AZ-700 Exam Study Reference & Lab Summary

Architectural Mechanics of Azure SDN, Guest OS IP Hardcoding, and Active Directory Coexistence

This technical summary documents the foundational networking behaviors, troubleshooting workflows, and identity replication structures encountered during the deployment of a highly available Active Directory Domain Services (AD DS) infrastructure on an Azure Virtual Network (VNet). This knowledge directly maps to core competencies tested within the **AZ-700: Designing and Implementing Microsoft Azure Networking Solutions** examination.

1. Core Architectural Pillars (AZ-700 Exam Alignment)

Azure Software-Defined Networking (SDN) vs. Guest Operating System

In a cloud-native architecture, Azure manages internal IP addressing routing via its Software-Defined Networking (SDN) fabric rather than relying on traditional physical hardware or guest-level DHCP configurations. When an infrastructure engineer sets a virtual machine's IP address to **Static** within the Azure Portal, the configuration shift occurs on the Azure virtual switch port mapping, binding that specific IP address indefinitely to the network interface's virtual MAC address.

Because Azure emulates a static lease via its cloud DHCP engine, the guest Windows Server operating system continues to initialize its network interface stack using dynamic DHCP client discovery. This creates a state where the guest OS remains fully functional, stable, and correctly bound to its allocated address without manual internal intervention.

The Risk of In-Guest IP Hardcoding Mismatches

A critical operational failure occurs if an engineer manually configures static TCP/IPv4 properties inside the Windows Guest OS while the underlying Azure fabric remains set to **Dynamic**. When the in-guest IP properties are manually altered, the active routing table inside the OS memory space is modified. If this address drifts from or breaks communication with the expected Azure fabric subnet gateway (***172.16.0.1***), the stateful connection drops. Because Azure Security Rules and SDN layers enforce policy at the virtual NIC level, an internal mismatch completely invalidates Remote Desktop Protocol (RDP) traffic channels, leading to a total remote lockout.

> **AZ-700 Architectural Axiom:** Always lock the IP resource state to **Static** within the Azure Portal fabric *before* mirroring or hardcoding those identical IP constraints within the guest Windows operating system properties. When both parameters match, communication remains seamless.

2. Out-of-Band Disaster Recovery Workflows

When in-guest networking properties corrupt and sever standard administrative planes (RDP/SSH), Azure provides dedicated out-of-band management vectors that bypass the OS network interface stack entirely:

1. **Azure VM Reset Access Extension:** Injects configuration scripts directly via the Azure Virtual Machine Guest Agent. This background mechanism allows administrators to force-reset administrative passwords, create fresh administrative credentials, or re-initialize broken RDP listeners from the outside portal without internal OS visual validation.
2. **Azure Serial Console (SAC Interface):** Connects a virtual terminal session directly into the virtual motherboard's COM1 serial port. This completely bypasses RDP dependency, enabling access to a raw Command Prompt channel even if the operating system's network adapter is fully un-bound or misconfigured.

The Core Network Interface Recovery Script

To drop the guest operating system's network interface back to standard behavior so that it re-synchronizes seamlessly with the external Azure SDN fabric, the following sequenced netsh commands are executed via the Special Administration Console (SAC) terminal:

```
netsh interface ip set address name="Ethernet" source=dhcp
netsh interface ip set dns name="Ethernet" source=dhcp
ipconfig /renew
```

3. The Coexistence Multi-Master Identity Architecture

When two separate Windows Server instances are promoted to Domain Controllers within the exact same VNet subnet (***172.16.0.4*** and ***172.16.0.5***), they form a load-sharing **Multi-Master Peer Configuration**. Active Directory eliminates the single point of failure inherent to primary/secondary architectures. However, clear boundaries exist defining what data synchronizes across the cloud network fabric and what remains isolated locally to the individual node.

What is Cloned (Synchronized Automatically)

The Active Directory engine leverages the **NTDS Database** and the **SYSVOL File System Replication Structure** to maintain absolute uniformity across all nodes within the forest boundary:

Replicated Component	Technical Mechanism & Exam Context
NTDS Security Database (ntds.dit)	All security principals (User Accounts, Groups, Computer objects, Managed Service Accounts) and password hashes are synchronized bi-directionally via the NTDS Replication Engine.
Group Policy Objects (GPOs)	Active Directory policy sets, administrative templates, logon/logoff scripts, and registry enforcement mappings live within the `SYSVOL` share and replicate natively.
Active Directory-Integrated DNS	DNS zones, service location (SRV) records, host records, and pointer records are stored directly within the NTDS database structure, ensuring lookup tables are fully mirrored.
Global Catalog Metadata	Forest-wide schema definitions, configuration maps, and domain indexing are universally maintained on both peers for rapid, localized authentication.

What is NOT Cloned (Must be Managed Individually)

Active Directory does not replicate standalone system server roles, application binaries, or localized web assets. The boundaries of independent infrastructure include:

Isolated Component	Technical Operational Reality
Web Server Engine & Roles (IIS)	Internet Information Services (IIS) is an independent local server role. Installing IIS on Server 1 does not install or trigger it on Server 2. Each machine handles its own application services.
Web Application Content	The physical file structure holding website assets (located at `C:\inetpub\wwwroot\`) is fully isolated. If an index page is created on Server 1, it will not appear on Server 2 unless an external storage layer or sync utility is introduced.
Local Storage File Systems	Local disk volumes, administrative file shares, and block-level updates are entirely native to the specific virtual machine instance.
In-Guest Hardware Binding Mappings	Individual OS network configuration bindings, custom registry keys for hardware performance, and system event logs remain localized to that specific machine instance.

> **High Availability Application Note:** To make the web application layer as resilient as the Active Directory layer, an engineer must install IIS on both servers, copy identical web assets to both nodes, and place an **Azure Load Balancer** or **Azure Application Gateway** in front of the pair to distribute client traffic between IPs ***172.16.0.4*** and ***172.16.0.5***.

4. Infrastructure-as-Code (Bicep / ARM) Integration

Azure Resource Manager (ARM) JSON and Bicep files operate strictly at the **Azure Fabric Control Plane** layer. They are ideal for rapid automation, deployment tearing-down, and cost containment. However, engineers must account for the following cloud-lifecycle behaviors:

- **What Bicep Recreates Perfectly:** The virtual hardware shell, including Virtual Network topologies, Subnets, Network Security Groups (NSGs), Network Interfaces (NICs), Public IP Resource Objects, and fresh, unconfigured Windows Server OS Managed Disks.
- **What Bicep Misses (The OS Boundary):** Bicep cannot see or restore data that resides within the guest Windows kernel. It does not know the server was promoted to a Domain Controller, nor does it retain the `stevepedwards.local` identity database or local guest TCP/IP modifications.
- **Cost Optimization Strategy:** For active identity labs, deleting resources entirely requires re-running the AD promotion wizards upon redeployment. To achieve zero compute costs while perfectly preserving the Active Directory configuration and database state, the virtual machines should be transitioned to a **Stopped (Deallocated)** status within the portal, leaving only the inexpensive managed storage disks intact overnight.