

SQL Migration CAF Governance Security Policies

**List of Contents**

[1. SQL Migration Azure Policy Configuration 3](#_Toc43903748)

[1.1 Compliance Manager 3](#_Toc43903749)

[1.2 Azure Policy 3](#_Toc43903750)

[2. Policy Initiatives 4](#_Toc43903751)

[3. Policy Samples 4](#_Toc43903752)

[3.1 SQL 4](#_Toc43903755)

[3.1.1 Transparent Data Encryption on SQL databases should be enabled 5](#_Toc43903756)

[3.1.2 Audit SQL server level Auditing settings 5](#_Toc43903757)

[3.1.3 Auditing should be enabled on advanced data security settings on SQL Server 5](#_Toc43903758)

[3.1.4 Deploy Threat Detection on SQL servers 6](#_Toc43903759)

[3.2 Security 6](#_Toc43903760)

[3.2.1 Vulnerability assessment should be enabled on your SQL servers 6](#_Toc43903761)

[3.2.2 Vulnerability assessment should be enabled on your SQL managed instances 6](#_Toc43903762)

[3.2.3 Vulnerability Assessment should be enabled on Virtual Machines 7](#_Toc43903763)

[3.2.4 Access through Internet facing endpoint should be restricted 7](#_Toc43903764)

[3.2.5 Enable Azure Security Center on your subscription 7](#_Toc43903765)

[3.2.6 Just-In-Time network access control should be applied on virtual machines 8](#_Toc43903766)

[3.2.7 Subnets should be associated with a Network Security Group 8](#_Toc43903767)

[3.3 Network 8](#_Toc43903768)

[3.3.1 Virtual networks should use specified virtual network gateway 8](#_Toc43903769)

[3.3.2 Virtual machines should be connected to an approved virtual network 9](#_Toc43903770)

[3.3.3 Network Watcher should be enabled 9](#_Toc43903771)

[3.3.4 All Internet traffic should be routed via your deployed Azure Firewall 10](#_Toc43903772)

[3.4 General 10](#_Toc43903773)

[3.4.1 Audit usage of custom RBAC rules 10](#_Toc43903774)

[3.4.2 Allowed locations for resource groups 11](#_Toc43903775)

[3.4.3 Allowed locations 11](#_Toc43903776)

[3.5 Compute 11](#_Toc43903777)

[3.5.1 Require automatic OS image patching on Virtual Machine Scale Sets 12](#_Toc43903778)

[3.5.2 Approved VM images 12](#_Toc43903779)

[3.6 Security Center 13](#_Toc43903780)

[3.6.1 Email notification for high severity alerts should be enabled 13](#_Toc43903781)

[3.6.2 MFA should be enabled on accounts with owner permissions on your subscription 13](#_Toc43903782)

[3.6.3 Monitor missing Endpoint Protection in Azure Security Center 14](#_Toc43903783)

[3.6.4 Vulnerabilities in security configuration on your machines should be remediated 14](#_Toc43903784)

# SQL Migration Azure Policy Configuration

Business has their own “Policies” to protect data and workloads in their infrastructures. Most of the time end goal of these policies is to make sure if “IT department” done their part to support business compliance requirements. There are two great tools available from Microsoft to make it easier for enterprises to reach their corporate compliance requirements within Azure environments. This section will specifically discuss following

* Compliance Manager
* Azure Policy

## Compliance Manager

This service can scan your azure environment and provide report of your compliance level against most common industry standard such as GDPR, ISO 27000 etc.

## Azure Policy

This is more to review continues compliance in corporate infrastructure policies. As an example, a corporate need to make sure all their Azure resources are deployed under west us region. With help of Azure policy, we can continuously monitor resources and make sure it does stay compliance with that policy. in event of breach it will flag it up as well.

Azure Policy does have inbuilt policy definitions (at the time this article written). These are covering most infrastructure Management, Audit, and security requirements. Users can use these inbuilt policies or build their own. Azure Policy definition are JSON based and each policy has following elements-

* Mode
* Parameters
* Display Name
* Description
* Policy Rule
* Logical Evaluation
* Effect

**Mode:**

This is to define the resource type considered in the policy. There are two modes in a policy.

