Best practice rules for Microsoft Azure

Microsoft® Azure best practice rules

Trend Micro Cloud One™ – Conformity has over 750+ cloud infrastructure configuration best practices for your Amazon Web Services, Microsoft® Azure, and Google Cloud™ environments. Here is our growing list of Azure best practice rules with clear instructions on how to perform the updates – made either through the Azure console or via the Command Line Interface (CLI).

Conformity provides real-time monitoring and auto-remediation for the security, compliance and governance of your cloud infrastructure. Leaving you to grow and scale your business with confidence.

AKS

Check for Kubernetes Version

Ensure that AKS clusters are using the latest available version of Kubernetes software.

Enable Kubernetes Role-Based Access Control

Ensure that Kubernetes Role-Based Access Control is enabled for Azure Kubernetes clusters.

Access Control

Remove Custom Owner Roles

Ensure there are no custom owner roles within your Microsoft Azure cloud account.

Resource Locking Administrator Role

Ensure that a resource locking administrator role is available for each Azure subscription.

Active Directory

Allow Only Administrators to Create Security Groups

Ensure that security groups can be created only by Active Directory (AD) administrators.

Allow Only Administrators to Manage Office 365 Groups

Ensure that Office 365 groups can be managed only by Active Directory (AD) administrators.

Allow Only Administrators to Manage Security Groups

Ensure that security groups can be managed only by Active Directory (AD) administrators.

Check for Active Directory Guest Users

Ensure there are no Microsoft Azure Active Directory guest users if they are not needed.

Disable Remembering Multi-Factor Authentication

Do not allow users to remember Multi-Factor Authentication (MFA) on their devices and browsers.

Disable Self-Service Group Management

Ensure that Active Directory (AD) self-service group management is disabled for non-administrator users.

Enable Authentication Reconfirmation

Ensure that user authentication information reconfirmation is enabled within Active Directory password reset policy.

Enable Dual Identification for Password Reset

Ensure that the number of methods required for user password reset is set to 2 (two).

Enable Multi-Factor Authentication for Non-Privileged Users

Ensure that Multi-Factor Authentication feature is enabled for all non-privileged users.

Enable Multi-Factor Authentication for Privileged Users

Ensure that Multi-Factor Authentication (MFA) is enabled for all privileged Azure users

Enable Notifications for Administrator Password Resets

Ensure that Microsoft Azure Active Directory (AD) admins are notified on password resets.

Enable Notifications for User Password Resets

Ensure that Microsoft Azure Active Directory (AD) users are notified on password resets.

Enable Security Defaults

Ensure that Security Defaults is enabled for Microsoft Azure Active Directory.

Enforce Administrators to Provide Consent for Apps Before Use

Require Active Directory administrators to provide consent for applications before use.

Limit Guest User Permissions

Ensure that Active Directory (AD) guest users permissions are limited.

Require MFA to Join Devices

Ensure that joining devices to Active Directory requires Multi-Factor Authentication.

Restrict Adding Gallery Apps to Access Panel

Ensure that Active Directory users are not allowed to add applications to Azure Access Panel.

Restrict Application Registration for Non-Privileged Users

Ensure that non-privileged users are not allowed to register third-party applications.

Restrict Guest User Invitations

Ensure that guest users cannot invite other guests to collaborate with your organization.

Restrict Invitations to Administrators Only

Ensure that only Active Directory administrators can invite guests to your directory.

Restrict Non-Admin Access to Administration Portal

Ensure that non-administrator users are not allowed to access Active Directory administration portal.

Restrict Office 365 Group Creation to Administrators Only

Ensure that Office 365 groups can be created only by Active Directory (AD) administrators.

Restrict User Access to AAD Group Features in Azure Access Panel

Activity Log

Create Alert for "Create Policy Assignment" Events

Ensure that an activity log alert is created for the "Create Policy Assignment" events.

Create Alert for "Create or Update Load Balancer" Events

Ensure that an activity log alert is created for "Create or Update Load Balancer" events.

Create Alert for "Create or Update Security Solution" Events

Ensure that an activity log alert is created for the "Create/Update Security Solution" events.

Create Alert for "Create or Update Virtual Machine" Events

Ensure that an activity log alert is created for "Create or Update Virtual Machine (Microsoft.Compute/virtualMachines)" events.

