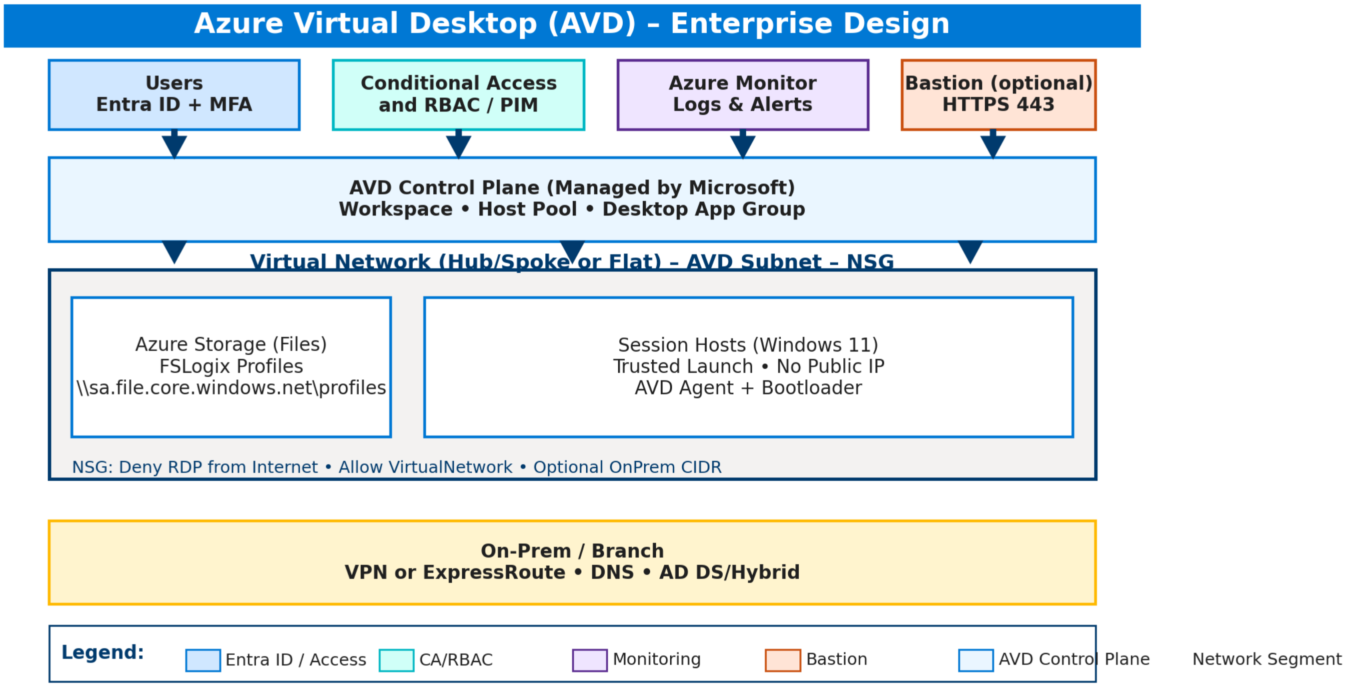
Azure Virtual Desktop (AVD) – Architecture Guide

Clean, secure, and repeatable design for production

Date: November 05, 2025


Azure Virtual Desktop (AVD) – Enterprise Design
Users
Entra ID + MFA
Conditional Access
and RBAC / PIM
Azure Monitor
Logs & Alerts
Bastion (optional)
HTTPS 443
AVD Control Plane (Managed by Microsoft)
Workspace • Host Pool • Desktop App Group
Virtual Network (Hub/Spoke or Flat) – AVD Subnet – NSG
Azure Storage (Files)
FSLogix Profiles
\\sa.file.core.windows.net\profiles
Session Hosts (Windows 11)
Trusted Launch • No Public IP
AVD Agent + Bootloader
NSG: Deny RDP from Internet • Allow VirtualNetwork • Optional OnPrem CIDR
On-Prem / Branch
VPN or ExpressRoute • DNS • AD DS/Hybrid
Legend:
Entra ID / Access
CA/RBAC
Monitoring
Bastion
AVD Control Plane
Network Segment

What we are building

- Identity is Entra ID with MFA. Access is controlled by Conditional Access and RBAC.
- AVD objects: one Workspace, a pooled Host Pool, and a Desktop App Group linked to the workspace.
- Session hosts are Windows 11. We use Trusted Launch, no public IPs, and the AVD agent/bootloader to join.
- Profiles go to Azure Files with FSLogix. We enforce TLS 1.2 and use storage keys at build time.
- Networking is a dedicated VNet and subnet with an NSG: block Internet RDP, allow VNet, and optionally allow a specific on■prem CIDR.
- Optional: Azure Bastion for just■in■time admin (HTTPS only).

Security stance

- Zero Trust posture: no inbound RDP from the Internet, brokered access only.
- Strong identity: MFA + Conditional Access + least■privilege RBAC.
- Trusted Launch (Secure Boot + vTPM) on the VMs.
- All profile traffic is encrypted; storage access is bootstrapped securely.
- Everything is observable: integrate with Azure Monitor for logs and alerts.

How the run works

1. Load Az modules and connect.
2. Pick subscriptions, host count (1–10), VM size.
3. Resolve region + image and check quota for the VM family.
4. Create or reuse RG, VNet/Subnet, and NSG rules.
5. Provision Azure Files share for FSLogix (profiles).
6. Create Host Pool, Desktop App Group, and Workspace; link DAG to the workspace.
7. Generate the registration token and deploy session hosts (no public IP, Trusted Launch).
8. Install AVD agent/bootloader, configure FSLogix, and optionally assign RBAC for users.

Network ports

Direction	Source	Destination	Port	Why
Inbound	Users	AVD Broker	443	User connections over HTTPS
Inbound	Azure control	Control plane	443	Azure platform operations
Outbound	Session hosts	Azure Files	445 / 443	FSLogix profile access