

Azure Enterprise-Scale / PCF V2

Low Level Design Document

Table of Contents

[1. Document Control 3](#_Toc134575338)

[1.1. Document Information 3](#_Toc134575339)

[1.2. Distribution List 3](#_Toc134575340)

[1.3. Supporting Documents 3](#_Toc134575341)

[2. Exec Summary 4](#_Toc134575342)

[2.1. Overview 4](#_Toc134575343)

[2.1. Purpose 4](#_Toc134575344)

[2.2. Audience 4](#_Toc134575345)

[3. Governance Overview 4](#_Toc134575346)

[4. Management Group Structure 4](#_Toc134575347)

[5. Azure Regions 6](#_Toc134575348)

[6. Naming Conventions 7](#_Toc134575349)

[6.1. Subscriptions 7](#_Toc134575350)

[6.1.1. Platform Management Group subscriptions: 7](#_Toc134575351)

[6.1.2. Landing Zone Management Group subscriptions: 7](#_Toc134575352)

[6.1.3. Sandbox Management Group subscriptions: 8](#_Toc134575353)

[6.2. Resources 8](#_Toc134575354)

[logic-weu-dev-opswkseslz2-01 9](#_Toc134575355)

[6.3. Policies 10](#_Toc134575356)

[7. Tags 10](#_Toc134575357)

[7.1. Mandatory Tags 10](#_Toc134575358)

[7.2. Subscription level tags 10](#_Toc134575359)

[7.3. Resource group level tags 11](#_Toc134575360)

[8. Azure baseline policy categories 11](#_Toc134575361)

[8.1. Compute 11](#_Toc134575362)

[8.2. General 11](#_Toc134575363)

[8.3. Security 12](#_Toc134575364)

[8.4. Allowed Locations 12](#_Toc134575365)

[8.5. Allowed Resource types 13](#_Toc134575366)

[8.6. Tags 13](#_Toc134575367)

[8.7. Naming enforcements 13](#_Toc134575368)

[8.8. Storage 14](#_Toc134575369)

[8.9. Resource Lock 14](#_Toc134575370)

[8.10. Network 14](#_Toc134575371)

[8.11. SQL 15](#_Toc134575372)

[8.12. KeyVault 17](#_Toc134575373)

[8.13. Monitoring 17](#_Toc134575374)

[9. Policy Initiative list 18](#_Toc134575375)

[Name: gov initiative network policy 19](#_Toc134575376)

[Name: gov initiative keyvault policy 20](#_Toc134575377)

[Name: gov initiative compute policy 21](#_Toc134575378)

[Name: gov initiative deploy microsoft defender for cloud configuration 21](#_Toc134575379)

# 1. Document Control

## 1.1. Document Information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Name | Role | Comments |
| 23/02/2023 | 1.0 | Mrunmayee Indap | Infra Technology Specialist | Initial draft |
| 23/02/2023 | 1.1 | Jobin Cyriac | Infra Architect | Reviewed |
|  |  |  |  |  |
|  |  |  |  |  |

Table 1: Document Information

## 1.2. Distribution List

|  |  |  |
| --- | --- | --- |
| Distributed to | Role | Company |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table 2: Distribution List

## 1.3. Supporting Documents

|  |  |
| --- | --- |
| **Document Name** | **Version** |
| Azure Enterprise-Scale / PCF V2  High Level Design Document | Version 1.0 |

Table 3: Supporting Documents

# Exec Summary

## 2.1. Overview

As part of the ESLZ initiative, this document aims to define the set of policies which are going to applied for ESLZ management groups and subscriptions.

This E2E framework is about to cover all the governance aspects like the management group structure on which the policies are defined, the set of all the policies which would be enforced in ESLZ also it will cover the naming convention of subscription, resource group and resources.

## Purpose

This LLD documents covers Governance framework infrastructure which will be deployed in Enterprise Scale@Uniper, its management groups and landing zone subscriptions.

## Audience

The intended audience for this document will be UNIPER architects and UNIPER Enterprise Scale@Uniper project management.

# Governance Overview

Uniper will use Azure Policy and Initiatives to control, restrict and govern overall resource compliance. Policies will be grouped into initiatives based on policy category and further categorized based on Common/Pre-Prod/Prod specific requirements. The segregation of initiatives further helps in tracking and managing the specific policy for any improvement area in the future.

The grouping of policies allows expandability in future and a single policy definition can be used in multiple initiatives. Below is the list of initiatives-based on category with a brief description of policies under each initiative. Initiatives can be managed and assigned individually without impacting the other policy rules which are part of other initiatives.

The list of initiatives will have policy effects such as “Deny” all the policy would be enforced. For detailed information related to the policies which are applied in Uniper please go through the below sheet:

[https://Uniper.sharepoint.com/sites/CloudWorksTeam/HaCT/Project%20Documentation/PCFv2/Policy%20Design/ESLZ%20Policy%20v.01.xlsx](https://uniper.sharepoint.com/sites/CloudWorksTeam/HaCT/Project%20Documentation/PCFv2/Policy%20Design/ESLZ%20Policy%20v.01.xlsx)

# Management Group Structure

Management Groups lets you organize your subscriptions into containers called "management groups" and apply your governance conditions (access, policies, and compliance) to the management groups.