Create Alert for "Create, Update or Delete SQL Server Firewall Rule" Events

Ensure that an activity log alert is created for the “Create/Update/Delete SQL Server Firewall Rule” events.

Create Alert for "Create/Update Azure SQL Database" Events

Ensure that an activity log alert is created for "Create/Update Azure SQL Database" events.

Create Alert for "Create/Update Network Security Group" Events

Ensure that an activity log alert is created for the "Create/Update Network Security Group" events.

Create Alert for "Create/Update Storage Account" Events

Ensure there is an activity log alert created for the "Create/Update Storage Account" events.

Create Alert for "Deallocate Virtual Machine" Events

Ensure that an activity log alert is created for the "Deallocate Virtual Machine (Microsoft.Compute/virtualMachines)" events.

Create Alert for "Delete Azure SQL Database" Events

Ensure that an activity log alert is created for "Delete Azure SQL Database (Microsoft.Sql/servers/databases)" events.

Create Alert for "Delete Key Vault" Events

Ensure there is an activity log alert created for the "Delete Key Vault" events.

Create Alert for "Delete Load Balancer" Events

Ensure there is an Azure activity log alert created for "Delete Load Balancer" events.

Create Alert for "Delete Network Security Group Rule" Events

Ensure that an activity log alert is created for the "Delete Network Security Group Rule" events.

Create Alert for "Delete Network Security Group" Events

Ensure that an activity log alert is created for the "Delete Network Security Group" events.

Create Alert for "Delete Security Solution" Events

Ensure that an activity log alert is created for the "Delete Security Solution" events.

Create Alert for "Delete Storage Account" Events

Ensure that an activity log alert exists for "Delete Storage Account" events.

Create Alert for "Delete Virtual Machine" Events

Ensure that an activity log alert exists for "Delete Virtual Machine" events.

Create Alert for "Power Off Virtual Machine" Events

Ensure that an activity log alert exists for "Power Off Virtual Machine" events.

Create Alert for "Rename Azure SQL Database" Events

Ensure that an activity log alert is created for "Rename Azure SQL Database" events.

Create Alert for "Update Key Vault" Events

Ensure that an activity log alert is created for "Update Key Vault (Microsoft.KeyVault/vaults)" events.

Create Alert for "Update Security Policy" Events

Ensure that an activity log alert is created for the "Update Security Policy" events.

Create Alert for “Create/Update MySQL Database” Events

Ensure that an activity log alert is created for “Create/Update MySQL Database” events.

Create Alert for “Create/Update Network Security Group Rule” Events

Ensure that an activity log alert is created for the “Create/Update Network Security Group Rule” events.

Create Alert for “Create/Update PostgreSQL Database” Events

Create Alert for "Delete PostgreSQL Database" Events

Ensure that an activity log alert is created for "Delete PostgreSQL Database" events.

Advisor

Check for Azure Advisor Recommendations

Ensure that Microsoft Azure Advisor recommendations are analyzed and implemented.

AppService

Check for Latest Version of .NET Framework

Enable HTTP to HTTPS redirects for your Microsoft Azure App Service web applications.

Check for Latest Version of Java

Ensure that Azure App Service web applications are using the latest stable version of Java.

Check for Latest Version of PHP

Ensure that Azure App Service web applications are using the latest version of PHP.

Check for Latest Version of Python

Ensure that Azure App Service web applications are using the latest version of Python.

Check for Sufficient Backup Retention Period

Ensure there is a sufficient backup retention period configured for Azure App Services applications.

Check for TLS Protocol Latest Version

Ensure that Azure App Service web applications are using the latest version of TLS encryption.

Disable Remote Debugging

Disable Remote Debugging feature for your Microsoft Azure App Services web applications.

Enable Always On

Ensure that your Azure App Services web applications stay loaded all the time by enabling the Always On feature.

Enable App Service Authentication

Ensure that App Service Authentication is enabled within your Microsoft Azure cloud account.

Enable Application Insights

Ensure that Azure App Services applications are configured to use Application Insights feature.

Enable Automated Backups

Ensure that all your Azure App Services applications are using the Backup and Restore feature.

Enable FTPS-Only Access

Enable FTPS-only access for your Microsoft Azure App Services web applications.