* **All*:*** All resource types. This is the recommended mode for policies
* **Indexed**: Resource types that support tags and locations

**Parameters:**

If you work with programming language or PowerShell, I am sure you already know what parameter is. Here it is the same meaning; Parameter is a special kind of variable which refer to piece of data. It simply the policy by reducing code. Following is extracted from a policy to show the parameter usage.

**"parameters": {**

**"publisher": {**

**"type": "String",**

**"metadata": {**

**"description": "The publisher of the extension",**

**"strongType": "type",**

**"displayName": "Extension Publisher"**

**}**

**Display Name & Description:**

It is just to identify the policy, description also used to add more meaning.

**Policy Rule:**

It is the heart of the policy, it describes the policy using **logical operators, conditions,** and **effect**.

Under the policy rule following Operators and Types supported.

|  |  |
| --- | --- |
| **Logical Operators:** | ***"not", "allOf", "anyOf"*** |
| **Conditions Types:** | **"equals", "notEquals", "like", "notLike", "match", "notMatch", "contains", "notContains", "in", "notIn", "containsKey", "notContainsKey", "exists"** |

Under a Policy Rule, following **effects** can use,

* **Deny:** Generate event in audit log and fail the request
* **Audit**: Only for auditing purpose and no request decision made
* **Append:**Add additional fields to the request
* **AuditIfNotExists:** Enable auditing if the resource not existing
* **DeployIfNotExists:** Deploy if resource is not existing

# Policy Initiatives

Azure Policy also allows to group policies together and apply it one scope. This is called Policy Initiative. This reduce the complexity of policy assignment. As an example, we can create policy initiative called “Infrastructure Security” and include all infrastructure security related policies to it.

# Policy Samples

This section will specifically discuss following

* SQL
* Security
* Network
* General
* Compute
* Security Center



## SQL

Following are SQL Policy Samples

### Transparent Data Encryption on SQL databases should be enabled

Transparent data encryption should be enabled to protect data-at-rest and meet compliance requirements.

To help secure a database, you can take precautions like:

* Designing a secure system.
* Encrypting confidential assets.
* Building a firewall around the database servers.

But a malicious party who steals physical media like drives or backup tapes can restore or attach the database and browse its data. One solution is to encrypt sensitive data in a database and use a certificate to protect the keys that encrypt the data. This solution prevents anyone without the keys from using the data. But you must plan this kind of protection in advance.

TDE does real-time I/O encryption and decryption of data and log files. The encryption uses a database encryption key (DEK). The database boot record stores the key for availability during recovery. The DEK is a symmetric key. It's secured by a certificate that the server's master database stores or by an asymmetric key that an EKM module protects.

TDE protects data at rest, which is the data and log files. It lets you follow many laws, regulations, and guidelines established in various industries. This ability lets software developers encrypt data by using AES and 3DES encryption algorithms without changing existing applications.

**Effects:** AuditIfNotExists, Disabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/SQL/SqlDBEncryption_Audit.json)

### Audit SQL server level Auditing settings

Auditing for Azure SQL Database or SQL Server on Azure tracks database events and writes them to an audit log in your Azure storage account, Log Analytics workspace, or Event Hubs. Auditing also:

* Helps you maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.
* Enables and facilitates adherence to compliance standards, although it doesn't guarantee compliance. For more information about Azure programs that support standards compliance, see the Azure Trust Center where you can find the most current list of Azure SQL compliance certifications.

Azure SQL Database auditing is optimized for availability and performance. During very high activity Azure SQL Database or Azure Synapse allows operations to proceed and may not record some audited events.

**Effects:** AuditIfNotExists, Disabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/SQL/SqlServerAuditing_Audit.json)

### Auditing should be enabled on advanced data security settings on SQL Server

This policy enables Advanced Data Security on SQL Servers. This includes turning on Threat Detection and Vulnerability Assessment. It will automatically create a storage account in the same region and resource group as the SQL server to store scan results, with a 'sqlva' prefix.

