DESIGN DOCUMENT – UNIFIED TEST ENVIRONMENT

ESI IAM

MAY 2, 2025

PROVIDENCE HEALTH

Contents

Overview

This design document outlines the architecture and components of an IAM test environment built using Azure InfrastructureasaService (IaaS). The environment is intended for development, testing, and validation of IAM solutions including integration with Entra ID, SailPoint, CyberArk, and other identity services.

Objectives

- Simulate a production like IAM environment.
- Enable testing of identity lifecycle, authentication, authorization, and privileged access management.
- Integrate hybrid identity scenarios using onprem AD and Entra ID.
- Support automation and customization testing.

HighLevel Architecture Diagram of UTE

Purpose

To create a secure and fully functional Identity and Access Management (IAM) test lab in the cloud using Entra ID and Azure IaaS to simulate hybrid identity environments. The environment will include:

- Entra ID (Entra ID)
- onpremises Active Directory (AD)
- SailPoint IdentityIQ
- CyberArk SaaS
- Entra ID Connect
- Entra ID Password Protection
- Hosted entirely in Azure, following a hubandspoke network topology.

Entra ID Tenant Design

1. Tenant Configuration

- Tenant Name: ProvidenceIAMTest.onmicrosoft.com
- Custom Domain Name: IAMTestProvidence.org
- DNS Provider: Infoblox
- DNS Records to Add:
  TXT record for domain verification: _msverify.IAMtest.providence.org Verification token from Entra ID
- Optional MX/CNAME/SRV records if testing additional services
- Domain Status: Verified and set as primary if required

2. Admin and Privileged Access Accounts

Privileged accounts in the test tenant are prefixed with 'pa' to clearly distinguish them from standard user identities. These accounts are granted Contributor access to Azure IaaS resources, enabling them to manage virtual machines, networks, and storage within defined scopes. The use of dedicated 'pa' accounts supports least privilege, role separation, and provides a cleaner audit trail for privileged activity in the test environment.

Admin Account pa.xxxx@providenceiamtest.onmicrosoft.com

Key Controls:

- All privileged accounts are cloud only
- Privileged Identity Management (PIM) enabled:
  - Eligible roles
  - MFA upon elevation
  - Justification, approval, and notifications configured

3. MFA & Conditional Access Configuration

Policy: Require MFA for Admins

- Applies to: All privileged role groups
- Conditions: All cloud apps
- Grant Controls: Require MFA

Policy: Baseline MFA for All Users (Excluding Break Glass)

- Applies to: All users
- Excludes: Break glass accounts
- Conditions: All locations or exclude trusted Ips
- Controls: Require MFA

MFA Methods:
Microsoft Authenticator App (default)

4. Identity Governance Features

PIM Setup:

- Eligible assignments, approval workflow
- Alerts and access reviews
- Assignments scoped by group

Break Glass Accounts:

Break glass accounts are highly privileged emergency access accounts designed for use only when normal administrative access is unavailable (e.g., Entra ID outage, Conditional Access misconfiguration). These accounts:

- Are cloud-only and not subject to Conditional Access or MFA,
- Have Global Administrator role assigned,
- Are monitored and tightly controlled, with login alerts configured,
- Use strong, complex passwords stored securely (e.g., in a vault),
- Are tested periodically to ensure readiness during critical incidents.

5. Enterprise Applications and App Registrations

SailPoint:

- Enterprise App: SailPoint IdentityIQ
- Permissions: Directory.Read.All, User.ReadWrite.All
- SAML config

CyberArk:

- App: CyberArk SAML Integration
- SAML

AD Connect Health:

- App: Entra ID Connect Health Agent

6. Logs and Monitoring

- Entra ID SignIn Logs: Enabled
- Audit Logs: Enabled
- Azure Monitor Integration: Optional

7. Recommended Security Best Practices

- Disable legacy authentication protocols (POP, IMAP, SMTP Auth)
- Implement Entra ID Identity Protection (optional in test lab)
- Use role based access and avoid direct Global Admin assignments

Azure IaaS Design

Management and Subscription Hierarchy

In the test tenant, we have a single Azure IaaS subscription used to host core infrastructure components such as VMs, networks, and storage for test and validation scenarios.
This subscription is organized under a dedicated management group, providing a governance layer for centralized control of policies, access, and compliance. The management group helps enforce role-based access control (RBAC), resource consistency, and cost tracking, ensuring that even in a test environment, resources follow enterprise standards.

