

Secure Hybrid Active Directory Accounts



Tim Warner

Microsoft Azure Solutions Architect

@TechTrainerTim TechTrainerTim.com



Overview



Configure password policies

Enable password block lists

Manage protected users

Manage account security on a Read-Only Domain Controller (RODC)

Harden domain controllers

Configure authentication policies silos



Windows Server 2022: Secure On-premises and Hybrid Infrastructure

Secure the Windows Server Operating System

Secure Hybrid Active Directory Accounts

Configure Hybrid Active Directory Account Security

Remediate Windows Server Security Issues with Azure Services

Secure Windows Server Networking

Secure Windows Server Storage



Password Policies and Protected Users



Password Policies

Group Policy

One password policy per domain

Originated from Windows NT domains

Reason for multi-domain forests

Microsoft recommends single-domain forests nowadays

Fine-grained

Separate password policies attached to AD groups

Precedence resolves conflicts when multiple policies apply to single user

Configure with Active Directory Administrative Center or Windows PowerShell



Azure AD Password Protection



Prevent password changes to weak passwords

Banned password lists:

Global: Microsoft-curated

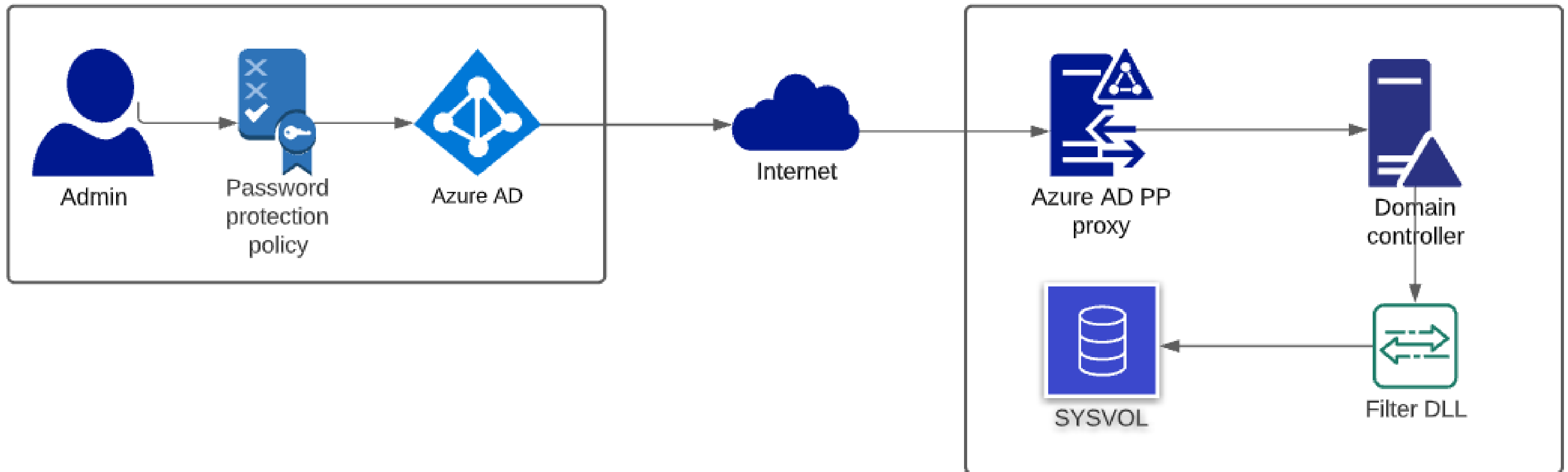
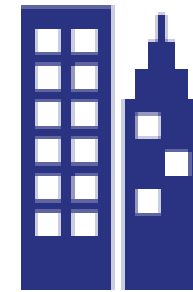
Custom: Administrator-defined

