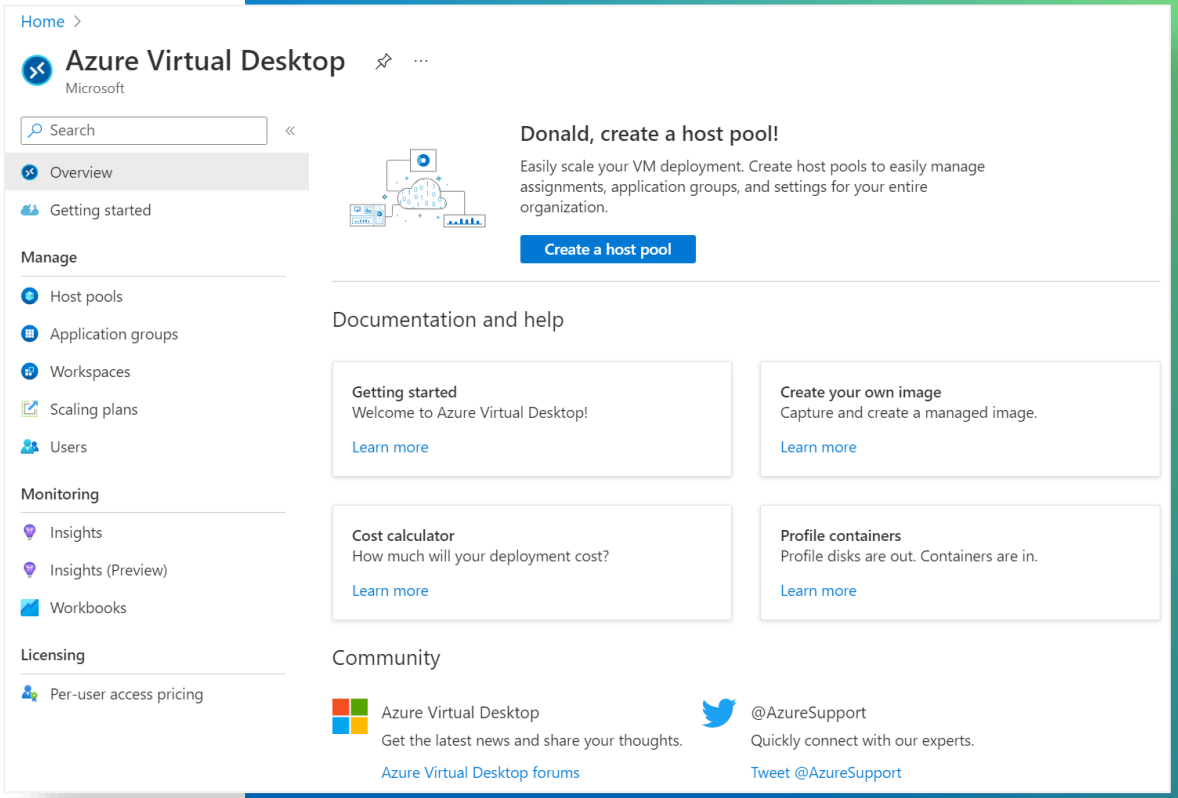
Azure Virtual Desktop simplifies VDI management

- Microsoft and Azure manage the entire infrastructure for you.
- Focus only on the users, apps, and OS images you need to use.
- Use Azure portal or automate deployment using ARM template.
- Easily scale by adding any number of hosts to a host pool.
- Use built-in monitoring with Azure Monitor and Log Analytics.



Configuring Azure Virtual Desktop

Azure Virtual Desktop provides a simple, clean interface for configuring and customizing a VDI environment using Azure portal