Enable HTTP/2

Ensure that Azure App Service web applications are using the latest stable version of HTTP.

Enable HTTPS-Only Traffic

Enable HTTP to HTTPS redirects for your Microsoft Azure App Service web applications.

Enable Incoming Client Certificates

Ensure that Azure App Service web applications are using incoming client certificates.

Enable Registration with Azure Active Directory

Ensure that registration with Azure Active Directory is enabled for Azure App Service applications.

CosmosDB

Enable Advanced Threat Protection

Ensure that Advanced Threat Protection is enabled for all Microsoft Azure Cosmos DB accounts.

Enable Automatic Failover

Enable automatic failover for Microsoft Azure Cosmos DB accounts.

Restrict Default Network Access for Azure Cosmos DB Accounts

Ensure that default network access (i.e. public access) is denied within your Azure Cosmos DB accounts configuration.

KeyVault

App Tier Customer-Managed Key In Use

Ensure that a Customer-Managed Key is created for your Azure cloud application tier.

Check for Allowed Certificate Key Types

Ensure that Azure Key Vault certificates are using the appropriate key type(s).

Check for Azure Key Vault Keys Expiration Date

Ensure that your Azure Key Vault encryption keys are renewed prior to their expiration date.

Check for Azure Key Vault Secrets Expiration Date

Ensure that your Azure Key Vault secrets are renewed prior to their expiration date.

Check for Certificate Minimum Key Size

Ensure that Azure Key Vault RSA certificates are using the appropriate key size.

Check for Key Vault Full Administrator Permissions

Ensure that no Azure user, group or application has full permissions to access and manage Key Vaults.

Check for Sufficient Certificate Auto-Renewal Period

Ensure there is a sufficient period configured for the SSL certificates auto-renewal.

Database Tier Customer-Managed Key In Use

Ensure that a Customer-Managed Key is created for your Microsoft Azure cloud database tier.

Enable AuditEvent Logging for Azure Key Vaults

Ensure that AuditEvent logging is enabled for your Microsoft Azure Key Vaults.

Enable Certificate Transparency

Ensure that certificate transparency is enabled for all your Azure Key Vault certificates.

Enable Key Vault Recoverability

Ensure that your Microsoft Azure Key Vault instances are recoverable.

Enable SSL Certificate Auto-Renewal

Ensure that Auto-Renewal feature is enabled for your Azure Key Vault SSL certificates.

Enable Trusted Microsoft Services for Key Vault Access

Allow trusted Microsoft services to access your Azure Key Vault resources (i.e. encryption keys, secrets and certificates).

Restrict Default Network Access for Azure Key Vaults

Ensure that default network access (i.e. public access) rule is set to "Deny" within your Azure Key Vaults configuration.

Set Azure Secret Key Expiration

Ensure that an expiration date is set for all your Microsoft Azure secret keys.

Set Encryption Key Expiration

Ensure that an expiration date is configured for all your Microsoft Azure encryption keys.

Web Tier Customer-Managed Key In Use

Ensure that a Customer-Managed Key is created for your Microsoft Azure cloud web tier.

Locks

Enable Azure Resource Locks

Ensure that resource locks are enabled for your high-impact Microsoft Azure resources.

Monitor

Activity Log All Activities

Ensure that Azure Log Profile is configured to export all control & management activities.

Activity Log All Regions

Ensure that Azure Log Profile is configured to capture activity logs for all regions.

Activity Log Retention

Ensure that Azure activity log retention period is set for 365 days or greater.

Azure Activity Log Profile in Use

Ensure that a Log Profile exists for each subscription available in your Azure account.

Use Bring Your Own Key (BYOK) for Azure activity log storage container encryption.

MySQL

Enable In-Transit Encryption for MySQL Servers

Ensure that in-transit encryption is enabled for your Azure MySQL database servers.

Network

Check for NSG Flow Log Retention Period

Ensure that Network Security Group (NSG) flow log retention period is greater than or equal to 90 days.

Check for Network Security Groups with Port Ranges

Ensure there are no network security groups with range of ports opened to allow incoming traffic.

Check for Unrestricted FTP Access

Ensure that no network security groups allow unrestricted inbound access on TCP port 20 and 21 (File Transfer Protocol – FTP).