Advanced Data Security (ADS) is a unified package for advanced SQL security capabilities. ADS is available for Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics. It includes functionality for discovering and classifying sensitive data, surfacing and mitigating potential database vulnerabilities, and detecting anomalous activities that could indicate a threat to your database. It provides a single go-to location for enabling and managing these capabilities.

**Effects:** DeployIfNotExists, Enabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/SQL/SqlServerAdvancedDataSecurity_Deploy.json)

### Deploy Threat Detection on SQL servers

This policy ensures that Threat Detection is enabled on SQL Servers.

Advanced Threat Protection for Azure SQL Database, Azure SQL Managed Instance detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases.

Advanced Threat Protection integrates alerts with [Azure Security Center](https://azure.microsoft.com/services/security-center/), which include details of suspicious activity and recommend action on how to investigate and mitigate the threat. Advanced Threat Protection makes it simple to address potential threats to the database without the need to be a security expert or manage advanced security monitoring systems.

For a full investigation experience, it is recommended to enable auditing, which writes database events to an audit log in your Azure storage account. To enable auditing, see [Auditing for Azure SQL Database and Azure Synapse](https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview) or [Auditing for Azure SQL Managed Instance](https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/auditing-configure).

**Effects:** DeployIfNotExists, Enabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/SQL/SqlDBEncryption_Audit.json)

## Security

Following are Security Policy Samples

### Vulnerability assessment should be enabled on your SQL servers

Audit Azure SQL servers which do not have recurring vulnerability assessment scans enabled. Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.

SQL Vulnerability Assessment is an easy-to-configure service that can discover, track, and help you remediate potential database vulnerabilities. Use it to proactively improve your database security. Vulnerability Assessment is part of the [Advanced Data Security](https://docs.microsoft.com/en-us/azure/azure-sql/database/advanced-data-security) offering, which is a unified package for advanced SQL security capabilities. Vulnerability Assessment can be accessed and managed via the central SQL Advanced Data Security portal.

**Effects:** AuditIfNotExists, Disabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/SQL/VulnerabilityAssessmentOnServer_Audit.json)

### Vulnerability assessment should be enabled on your SQL managed instances

Audit SQL managed instances which do not have recurring vulnerability assessment scans enabled. Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities. SQL Vulnerability Assessment is an easy-to-configure service that can discover, track, and help you remediate potential database vulnerabilities. Use it to proactively improve your database security.

Vulnerability Assessment is part of the [Advanced Data Security](https://docs.microsoft.com/en-us/azure/azure-sql/database/advanced-data-security) offering, which is a unified package for advanced SQL security capabilities. Vulnerability Assessment can be accessed and managed via the central SQL Advanced Data Security portal.

**Effects:** AuditIfNotExists, Disabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/SQL/VulnerabilityAssessmentOnServer_Audit.json)

### Vulnerability Assessment should be enabled on Virtual Machines

Monitors vulnerabilities detected by Azure Security Center Vulnerability Assessment on Virtual Machines.

**Effects:** AuditIfNotExists, Disabled

A core component of every cyber risk and security program is the identification and analysis of vulnerabilities. Azure Security Center's Standard pricing tier includes vulnerability scanning for your virtual machines at no extra cost. Additionally, Security Center can automatically deploy this tool for you.

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Security%20Center/ASC_ServerVulnerabilityAssessment_Audit.json)

### Access through Internet facing endpoint should be restricted

Azure Security center has identified some of your Network Security Groups' inbound rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to easily target your resources.

Azure Security Center will recommend that you restrict access through Internet-facing endpoints if any of your Network Security Groups (NSGs) has one or more inbound rules that allow access from “any” source IP address. Opening access to “any” may enable attackers to access your resources. Security Center will recommend that you edit these inbound rules to restrict access to source IP addresses that actually need access. To comply to this recommendation, you should restrict the NSG rules that have source IP address “any”, or remove the whole NSG rule. Solutions like JIT VM Access are perfect to resolve this recommendation.