A picture containing text, screenshot, diagram, line

Description automatically generated

Figure 1:Management Group Structure

* Uniper will follow a multi-subscription model, which is based on the environments. Multiple subscriptions will help overcome the limitation of single subscription and manage the resources more effectively. Multiple subscription also helps in providing more control on billing and chargeback as well.
* Uniper’s Management Group will be based on Geographical regions including data remains in a specific region to comply with GDPR, and environments.

|  |  |  |
| --- | --- | --- |
| **Management Group** | **Name** | **Description** |
| **Root Management Group** | Tenant root group | All management groups in the Azure AD are under the root management group |
| All Azure users can see the root management group |
| New subscriptions are automatically placed in the root management group when created |
| **Enterprise Scale Uniper Root Management Group** | UPCF v2 | This management group is located directly under the tenant root group. |
| This management group purposely avoids the usage of the root group so that organizations can move existing Azure subscriptions into the hierarchy |
| This management group is a parent to all the other management groups in Enterprise Scale@Uniper |
| **Platform** | Platform | This management group contains all the platform child management groups, like management, connectivity, and identity. |
| **Management** | Management | This management group contains a dedicated subscription for management, monitoring, and security. |
| The management subscription will host an Azure Log Analytics workspace, including associated solutions, and an Azure Automation account. |
| **Connectivity** | Connectivity | This management group contains a dedicated subscription for connectivity. |
| This subscription will host the Azure networking resources required for the platform, like Azure Virtual WAN, Azure Firewall, and Azure DNS private zones. |
| **Identity** | Identity | This subscription is a placeholder for Windows Server Active Directory Domain Services (AD DS) virtual machines (VMs) or Azure Active Directory Domain Services. |
| This management group contains a dedicated subscription for identity. |
| **Landing Zone** | Landing Zone | This management group structure will be the root for all application data holding subscriptions. |
| The management group shall be containing the common policies for landing zones |
| **Corp** | Corp-weu/Corp-uks/Corp-swc | This management group is to organize the subscriptions as per GDPR requirements under landing zone management group~~s~~. |
| This MG will have policies restrict cross region deployments of Azure resources other than the intended regions for Uniper. |
| This will also have region policies based on specific Uniper region. |
| The dedicated management group for corporate landing zones |
| This group is for Azure resources that require hybrid connectivity with the corporate network via the hub in the connectivity subscription. |
| **Environments** | Prod/UAT/Dev | The dedicated Subscription for landing zones based on their environments. |
| Prod and UAT will have policies which will restrict any UI based deployments as deployments via IaC is allowed in higher environments. |
| Dev will allow application team to deploy Azure resources from portal as well as IaC |
| **Sandboxes** | Test bed subscriptions | The dedicated management group for subscriptions that will only be used for testing and exploration |
| These subscriptions will be securely disconnected from the corporate landing zones. |
| Sandboxes also have a less restrictive set of policies assigned to enable testing, exploration, and configuration of Azure services. |

Table 4: Management group descriptions

# Azure Regions

Below are the regions used for Resource deployment in-scope at Uniper

* West Europe(weu) à Primary region hosting all resources.
* UK South(uks) à Primary region hosting all resources.
* Sweden Central(swc) à Primary region hosting all BU related resources.

The list of paired regions which are yet to considered.

* North Europe(neu) à secondary region.
* UK North(ukn) à Secondary region for specific spoke.
* Sweden South(sws) à Secondary region for specific spoke.

# Naming Conventions

## Subscriptions

Standardizing on a naming convention for subscriptions is extremely important. In ESLZ, Resource naming controls are applied through policies. The primary regions are W.Europe and N.Europe. The allowed string size for subscription can have maximum 256 characters. An example on how the naming convention for the MVP 1.0 would be as follows:

ESLZ-                 CORP-                POC-             F\_OI3-            HaCT-                       01

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Enterprise Scale Landing Zone | Corporate / Internet | Environment   (prd/uat/dev/poc) | Business Unit | Core IT/LOB/Project | Number that will be incremented |

### Platform Management Group subscriptions:

The Platform MG is divided into three management group as follows:

* Connectivity

An example on how the naming convention for the MVP 1.0 would be as follows:

ESLZ-                  CORP-      Connectivity-      F\_OI3-            HaCT-                       01

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Enterprise Scale Landing Zone | Corporate / Intranet | Connectivity | Business Unit | Core IT/LOB/Project | Number that will be incremented |

* Identity

An example on how the naming convention for the MVP 1.0 would be as follows:

ESLZ-                  CORP-      Identity-      F\_OI3-            HaCT-                       01

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Enterprise Scale Landing Zone | Corporate / Intranet | Identity | Business Unit | Core IT/LOB/Project | Number that will be incremented |