Check for Unrestricted MS SQL Server Access

Ensure that no network security groups allow unrestricted inbound access on TCP port 1433 (Microsoft SQL Server).

Check for Unrestricted MySQL Database Access

Ensure that no network security groups allow unrestricted ingress access on TCP port 3306 (MySQL Database).

Check for Unrestricted Oracle Database Access

Ensure that no network security groups allow unrestricted inbound access on TCP port 1521 (Oracle Database).

Check for Unrestricted PostgreSQL Database Access

Ensure that no network security groups allow unrestricted inbound access on TCP port 5432 (PostgreSQL Database Server).

Check for Unrestricted RDP Access

Ensure that no network security groups allow unrestricted inbound access on TCP port 3389 (Remote Desktop Protocol – RDP).

Check for Unrestricted RPC Access

Ensure that no network security groups allow unrestricted inbound access on TCP port 135 (Remote Procedure Call – RPC).

Check for Unrestricted SSH Access

Ensure that no network security groups allow unrestricted inbound access on TCP port 22 (SSH).

Enable Azure Network Watcher

Ensure that Network Watcher service is enabled for all your Microsoft Azure subscriptions.

Enable DDoS Standard Protection for Virtual Networks

Ensure that DDoS standard protection is enabled for production Azure virtual networks.

Monitor Network Security Group Configuration Changes

Network security group changes have been detected in your Microsoft Azure cloud account.

Review Network Interfaces with IP Forwarding Enabled

Ensure that the Azure network interfaces with IP forwarding enabled are regularly reviewed.

Policy

Policy Assignment Created

Policy assignment changes have been detected in your Microsoft Azure cloud account.

PostgreSQL

Check for PostgreSQL Log Retention Period

Ensure that PostgreSQL database servers have a sufficient log retention period configured.

Check for PostgreSQL Major Version

Ensure that PostgreSQL database servers are using the latest major version of PostgreSQL database.

Enable "CONNECTION_THROTTLING" Parameter for PostgreSQL Servers

Ensure that "connection_throttling" parameter is set to "ON" within your Azure PostgreSQL server settings.

Enable "LOG_CHECKPOINTS" Parameter for PostgreSQL Servers

Enable "log_checkpoints" parameter for your Microsoft Azure PostgreSQL database servers.

Enable "LOG_CONNECTIONS" Parameter for PostgreSQL Servers

Enable "log_connections" parameter for your Microsoft Azure PostgreSQL database servers.

Enable "LOG_DISCONNECTIONS" Parameter for PostgreSQL Servers

Enable "log_disconnections" parameter for your Microsoft Azure PostgreSQL database servers.

Enable "LOG_DURATION" Parameter for PostgreSQL Servers

Enable "log_duration" parameter on your Microsoft Azure PostgreSQL database servers.

Enable Geo-Redundant Backups

Ensure that geo-redundant backups are enabled for your Azure PostgreSQL database servers.

Enable In-Transit Encryption for PostgreSQL Database Servers

Ensure that in-transit encryption is enabled for your Azure PostgreSQL database servers.

Enable Storage Auto-Growth

Ensure that storage auto-growth is enabled for your Microsoft Azure PostgreSQL database servers.

Use Azure Active Directory Admin for PostgreSQL Authentication

Ensure that an Azure Active Directory (AAD) admin is configured for PostgreSQL authentication.

Recovery Services

Enable Email Notifications for Backup Alerts

Ensure that email notifications are enabled for virtual machine (VM) backup alerts.

Redis Cache

Check for TLS Protocol Latest Version

Ensure that Azure Redis Cache servers are using the latest version of the TLS protocol.

Enable In-Transit Encryption for Redis Cache Servers

Ensure that in-transit encryption is enabled for all Microsoft Azure Redis Cache servers.

Resources

Tags

Ensure there is a tagging strategy in use for identifying and organizing Azure resources by name, purpose, environment, and other criteria.

Search

Enable System-Assigned Managed Identities

Ensure that Azure Search Service instances are configured to use system-assigned managed identities.

Security Center

Check for Azure Security Center Recommendations

Ensure that Microsoft Azure Security Center recommendations are examined and resolved.

Configure Additional Email Addresses for Azure Security Center Notifications

Ensure that additional email addresses are provided to receive security notifications.