**Effects**: AuditIfNotExists, Disabled

**Json File**: [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Security%20Center/ASC_UnprotectedEndpoints_Audit.json)

### Enable Azure Security Center on your subscription

Identifies existing subscriptions that are not monitored by Azure Security Center (ASC). Subscriptions not monitored by ASC will be registered to the free pricing tier. Subscriptions already monitored by ASC (free or standard), will be considered compliant. To register newly created subscriptions, open the compliance tab, select the relevant non-compliant assignment and create a remediation task. Repeat this step when you have one or more new subscriptions you want to monitor with Security Center.

**Effects:** deployIfNotExists

**Json File**: [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Security%20Center/ASC_Register_To_Azure_Security_Center_Deploy.json)

### Just-In-Time network access control should be applied on virtual machines

Possible network Just in Time (JIT) access will be monitored by Azure Security Center as recommendations.

In most common scenarios hackers targets open ports in servers to gain access. It can be web server port, RDP ports, SQL ports etc. If genuine users also use same ports to access the system, it’s hard to keep these ports closed. There are other methods such as firewalls that we can use to secure the access, but it will still keep the ports open. when it comes to public clouds, its increase your infrastructure’s public facing part. Its clients, administrators may access services over the internet mostly. In that case it will give more time and room for attackers to target open ports.

Azure Just-in-Time VM Access is a great option to control this. As an example, if engineers need to do work in their VM’s mostly they RDP into the system. Let’s assume they work 1 hour per day on servers. so, keeping port open for 24 hours not giving any benefits rather than risk. Using Just-in-Time VM Access we can limit the time it keeps RDP ports open.

When Just-in-Time VM Access enabled, we can define what VM and what ports will be controlled. In most scenarios you do not need to control access to ports used by your applications or services. It will be more in to ports related to management tasks. This all done by using azure network security group rules. You can find more about NSG using <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg>

**Effects:** AuditIfNotExists, Disabled

**Json File**: [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Security%20Center/ASC_JITNetworkAccess_Audit.json)

### Subnets should be associated with a Network Security Group

Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.

Azure Security Center recommends that you enable a network security group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your VM instances in a Virtual Network. NSGs can be associated with either subnets or individual VM instances within that subnet. When an NSG is associated with a subnet, the ACL rules apply to all the VM instances in that subnet. In addition, traffic to an individual VM can be restricted further by associating an NSG directly to that VM.

If you do not have NSGs enabled, Security Center presents two recommendations to you: Enable Network Security Groups on subnets and Enable Network Security Groups on virtual machines. You choose which level, subnet or VM, to apply NSGs.

**Effects:** AuditIfNotExists, Disabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Security%20Center/ASC_NetworkSecurityGroupsOnSubnets_Audit.json)

## Network

Following are Network Policy Samples

### Virtual networks should use specified virtual network gateway

A virtual network gateway serves two purposes: exchange IP routes between the networks and route network traffic.

The two gateway types are:

* **VPN** - To send encrypted traffic across the public Internet, you use the gateway type 'Vpn'. This is also referred to as a VPN gateway. Site-to-Site, Point-to-Site, and VNet-to-VNet connections all use a VPN gateway.
* **ExpressRoute** - To send network traffic on a private connection, you use the gateway type 'ExpressRoute'. This is also referred to as an ExpressRoute gateway and is the type of gateway used when configuring ExpressRoute.

Each virtual network can have only one virtual network gateway per gateway type. For example, you can have one virtual network gateway that uses -GatewayType Vpn, and one that uses -GatewayType ExpressRoute.

You can set up policies to govern which virtual network gateway should be used by a resource. This policy audits any virtual network if the default route does not point to the specified virtual network gateway.