Management Group:

- Name: ProvidenceIAMTest
- Centralized governance, inherited policy application\

Subscription:

- Name: ESI-IAM
- Linked to ProvidenceIAMTest
- PayAsYouGo or Dev/Test type

- Billing scoped to this subscription

2. Resource Group Structure

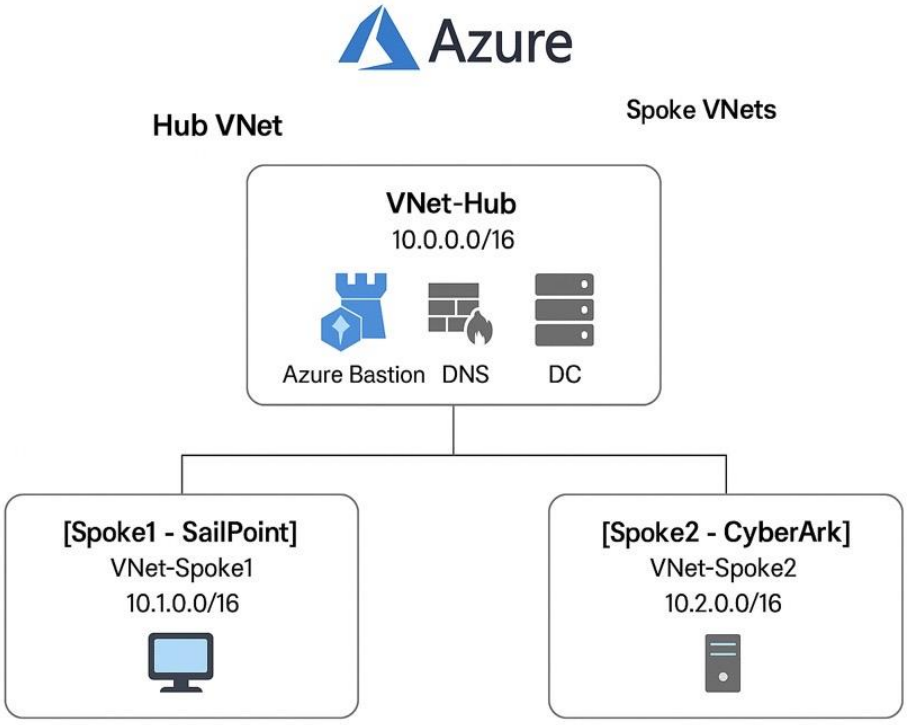
In our Azure environment, we've structured resource groups based on key IAM pillars—Authentication, IALM, directory services and Privileged Access.
Each resource group contains relevant components (e.g., connectors, automation, VMs) specific to its pillar, enabling logical separation, easier management, and targeted access control. This structure supports clearer ownership, more effective cost tracking, and aligns with our modular, test-driven IAM architecture.
Resource groups segmented by service line for separation of duties and RBAC:

- Rg-SharedInfra: VNet, Bastion, Firewall, DNS
- Rg-DirectoryServices: Domain Controllers, AD Sites & Services
- Rg-IALM: SailPoint IAM components
- Rg-PAM: PAM components (Vault, PVWA, CPM)
- Rg-EISAUth

3. Network Configuration and Topology

Our Azure environment uses a hub-and-spoke network topology to ensure secure, scalable, and modular connectivity.
The hub virtual network acts as a central point for shared services like firewalls, DNS, and VPN gateways. Multiple spoke virtual networks connect to the hub via VNet peering, each isolating workloads such as IAM test components or app environments.
This design allows for centralized control, reduced management overhead, and segmentation of workloads, while supporting secure east-west traffic flow and hybrid connectivity to on-prem resources.

- Topology: HubandSpoke
- Hub VNet: vNet-Hub,
- Spoke VNets: VNet-AD, VNet-IALM, VNet-PAM,
- VNet Peering: Enabled
- Private DNS Zones: IAMTestProvidence.org, conditional forwarding to internal DNS
- Azure Bastion: Deployed in rg-sharedinfra for secure RDP/SSH access



Azure Policies

Policies assigned at management group level:
Allowed Locations: East US, West US
Tag Enforcement: Environment, Owner, CostCenter
Audit VMs without backup
Deny Public IPs on VMs

RoleBased Access Control (RBAC)

In our tenant, **Azure Role-Based Access Control (RBAC)** is used to manage access to resources based on the principle of **least privilege**.
Roles are assigned at appropriate scopes—**management group**, **subscription**, **resource group**, or **resource level**—ensuring users and service principals have only the permissions needed to perform their tasks.
We leverage **built-in roles** (like Reader, Contributor, Owner) and will selectively use **custom roles** for fine-grained control. This structured approach enhances **security**, **auditability**, and **operational clarity** across our Azure environment

Scoped Roles at RG Level:

