HPE POINTNEXT SERVICES

Design Guide

Hybrid IT Management Framework

Document Revision History

Project Name: Hybrid IT Management Framework – Design Guide

Document Status: Final

Document Version	Date	Prepared / Modified by	Reviewed by	Approved by	Section and Text Revised
1.0	20 May 2021	Sien Van Broekhoven	Dries Verschaeve		Full document

Table of Contents

Document Revision History 2

Introduction 5

- What is the Hybrid IT Management Framework? 5
- Architecture Design Module 5
- Environments 5

Networking Architecture 8

Network Components 8

- Virtual Networks (vNETs) 8
- Subnets 8
- VPN Gateway 9
- Gateway Subnet 9
- Connectivity 9
- Peering 10
- Name Resolution 10
- Permissions and Policies 10
- Virtual Network Encryption 10
- Network Security Groups (NSGs) 10
- Bastion 11

Logging and Monitoring 12

- Data being logged 12
- NSG flow logs 12
- Where the data is stored 12
- Services used for logging and storage 12

Security 14

- Default encryption provided by Azure 14
- Local Administrator Password Solution 14
- Azure Sentinel 14

Role Based Access Control 15

- Azure Policies 16

Identity and Access Management 17

- On Premise Active Directory 17
- Cloud AD domain controller 17
- Azure Active Directory 17
- Azure AD Connect 17

Server Management 19

- Windows Admin Center 19
- Azure ARC 20

Infrastructure as Code (IaC) 21

Firewall 22

Sources 22

Introduction

This document serves as a design guide for the Hybrid IT Management Framework. The goal of this document is to provide more information about the design decisions that were made, why these decisions were made, and to provide an overall view of the infrastructure design.

Configuration files and other code will not be included in this document, this will be included in an installation manual and code repository. The business reasons behind why this framework is developed can be found in a Plan of Action document.

What is the Hybrid IT Management Framework?

The Hybrid IT Management Framework is an architecture design that provides a solution to efficiently manage and administrate hybrid IT environments. This design provides centralized server management, and centralized identity management and authentication as its core components. The solution will be using as much Infrastructure as Code scripts (Terraform, PowerShell) as possible to make it easy to quickly deploy the cloud part of the infrastructure to an Azure subscription.

This framework forms a solution for organizations wanting to migrate to the Azure cloud and include management and authorization tools in their hybrid environment.

Architecture Design Module

The Hybrid IT Management Framework infrastructure design consists of an on-premise environment, which is connected to a virtual environment in Azure. The on-premise environment often already exists for an organization, it can consist of physical servers and client computers either at the organization itself, or in a datacenter. The virtual environment will be built in the Microsoft Azure cloud and is divided in a shared environment (hub) and a services environment (spokes).

- Azure Shared Virtual Environment: Shared Azure resources such as the Domain controller, jumphost, management servers. These resources provide centralized management solutions.
- Azure Spoke Environment: All resources needed to host a specific application or to offer a service.

This model works as a hub and spoke model, where the Azure shared environment is the hub, and the Azure spoke environment is a spoke.

Working with a hub and spoke model makes it easy to expand the services you want to offer in the cloud environment. For every service a new spoke can be created. This way you can also provide separation between the different services, which improves security and manageability.

Environments

The infrastructure design is based on a hybrid IT infrastructure design. This is a design where there is a mixture of on-premise systems and clients, and private/public cloud systems and services.

In this model there are three different environments, the on-premise environment, the Azure Shared Virtual environment, and the Azure spoke environment.

