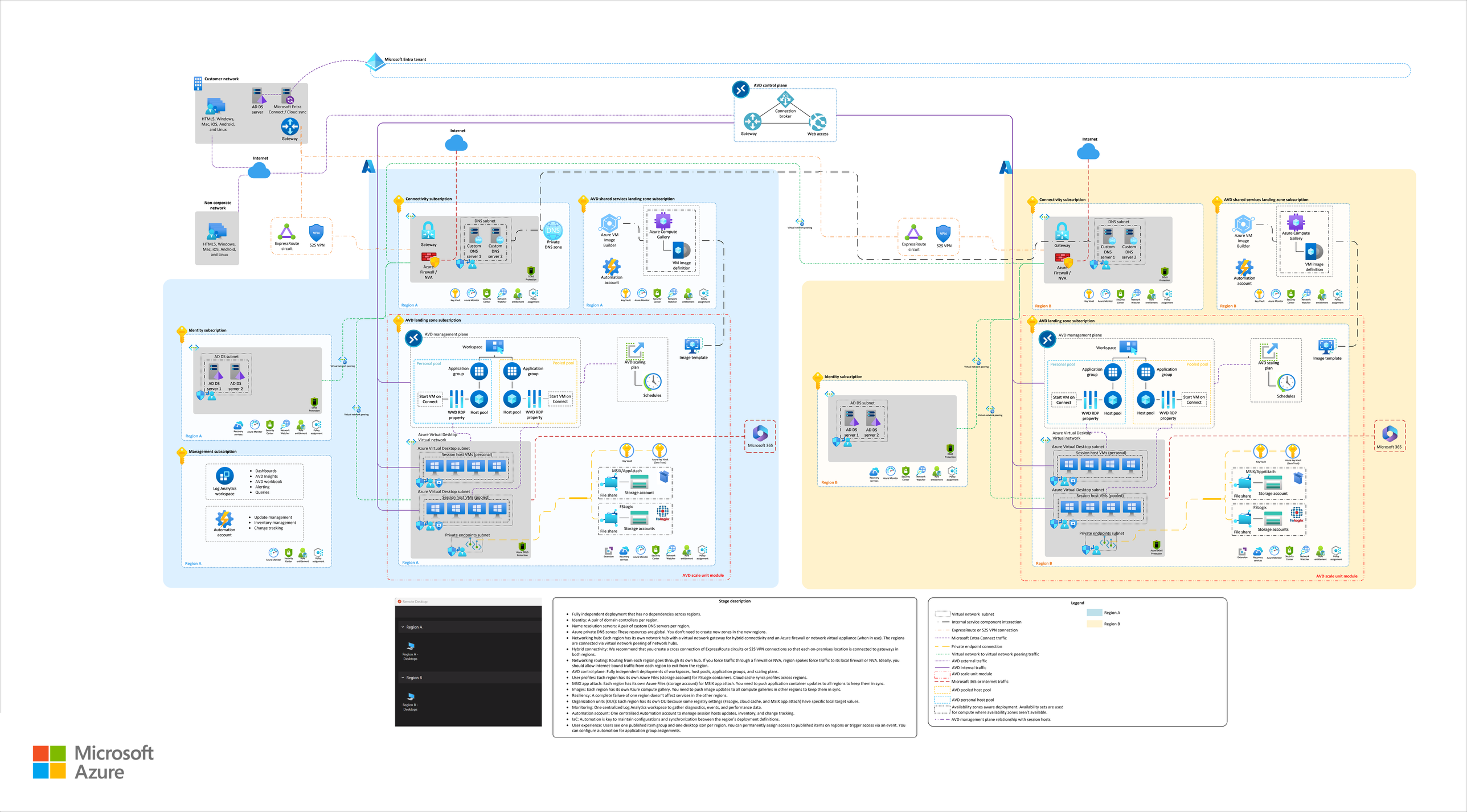

Stage description

- Fully independent deployment that has no dependencies across regions.
- Identity: A pair of domain controllers per region.
- Name resolution servers: A pair of custom DNS servers per region.
- Azure private DNS zones: These resources are global. You don't need to create new zones in the new regions.
- Networking hub: Each region has its own network hub with a virtual network gateway for hybrid connectivity and an Azure firewall or network virtual appliance (when in use). The regions are connected via virtual network peering of network hubs.
- Hybrid connectivity: We recommend that you create a cross connection of ExpressRoute circuits or S2S VPN connections so that each on-premises location is connected to gateways in both regions.
- Networking routing: Routing from each region goes through its own hub. If you force traffic through a firewall or NVA, region spokes force traffic to its local firewall or NVA. Ideally, you should allow internet-bound traffic from each region to exit from the region.
- AVD control plane: Fully independent deployments of workspaces, host pools, application groups, and scaling plans.
- User profiles: Each region has its own Azure Files (storage account) for FSLogix containers. Cloud cache syncs profiles across regions.
- MSIX app attach: Each region has its own Azure Files (storage account) for MSIX app attach. You need to push application container updates to all regions to keep them in sync.
- Images: Each region has its own Azure compute gallery. You need to push image updates to all compute galleries in other regions to keep them in sync.
- Resiliency: A complete failure of one region doesn't affect services in the other regions.
- Organization units (OUs): Each region has its own OU because some registry settings (FSLogix, cloud cache, and MSIX app attach) have specific local target values.
- Monitoring: One centralized Log Analytics workspace to gather diagnostics, events, and performance data.
- Automation account: One centralized Automation account to manage session hosts updates, inventory, and change tracking.
- IaC: Automation is key to maintain configurations and synchronization between the region's deployment definitions.
- User experience: Users see one published item group and one desktop icon per region. You can permanently assign access to published items on regions or trigger access via an event. You can configure automation for application group assignments.

Legend

- Virtual network subnet
- Internal service component interaction
- ExpressRoute or S2S VPN connection
- Microsoft Entra Connect traffic
- Private endpoint connection
- Virtual network to virtual network peering traffic
- AVD external traffic
- AVD internal traffic
- AVD scale unit module
- Microsoft 365 or internet traffic
- AVD pooled host pool
- AVD personal host pool
- Availability zones aware deployment. Availability sets are used for compute where availability zones aren't available.
- AVD management plane relationship with session hosts
- Region A
- Region B

Microsoft Azure