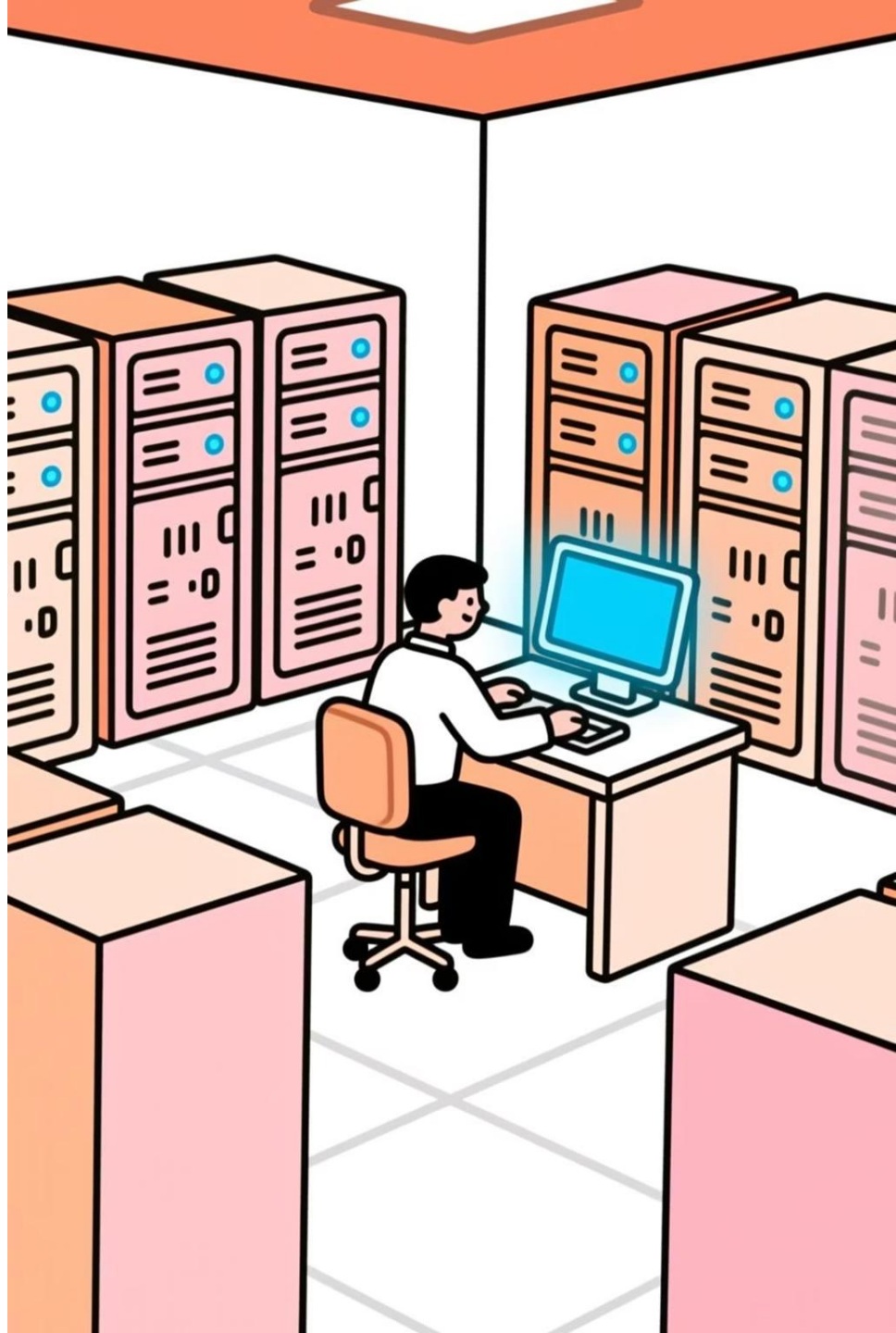
Host & Server Management: OS Installation, Active Directory Integration & Linux Server Administration

A comprehensive guide to enterprise server infrastructure management, covering operating system deployment, identity integration, and system administration best practices for modern IT environments.