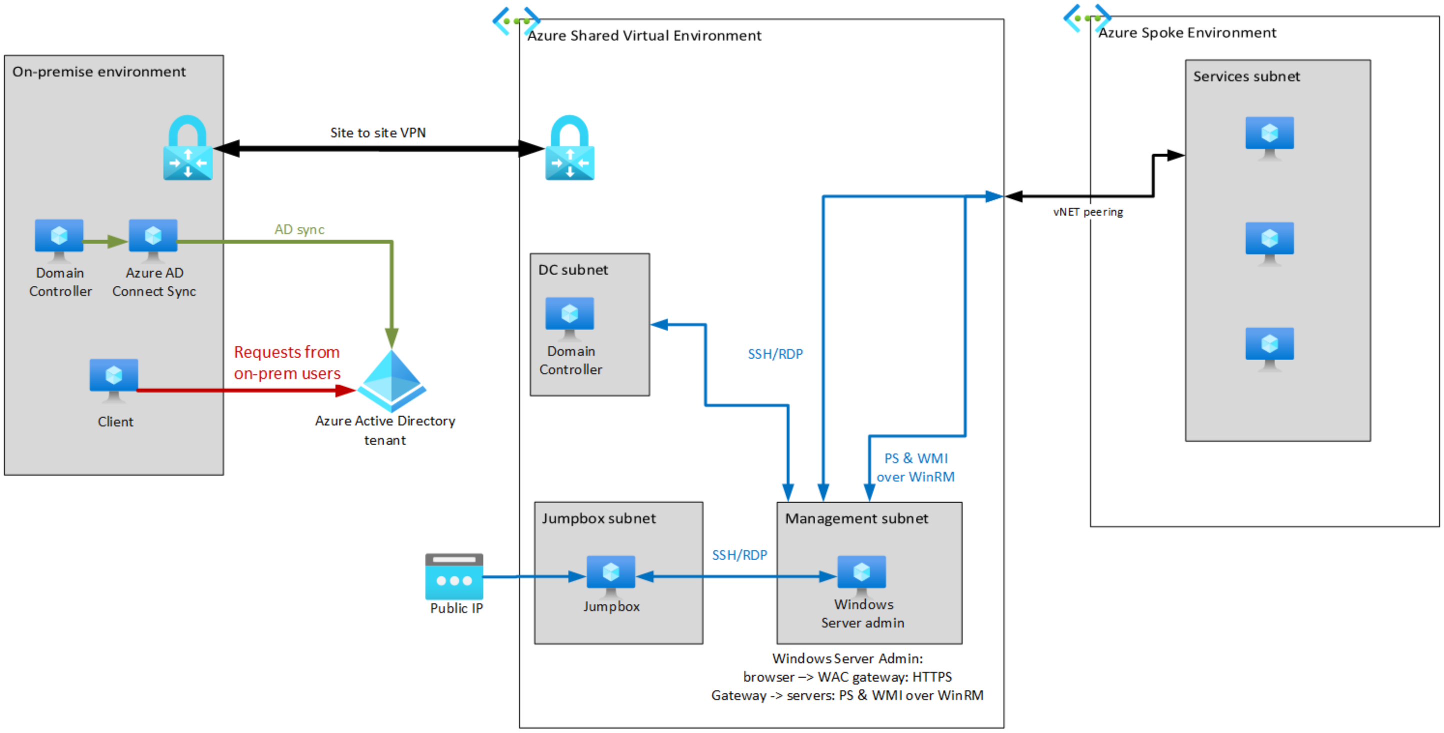


Figure 1: Architecture design

- **On-premise environment:** In the on-premise environment, an organization can have their physical Active Directory domain controller, configured with an Active Directory forest and domain. You can imagine the on-premise environment as a physical office where you have a few servers (like the domain controller), and some clients, such as physical computers.

Note

Many organizations/companies already have this environment, and wish to expand further to the cloud.

- **Azure Shared Virtual environment:** This Azure environment is configured to deliver access to cloud services for the clients in the on-premise environment. It will also provide a solution to centrally manage the entire environment, along with providing solutions for identity authentication and authorization in Azure Active Directory.
- **Azure spoke environment:** The resources of offered services and applications are located in this environment. Multiple spoke environments can be made, one for every offered service/application.

Resource Groups

Resource groups are containers that hold related resources in an Azure environment. All resources that deliver a similar service will be bundled together in a resource group, for example: all networking components are in the resource group rg_Network, and all security and monitoring components are in the resource group rg_Security.

For structural purposes, and keeping a clean overview, it is important that the resource groups are adequately named. The names of the resource groups will be based on the functions they deliver to the infrastructure. Tags can also be applied to resource groups to logically organize resources by category.