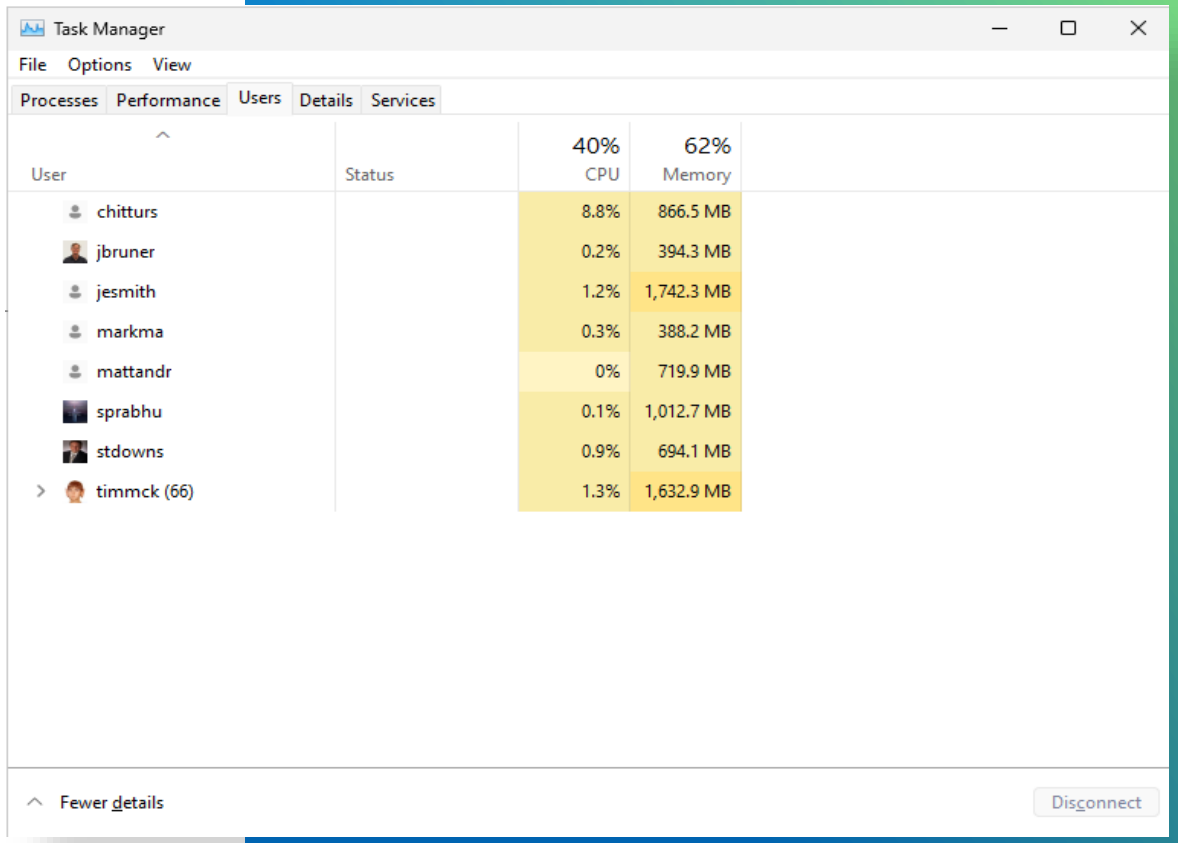


Multi-session is an exclusive feature for Azure Virtual Desktop and drives cost efficiency without impacting user experience

Multi-session allows administrators to place multiple users in the same virtual machine (VM).

Azure Virtual Desktop multi-session can share resources across users and place many users into the VM.

Multi-session is available with pooled desktops and requires FSLogix for user profile roaming.



Azure Virtual Desktop host sizing recommendations (multi-session and single session)

Multi-session recommendations

The following table lists the maximum suggested number of users per virtual central processing unit (vCPU) and the minimum virtual machine (VM) configuration for each workload. These recommendations are based on Remote Desktop workloads.

Workload type	Maximum users per vCPU	vCPU/RAM/OS storage minimum	Example Azure instances	Profile container storage minimum
Light	6	2 vCPUs, 8 GB RAM, 16 GB storage	D2s_v3, F2s_v2	30 GB
Medium	4	4 vCPUs, 16 GB RAM, 32 GB storage	D4s_v3, F4s_v2	30 GB
Heavy	2	4 vCPUs, 16 GB RAM, 32 GB storage	D4s_v3, F4s_v2	30 GB
Power	1	6 vCPUs, 56 GB RAM, 340 GB storage	D4s_v3, F4s_v2, NV6	30 GB

Single-session/personal desktop recommendations

- Sizing largely dependent on the workload, apps deployed, and user type.
- We recommend at least two physical CPU cores per VM (typically four vCPUs with hyperthreading).
- If you need more specific VM sizing recommendations for single-session scenarios, check with your software vendors specific to your workload .
- VM sizing for single-session VMs will likely align with physical device guidelines .
- Use other tools to get granular level sizing and scaling recommendations.