Facilitators: Abdallah Ibrahim Nyero, Hajarah Ali Namuwaya, Dr. Ali Mwase, and Charles Kikwanga



What Is Host & Server Management?

- Involves **installation, configuration, and maintenance** of server operating systems.
- Ensures **availability, performance, and security** of networked systems.
- Covers both **on-premises** and **cloud environments (Azure, AWS)**.

Operating System Installation & Configuration

- Install OS (Windows Server, Ubuntu, CentOS).
- Configure **network interfaces**, **storage partitions**, and **updates**.
- Apply **security patches** and **system hardening**.
- Manage **roles and features** (DNS, DHCP, IIS).

What is Active Directory (AD)?

Active Directory is Microsoft's directory service for Windows domain networks, providing a centralized database of objects representing network resources:

Core Components

Domain Controllers: Servers that host the AD database

Forest & Domains: Hierarchical structure of resources

Schema: Defines object types and attributes

Global Catalog: Contains partial information about all objects

Key Services

Authentication: Kerberos and NTLM protocols

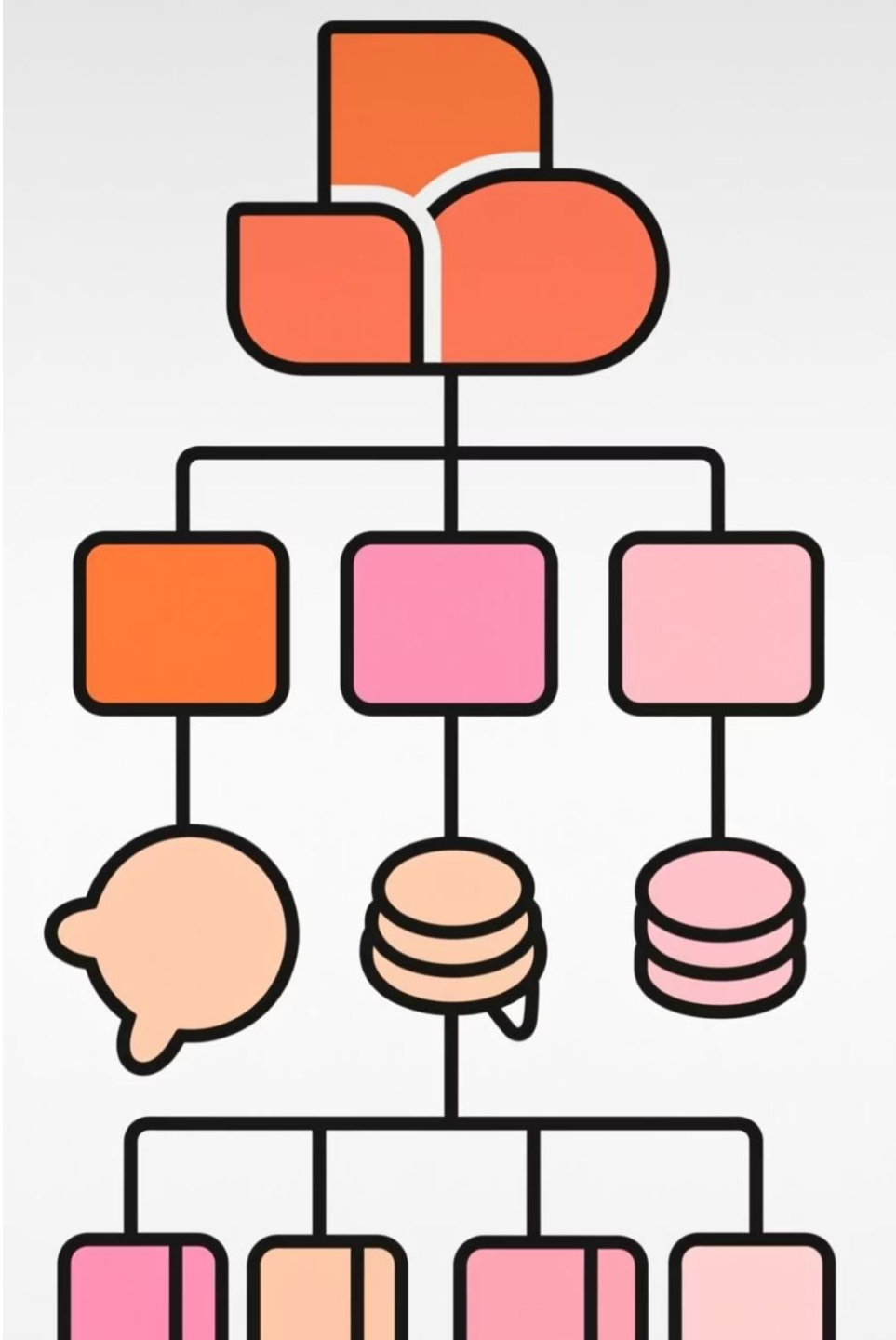
Directory: LDAP-based object queries and management