- Contributor to rg* for Identity Admins
- Network Contributor to rg-sharedInfra for Infra Admins
- VM Contributor to rg* for Server Team

PIMEnabled Roles:

- Owner, Contributor, User Access Administrator
- 8hour activation, approval workflow, justification required

VM and Compute Considerations

VM Sizing & Cost Optimization

- Choose appropriate VM sizes (e.g., B-series for burstable workloads, D-series for domain controllers or app servers).
- Use auto-shutdown, spot instances, or scale sets if applicable to manage cost.
- Separate compute resources by IAM pillar (auth, lifecycle, privileged access) using resource groups and spoke networks to isolate traffic and access.
- Use Availability Sets or Zones for key services (e.g., AD DS) to ensure fault tolerance.
  Integration Needs
- Ensure compute can securely connect to services like Entra ID, CyberArk, SailPoint, and AD Connect using appropriate networking and NSGs.
- Use shared image gallery or custom VM images for consistency across deployments.

VM SKUs:

- B-series for cost-effective workloads
- Dv5 or E-series for performance critical roles

Storage:
Premium SSD for AD, IAM systems

Encryption:
Azure Disk Encryption with Microsoft managed keys

Backup:
Azure Backup Vault in rgcoreinfra
Daily snapshot backups

7. Integration with Entra ID

- RBAC assignments use Entra ID users/groups
- Example groups: priv.azure.IALM
- Conditional Access policies enforce MFA for portal/CLI

8. Monitoring and Logging

- Azure Monitor and Log Analytics in rg monitoring
- Diagnostic settings on, VNets, VMs
- Log collection: RBAC changes, policy noncompliance, VM activity
- Optional: Azure Sentinel for security analytics

Active Directory Domain Services (AD DS)

1. Purpose and Scope

AD DS serves as the core identity provider for legacy services requiring Kerberos, NTLM, and GPOs.
It integrates with Entra ID using Entra ID Connect for identity synchronization.

2. Deployment Location

Resource Group: rg-SharedInfra

Virtual Network: VNet-Hub

Subnet: SubnetDCs

Region: West US

3. Domain Information

- Forest Name: : IAMTestProvidence.org
- Domain Functional Level: Windows Server 2022

- Forest Functional Level: Windows Server 2022
- DNS: ADintegrated DNS zone
- NetBIOS Name: IAMTESTProvidence

4. Domain Controller VM Specifications

DC1:
OS: Windows Server 2022
Size: D2as_v5
Storage: Premium SSD (OS + Data)
Roles: FSMO, GC, DNS

DC2:
OS: Windows Server 2022
Size: D2as_v5
Storage: Premium SSD
Roles: GC, DNS, replication partner

High availability: Configured in an availability set
Backup: Daily VM snapshot via Azure Backup

5. DNS Configuration

- ADintegrated zone: corp.providenceiamtest.onmicrosoft.
- Forwarders: Azure DNS \or custom
- Conditional forwarding to Azure Private DNS if applicable
- Vnet-hub DNS settings point to internal IPs of DC1 and DC2

6. GPOs and OU Structure (Test Environment)

Example GPOs:
Password Policy
Disable SMBv1
Logon banners

OU Structure:
OU=ServiceAccounts
OU=TestUsers

OU=IAMServers

7. Security and Hardening

- Local admin access via GPO and LAPS (optional)
- Event auditing: authentication, privilege use, object access
- Forward logs to Azure Monitor or Log Analytics
- NLA required for RDP
- Defender or antimalware enabled

8. Connectivity and Replication

- Single AD site: Azure West US2
- Replication over private VNet
- Replication interval: 15 minutes
- DNS scavenging enabled to clean stale records

9. Integration with Azure

- Entra ID Connect uses AD DS for synchronization to Entra ID
- DCs allow traffic from AAD Connect and Entra ID
- Kerberos based integrations with apps in other VNets via peering

Entra ID Connect IAM Test Environment

1. Purpose and Scope

Entra ID Connect (AADC) is used to synchronize identities from the on-premises AD DS (corp.providenceiamtest.onmicrosoft.) to Entra ID.
This ensures that hybrid identity management is possible and that users can authenticate using the same credentials.