Detect Create, Update or Delete Security Solution Events

Security solution changes have been detected within your Microsoft Azure cloud account.

Detect Update Security Policy Event

Azure security policy changes have been detected within your Microsoft Azure cloud account.

Enable Adaptive Application Safelisting Monitoring

Enable adaptive application safelisting monitoring for Microsoft Azure virtual machines.

Enable Alert Notifications for Subscription Owners

Ensure that "Also send email notification to subscription owners" feature is enabled within Azure Security Center.

Enable All Parameters for ASC Default Policy

Ensure that all the supported ASC Default policy parameters are enabled.

Enable Automatic Provisioning of the Monitoring Agent

Ensure that "Automatic provisioning of monitoring agent" feature is enabled to enhance security at the virtual machine (VM) level.

Enable Azure Defender for Azure SQL Database Servers

Ensure that Azure Defender is enabled for Microsoft SQL database servers.

Enable Azure Defender for Azure Storage Accounts

Ensure that the Azure Defender feature is enabled for Azure Storage accounts.

Enable DDoS Protection Standard Monitoring for Public Virtual Networks

Ensure that monitoring of DDoS protection at the Azure virtual network level is enabled.

Enable Disk Encryption Monitoring

Enable disk encryption monitoring for Microsoft Azure virtual machines (VMs).

Enable Email Notification for Alerts

Ensure that "Email Notification for Alerts" security feature is enabled within Azure Security Center.

Enable Endpoint Protection Monitoring

Enable endpoint protection monitoring and recommendations for Microsoft Azure virtual machines.

Enable JIT Network Access Monitoring

Ensure that JIT network access monitoring for Azure virtual machines (VMs) is enabled.

Enable Monitoring for OS Vulnerabilities

Enable OS vulnerability monitoring for Microsoft Azure virtual machines (VMs).

Enable Monitoring of Deprecated Accounts

Ensure that monitoring of deprecated accounts within your Azure subscription(s) is enabled.

Enable Network Security Group Monitoring

Enable network security group recommendations for Microsoft Azure virtual machines (VMs).

Enable Next Generation Firewall (NGFW) Monitoring

Ensure that next generation firewall monitoring for Azure virtual machines (VMs) is enabled.

Enable SQL Auditing Monitoring

Enable SQL auditing and threat detection monitoring for Microsoft Azure SQL servers.

Enable SQL Encryption Monitoring

Enable SQL encryption monitoring and recommendations for Microsoft Azure SQL servers.

Enable Standard Pricing Tier

Ensure that Security Center standard pricing tier is enabled in your Microsoft Azure account.

Enable Storage Encryption Monitoring

Enable storage encryption monitoring and recommendations for Azure Storage

Enable Web Application Firewall Monitoring

Enable web application firewall monitoring for Microsoft Azure virtual machines (VMs).

Monitor External Accounts with Write Permissions

Ensure that the external accounts with write permissions are monitored using Azure Security Center.

Monitor the Total Number of Subscription Owners

Ensure that the total number of subscription owners within your Azure account is monitored.

Security Contact Emails In Use

Ensure that one or more security contact email addresses are defined within Azure Security Center settings.

Security Contact Phone Numbers In Use

Ensure that a security contact phone number is provided in the Azure Security Center settings.

Sql

Advanced Data Security for SQL Servers

Ensure that Advanced Data Security (ADS) is enabled at the Azure SQL database server level.

Check for Publicly Accessible SQL Servers

Ensure that Azure SQL database servers are accessible via private endpoints only.

Check for Sufficient Point in Time Restore (PITR) Backup Retention Period

Ensure there is a sufficient PITR backup retention period configured for Azure SQL databases.

Check for Unrestricted SQL Database Access

Ensure that no SQL databases allow unrestricted inbound access from 0.0.0.0/0 (any IP address).

Configure "AuditActionGroup" for SQL Server Auditing

Ensure that "AuditActionGroup" property is well configured at the Azure SQL database server level.

Detect Create, Update, and Delete SQL Server Firewall Rule Events

SQL Server firewall rule changes have been detected in your Microsoft Azure cloud account.

Enable All Types of Threat Detection on SQL Servers

Enable all types of threat detection for your Microsoft Azure SQL database servers.

Enable Auditing for SQL Servers

Ensure that database auditing is enabled at the Azure SQL database server level.