Free to use in cloud-only environments

**Azure AD Premium P1 or P2 license required
for hybrid scenarios**



Azure AD Password Protection



Protected Users

**Built-in domain
global security
group**

**Non-configurable
account protections**

Disable NTLM

**Disable Kerberos
caching**

**Disable
Kerberos/CredSSP
delegation**

**Don't use with
gMSAs or computer
accounts**



Demo



1

Password policy

Fine-grained password policy

Protected Users

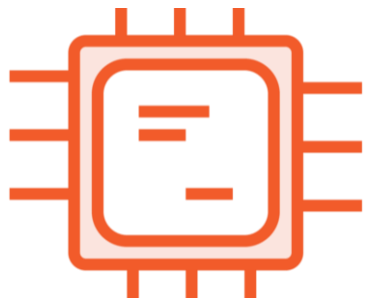
Azure AD Password Protection



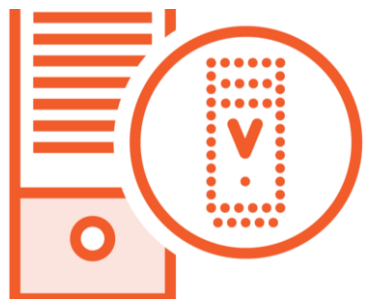
Harden AD DS Domain Controllers



Harden Domain Controllers



Secure the server hardware (TPM, UEFI, Secure Boot, BitLocker)



Enable Guarded Fabric and Shielded Hyper-V VMs



Deploy RODCs to smaller branch office locations



Run only trusted code with AppLocker or Defender App Control



Harden Read-Only Domain Controllers (RODCs)

Administrator Role Separation

Allowed/Denied RODC Password Replication Group

Strong DSRM password

Filtered Attribute Set (FAS)