**Effects:** AuditIfNotExists, Disabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Network/VirtualNetwork_ApprovedVirtualNetworkGateway_AuditIfNotExists.json)

### Virtual machines should be connected to an approved virtual network

Azure requires virtual machines to be connected to an Azure Virtual Network. A virtual network is a logical construct built on top of the physical Azure network fabric. Each virtual network is isolated from all other virtual networks. This helps ensure that network traffic in your deployments is not accessible to other Azure customers.

It is essential that the virtual network is reviewed to ensure security and high availability of resources connected to it.

This policy audits any virtual machine connected to a virtual network that is not approved.

**Effects:** Audit, Deny, Disabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Network/ApprovedVirtualNetwork_Audit.json)

### Network Watcher should be enabled

Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in an Azure virtual network. Network Watcher is designed to monitor and repair the network health of IaaS (Infrastructure-as-a-Service) products which includes Virtual Machines, Virtual Networks, Application Gateways, Load balancers, etc.

**Monitoring capabilities**: Scenario level monitoring enables you to diagnose problems at an end to end network level view.

* Monitor communication between a virtual machine and an endpoint
* View resources in a virtual network and their relationships

**Diagnostics capabilities**: Network diagnostic and visualization tools available with Network Watcher help you understand, diagnose, and gain insights to your network in Azure.

* Diagnose network traffic filtering problems to or from a VM
* Diagnose network routing problems from a VM
* Diagnose outbound connections from a VM
* Capture packets to and from a VM
* Diagnose problems with an Azure Virtual network gateway and connections

When you create or update a virtual network in your subscription, Network Watcher will be enabled automatically in your Virtual Network's region. There is no impact to your resources or associated charge for automatically enabling Network Watcher. Create a policy to audit if network watcher is not enabled.

**Effects:** auditIfNotExists

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Network/NetworkWatcher_Enabled_Audit.json)

### All Internet traffic should be routed via your deployed Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall-as-a-service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.

**Outbound SNAT support**: All outbound virtual network traffic IP addresses are translated to the Azure Firewall public IP (Source Network Address Translation). You can identify and allow traffic originating from your virtual network to remote Internet destinations. If your organization uses a public IP address range for private networks, Azure Firewall will SNAT the traffic to one of the firewall private IP addresses in AzureFirewallSubnet. You can configure Azure Firewall to not SNAT your public IP address range. For more information, see [Azure Firewall SNAT private IP address ranges](https://docs.microsoft.com/en-us/azure/firewall/snat-private-range).

**Inbound DNAT support**: Inbound Internet network traffic to your firewall public IP address is translated (Destination Network Address Translation) and filtered to the private IP addresses on your virtual networks.

**Forced tunneling**: You can configure Azure Firewall to route all Internet-bound traffic to a designated next hop instead of going directly to the Internet. For example, you may have an on-premises edge firewall or other network virtual appliance (NVA) to process network traffic before it's passed to the Internet. For more information, see [Azure Firewall forced tunneling](https://docs.microsoft.com/en-us/azure/firewall/forced-tunneling). Azure Security Center can identify subnets that aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall.

**Effects**: AuditIfNotExists, Disabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Network/ASC_All_Internet_traffic_should_be_routed_via_Azure_Firewall.json)

## General

Following are General Policy Samples

### Audit usage of custom RBAC rules

Sometimes you need information about Azure role-based access control (Azure RBAC) changes, such as for auditing or troubleshooting purposes. Anytime someone makes changes to role assignments or role definitions within your subscriptions, the changes get logged in [Azure Activity Log](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/platform-logs-overview). You can view the activity logs to see all the Azure RBAC changes for the past 90 days. Here are the Azure RBAC-related operations that are logged in Activity Log:

* Create role assignment
* Delete role assignment
* Create or update custom role definition
* Delete custom role definition

[Azure Monitor logs](https://docs.microsoft.com/en-us/azure/log-analytics/log-analytics-overview) is another tool you can use to collect and analyze Azure RBAC changes for all your Azure resources. Azure Monitor logs has the following benefits:

* Write complex queries and logic
* Integrate with alerts, Power BI, and other tools
* Save data for longer retention periods
* Cross-reference with other logs such as security, virtual machine, and custom

If the Azure built-in roles don't meet the specific needs of your organization, you can create your own custom roles. Just like built-in roles, you can assign custom roles to users, groups, and service principals at management group, subscription, and resource group scopes. Create a policy to audit built-in roles such as 'Owner, Contributer, Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and requires a rigorous review and threat modeling.