Azure Virtual Desktop GPU use cases

GPUs for Visualization – Architects, designers, graphic artists

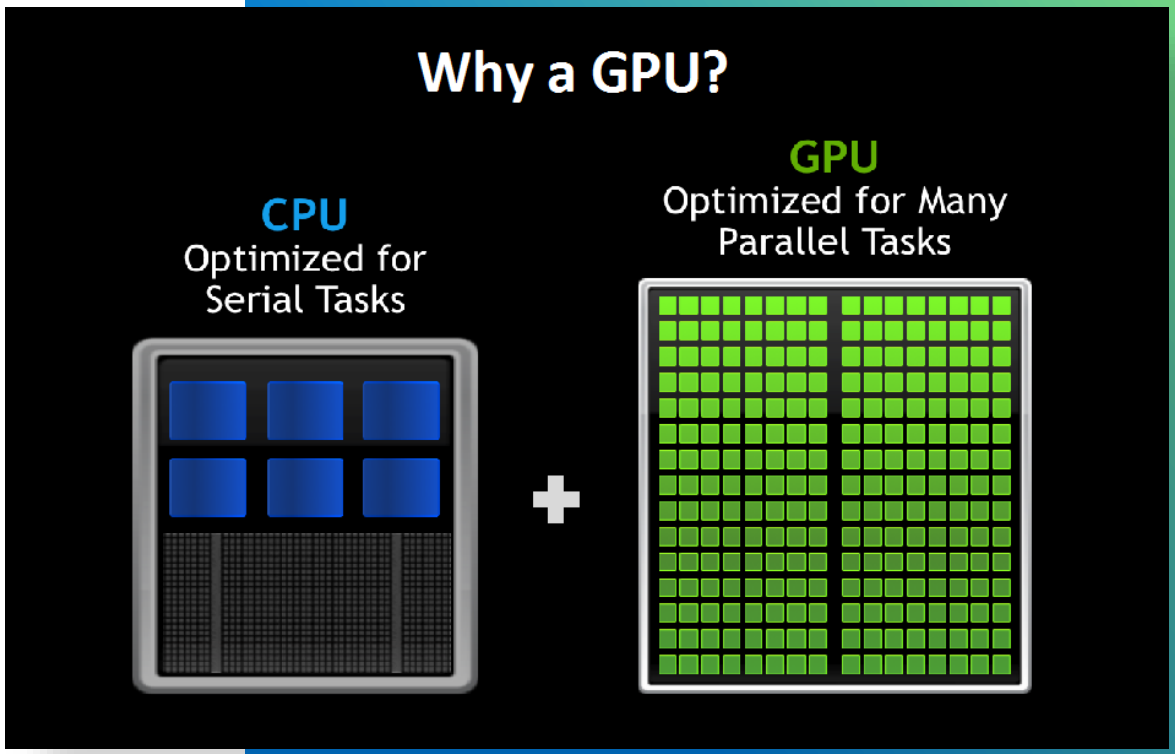
CAD/CAE

GPU for HPC – Developers, scientists

Supercomputers for high-end simulations

GPU for AI – Data scientists

Supercomputing training deep learning models



Azure Virtual Desktop for Azure Local GPU options

Azure Local supports GPUs with DDA (passthrough) and GPU_P (partitioning).

Use GPU partitioning with NVIDIA GPUs to unlock graphic capabilities for your applications and optimize for cost and performance

Use Windows Admin Center to manage your GPU resources and assign them to HCI session hosts

The following GPUs support GPU partitioning:

NVIDIA A2

NVIDIA A10

NVIDIA A16

NVIDIA A40

NVIDIA L4

NVIDIA L40

NVIDIA L40S

Refer to Partition and share GPUs for latest information. Also refer to HCI Catalog for GPU information on supported hardware solutions.

User profile management with FSLogix

Persistent desktop experience

Users can customize their desktop and have a persistent experience every time they sign in.