* Management

An example on how the naming convention for the MVP 1.0 would be as follows:

ESLZ-                  CORP-      Management-      F\_OI3-            HaCT-                       01

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Enterprise Scale Landing Zone | Corporate / Intranet | Management | Business Unit | Core IT/LOB/Project | Number that will be incremented |

### Landing Zone Management Group subscriptions:

An example on how the naming convention for the MVP 1.0 would be as follows:

ESLZ-                  CORP-      Environment-      F\_OI3-            HaCT-                       01

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Enterprise Scale Landing Zone | Corporate / Intranet | Environment  (dev/prod/uat) | Business Unit | Core IT/LOB/Project | Number that will be incremented |

### Sandbox Management Group subscriptions:

An example on how the naming convention for the MVP 1.0 would be as follows:

ESLZ-                  CORP-      Environment-      F\_OI3-            POC-                       01

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Enterprise Scale Landing Zone | Corporate / Intranet | Environment  (dev/prod/uat) | Business Unit | Core IT/LOB/Project | Number that will be incremented |

## Resources

Naming standards are very important within Azure to ensure that all resources deployed are easily identifiable. A consistent naming standard should be followed. All resources will be named in alignment with a best practice naming convention provided by Cognizant, with example resources provided in the following table.

|  |  |  |
| --- | --- | --- |
| Object/Resource | Nomenclature | Examples |
| Resource Group Name | <resourcetype>-<location>(weu/neu/uks/ukw/swc)-<environment>(prd/uat/dev/poc/rnd)-<app or service>(alphanumeric 3-15 letters)-<int>(00-99)  Resource type for resource group is ‘rg’ | rg-weu-prd-aks-01  Length: 1-64 |
| Virtual Network Name | <resourcetype>-<location>(weu/neu/uks/ukw/swc)-<environment>(prd/uat/dev/poc/rnd)-<purpose>(alphanumeric 3-15 letters)-<int> (00-99)  Resource type for virtual network is ‘vnet’ | vnet-weu-prd-aks-01  Length: 2-80 |
| Subnet Name | <resourcetype>-<purpose>(alphanumeric 3-15 letters, E.g. App gateway, Bastion, postgressql, Mysql, etc)-<int> (00-99)  Resource type for Subnet is ‘sn’ | sn-ad-01  Length: 2-80 |
| Storage Account Name | <resourcetype><location>(weu/neu/uks/ukw/swc)<environment><service><service-tier>(Hot Access tier, Cool Access tier, and Archive tier)<integer> (00-99)  Resource type for Storage account is ‘st’ | Stweuprdakshat01  Length: 3-24 (lower case) |
| Key Vault | <resourcetype>-<location>(weu/neu/uks/ukw/swc)-<environment>(prd/uat/dev/poc/rnd)-<app or service> (alphanumeric 3-15 letters)-<int>​ (00-99)  Resource type for key vault is ‘kv’ | kv-weu-prd-aks-01 |
| Route Table | <resourcetype>-<location>(weu/neu/uks/ukw/swc)-<environment>(prd/uat/dev/poc/rnd)-<app or service> (alphanumeric 3-15 letters)-<int>​ (00-99)  Resource type for route table is ‘rt | rt-weu-prd-aks-01 |
| Network Security Group | <resourcetype>-<location>(weu/neu/uks/ukw/swc)-<environment>(prd/uat/dev/poc/rnd)-<app or service> (alphanumeric 3-15 letters)-<int>​ (00-99)  Resource type for network security group is ‘nsg’ | nsg-weu-prd-aks-01  Length: 1-80 |
| Load balancer (internal) | <resourcetype>-<location>(weu/neu/uks/ukw/swc)-<environment>(prd/uat/dev/poc/rnd)-<app or service> (alphanumeric 3-15 letters)-<int>​ (00-99)  Resource type for network security group is ‘lbi’ | lbi-weu-prd-aks-01 |
| Load balancer (external) | <resourcetype>-<location>(weu/neu/uks/ukw/swc)-<environment>(prd/uat/dev/poc/rnd)-<app or service> (alphanumeric 3-15 letters)-<int>​ (00-99)  Resource type for network security group is ‘lbe’ | lbe-weu-prd-aks-01 |
| Application Security Group | <resourcetype>-<location>(weu/neu/uks/ukw/swc)-<environment>(prd/uat/dev/poc/rnd)-<app or service> (alphanumeric 3-15 letters)-<int>​ (00-99)  Resource type for application security group is ‘asg’ | asg-weu-prd-aks-01 |
| Managed Identity | <resourcetype>-<location>(weu/neu/uks/ukw/swc)-<environment>(prd/uat/dev/poc/rnd)-<app or service> (alphanumeric 3-15 letters)-<int>​ (00-99)  Resource type for application security group is ‘id | mid-weu-prd-aks-01 |
| Application Gateway | <resourcetype>-<location>(weu/neu/uks/ukw/swc)-<environment>(prd/uat/dev/poc/rnd)-<app or service> (alphanumeric 3-15 letters)-<int>​​ (00-99)  Resource type for application gateway is ‘agw’ | agw-weu-prd-aks-01 |
| Azure Monitor Private Link Scope | <resource type>- <service name> (alphanumeric 3-15 letters) - subscriptionname (name of the subscription)>-< (int)-01(00-99)>  Resource type for resource group is ‘ampl’ | ampls-eslz-corp-connectivity-f\_oi3-hact-01 |
| Log Analytics Workspace | <resourcetype>-<region(weu/neu/uks/ukw/swc)><project name/subscriptionname>(alphanumeric 3-26 letters)-< 01(00-99)>  Resource type for resource group is ‘law’ | law-weu-DEV-C-MA3-DTFU081-01 |
| Automation Account name | <resourcetype>-<region(weu/neu/uks/ukw/swc)>-<project name>(0-15 alphanumeric)-01(00-99)  Resource type for resource group is ‘aa’ | aa-weu-workspace-01 |
| Alert Rule Name for Applications | <resourcetype>-<region(weu/neu/uks/ukw/swc)>-<projectname>(0-15 alphanumeric)>-< 01(00-99)>-<alert criticality(\_c/\_w/\_i-alert)  Resource type for resource group is ‘altrule’ | altrule-weu-logsearch-lbcreateordel-project123\_c-alert |
| Action Group Name | <resourcetype>-<teamname(15char)>-<subscriptionname (name of the subscription)>-< 01(00-99)>  Resource type for resource group is ‘actgrp’ | ag-hactwinteam-eslz-corp-dev-c\_ma3-dtfu081-01 |
| Diagnostics Setting Name | <resourcetype>-<resourcename(10char)><projectname (0-15 alphanumeric)>-< 01(00-99)>  Resource type for resource group is ‘diagset’ | diagset-logicapp-project123-01 |
| Logic App | <resourcetype>-<location>(weu/neu/uks/ukw/swc)-<environment>(prd/uat/dev/poc/rnd)-<app or service> (alphanumeric 3-15 letters)-<int>​ (00-99)  Resource type for resource group is ‘logic’ | logic-weu-dev-opswkseslz2-01 |