**Effects**: Audit, Disabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/General/Subscription_AuditCustomRBACRoles_Audit.json)

### Allowed locations for resource groups

Resource group is a container that holds related resources for an Azure solution. The resource group includes those resources that you want to manage as a group. You decide which resources belong in a resource group based on what makes the most sense for your organization. A resource group can contain resources that are located in different regions.

When creating a resource group, you need to provide a location for that resource group. The resource group stores metadata about the resources. When you specify a location for the resource group, you're specifying where that metadata is stored. For compliance reasons, you may need to ensure that your data is stored in a particular region. This policy enables you to restrict the locations your organization can create resource groups in. Use to enforce your geo-compliance requirements.

**Effects**: deny

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/General/ResourceGroupAllowedLocations_Deny.json)

### Allowed locations

For compliance reasons, you may need to ensure that your data in the resource is stored in a particular region. This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforceyour geo-compliance requirements. Excludes resource groups, Microsoft.AzureActiveDirectory/b2cDirectories, and resources that use the 'global' region.

**Effects:** deny

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/General/AllowedLocations_Deny.json)

## Compute

Following are Compute Policy Samples

### Require automatic OS image patching on Virtual Machine Scale Sets

Azure virtual machine scale sets let you create and manage a group of identical, load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs. With virtual machine scale sets, you can build large-scale services for areas such as compute, big data, and container workloads. Enabling automatic OS image upgrades on your scale set helps ease update management by safely and automatically upgrading the OS disk for all instances in the scale set.

Automatic OS upgrade has the following characteristics:

* Once configured, the latest OS image published by image publishers is automatically applied to the scale set without user intervention.
* Upgrades batches of instances in a rolling manner each time a new image is published by the publisher.
* Integrates with application health probes and [Application Health extension](https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-health-extension).
* Works for all VM sizes, and for both Windows and Linux images.
* You can opt out of automatic upgrades at any time (OS Upgrades can be initiated manually as well).
* The OS Disk of a VM is replaced with the new OS Disk created with latest image version. Configured extensions and custom data scripts are run, while persisted data disks are retained.
* Extension sequencing is supported.
* Automatic OS image upgrade can be enabled on a scale set of any size.

This policy enforces enabling automatic OS image patching on Virtual Machine Scale Sets to always keep Virtual Machines secure by safely applying latest security patches every month.

**Effects**: Deny

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Compute/VMSSOSUpgradeHealthCheck_Deny.json)

### Approved VM images

A VM Image encompasses the full definition of a virtual machine’s storage, containing the OS disk and all data disks. It captures the disk properties (such as host caching) you need in order to deploy a VM in a reusable unit. Similar to OS Images, a VM Image is a collection of metadata and pointers to a set of VHDs (one VHD per disk) stored as page blobs in Azure Storage. A VM Image containing a single VHD with a generalized operating system is essentially the OS image. There are two types of VM Images

* A generalized VM Image contains an OS disk, which, as the name suggests, has been generalized and needs to be provisioned during deployment time. OS Images today are generalized. This type of VM Image is meant to be used as a “model” to quickly stamp out similar virtual machines, such as scaling out a front-end to your application in production or spinning up and tearing down similar development and test environments quickly.
* A specialized VM Image contains an OS disk, which is already provisioned. It is similar to a disk today in that it is “ready-to-use”, but unlike a disk, the VHDs of a VM Image are treated as read-only and copied when deploying a new virtual machine. A specialized VM Image is meant to be used as a “snapshot” to deploy a VM to a good known point in time, such as checkpointing a developer machine, before performing a task which may go wrong and render the virtual machine useless. It is not meant to be a mechanism to clone multiple identical virtual machines in the same virtual network due to the Windows requirement of Sysprep for image replication.