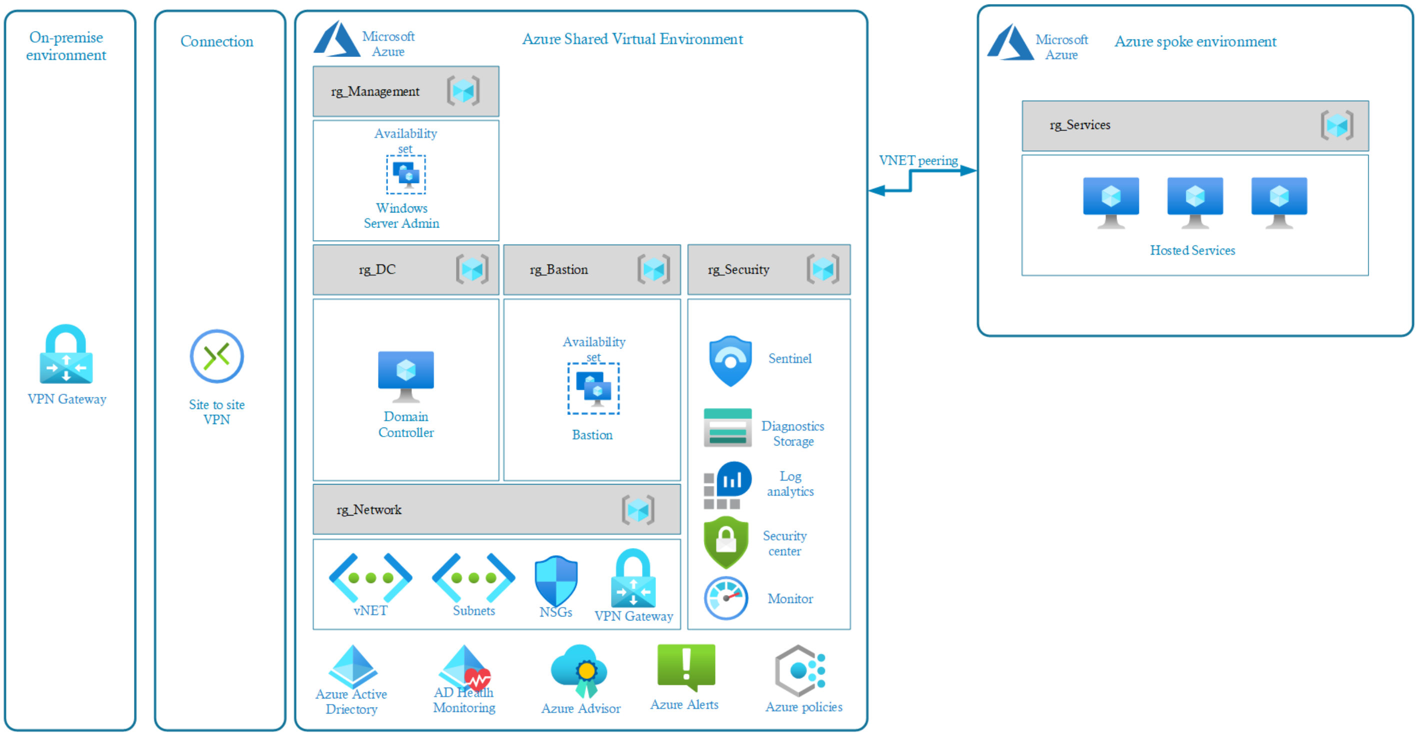


Figure 2: Resource groups

Table 1: Resource groups

Name	Resource Group Description
rg_Services	Contains servers that will provide resources of hosted services/applications
rg_Management	Contains servers to provide management solutions to the environment
rg_DC	Contains a Windows Server that will serve as a domain controller in the Active Directory forest
rg_Bastion	Contains a Bastion jumphost that makes it possible to remotely access internal systems in a secure way
rg_Security	Contains services that will provide security and monitoring solutions to the environment
rg_Network	Contains all networking infrastructure resources

Networking Architecture

The following figure shows what the networking architecture will look like.