Faster login and application launch

Optimized profile containers have much shorter launch times than roaming profiles and folder redirection.

Multiple storage options available

Store profile containers in Azure files/Azure NetApp Files/file server clusters.

For Azure Local, consider file server for low latency.

Migrate existing user profiles

Perform mass conversions of user profiles from various types to FSLogix-based profile containers at scale.

Apps with FSLogix & MSIX

Minimize number of master images by creating a single image with all applications

Why App Masking with FSLogix?

- Excellent app compatibility with no packaging, sequencing, backend infrastructure, or virtualization
- Control app licensing costs by limiting access to specific users
- Reduce the amount of host pools

Why MSIX?

- Single format for physical and virtual environments
- Doesn’t require packaging to be delivered
- Clean install/uninstall
- Secured by default
- Optimized storage and network bandwidth

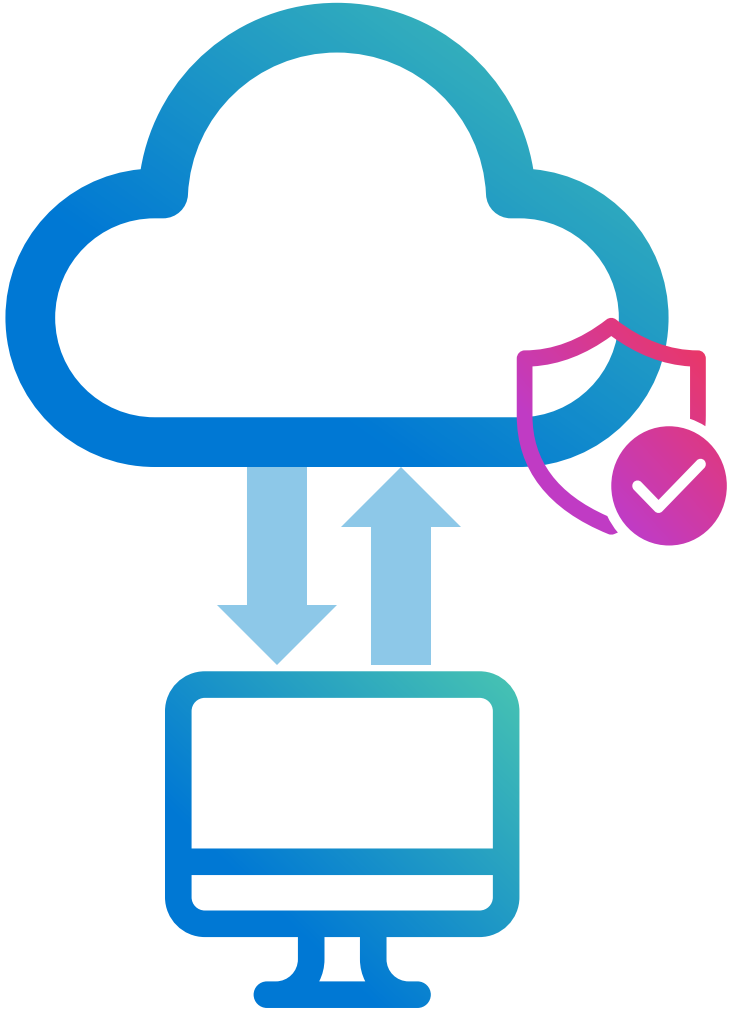
Why MSIX app attach?

- Dynamic application delivery
- Only authorized users can see or access apps running on multiple user instances
- MSIX apps behave like natively installed apps

Azure Virtual Desktop: Remote Desktop Protocol (RDP)

RDP is a collection of services that streams from the cloud to a local client.

RDP supports various scenarios across connection reliability, remote content streaming, local input & device redirections (USB, mouse, location, etc.), media streaming optimizations, security features (single sign-on, passwordless authentication, watermarking, etc.) and more.