Table 5: Naming conventions

Here are the most common naming components to keep in mind when coming up with a naming convention:

|  |  |
| --- | --- |
| Naming component | Description |
| **Resource type** | An abbreviation that represents the type of Azure resource or asset. This component is often used as a prefix or suffix in the name. Examples: rg, vm, nsg |
| **Application or service name** | Name of the application, workload, or service that the resource is a part of. Examples: aks, core |
| **Subscription Name** | Summary description of the purpose of the subscription that contains the resource. Often broken down by environment or specific workloads. Examples: prod, shared,Hact |
| **Environment** | The stage of the development lifecycle for the workload that the resource supports. Examples: prod, uat, dev, poc |
| **int** | A number or letter indicating uniqueness when you have multiple instances of this resources for the same workload.  Such as 001. |
| Location | The Azure region where the resource is deployed. Examples: weu/neu/uks/ukn/sws/swc |

Table 6: Naming abbreviations

## Policies

Policies are handles by multiple departments.

To identify policies handled by Governance team, all the policies are created with prefix ‘gov’

|  |  |
| --- | --- |
| Prefix | gov |
| Type of policy | Built In or Custom |
| Definition or Assignment | * Policy definition- gov policy * Policy initiative – gov initiative * Policy Assignment – gov initiative\_assign\_ |

Table 7: Policy naming convention.

# Tags

Resource Manager provides a tagging feature that enables Uniper to categorize resources as per the requirements for managing or billing. The practice of tagging resources allows resources to be logically organised into categories which can later be used for billing, reporting, maintenance, and automation purposes. Tagging is essential to maintaining resource consistency and implementing an effective organisation taxonomy. All tag names and values will be lower-case, for standardization purposes

## Mandatory Tags

Mandatory tag policy present and inherited through resource groups.

|  |  |  |
| --- | --- | --- |
| **Tag** | **Scope** | **Purpose** |
| Owner\_Email | Resource Group | The owner of the service – commonly used as a point of contact |
| eam\_id | Resource Group | EAM ID from SNOW Enterprise Application Management |
| bu\_id | Resource Group | Business Unit ID. Identify the cost centre for billing purposes |
| application\_name | Resource Group | Identify the Project / Application name |
| environment | Resource Group | The environment of an application. |
| lob\_parent | Resource Group | Line of Business Parent |
| created\_date | Resource Group | Creation date of resource |
| ic\_relevancy | Resource Group | Is the application relevant for Internal Controls. |

Table 8: Mandatory tags

## Subscription level tags

Subscriptions are provisioned through automation and the below tags shall be stamped at subscription level as part of subscription vending process.

|  |  |  |
| --- | --- | --- |
| **Tag** | **Scope** | **Purpose** |
| Owner\_Email | Resource Group | The owner of the service – commonly used as a point of contact |
| bu\_id | Resource Group | Business Unit ID. Identify the cost centre for billing purposes |
| created\_date | Resource Group | Creation date of resource |

Table 9: Mandatory tags at subscriptions

## Resource group level tags

Uniper have enforced the mandatory tags for the resource group. The policy is set to inherit the RG level tags to the resources underneath.