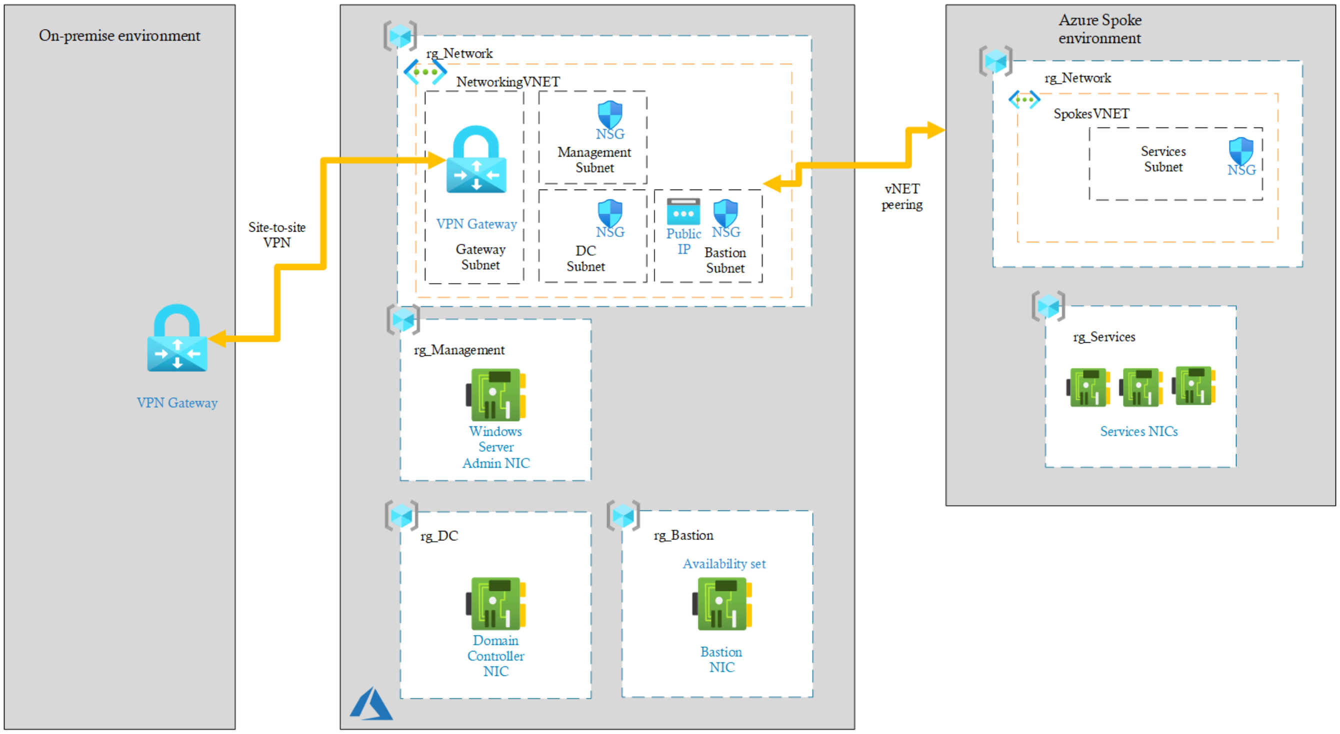


Figure 3: Networking architecture

Network Components

The different components in the networking architecture are explained next.

Virtual Networks (vNETs)

A virtual network is a representation of a cloud network. Resources in a virtual network can communicate with each other directly and securely, they are isolated from resources that are in other virtual networks.

Virtual networks can only contain resources that are in the same region and resource group. Resources from different vNETs can communicate with each other through vNET peering or through VPN gateways.

vNETs are required in the Azure environments to allow resources to communicate with each other. Without a vNET there is no connectivity.

Subnets

Subnets are logical subdivisions of IP networks/ vNETs. They are a way to divide networks into smaller segmented networks. This is not only important for maintaining a proper overview of the infrastructure, but also for the security of the network and resources.

Subnets can help minimize traffic. Without subnets all traffic would reach all resources, subnets make sure that the traffic is contained to the subnet.

The following table provides an overview of the different subnets in the environments.

Table 1: Subnets

Name	Subnet Description
GatewaySubnet	Contains a VPN gateway to connect to the on-premises environment
ManagementSubnet	Contains servers to provide management solutions to the environment
ServicesSubnet	Contains resources for hosted services/applications
DCSubnet	Contains a windows server, serving as a domain controller
BastionSubnet	Contains bastion servers

VPN Gateway

A VPN gateway can be used to connect the on-premises network to the Azure virtual network. A site-to-site VPN can be configured on these gateways. Site-to-site VPNs use IPsec/IKE tunneling technologies to route the traffic.

This VPN gateway will be configured in active-active mode. This means that two public IPs will be configured for the gateway, creating two IPsec tunnels. Both IPsec tunnels will be active simultaneously, meaning they will both route traffic at the same time. Clients will experience a higher throughput rate, and if something were to go wrong with one of the tunnels then the other tunnel should still be available.

Note

Active-passive mode is an alternative which keeps one tunnel active while the other tunnel is in standby mode until the active tunnel goes offline, then the standby tunnel will take over. Both active-active mode and active-passive mode provide failover support, but active-active mode provides a higher throughput rate.

A site-to-site VPN routes encrypted traffic securely over the public network, which provides connectivity between the on-premise environment and the Azure environment. An alternative to this could be an Express route, which routes all traffic over a private network instead of over a public network. This provides a higher level of security, and thus is more recommended for business-critical data. However, for general data, a site-to-site VPN is a well-fitting solution.

Gateway Subnet

In order to create a VPN gateway and connect the on-premises environment with the Azure virtual environment, a gateway subnet needs to be configured. This subnet contains the IP addresses that the virtual network resources and services use.

When a virtual network gateway is created, gateway VMs will be deployed to the gateway subnet. These VMs are configured with the required VPN gateway settings to make the gateway work properly. It is important that nothing else is deployed in this gateway subnet. This deployment will happen automatically when a VPN gateway is created.

The name of this subnet should be “GatewaySubnet”. Doing this lets Azure know that this is the subnet to deploy the virtual network gateway VMs and services to.

This gateway subnet needs to be created when making use of a site-to-site VPN or an Express route VPN.

Connectivity

Azure virtual networks can be connected to each other by using virtual network peering, which is useful if you want to use mulitple virtual environments. Connecting the on-premises environment to the Azure virtual environment can be configured through a VPN gateway.

The on-premises environment is connected to the Azure virtual environment so that clients from the on-prem environment can connect to services hosted in the Azure virtual cloud environment. Administration of the entire environment can then also happen through the cloud environment.

Peering

When there are multiple virtual networks in the Azure cloud that need to be connected with each other, virtual network peering technologies can be used. This technology eliminates having to route your traffic over the internet in order to create connectivity between resources in different virtual networks.

Name Resolution

Machines in the cloud environment will be configured to use the cloud domain controller as their primary DNS server, and the on-premises DNS server as their secondary DNS server.

When using the Domain controllers as their DNS servers, machines will be able to locate and connect to other servers and services in the active directory domain. This eliminates the need for services to be published over a public IP address. Clients will be able to reach the services over their private IP addresses.

Important

Clients in an already existing on-premise system normally already use a DC as their DNS server. Make sure the DNS settings of the on-premise domain controller point to a secondary DC to provide failover support.