Connection performance – RDP Shortpath

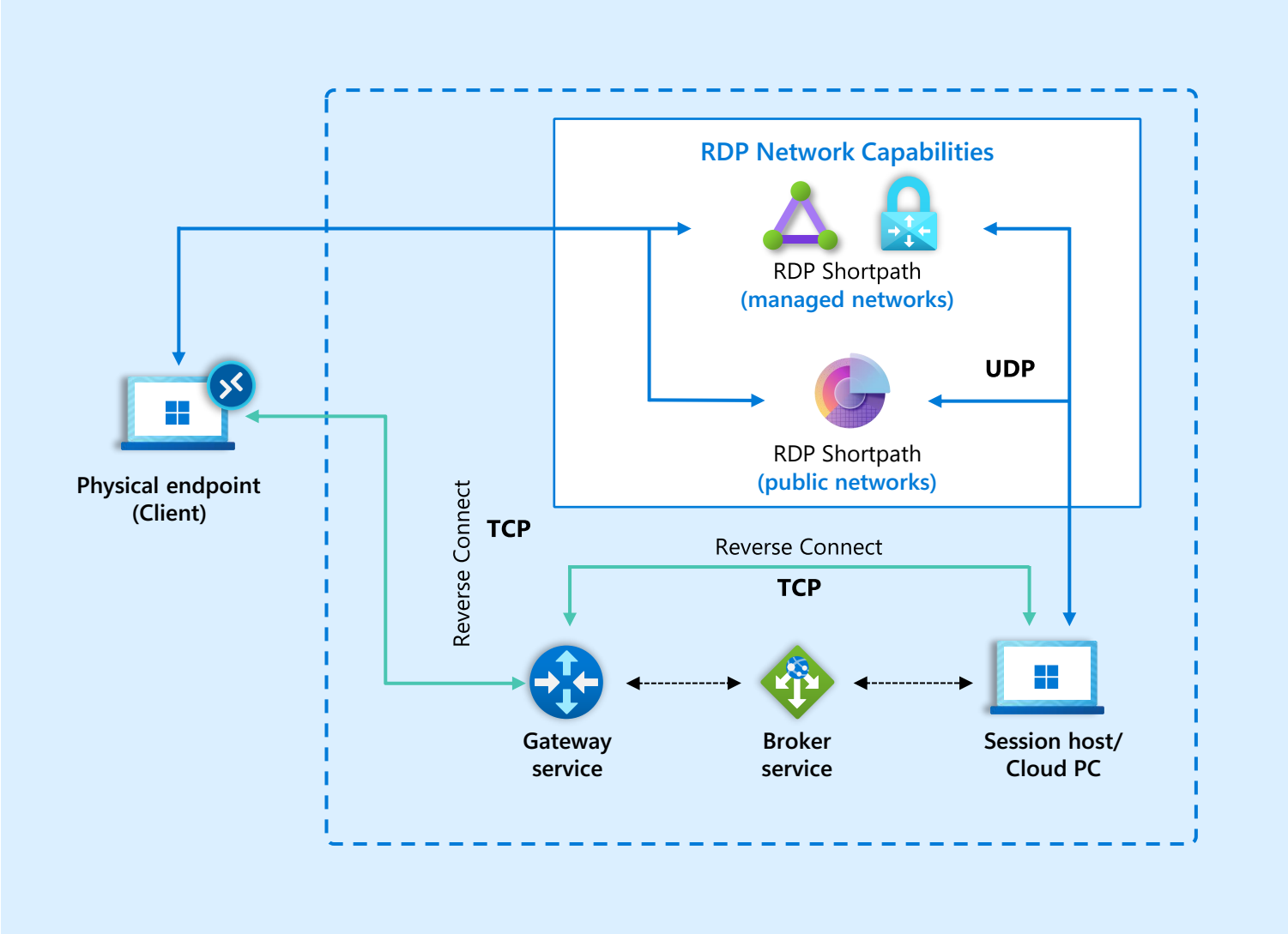
Connection performance is a collection of **protocol transport improvements** that fit under the umbrella of the evolved RDP experience.

RDP Shortpath establishes **reliable UDP-based transport** with the goal of improving the **connection reliability and reducing overall latency**.

Previously all connections were made via TCP (reverse connect) which allowed retransmission of packets at the cost of latency.

RDP Shortpath ensures that RDP connections have **high connectivity** and **lower latency than TCP** based connections.