Policy: Group Policy for centralized configuration

Replication: Multi-master replication between DCs

Management Tools

- **Active Directory Users & Computers**
- **Group Policy Management Console**
- **PowerShell with AD module**
- Active Directory Administrative Center



Azure Active Directory Overview

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, forming the backbone of Microsoft 365 and serving as the authentication layer for cloud applications:

Identity as a Service (IDaaS): Cloud-native user and group management

Multi-tenant architecture: Securely isolates organizations

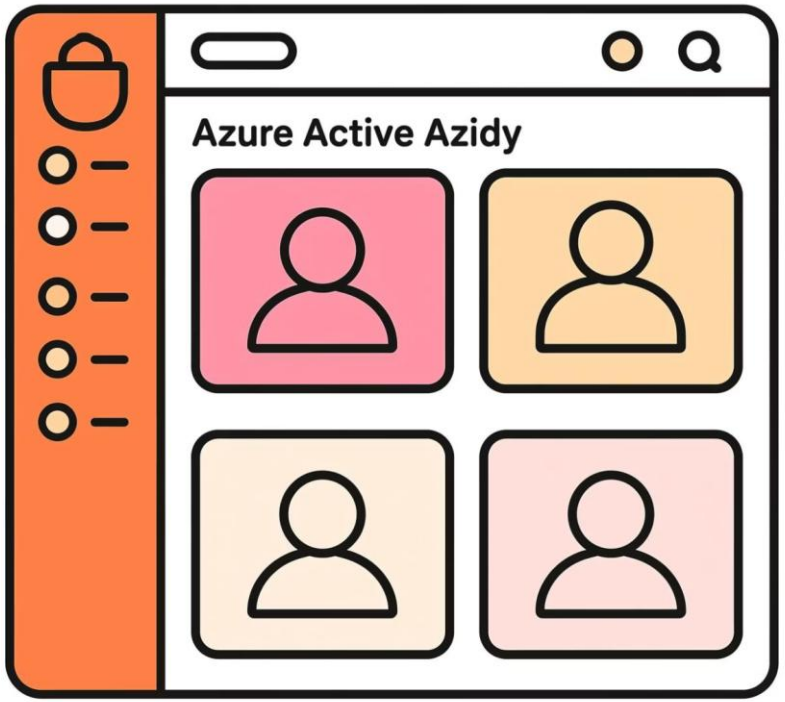
Modern protocols: OAuth 2.0, OpenID Connect, and SAML

Conditional Access: Risk-based authentication policies

B2B/B2C capabilities: External user collaboration

Hybrid Identity: Integration with on-premises AD

Key Difference: Unlike traditional AD, Azure AD is designed as a web-based service for modern applications rather than for managing domain-joined workstations.



Azure AD Connect synchronizes identities between on-premises Active Directory and Azure AD, enabling hybrid identity scenarios across cloud and on-premises resources.

Why Integrate Linux Servers with AD?

Unified Identity Management

Maintain a single source of truth for user accounts across Windows and Linux environments. When employees join or leave, a single change in AD automatically propagates to all integrated systems.