# Azure baseline policy categories

Azure policies are scoped and defined based on categories. The below list of categories the baseline policies are placed.

## Compute

|  |  |
| --- | --- |
| **Compute Policy** | **Description** |
| gov policy not allowed resource types\_deny | Restrict which resource types can be deployed in your environment. Limiting resource types can reduce the complexity and attack surface of your environment while also helping to manage costs. Compliance results are only shown for non-compliant resources. |
| gov policy allowed virtual machine size skus\_deny | This policy enables you to specify a set of virtual machine size SKUs that your organization can deploy. |
| gov policy virtual machines and virtual machine scale sets should have encryption at host enabled\_deny | Use encryption at host to get end-to-end encryption for your virtual machine and virtual machine scale set data. Encryption at host enables encryption at rest for your temporary disk and OS/data disk caches. Temporary and ephemeral OS disks are encrypted with platform-managed keys when encryption at host is enabled. OS/data disk caches are encrypted at rest with either customer-managed or platform-managed key, depending on the encryption type selected on the disk. Learn more at https://aka.ms/vm-hbe. |
| gov policy only approved vm extensions should be installed\_deny | This policy governs the virtual machine extensions that are not approved. |
| gov policy azure backup should be enabled for virtual machines\_deployifnotexists | Enforce backup for all virtual machines by deploying a recovery services vault in the same location and resource group as the virtual machine. Doing this is useful when different application teams in your organization are allocated separate resource groups and need to manage their own backups and restores. You can optionally exclude virtual machines containing a specified tag to control the scope of assignment. See https://aka.ms/AzureVMAppCentricBackupExcludeTag. |

## General

|  |  |
| --- | --- |
| Tags | Description |
| Enable Monitoring in Azure Security Center | Monitor all the available security recommendations in Azure Security Centre. This is the default policy for Azure Security Centre. This is a built-in policy. |
| Transparent Data Encryption on SQL databases should be enabled​ | Audit transparent data encryption status for SQL databases. This is a built-in audit policy. |
| API App should only be accessible over HTTPS​ | Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks. ​ This is a built-in policy. |
| Enforce HTTPS for Storage Connection​ | This policy requires storage accounts to use HTTPS traffic. This is a custom policy. |
| Audit for storage account file and blob encryption | This policy audits if file and blob encryption is enabled for storage accounts. This is a custom policy. |

## Security

|  |  |
| --- | --- |
| **Security Compliance** | **Description** |
| gov policy Guest accounts with write permissions on Azure resources should be removed\_disabled | External accounts with write privileges should be removed from your subscription to prevent unmonitored access. |
| gov policy Guest accounts with owner permissions on Azure resources should be removed\_disabled | External accounts with owner permissions should be removed from your subscription to prevent unmonitored access. |
| gov policy dbformysql security mintlsversion 1.2\_deny | This policy ensures that the affected resource should enforce TLS 1.2 for DBforMySQL-connections |
| gov policy postgresql security mintlsversion 1.2\_deny | This policy ensures that affected resource should enforce TLS 1.2 for PostgreSQL-connections |
| gov policy storage security mintlsversion 1.2\_deny | This policy ensures that affected resource should enforce TLS Version 1.2 on all the Storage Accounts |
| gov policy web sites security mintlsversion 1.2\_deployifnotexists | Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance speed. Upgrade to the latest TLS version for App Service apps to take advantage of security fixes, if any, and/or new functionalities of the latest version. |
| gov policy sql security mintlsversion 1.2\_deny | This policy ensures that the setting TLS version to 1.2 or newer improves security by ensuring your Azure SQL Database can only be accessed from clients using TLS 1.2 or newer. Using versions of TLS less than 1.2 is not recommended since they have well documented security vulnerabilities. |
| gov initiative Deploy Microsoft Defender for Cloud configuration | This initiative is consisting of all the policies which are related to Microsoft Defender for cloud configuration. |
|  |

## Allowed Locations

|  |  |
| --- | --- |
| Allowed locations | Description |
| Regions Restriction | This policy enables clients to restrict the locations when deploying resources. Used to enforce geo-compliance requirements.    West Europe  North Europe  UK South  UK North  Sweden Central  Sweden South  Global (for any global services) |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

## Allowed Resource types

|  |  |
| --- | --- |
| Policy | Description |
| Not Allowed Resource Types | This policy will restrict the service which users cannot deploy, it’s an extremely important policy which will need to be maintained as new services are on-boarded. This is a built-in policy. |

## Tags

|  |  |
| --- | --- |
| Tags | Description |
| Require specified tag on resource groups | Enforces existence of a tag. Specifically, for UNIPER these are the some of the tags:  Owner\_Email  eam\_id  bu\_id  application\_name  environment  lob\_parent  created\_date |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| Inherit tag and its value from the resource group ​ | Inherit the specified tag with its value from the resource group when any resource which is missing this tag is created or updated. Does not modify the tags of resources created before this policy was applied until those resources are changed. |  |
|  |

## Naming enforcements

Resource Group naming conventions are enforced.