[RDP Shortpath - Azure Virtual Desktop | Microsoft Learn]

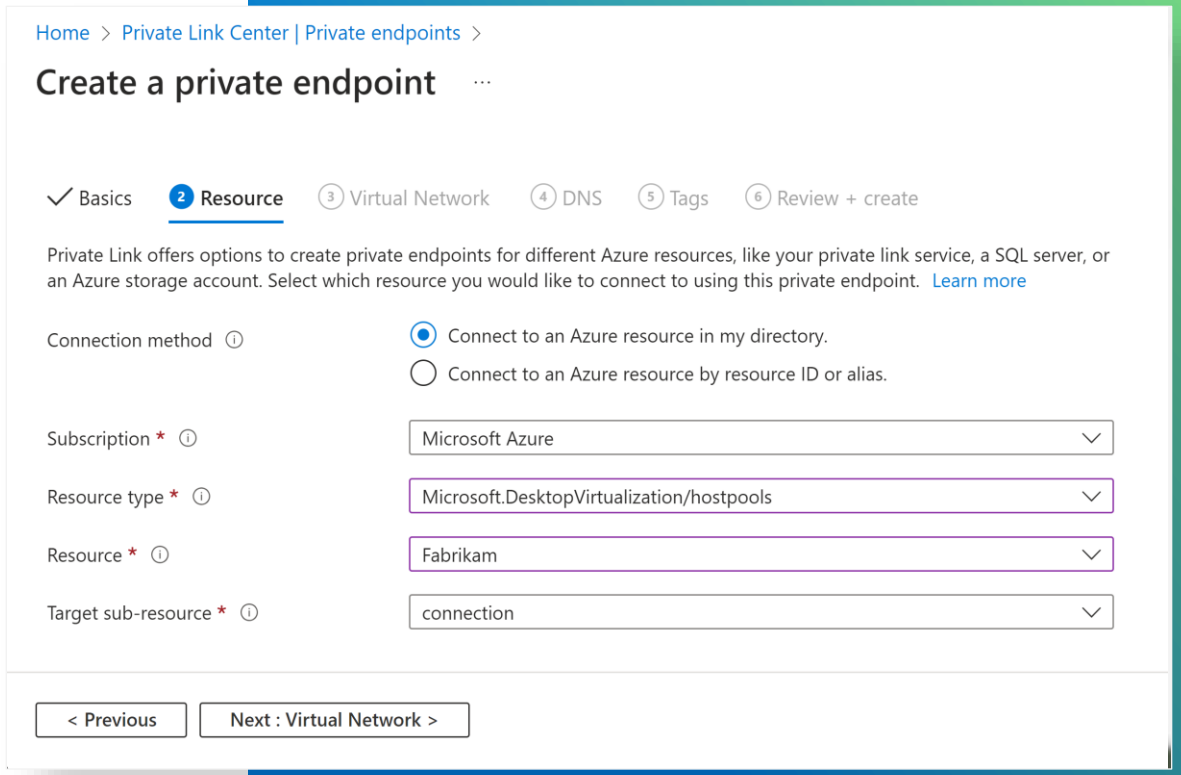


Azure Private Link

Private Link for Azure Virtual Desktop allows users to establish secure connections to remote resources by using private endpoints.

Private Link gives customers added security, allowing access to remote resources via private endpoints within the protected Microsoft Backbone network.

Follow these steps to [configure Private Link for Azure Virtual Desktop (learn.microsoft.com/azure/virtual-desktop/private-link-setup)]



Watermarking

Watermarking support enables QR codes which are displayed on the session desktop.

It is a deterrent, preventing sensitive information from being captured and shared on Azure Virtual Desktop client endpoints.

Download administrative templates:

- Enable Group Policy (Watermark, Screen Cap Protection)
- Scan the QR code to show the Activity ID GUID
- Admin uses log analytics WVDConnection table to investigate the image origination