Permissions and Policies

Permissions on the Azure resources can be arranged through Azure Role Based Access Control (RBAC). This is a solution that helps you manage which user has access to which resources, what they can do with these resources, and what areas of the resource they have access to.

Role based access control uses Azure roles to define access. Roles can be assigned to users, groups, service principals, and managed identities. A role is a collection of permissions, it declares read, write, delete, and other operations rights.

Roles can be applied to scopes. Scopes can be specified at four levels: management group, subscription, resource group, or resource. The lower levels are helpful if you want to assign roles based on specific resources instead of specifying them globally.

Role based access control can be further configured on application levels. An example is the Windows Admin Center application. Through Azure active directory enterprise applications, specific users can be granted/denied access to this application.

It is important that proper permissions are set in place to make sure that every user only has access to the resources they are authorized for. RBAC is a way to achieve this.

Virtual Network Encryption

Encryption can be enabled on subnets. All traffic flowing through these subnets will be encrypted.

Datagram Transport Layer Security (DTLS) is used to encrypt the data. DTLS protects against eavesdropping, tampering, and forgery by anyone with access to the network.

Network Security Groups (NSGs)

Network Security Groups contain security rules that allow or deny traffic based on certain parameters of the network traffic. These rules can be declared on incoming interfaces, which means traffic coming into the resources; and on outgoing interfaces, which means traffic that gets send to the outside from the resource.

For each rule you can specify source and destination ports and protocols as parameters to declare rules on.

These Network Security Groups can be applied to subnets to have more control over which traffic is allowed.

Bastion

An Azure bastion, or sometimes also called a jumphost, is a server that users can connect with to access other servers. This is usually used for performing administrational tasks on servers that don’t have a public IP address, but instead are connected to this bastion. This practice provides extra security for the internal servers, while still allowing them to be managed remotely.

It is important that access to the bastion is restricted with role-based access control, and that all session information is logged.

Logging and Monitoring

Monitoring of an IT environment is always important to make sure that the environment is healthy, and that no actions are taking place that should not be taking place. Monitoring enables IT admins to discover potential vulnerabilities and/or underlying issues before they can have a negative effect on the environment.

This section provides an overview of which data is being logged, where it is stored, and which services are used for this logging.

Data being logged

Azure platform logs provide detailed diagnostic and auditing information for Azure resources and the Azure platform they depend on. There are three different types of platform logs, all on different layers of Azure.

1. **Resource logs:** (Azure resources layer) - These are logs that provide insight into operations that were performed within an Azure resource.
2. **Activity logs:** (Azure subscription layer) - Logs what, who, and when any write operation (PUT, POST, DELETE) on a resource in a subscription took place.
3. **Azure Active Directory logs:** (Azure tenant) - These logs contain information about sign-in activity history and an audit trail of changes made in the Active directory for an Azure tenant.

Event data of the machines is collected by Active Directory. In AD, rules can be configured to specify which events you want to log per system. This data is written to the Security log. An audit entry in the security log contains information about which user did what action, and whether or not this action was successful.

Note
Security logs can be collected for both on-premise and virtual machines.

NSG flow logs

Network Security Group logs provide information about incoming and outgoing traffic through a network security group. These logs are shown on a per rule basis.

These logs provide insight into how many packets were denied/allowed access to a network. Monitoring these logs can discover potential network attack attempts.

Where the data is stored

There are different options to export the logs.

- **Storage account:** Logs can be stored in a storage account so that third party tools can pull subsets of these logs. The logs can also be pushed to log analytics for analysis.
- **Event hubs:** Logs can also be sent to event hubs for ingestion by analytics solutions, such as Power BI.

Note
NSG flow logs can currently only be exported to storage accounts, not to event hubs.

Services used for logging and storage

The following services are available for logging and storage.

- **Azure Monitor:** Provides different services, all used for collecting, analyzing, and acting on telemetry from the cloud and on-premises environment. The different functions that Azure monitor delivers are:
  - **Insights:** Provide insights in applications, containers, VMS, monitoring solutions
  - **Visualize:** Create dashboards, views, workbooks, use Power BI
  - **Analyze:** Analyze metric analytics, log analytics
  - **Respond:** Enable alerts, use auto scale functions

  - – **Integrate:** Export data to APIs, use logic apps

Data collected by Azure Monitor on resources can be viewed in their resource page. The values of multiple metrics over time can be charted in the metrics explorer.

- **Log analytics:** Data collected by Azure Monitor can be analyzed with queries to quickly retrieve, consolidate, and analyze collected data.
- **Alerts:** Alerts in Azure monitor proactively create notifications about critical conditions; they can also potentially attempt to take corrective actions.

Event logs per machine can be viewed in the Windows Admin Center portal, or through Azure Sentinel workbooks.