## Storage

|  |  |
| --- | --- |
| **Storage Account policy** | **Description** |
| gov policy Storage accounts should restrict network access using virtual network rules\_deny | This policy protects your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts. |
| gov policy public network access should be disabled for azure file sync\_deny | Disabling the public endpoint allows you to restrict access to your Storage Sync Service resource to requests destined to approved private endpoints on your organization's network. There is nothing inherently insecure about allowing requests to the public endpoint, however, you may wish to disable it to meet regulatory, legal, or organizational policy requirements. You can disable the public endpoint for a Storage Sync Service by setting the incomingTrafficPolicy of the resource to AllowVirtualNetworksOnly. |
| gov policy storage account public access should be disallowed\_deny | Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it. |
| gov policy secure transfer to storage accounts should be enabled\_deny | This policy ensures that Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking |
| gov policy storage accounts should have the specified minimum tls version\_deny | This policy ensures to configure a minimum TLS version for secure communication between the client application and the storage account. To minimize security risk, the recommended minimum TLS version is the latest released version, which is currently TLS 1.2. |
| gov policy Storage Account should have soft delete enabled\_deny | This policy ensures that the storage account should have soft delete enabled |

## Resource Lock

|  |  |
| --- | --- |
| Lock Policy |  |
| gov initiative locks | This policy ensures policy to enforce user to apply locks on resource. |

## Network

|  |  |
| --- | --- |
| **Network Policy** | **Description** |
| gov policy network interfaces should disable ip forwarding\_deny | This policy denies the network interfaces which enabled IP forwarding. The setting of IP forwarding disables Azure's check of the source and destination for a network interface. This should be reviewed by the network security team. |
| gov policy azure web application firewall should be enabled for azure front door entry-points\_deny | This policy enforces to deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules. |
| gov azure policy to block public ip | This policy blocks the creation of public IP address. |
| gov policy web application firewall (waf) should be enabled for application gateway\_deny | This policy enforced to deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules. |
| gov policy to use internal load balancers for kubernetes clusters | Use internal load balancers to make a Kubernetes service accessible only to applications running in the same virtual network as the Kubernetes cluster. For more information |
| gov policy to disable network related Deployment | Use this policy to block all the network deployment. |

## SQL

|  |  |
| --- | --- |
| **SQL Policy** | **Description** |
| gov policy azure sql database should have azure active directory only authentication enabled\_deny | Disabling local authentication methods and allowing only Azure Active Directory Authentication improves security by ensuring that Azure SQL Databases can exclusively be accessed by Azure Active Directory identities. |
| gov policy azure sql managed instance should have azure active directory only authentication enabled\_deny | Disabling local authentication methods and allowing only Azure Active Directory Authentication improves security by ensuring that Azure SQL Managed Instances can exclusively be accessed by Azure Active Directory identities. |
| gov policy public network access on azure sql database should be disabled\_deny | Disabling the public network access property improves security by ensuring your Azure SQL Database can only be accessed from a private endpoint. This configuration denies all logins that match IP or virtual network-based firewall rules. |
| gov policy enforce ssl connection should be enabled for postgresql database servers\_deny | Azure Database for PostgreSQL supports connecting your Azure Database for PostgreSQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This configuration enforces that SSL is always enabled for accessing your database server. |
| gov policy enforce ssl connection should be enabled for mysql database servers\_deny | Azure Database for MySQL supports connecting your Azure Database for MySQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This configuration enforces that SSL is always enabled for accessing your database server. |
| gov policy private endpoint connections on azure sql database should be enabled\_audit | Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database. |
| gov policy private endpoint should be enabled for mysql servers\_auditifnotexist | Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure. |
| gov policy to enforce an azure active directory administrator for PostgreSQL servers | Audit provisioning of an Azure Active Directory administrator for your PostgreSQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services |
| gov policy Private endpoint should be enabled for PostgreSQL servers\_auditifnotexist | Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure. |

## KeyVault

|  |  |
| --- | --- |
| **KeyVault Policy** | **Description** |
| gov policy key vaults should have purge protection enabled\_deny | Malicious deletion of a key vault can lead to permanent data loss. A malicious insider in your organization can potentially delete and purge key vaults. Purge protection protects you from insider attacks by enforcing a mandatory retention period for soft deleted key vaults. No one inside your organization or Microsoft will be able to purge your key vaults during the soft delete retention period. |
| gov policy key vaults should have soft delete enabled\_deny | Deleting a key vault without soft delete enabled permanently deletes all secrets, keys, and certificates stored in the key vault. Accidental deletion of a key vault can lead to permanent data loss. Soft delete allows you to recover an accidentally deleted key vault for a configurable retention period. |
| gov policy to enforced key vault should use a virtual network service endpoint\_deny | This policy audits any Key Vault not configured to use a virtual network service endpoint. |