Simplified Access Control

Leverage AD groups to grant and revoke access to Linux systems. Administrators can define role-based access using familiar AD tools, without managing separate user databases on each server.

Enhanced Security

Enforce consistent password policies, multi-factor authentication, and account lockout settings across all platforms. Centralized auditing provides visibility into authentication attempts across the environment.

Single Sign-On Experience

Users can access Linux resources using their AD credentials without re-authentication. Kerberos tickets obtained on Windows workstations can be used to access integrated Linux servers seamlessly.

Challenges of Linux-AD Integration

Identity Model Differences

Linux and Active Directory use fundamentally different approaches to identify users and groups:

Linux: Numeric UIDs/GIDs with local files (/etc/passwd)

Active Directory: Security Identifiers (SIDs) in a distributed database

Challenge: Mapping between these two systems consistently

Protocol Complexity

- Kerberos configuration requires precise time synchronization
- LDAP queries need proper filtering and connection security
- Multiple moving parts can complicate troubleshooting

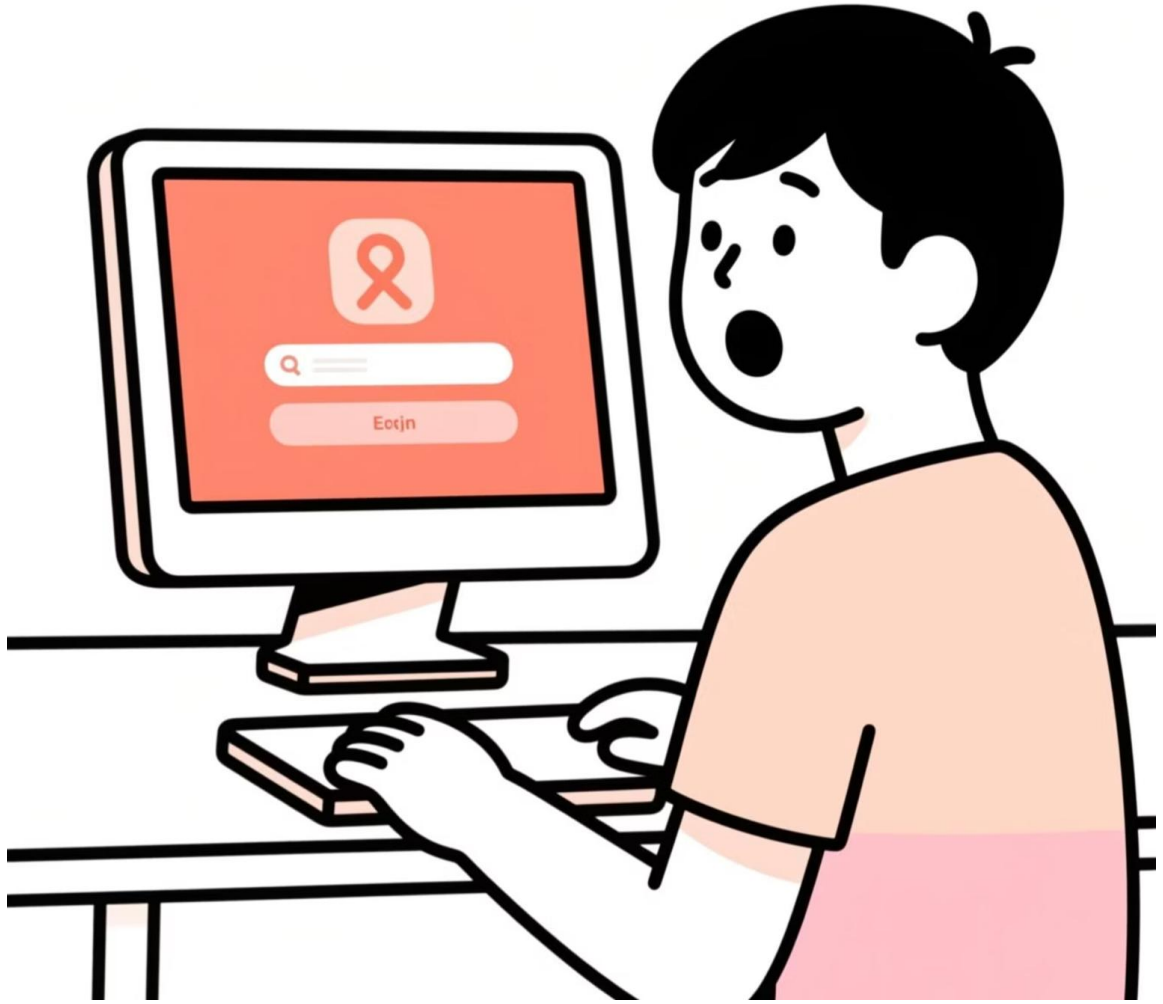
User Experience Considerations

Home directories: Must be created and managed for AD users

Shell access: Determining which AD users should have SSH access

Sudo privileges: Mapping AD groups to administrative access

Critical Point: Without careful planning, Linux-AD integration can lead to inconsistent user experiences and security gaps as users move between systems.



Tools for Linux-AD Integration

SSSD

System Security Services Daemon provides identity, authentication, and authorization services. It caches credentials for offline authentication and offers flexible ID mapping. SSSD is the modern, recommended approach for enterprise Linux distributions.

realmd

Simplifies domain discovery and joining process by automatically configuring underlying services like SSSD and Kerberos. It provides a unified interface across different Linux distributions for domain operations.

Samba & Winbind