2. Deployment Location

Resource Group: rg-sharedinfra
Virtual Network: VNetAD (spoke)
Subnet: SubnetSync
Region: East US

3. VM Specifications for AAD Connect Server

Hostname: AADConnect1
OS: Windows Server 2022
Size: D2as_v5
Storage: Premium SSD
Availability: Single instance (no HA in test)
Backup: Daily VM snapshot via Azure Backup

4. Synchronization Configuration

Sync Type: Password Hash Sync (default)
Filtering: OUbased (sync only OU=ServiceAccounts, OU=TestUsers)
Writeback (optional for test):
  Password writeback: Enabled
  Group writeback: Disabled
  Device writeback: Disabled
Sync Schedule: Every 30 minutes (default)
Manual sync: Enabled via PowerShell (StartADSyncSyncCycle)

5. Service Account and Permissions

AD DS Account: AADCServiceAccount (delegated permissions on synced OUs)
Entra ID Account: Global Admin or Hybrid Identity Admin (initial setup)
Local Admin on AAD Connect VM for installation

6. Firewall and Network Configuration

Outbound to internet: TCP 443 (for AAD endpoints)
Inbound RDP: Restricted via NSG + Bastion
Connectivity to AD DS DCs (TCP/UDP 389, 636, 3268, 3269, 88, 445)
DNS resolution configured to use DC IPs

7. Monitoring and Logging

Event Viewer: Directory Synchronization logs
Entra ID Connect Health Agent: Optional (enabled if Entra P1+ license)
Log Analytics: Agent installed for central logging (optional)

8. Security Hardening

MultiFactor Authentication (MFA) required for Entra ID accounts
VM access via Bastion or JIT (JustinTime) access via Azure Security Center
Windows Defender enabled
Local Administrator access restricted

CyberArk Infrastructure Design

Overview

This document outlines the deployment of CyberArk infrastructure for a test tenant using Azure VMs and CyberArk SaaS module. The setup includes:

- 2 PSM/CPM servers
- 2 CCP servers (Identity connector and Management Agent)
- 2 PSMP servers
- PVWA in SaaS Cloud

Virtual Network Design

Resource Group: rgPAM

Description: This resource group will contain all the servers, network configurations, and the Bastion host.

Virtual Network: vnet-PAM

Address Space: 10.1.0.0/16

Subnets

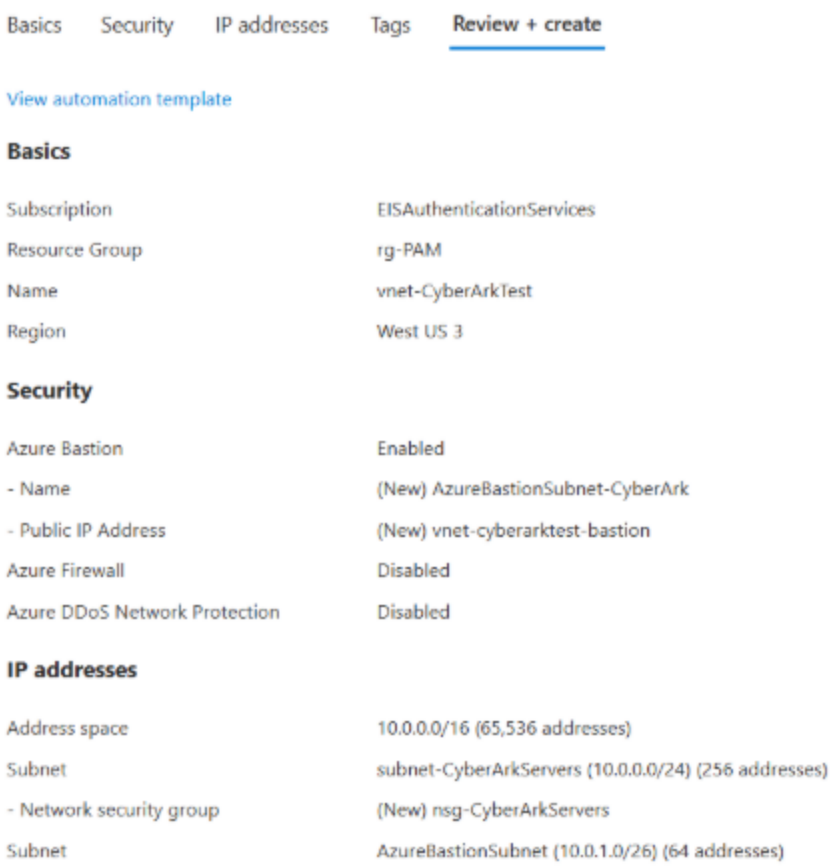
- **Subnet for Servers:** subnetCyberArkServers
  - **Description:** The subnet within the virtual network where all CyberArk VMs (PSM/CPM/PSM/CCP) instance will be deployed.
  - **Address Range:** 10.1.0.0/24
- **Subnet for Bastion Host:** AzureBastionSubnetCyberArk
  - **Address Range:** 10.0.1.0/27
  - **Description:** A dedicated subnet for the Azure Bastion host