This policy governs that only a VM image from the approved list of VM images can be installed.

**Effects**: deny

**Json File:** [Link](https://github.com/people-tech-group/wvdcaf/blob/master/wvd/policies/vmImages/approvedVMimages.json)

## Security Center

Following are Security Center Policy Samples

### Email notification for high severity alerts should be enabled

Azure Security Center will recommend that you provide security contact details for your Azure subscription if you haven't already. This information will be used by Microsoft to contact you if the Microsoft Security Response Center (MSRC) discovers that your customer data has been accessed by an unlawful or unauthorized party. MSRC performs select security monitoring of the Azure network and infrastructure and receives threat intelligence and abuse complaints from third parties.

An email notification is sent on the first daily occurrence of an alert and only for high severity alerts. Email preferences can only be configured for subscription policies. Resource groups within a subscription will inherit these settings. Alerts are available only in the Standard tier of Azure Security Center.

Alert email notifications are sent:

* To a single email recipient per alert type per day
* No more than 3 email messages are sent to a single recipient in a single day
* Each email message contains a single alert, not an aggregation of alerts
* Only for high severity alerts

Enable emailing security alerts to the security contact, in order to have them receive security alert emails from Microsoft. This ensures that the right people are aware of any potential security issues and are able to mitigate the risks.

**Effects**: AuditIfNotExists, Disabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Security%20Center/ASC_Email_notification.json)

### MFA should be enabled on accounts with owner permissions on your subscription

Multi-factor authentication (MFA) is a process where a user is prompted during a sign-in event for additional forms of identification. This prompt could be to enter a code on their cellphone or to provide a fingerprint scan. When you require a second form of authentication, security is increased as this additional factor isn't something that's easy for an attacker to obtain or duplicate. Azure Multi-Factor Authentication and Conditional Access policies give the flexibility to enable MFA for users during specific sign-in events.

The recommended way to enable and use Azure Multi-Factor Authentication is with Conditional Access policies. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.

Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.

**Effects**: AuditIfNotExists, Disabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Security%20Center/ASC_EnableMFAForOwnerPermissions_Audit.json)

### Monitor missing Endpoint Protection in Azure Security Center

Microsoft Endpoint Protection for Azure helps protect your virtual machine from malicious software (malware) such as viruses, spyware, and other potentially harmful software. It offers three ways to help protect your virtual machine from malware and other potentially unwanted software:

* **Real-time protection**. Microsoft Endpoint Protection for Azure alerts you when malware, spyware, or potentially unwanted software attempts to install or run on your virtual machine. It also alerts you when programs attempt to change important Windows settings.
* **Scanning options**. You can use Microsoft Endpoint Protection for Azure to scan for threats, viruses, spyware, and other potentially unwanted software that might be installed on your virtual machine, to schedule scans on a regular basis, and to automatically remove any malicious software that is detected during a scan.
* **Detection/Remediation**. Should malicious software be detected on your virtual machine, certain actions will automatically be taken to, remove the malicious software and protect your virtual machine from potential further infection. Once the malicious software is removed, Microsoft Endpoint Protection for Azure may also reset some Windows settings (such as your home page and search provider).

Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations.

**Effects**: AuditIfNotExists, Disabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Security%20Center/ASC_MissingEndpointProtection_Audit.json)

### Vulnerabilities in security configuration on your machines should be remediated

Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations. Recommendations are actions for you to take in order to secure your resources. Security Center periodically analyzing the security state of your Azure resources to identify potential security vulnerabilities. It then provides you with recommendations on how to remove them. Each recommendation provides you with:

* A short description of what is being recommended.
* The remediation steps to carry out in order to implement the recommendation.
* Which resources are in need of you performing the recommended action on them.
* The Secure Score impact, which is the amount that your Secure Score will go up if you implement this recommendation.

**Effects**: AuditIfNotExists, Disabled

**Json File:** [Link](https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Security%20Center/ASC_OSVulnerabilities_Audit.json)