Enable Auto-Failover Groups

Ensure that your Azure SQL database servers are configured to use auto-failover groups.

Enable Automatic Tuning for SQL Database Servers

Ensure that Automatic Tuning feature is enabled for Microsoft Azure SQL database servers.

Enable Email Alerts for Administrators and Subscription Owners

Enable administrators and subscription owners to receive threat detection email notification alerts for SQL servers.

Enable Email Alerts for SQL Threat Detection Service

Enable threat detection email notification alerts for your Microsoft Azure SQL servers.

Enable Transparent Data Encryption for SQL Databases

Ensure that Transparent Data Encryption (TDE) is enabled for every Azure SQL database.

SQL Auditing Retention

Ensure that SQL database auditing has a sufficient log data retention period configured.

Use Azure Active Directory Admin for SQL Authentication

Ensure that an Azure Active Directory (AAD) admin is configured for SQL authentication.

Use BYOK for Transparent Data Encryption

Use Bring Your Own Key (BYOK) support for Transparent Data Encryption (TDE).

Enable Virtual Machine IP Forwarding Monitoring

Ensure that IP forwarding enabled on your Azure virtual machines (VMs) is being monitored.

Enable Vulnerability Assessment Monitoring

Ensure that vulnerability assessment monitoring for Azure virtual machines (VMs) is enabled.

Storage Accounts

Allow Shared Access Signature Tokens Over HTTPS Only

Ensure that Shared Access Signature (SAS) tokens are allowed only over the HTTPS protocol.

Check for Overly Permissive Stored Access Policies

Ensure that Azure Storage shared access signature (SAS) tokens are not using overly permissive access policies.

Check for Publicly Accessible Web Containers

Ensure that Azure Storage containers created to host static websites are not publicly accessible.

Check for Sufficient Soft Deleted Data Retention Period

Ensure there is a sufficient retention period configured for Azure Blob Storage soft deleted data.

Disable Anonymous Access to Blob Containers

Ensure that anonymous access to blob containers is disabled within your Azure Storage account.

Enable Blob Storage Lifecycle Management

Ensure that Azure Blob Storage service has a lifecycle management policy configured.

Enable Immutable Blob Storage

Ensure that critical Azure Blob Storage data is protected from accidental deletion or modification.

Enable Logging for Azure Storage Queue Service

Ensure that detailed storage logging is enabled for the Azure Storage Queue service.

Enable Secure Transfer in Azure Storage

Ensure that "Secure transfer required" security feature is enabled within your Azure Storage account configuration.

Enable Soft Delete for Azure Blob Storage

Ensure that Soft Delete feature is enabled for your Microsoft Azure Storage blob objects.

Enable Trusted Microsoft Services for Storage Account Access

Allow Trusted Microsoft Services to access your Azure Storage account resources.

Expire Shared Access Signature Tokens

Ensure that your Shared Access Signature (SAS) tokens expire within an hour.

Limit Storage Account Access by IP Address

Ensure that Azure Storage account access is limited only to specific IP address(es).

Regenerate Storage Account Access Keys Periodically

Regenerate storage account access keys periodically to help keep your storage account secure.

Restrict Default Network Access for Storage Accounts

Ensure that the default network access rule is set to "Deny" within your Azure Storage account.

Review Storage Accounts with Static Website Configuration

Ensure that Azure Storage Accounts with static website configuration are regularly reviewed (informational).

Use BYOK for Storage Account Encryption

Use customer-managed keys (CMKs) for Microsoft Azure Storage accounts encryption.

Subscriptions

Check for Azure Cloud Budget Alerts

Ensure there are budget alerts configured to warn about forthcoming budget overages within your Azure cloud account.

Check for the Number of Subscription Owners

Ensure there is more than one owner assigned to your Microsoft Azure subscription.

Ensure "Not Allowed Resource Types" Policy Assignment in Use

To prevent certain resource types from being deployed ensure that "Not Allowed Resource Types" policy is assigned.

Virtual Machines

Apply Latest OS Patches

Ensure that the latest OS patches available for Microsoft Azure virtual machines are applied.

Approved Azure Machine Image in Use

Ensure that all your Azure virtual machine instances are launched from approved machine images only.