Network Security Groups (NSGs)

- **NSG for Servers:** nsgCyberArkServers
  - **Rules:**
  - Allow inbound traffic on port 443 (HTTPS)
  - Allow inbound traffic on port 22 (SSH)
  - Allow inbound traffic on port 3389 (RDP)
  - Allow inbound traffic on port 5432 (PostgreSQL)
  - Allow inbound traffic on port 1858 (CyberArk Vault)

NSG for Bastion Host: nsgCyberArkBastion

  - **Rules**
  - Allow inbound traffic on port 443 from the internet
  - Allow inbound and outbound traffic to/from the server subnet (subnetCyberArkServers)



Azure VM Configuration

[Recommended Server Specifications | CyberArk Docs]

PSM Servers (CYBRKPSMCPM1)

- **VM Names:** (CYBRKPSMCPM1)
- **Size:** Standard*D2s*v3
- **OS:** Windows Server 2019
- **NIC:** Associated with subnetCyberArkServers and bound to nsgCyberArkServers
- **Ports:** 443, 3389

CPM Servers

- **VM Names:** (CYBRKPSMCPM2)
- **Size:** Standard*D2s*v3
- **OS:** Windows Server 2019

- **NIC:** Associated with subnetCyberArkServers and bound to nsgCyberArkServers
- **Ports:** 443, 5432

CCP Servers

- **VM Names:** CCP1, CCP2
- **Size:** Standard*D2s*v3
- **OS:** Windows Server 2019
- **NIC:** Associated with subnetCyberArkServers and bound to nsgCyberArkServers
- **Ports:** 443, 5432

PSMP Servers

- **VM Names:** PSMP1, PSMP2
- **Size:** Standard*D2s*v3
- **OS:** Windows Server 2019
- **NIC:** Associated with subnetCyberArkServers and bound to nsgCyberArkServers
- **Ports:** 443, 22

Bastion Host Configuration

- **Name:** bastionCyberArk
- **Subnet:** AzureBastionSubnetCyberArk
- **NSG:** nsgCyberArkBastion
- **Configuration:** Deploy an Azure Bastion host within the specified subnet for secure RDP/SSH access.

CyberArk SaaS Module

- **PVWA:** Hosted in SaaS Cloud
- **Connection:** Ensure all servers (PSM, CPM, CCP, PSMP) can communicate with PVWA in the SaaS Cloud over HTTPS (port 443,1858).

Active Directory Integration

- **Connection:** All servers should have connectivity to the onpremises Active Directory for authentication and we use CyberArk (SAAS) for authorization purposes.

HighLevel Diagram (TBD)

Port Numbers Required

- **PSM Servers:** 443, 3389
- **CPM Servers:** 443, 5432,1858
- **CCP Servers:** 443, 5432
- **PSMP Servers:** 443, 22
- **Bastion Host:** 443

Access Requirements

Resource Group: rgCyberArkTest

- **Owner:** IT administrator or project lead
- **Contributor:** Team members responsible for deploying and managing resources
- **Reader:** Stakeholders who need to monitor the resources

Virtual Network: vnetCyberArkTest

- **Contributor:** Network administrators
- **Reader:** IT staff

Network Security Groups: nsgCyberArkServers, nsgCyberArkBastion

- **Contributor:** Security team members
- **Reader:** IT staff and auditors

Virtual Machines: (PSM1, PSM2), (CPM1, CPM2), CCP1, CCP2, PSMP1, PSMP2

- **Contributor:** DevOps engineers, application developers, and administrators
- **Reader:** Monitoring team members

Bastion Host: bastionCyberArk

- **Contributor:** Network and security administrators
- **Reader:** IT staff

Detailed Steps for Communication Flow

1. **User Accessing CyberArk Portal**
   - The user initiates a connection to the CyberArk Portal (PVWA) hosted in the SaaS Cloud using HTTPS (port 443).
2. **PVWA Communicating with CPM/PSM and PSMP Servers**
   - PVWA communicates with CPM/PSM and PSMP servers over HTTPS (port 443) to manage privileged accounts and sessions.
3. **CPM/PSM and PSMP Communicating with SaaS Module**
   - CPM/PSM and PSMP servers communicate with the SaaS Module over HTTPS (port 443) for various operations such as password management and session monitoring.
4. **AD Connectivity**
   - CPM/PSM and PSMP servers connect to the onpremises Active Directory using LDAPS (port 636) for secure authentication and authorization.
5. **CPM to PVWA Vault Communication**
   - CPM/PSM servers communicate with the PVWA Vault using port 1858 for vault operations.