Security

It is important that the systems and data in the environment are properly secured. Network security groups were already discussed earlier to allow/deny traffic to/from systems. The VPN gateway between the on-premises network and the cloud network is secured with IPsec tunneling technology. Azure also offers encryption that can be enabled on subnets, and encryption that is enabled by default on several of their services.

Default encryption provided by Azure

The following encryption is- or can be enabled on Azure services.

- **Data-link layer encryption:** Packets are encrypted before being sent over networks. This is enabled by default.
- **TLS encryption:** Transport Layer Security (TLS) can be enabled to protect data when it's travelling between cloud services and clients. The data in the solutions architecture would be going through an IPsec tunnel which already is encrypted, so enabling TLS here is not necessary.

  TLS can also be enabled to protect RDP sessions, which is recommended to configure to connect to the bastion.

Encryption protects against eavesdropping, tampering, and forgery by anyone with access to the network.

Local Administrator Password Solution

Local Administrator Password Solution (LAPS) is a solution that resets the local administrator passwords of servers to a randomly generated complex password. These passwords are then saved in Active Directory. A rotation schedule can be configured on this tool to reset the passwords every few days/weeks/months.

Local administrator accounts should not be used to perform administrative tasks on a machine, instead domain administrator accounts should be used. It is important that the passwords of these local admin accounts are safeguarded in a secure place, and that the passwords are random so that they cannot be easily remembered.

Specific users can be given access to read the passwords of the local administrator accounts through the LAPS solution in case of an emergency where a local admin account must be used. All other users will not be able to read these passwords, and thus will not be able to log onto local administrator accounts.

Azure Sentinel

Azure Sentinel is Microsoft's cloud-native security information and event manager (SIEM) platform. This solution uses built-in AI to help analyze large volumes of data. This solution can be used to collect data and visualize it in workbooks. Alerts can also be configured to notify admins when a certain event takes place, such as suspicious activity or when a threat is detected.

Sentinel has the ability to execute automated response playbooks when an incident happens, or when an alert is generated. These automated responses greatly reduce response time, and thus reduce the time an issue has to spread further in the environment.

Role Based Access Control

Role based access control (RBAC) can be configured in Azure Active Directory to configure who has access to which azure resources, and what they can do with these resources. This is to configure access for IT employees to manage the environment, it is not to configure file/folder access for clients on their systems. This was already briefly explained in Permissions and Policies, and will be explained further here.

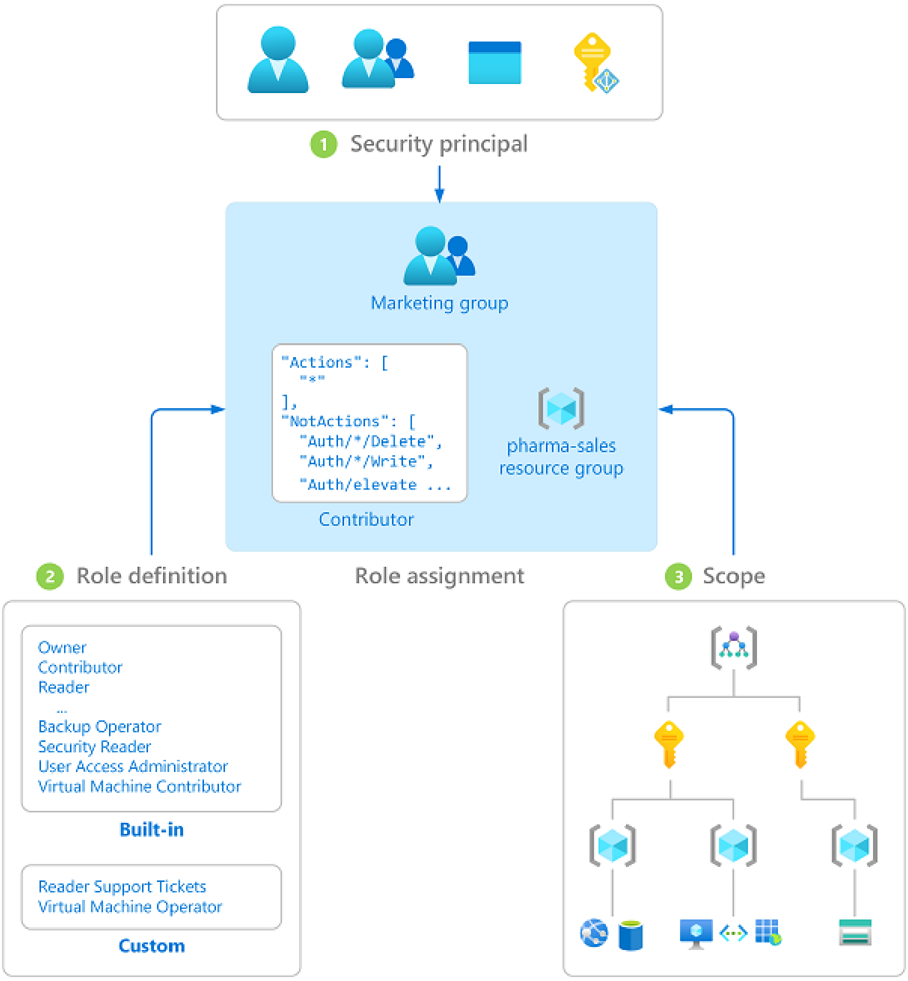
Role based access control is configured through role assignment in Azure AD. Roles can be assigned to:

- **Users:** profiles in Azure AD
- **Groups:** groups of users in Azure AD
- **Service Principals (SP):** security identities used by applications to access specific Azure resources

A role is a collection of permissions that declares what operations the user/group/SP can or cannot do. Examples of operations are read, write, and delete.