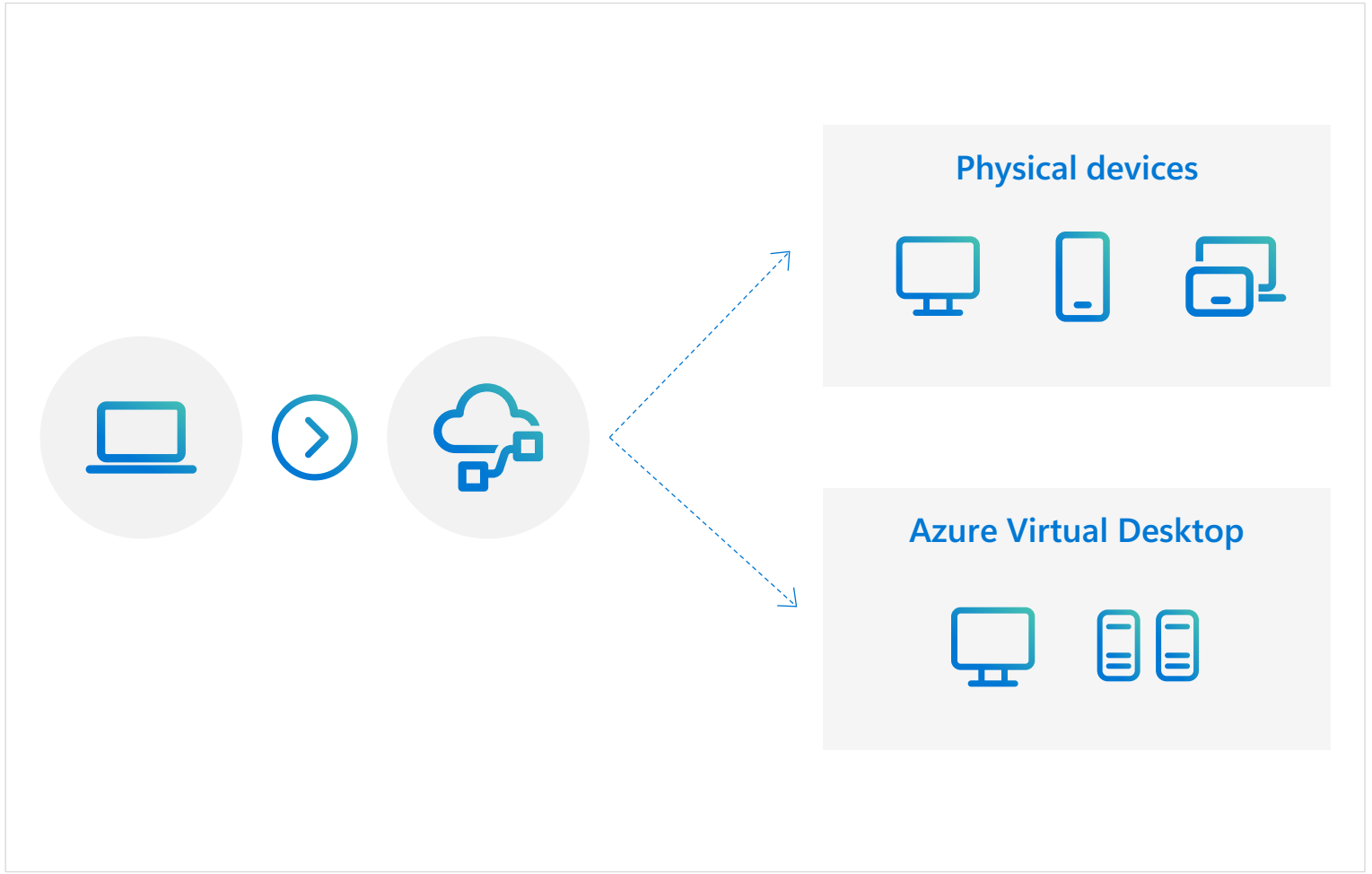
Microsoft Intune support for multi-session

Manage both virtual and physical assets

Microsoft Intune gives admins a single tool to manage physical devices and virtual desktops integrated with Azure Virtual Desktop.

Windows 11 and 10 multi-session device configuration is generally available:

- Enroll Azure Virtual Machines in Microsoft Intune
- Manage using the settings catalog
- Use Microsoft 365 security features such as Conditional Access.



Azure Virtual Desktop Insights

- Provides native monitoring for Azure Virtual Desktop deployments.
- Allows IT administrators and other users to understand the user experience and diagnostic output in their environment.
- Provides visibility into performance characteristics of Azure Virtual Desktop without requiring an investment in third-party monitoring software.
- Exposes diagnostic output from Log Analytics that would otherwise require manual querying or data extraction.