Traditional integration method that excels at file sharing scenarios. Winbind handles the translation between Windows SIDs and Unix UIDs/GIDs. Still useful for specific use cases, especially those involving SMB file services.

Modern enterprise Linux deployments typically use SSSD with realmd for the most reliable integration experience. This combination offers the best performance, security, and maintainability for production environments.

Tools for Linux-AD Integration

SSSD

System Security Services Daemon provides identity, authentication, and authorization services. It caches credentials for offline authentication and offers flexible ID mapping. SSSD is the modern, recommended approach for enterprise Linux distributions.

realmd

Simplifies domain discovery and joining process by automatically configuring underlying services like SSSD and Kerberos. It provides a unified interface across different Linux distributions for domain operations.

Samba & Winbind

Traditional integration method that excels at file sharing scenarios. Winbind handles the translation between Windows SIDs and Unix UIDs/GIDs. Still useful for specific use cases, especially those involving SMB file services.

Modern enterprise Linux deployments typically use SSSD with realmd for the most reliable integration experience. This combination offers the best performance, security, and maintainability for production environments.

Step-by-Step: Joining a Linux Host to AD Using SSSD & realmd

Prepare the System

Ensure the system meets prerequisites:

```
# Set correct hostname and verify DNS resolutionhostnamectl set-hostname
srv01.example.comping -c3 example.comping -c3 dc01.example.com# Install required
packagesdnf install sssd realmd oddjob oddjob-mkhomedir adcli samba-common-tools
```

Join the Domain

Join the domain with administrative credentials:

```
# Join the domain (will prompt for password)realm join -U admin example.com#
Enable automatic home directory creationrealm permit --all
```

Discover the Domain

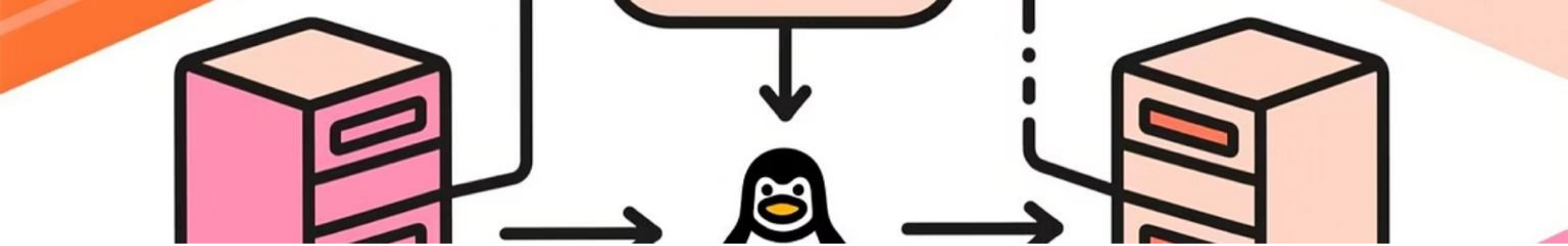
Verify domain discovery works correctly:

```
# Discover available realmsrealm discover example.com# This should return
information about the domain# including authentication servers and supported
interfaces
```