Prepopulate password cache and airgap network



Authentication Policy Silos

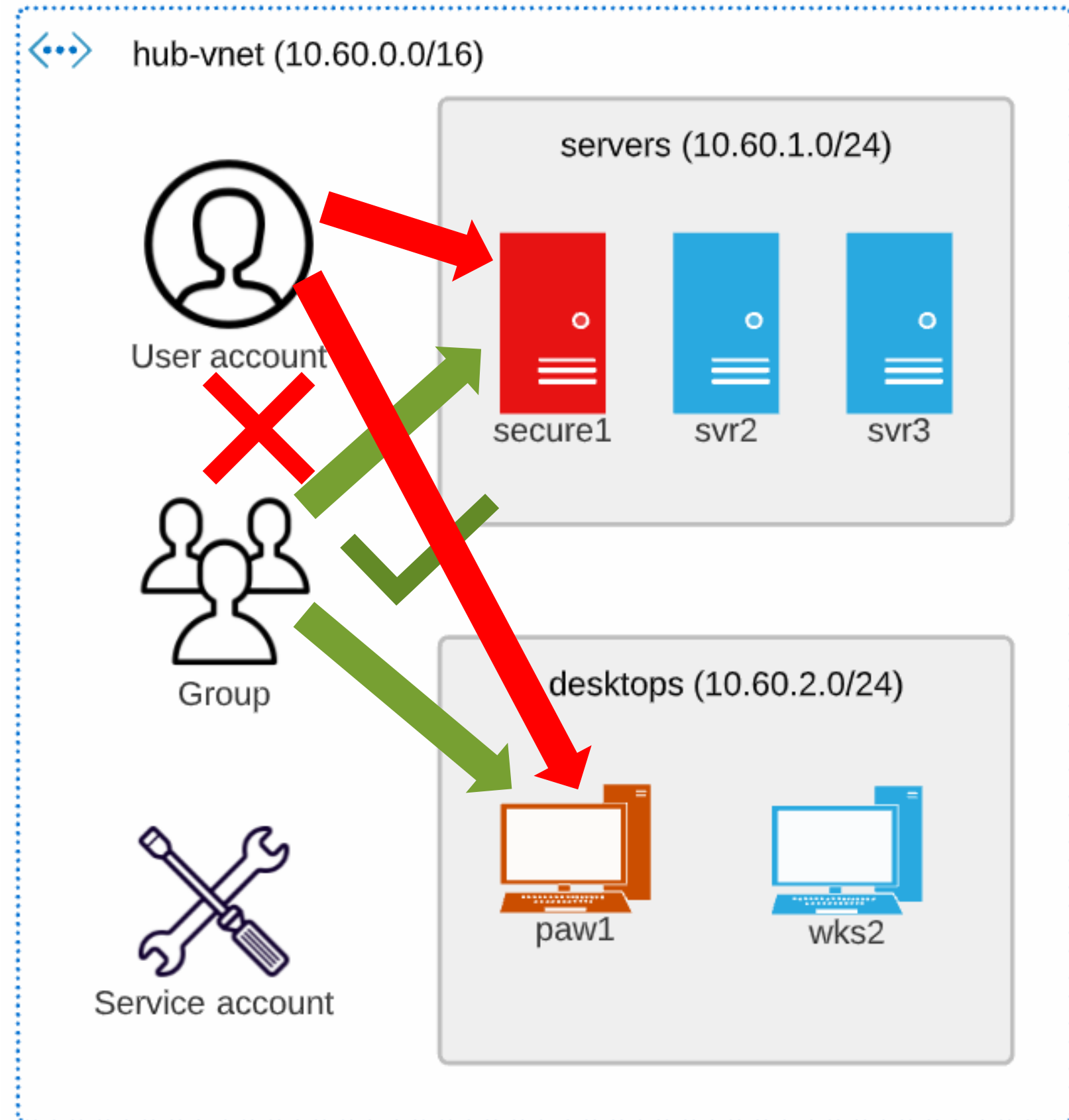
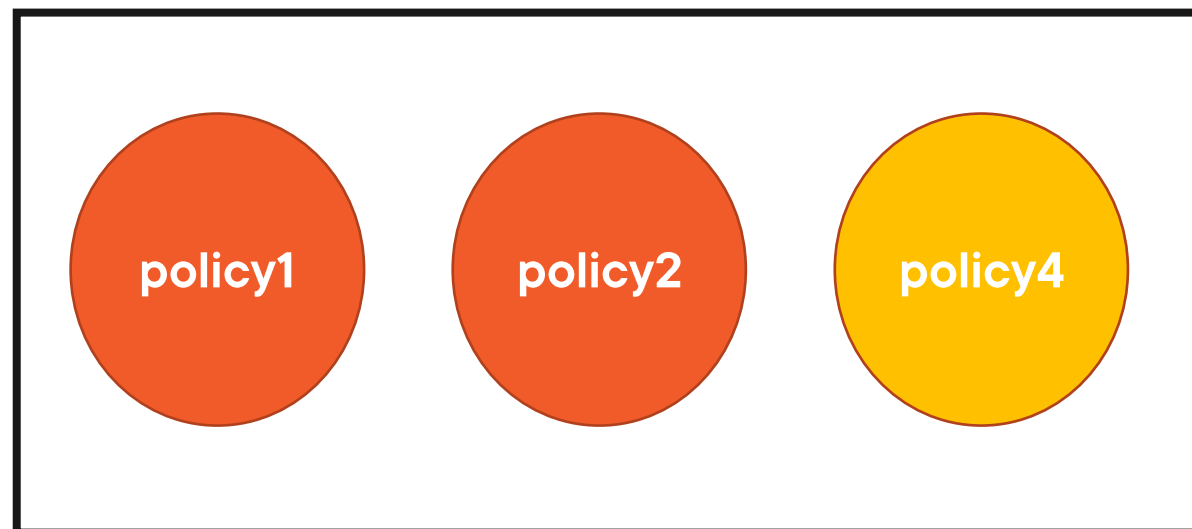


Authentication Policy Silos

siloA



siloB



Demo



2

Install and harden RODCs
Authentication policy silos



Summary



Windows Server domain controller security has remained largely stable over the years

Trend: cloud-based AI-powered assistance

Trend: Less frequent password changes

- Banned password lists
- MFA



Up Next:

Configure Hybrid Active Directory
Account Security