## Monitoring

|  |  |
| --- | --- |
| Monitoring Policy | Description |
| Deploy Diagnostic Settings for Service Bus to Log Analytics workspace | Deploys the diagnostic settings for Service Bus to stream to a regional Log Analytics workspace when any Service Bus which is missing this diagnostic settings is created or updated. |
| Deploy Diagnostic Settings for Search Services to Log Analytics workspace | Deploys the diagnostic settings for Search Services to stream to a regional Log Analytics workspace when any Search Services which is missing this diagnostic settings is created or updated. |
| Deploy Diagnostic Settings for Event Hub to Log Analytics workspace | Deploys the diagnostic settings for Event Hub to stream to a regional Log Analytics workspace when any Event Hub which is missing this diagnostic settings is created or updated. |
| Deploy Diagnostic Settings for Stream Analytics to Log Analytics workspace | Deploys the diagnostic settings for Stream Analytics to stream to a regional Log Analytics workspace when any Stream Analytics which is missing this diagnostic settings is created or updated. |
| Configure diagnostic settings for Storage Accounts to Log Analytics workspace | Deploys the diagnostic settings for Storage accounts to stream resource logs to a Log Analytics workspace when any storage accounts which is missing this diagnostic settings is created or updated. |
| Deploy - Configure diagnostic settings for Azure Kubernetes Service to Log Analytics workspace | Deploys the diagnostic settings for Azure Kubernetes Service to stream resource logs to a Log Analytics workspace. |
| Configure Azure SQL database servers diagnostic settings to Log Analytics workspace | Enables auditing logs for Azure SQL Database server and stream the logs to a Log Analytics workspace when any SQL Server which is missing this auditing is created or updated |
| Deploy - Configure diagnostic settings for Azure Key Vault to Log Analytics workspace | Deploys the diagnostic settings for Azure Key Vault to stream resource logs to a Log Analytics workspace when any Key Vault which is missing this diagnostic settings is created or updated. |
| Configure diagnostic settings for Blob Services to Log Analytics workspace | Deploys the diagnostic settings for Blob Services to stream resource logs to a Log Analytics workspace when any blob Service which is missing this diagnostic settings is created or updated. |
| Deploy - Configure diagnostic settings for SQL Databases to Log Analytics workspace | Deploys the diagnostic settings for SQL Databases to stream resource logs to a Log Analytics workspace when any SQL Database which is missing this diagnostic settings is created or updated. |
| Deploy Diagnostic Settings for Logic Apps to Log Analytics workspace | Deploys the diagnostic settings for Logic Apps to stream to a regional Log Analytics workspace when any Logic Apps which is missing this diagnostic settings is created or updated. |
| Deploy Diagnostic Settings for Key Vault to Log Analytics workspace | Deploys the diagnostic settings for Key Vault to stream to a regional Log Analytics workspace when any Key Vault which is missing this diagnostic settings is created or updated. |
| Deploy Diagnostic Settings for Batch Account to Log Analytics workspace | Deploys the diagnostic settings for Batch Account to stream to a regional Log Analytics workspace when any Batch Account which is missing this diagnostic settings is created or updated. |
| Configure diagnostic settings for Azure Machine Learning workspace to Log Analytics workspace | Deploys the diagnostic settings for Azure Machine Learning workspace to stream resource logs to a Log Analytics workspace when any Azure Machine Learning workspace which is missing this diagnostic settings is created or updated. |

# Policy Initiative list

The below list of initiatives is grouped and classified based on the need over the landing zones.