A role can be assigned a scope to further configure access. Scopes can be specified at four levels: management group, subscription, resource group, or resource. This is helpful if you want to assign roles based on resources instead of specifying them globally.

The following figure from Azure Docs provides an overview of how RBAC works.



```
"Actions": [
   "*"
],
"NotActions": [
   "Auth/*/Delete",
   "Auth/*/Write",
   "Auth/elevate ...
```

Owner
Contributor
Reader
...
Backup Operator
Security Reader
User Access Administrator
Virtual Machine Contributor

Reader Support Tickets
Virtual Machine Operator

Figure 4: Microsoft Role Based Access Control

A user/group/SP can be assigned multiple roles. The effective permissions are then a sum of the role assignments. Deny assignments precede over allow assignments. So, if a user has two roles, one of which allows write operations, and another one which denies write operations, the user will not be able to perform write operations.

Azure provides several pre-defined roles, but custom roles can also be created.

Azure Policies

Azure policies can be configured in the Azure Policy service to help enforce organizational standards to assess compliance at-scale.

Note
An organization can use this solution to make sure that all created resources are meeting organizational standards. These standards are different per organization.

Azure Policy evaluates resources by comparing the properties of the resources to business rules. Business rules can be configured in a JSON format, and can then be assigned to a scope or resource.

Evaluations happen at these different times:

- When a resource is created, updated, or deleted in a scope with a policy assignment
- When a policy is newly assigned to a scope
- When a policy which is already assigned to a scope, is updated
- During the standard compliance evaluation cycle, which is once every 24 hours

If a resource is non-compliant to these business rules, several actions can be configured to execute:

- Deny the resource change
- Log the change to the resource
- Alter the resource before the change
- Alter the resource after the change
- Deploy rated compliant resources

It is important to properly configure policies, they make sure that no actions can take place that don’t comply with organizational standards.

Identity and Access Management

An Active Directory forest with a domain will be configured to manage clients in the environment. This domain will consist of one on-premises domain controller, one cloud domain controller, Azure Active Directory to move the management and authentication to the cloud, and Azure Active Directory Sync to perform synchronization between the on-premises AD and Azure AD.

Note
More domain controllers and domains can be configured based on organizational needs, the text above explains my lab environment setup.

On Premise Active Directory

A windows server 2019 which is configured as the first domain controller in a new forest will be the main domain controller for a new domain. This domain controller will carry all 5 FSMO roles, and will also perform as a DNS server.

Note
Most organizations already have an on-premise environment configured with Active Directory. The amount of domain controllers, and which domain controllers carry which FSMO roles is different from organization to organization.

Cloud AD domain controller

In the Azure cloud environment, another Windows 2019 server will be configured to serve as a domain controller. This is a secondary domain controller and will not carry any FSMO roles. It will perform as a DNS server to properly route traffic in the cloud environment, and provide failover support.

When the domain controller joins the AD domain, replication is automatically configured. This replication happens through the site-to-site VPN that is configured between the two environments. This connection is private and encrypted.

This second domain controller will provide failover support if something were to go wrong with the primary domain controller.

Note
If an organization already has multiple domain controllers on-premise then it is still recommended to configure an additional domain controller in the virtual environment to provide failover support if the VPN/Expressroute were to go down.

Azure Active Directory

Azure Active Directory will be configured to move the identity authentication process and management of the Active Directory forest/domain to the cloud. When clients send an authentication request, this will be sent to the Azure Active Directory instead of to the on-premises or cloud domain controller. This will not happen automatically, and needs to be configured.

Role based access control, device management, identity governance, conditional access, and much more can all be configured in this solution.

Azure AD Connect

Azure AD Connect provides two services:

1. **Azure AD Connect Sync:** This is a service used to provide:
   - Password hash synchronization between the on-premises domain controller (where password hashes are kept) and the Azure AD (which stores a hash of the password hash).
   - Pass-through authentication, which allows users to authenticate in cloud services with the same password they use on-premises, without the password being stored in Azure AD.

- General synchronization between the on-premises active directory and Azure AD.

2. **Azure AD Connect Health:** This is a service that provides monitoring of on-premises identity infrastructure. It provides alerts, performance monitoring, usage information, and other information.