Verify Configuration

Test that authentication works properly:

```
# List domain informationrealm list# Test user lookupid user@example.com# Verify
SSSD is runningsystemctl status sssd
```



Integrating Linux Servers with Azure AD

Azure AD Domain Services (AAD DS)

Microsoft's managed domain service provides traditional AD capabilities in Azure:

- LDAP, Kerberos, and NTLM authentication
- Domain join for Linux VMs in Azure
- Similar configuration to on-premises AD integration

Hybrid Identity with Azure AD Connect

Synchronization between on-premises AD and Azure AD:

- Password hash synchronization or pass-through authentication
- Enables consistent identity across environments
- Supports conditional access policies

Direct Azure AD Integration

Modern authentication options for Linux:

- Azure AD login extension for Linux
- OAuth/OpenID Connect authentication
- Microsoft Authentication Libraries (MSAL)

Emerging Technology: Direct Azure AD integration for Linux is an evolving area with new capabilities being developed for cloud-native identity management scenarios.

Creating and Managing AD Users for Linux Services

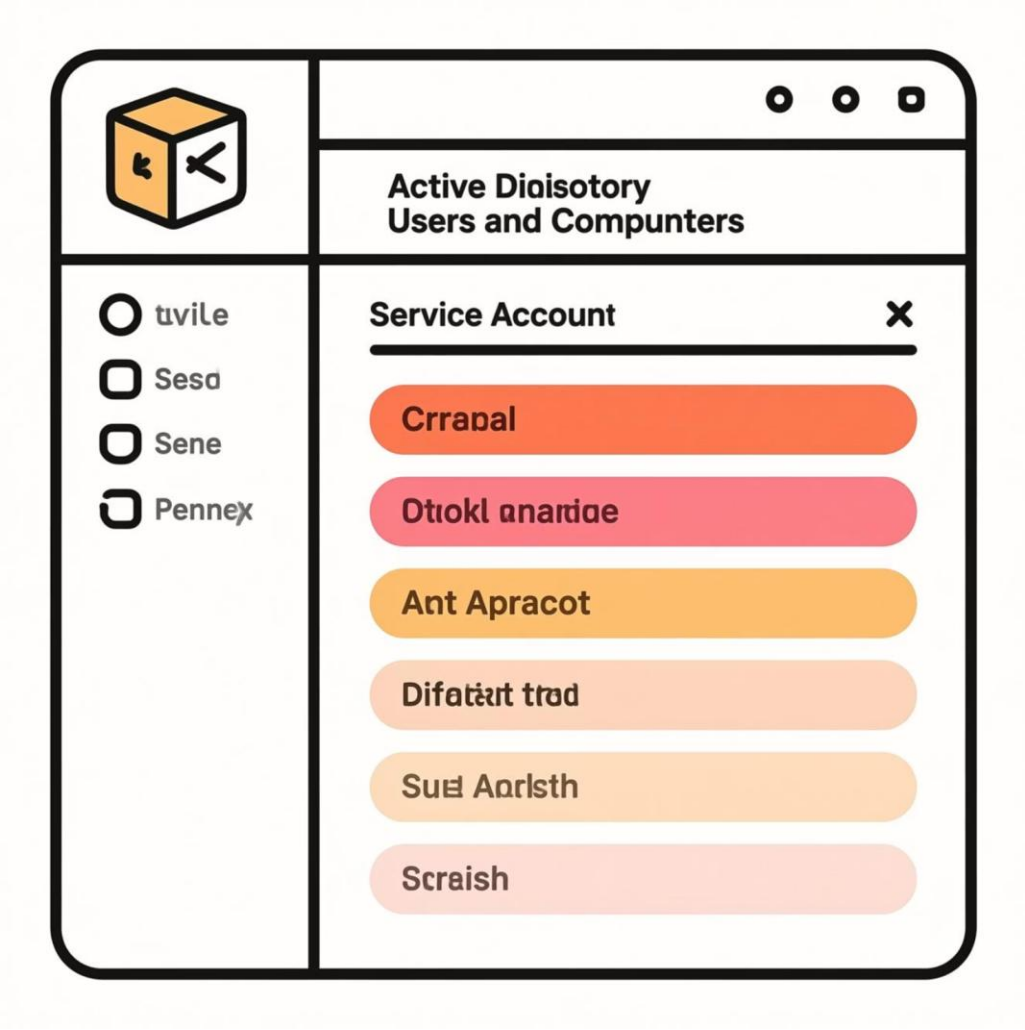
PowerShell Commands for Service Accounts