|  |  |  |
| --- | --- | --- |
| S. No | Initiatives Name | Policy Display Name |
| 1 | Name: gov initiative security compliance | * gov policy Guest accounts with write permissions on Azure resources should be removed\_disabled * gov policy Guest accounts with owner permissions on Azure resources should be removed\_disabled * gov policy dbformysql security mintlsversion 1.2\_deny * gov policy postgresql security mintlsversion 1.2\_deny * gov policy storage security mintlsversion 1.2\_deny * gov policy web sites security mintlsversion 1.2\_deployifnotexists * gov policy sql security mintlsversion 1.2\_deny |
| 2 | Name: [gov initiative storage account](https://portal.azure.com/?feature.msaljs=false) | * gov policy Storage accounts should restrict network access using virtual network rules\_deny * gov policy public network access should be disabled for azure file sync\_deny * gov policy storage account public access should be disallowed\_deny * gov policy secure transfer to storage accounts should be enabled\_deny * gov policy storage accounts should have the specified minimum tls version\_deny * gov policy Storage Account should have soft delete enabled\_deny |
| 3 | Name: gov initiative locks | * gov policy enforce cannotdelete resource lock\_deployifnotexist |
| 4 | Name: gov initiative network policy | * gov policy network interfaces should disable ip forwarding\_deny * gov azure policy to block public ip * gov policy to disable network related Deployment * gov policy azure web application firewall should be enabled for azure front door entry-points\_deny * gov policy web application firewall (waf) should be enabled for application gateway\_deny |
| 5 | Name: gov initiative sql policy | * gov policy azure sql database should have azure active directory only authentication enabled\_deny * gov policy azure sql managed instance should have azure active directory only authentication enabled\_deny * gov policy public network access on azure sql database should be disabled\_deny * gov policy enforce ssl connection should be enabled for postgresql database servers\_deny * gov policy enforce ssl connection should be enabled for mysql database servers\_deny * gov policy private endpoint connections on azure sql database should be enabled\_deny * gov policy private endpoint should be enabled for mysql servers\_deny * gov policy Private endpoint should be enabled for PostgreSQL servers\_deny |
| 6 | Name: gov initiative keyvault policy | * gov policy key vaults should have purge protection enabled\_deny * gov policy key vaults should have soft delete enabled\_deny * gov policy to enforced key vault should use a virtual network service endpoint\_deny |
| 7 | Name: gov initiative tag policy | * gov policy require owner\_email tag and its value on resource groups\_deny * gov policy require eam\_id tag and its value on resource groups\_deny * gov policy require a bu\_id tag and its value on resource groups\_deny * gov policy require a application\_name tag and its value on resource groups\_deny * gov policy require a lob\_parent tag and its value on resource groups\_deny * gov policy require a environment tag and its value on resource groups\_deny * gov policy require a ic\_relevancy tag and its value on resource groups\_deny * gov policy require a created\_date tag and its value on resource groups\_deny * gov policy inherit mandatory tags from the resource group\_modify * gov policy inherit mandatory tags from the resource group\_modify * gov policy inherit mandatory tags from the resource group\_modify |
| 8 | Name: gov initiative general policy | * gov policy allowed locations for resource groups\_deny * gov policy allowed locations\_deny |
| 9 | Name: gov initiative allowed location in uk region | * gov policy allowed locations uk region\_deny * gov policy allowed locations for resource groups uk region\_deny |
| 10 | Name: [gov initiative allowed location in west europe region](https://portal.azure.com/?feature.msaljs=false) | * gov policy allowed locations for resource groups west europe region\_deny * gov policy allowed locations west europe region\_deny |
| 11 | Name: gov initiative naming convention resource group | * gov policy resource group naming convention\_deny |
| 12 | Name: gov initiative compute policy | * gov policy not allowed resource types\_deny * gov policy allowed virtual machine size skus\_deny * gov policy virtual machines and virtual machine scale sets should have encryption at host enabled\_deny * gov policy only approved vm extensions should be installed\_deny * gov policy azure backup should be enabled for virtual machines\_deployifnotexists |
| 13. | Name: gov initiative deploy microsoft defender for cloud configuration | * Enable Microsoft Defender for Cloud on your subscription * Configure Azure Defender for App Service to be enabled * Configure Azure Defender for Azure SQL database to be enabled * Configure Azure Defender for open-source relational databases to be enabled * Configure Microsoft Defender for Azure Cosmos DB to be enabled * Configure Azure Defender to be enabled on SQL managed instances * Configure Azure Defender for DNS to be enabled * Configure Azure Defender for Key Vaults to be enabled * Configure Azure Defender for Resource Manager to be enabled * Configure Azure Defender for Storage to be enabled * Configure Microsoft Defender for Containers to be enabled * Deploy Azure Policy Add-on to Azure Kubernetes Service clusters * Configure Azure Kubernetes Service clusters to enable Defender profile * Subscriptions should have a contact email address for security issues * Configure Azure Arc enabled Kubernetes clusters to install the Azure Policy extension * [Preview]: Configure Azure Arc enabled Kubernetes clusters to install Microsoft Defender for Cloud extension |
| 14. | Name: gov initiative for diagnostics setting enabled | * Deploy Diagnostic Settings for Service Bus to Log Analytics workspace * Deploy Diagnostic Settings for Search Services to Log Analytics workspace * Deploy Diagnostic Settings for Event Hub to Log Analytics workspace * Deploy Diagnostic Settings for Stream Analytics to Log Analytics workspace * Configure diagnostic settings for Storage Accounts to Log Analytics workspace * Deploy - Configure diagnostic settings for Azure Kubernetes Service to Log Analytics workspace * Configure Azure SQL database servers diagnostic settings to Log Analytics workspace * Deploy - Configure diagnostic settings for Azure Key Vault to Log Analytics workspace * Configure diagnostic settings for Blob Services to Log Analytics workspace * Deploy - Configure diagnostic settings for SQL Databases to Log Analytics workspace * Deploy Diagnostic Settings for Logic Apps to Log Analytics workspace * Deploy Diagnostic Settings for Key Vault to Log Analytics workspace * Deploy Diagnostic Settings for Batch Account to Log Analytics workspace * Configure diagnostic settings for Azure Machine Learning workspace to Log Analytics workspace |