Check for Associated Load Balancers

Ensure that your Azure virtual machine scale sets are using load balancers for traffic distribution.

Check for Desired VM SKU Size(s)

Ensure that your virtual machine instances are of a given SKU size (e.g. Standard_A8_v2).

Check for Empty Virtual Machine Scale Sets

Identify and remove empty virtual machine scale sets from your Azure cloud account.

Check for SSH Authentication Type

Ensure that Azure Linux-based virtual machines (VMs) are configured to use SSH keys.

Check for Sufficient Daily Backup Retention Period

Ensure there is a sufficient daily backup retention period configured for Azure virtual machines.

Check for Sufficient Instant Restore Retention Period

Ensure there is a sufficient instant restore retention period configured for Azure virtual machines.

Check for Unused Load Balancers

Identify and remove unused load balancers from your Microsoft Azure cloud account.

Check for Zone-Redundant Virtual Machine Scale Sets

Ensure that Azure virtual machine scale sets are configured for zone redundancy.

Disable Premium SSD

Ensure that Azure virtual machines are using Standard SSD disk volumes instead of Premium SSD volumes to optimize VM costs.

Enable Accelerated Networking for Virtual Machines

Ensure that Microsoft Azure virtual machines are configured to use accelerated networking.

Enable Auto-Shutdown

Configure your Microsoft Azure virtual machines to automatically shut down on a daily basis.

Enable Automatic Instance Repairs

Ensure that Azure virtual machine scale sets are configured to use automatic instance repairs

Enable Automatic OS Upgrades

Ensure that Automatic OS Upgrades feature is enabled for your Azure virtual machine scale sets.

Enable Autoscale Notifications

Ensure that autoscale notifications are enabled for Azure virtual machine scale sets.

Enable Backups for Azure Virtual Machines

Ensure that Microsoft Azure Backup service is in use for your Azure virtual machines (VMs).

Enable Encryption for App-Tier Disk Volumes

Ensure that Azure virtual machine disk volumes created for the app tier are encrypted.

Enable Encryption for Boot Disk Volumes

Ensure that encryption is enabled for Azure virtual machine boot volumes to protect data at rest.

Enable Encryption for Non-Boot Disk Volumes

Ensure that encryption at rest is enabled for Microsoft Azure virtual machine non-boot volumes.

Enable Encryption for Unattached Disk Volumes

Ensure that encryption at rest is enabled for unattached Azure virtual machine disk volumes.

Enable Encryption for Web-Tier Disk Volumes

Ensure that Azure virtual machine disk volumes deployed within the web tier are

monitoring.

Enable Instance Termination Notifications for Virtual Machine Scale Sets

Ensure that instance termination notifications are enabled for your Azure virtual machine scale sets.

Enable Just-In-Time Access for Virtual Machines

Ensure that Microsoft Azure virtual machines are configured to use Just-in-Time (JIT) access.

Enable Performance Diagnostics for Azure Virtual Machines

Ensure that Azure virtual machines are configured to use the Performance Diagnostics tool.

Enable System-Assigned Managed Identities

Ensure that Azure virtual machines are configured to use system-assigned managed identities.

Enable Virtual Machine Access using Active Directory Authentication

Configure your Microsoft Azure virtual machines to use Azure Active Directory credentials for secure authentication.

Enable Virtual Machine Boot Diagnostics

Ensure that Microsoft Azure virtual machines are configured to use Boot Diagnostics feature.

Enable and Configure Health Monitoring

Ensure that the health of your Microsoft Azure scale set instances is being monitored.

Install Approved Extensions Only

Ensure that only approved extensions are installed on your Microsoft Azure virtual machines.

Install Endpoint Protection

Ensure that endpoint protection is installed on your Microsoft Azure virtual machines.

Remove Old Virtual Machine Disk Snapshots

Identify and remove old virtual machine disk snapshots in order to optimize cloud costs.

Remove Unattached Virtual Machine Disk Volumes

Remove any unattached Azure virtual machine (VM) disk volumes to improve security and reduce costs

Use BYOK for Disk Volumes Encryption

Use customer-managed keys for Microsoft Azure virtual machine (VM) disk volumes encryption.

Use Managed Disk Volumes for Virtual Machines

Ensure that your Microsoft Azure virtual machines are using managed disk volumes.