Creating service accounts for Linux applications requiring AD authentication:

```
# Create a new service account for SQL ServerNew-ADUser -Name "sql_service" -SamAccountName "sql_service" `  -UserPrincipalName "sql_service@example.com" `  -Path "OU=Service Accounts,DC=example,DC=com" `  -AccountPassword (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -Force) `  -Enabled $true -PasswordNeverExpires $true# Add required SPN for Kerberos authenticationsetspn -A MSSQLSvc/sqlserver.example.com:1433 sql_service
```

Linux-side Configuration

```
# Generate keytab for the service accountktutiladdent -password -p sql_service@EXAMPLE.COM -k 1 -e aes256-ctswkt /etc/sql_service.keytabquit# Set appropriate permissionschown mssql:mssql /etc/sql_service.keytabchmod 400 /etc/sql_service.keytab
```



Security Note: Always follow the principle of least privilege for service accounts. Grant only the permissions needed for the specific service, and use strong, unique passwords.

Service Principal Names (SPNs) are crucial for Kerberos authentication. They uniquely identify the

Troubleshooting Common AD Integration Issues

DNS Resolution Failures

Symptoms: `realm discover` fails, cannot find domain controllers

Troubleshooting:

Verify DNS settings: `cat /etc/resolv.conf`

Test DNS resolution: `nslookup _ldap._tcp.example.com`

Check SRV records: `dig _ldap._tcp.example.com SRV`

Solution: Configure proper DNS servers pointing to AD domain controllers

Time Synchronization Errors

Symptoms: Kerberos errors about clock skew, authentication failures

Troubleshooting:

Check time difference: `date; ssh dc01 date`

Verify chrony/NTP status: `chronyc tracking`

Look for Kerberos errors: `klist -e`

Solution: Configure chrony to sync with domain controllers

SSSD Cache Issues

Symptoms: Stale user information, group membership not updated

Troubleshooting:

Check SSSD logs: `tail -f /var/log/sssd/*.log`

Test user lookup: `getent passwd username@example.com`

Verify group membership: `id username@example.com`

Solution: Clear SSSD cache: `sss_cache -E` or restart SSSD

How AD Works

- User logs in → DC verifies credentials
- GPOs apply rules (passwords, software restrictions)
- Resources accessed based on roles and permissions

Azure Active Directory (Azure AD)
A **cloud-based identity and access management service** by Microsoft.

Functions:

- Manages users for **Microsoft 365, Azure, and other cloud apps**
- Supports **Single Sign-On (SSO)**
- Integrates with on-premises AD

Azure AD vs. Active Directory

Feature	Active Directory (AD DS)	Azure AD
Location	On-premises	Cloud-based
Authentication	Kerberos/NTLM	OAuth, SAML
Management	Domain Controller	Azure Portal
Use Case	Internal enterprise network	Cloud applications

Linux Server Administration

- **User management:** useradd, passwd, groups
- **File permissions:** chmod, chown, ls -l
- **Remote management:** SSH, scp
- **Service control:** systemctl start nginx, etc.