Azure AD connect needs to be configured in order to connect the on-premise Active Directory to Azure Directory and to enable synchronization between these two services.

Server Management

There will be several servers in both the on-premises environment and the Azure cloud environment, it is important that it is possible to centrally manage all of these servers, and have a proper overview of current configurations.

Windows Admin Center

Windows Admin Center will be used to manage the Windows Servers in the entire hybrid IT environment. The servers hosting Windows Admin Center will be deployed in an availability set in the Cloud environment. It will not have a public IP address, but instead will only be available to access through the private IP, this is to provide extra security.

The following figure shows how the servers running Windows Admin Center will be deployed in the environment. A load balancer will distribute traffic between two Windows Server VMs which form an availability set. The two VMs will share a managed SSD disk on which Windows Admin Center will be installed. If one of the two VMs would fail, the other one is still available to take over all the traffic.

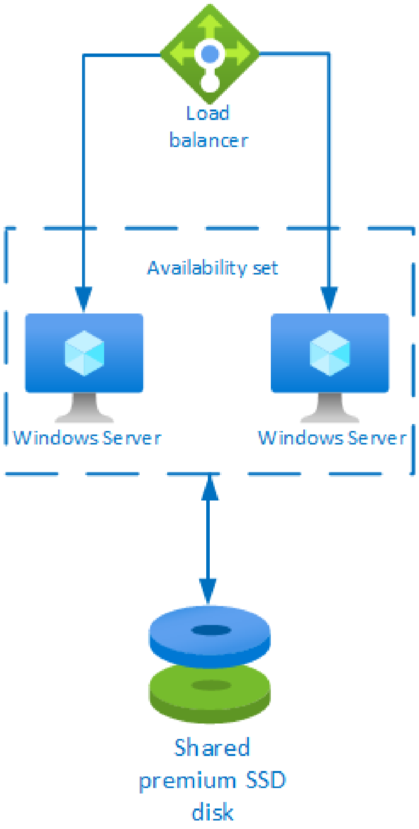


Figure 5: Windows Admin Center architecture

Windows Admin Center is a solution that provides centralized server management in a hybrid IT environment. It can provide an overview of the statistics of a server, as well as provide remote configuration options (Remote PowerShell, RDP).

Note

On-premise systems can also be added to the server list of Windows Admin Center. Organizations that have a lot of on-premise servers can thus also manage their on-premise machines through a cloud hosted solution.

Azure ARC

To add our on-premises systems to the cloud services Azure offers, such as monitoring, and alerts; Azure ARC can be installed on the on-premises systems, this is an agent that can be downloaded and installed on the required machines. When Azure ARC is installed on these systems, they are added as resources in the Azure portal.

Infrastructure as Code (IaC)

Most of the cloud infrastructure in this solution will be written in Infrastructure as Code files to make it a quick and easy solution to deploy.

Hashicorp Terraform is the tool that will be used to deploy these configuration files. The configuration is written in the declarative HashiCorp Language (HCL). These HCL files will be written in a modular way, making it possible to quickly add/remove/change components from the infrastructure.

Configurations of these cloud systems can mostly be configured through PowerShell scripts that can be deployed on the target systems.

Terraform uses Azure modules to integrate Azure AD possibilities in the solution.

Firewall

The following network flows are required:

GroupName	Servers
DC-SUBNET	DC – 10.1.1.4
MANAGEMENT-SUBNET	ManagementVM0 – 10.1.2.4 ManagementVM1 – 10.1.2.6
BASTION-SUBNET	Bastion – 10.1.3.1
SERVICES-SUBNET	10.3.1.0/24

Source	Destination	Protocol/port	Reason
BASTION-SUBNET	Management-Subnet	TCP/3389 UDP/3389 TCP/22 UDP/22	Bastion access
DOMAIN	Management-Subnet	TCP/443	HTTPS for WAC portal
MANAGEMENT-SUBNET	DC-Subnet	TCP/3389	RDP from Management-Subnet
MANAGEMENT-SUBNET	DC-Subnet	TCP/5986	WinRM from Management-Subnet
MANAGEMENT-SUBNET	Services-Subnet	TCP/3389	RDP from Management-Subnet
MANAGEMENT-SUBNET	Services-Subnet	TCP/5986	WinRM from Management-Subnet
INTERNET	Bastion-Subnet	TCP/443	Access over internet
GATEWAYMANAGER	Bastion-Subnet	TCP/443	GatewayManager
BASTION-SUBNET	Domain	TCP/22 UDP/22 TCP/3389 UDP/3389	SSH and RDP from bastion
BASTION-SUBNET	Domain	TCP/8080 UDP/8080 TCP/5701 UDP/5701	Bastion-Subnet

Also allow the required ports for Active Directory communication between DCs and clients, as can be found here.

Sources

Information about Microsoft services (Azure, Windows Admin Center) is all researched on the Microsoft Docs website

Figure of Azure role based access control: Azure RBAC

Terraform information: Terraform Docs