**Azure Security best practices and Automated build**

|  |  |
| --- | --- |
| **Author:** | Veeravenkat Satyanarayan.  [Veeravenkat.Satyanarayan@cognizant.com](mailto:Veeravenkat.Satyanarayan@cognizant.com) and Team |
| **Project Code:** |  |
| **Version Number:** | 1.0 |
| **Template Version:** |  |
| **Status:** |  |
|  |  |
| **Date Issued:** |  |

# Document Control

## Table of Contents

Contents

[1 Document Control 1](#_Toc511732980)

[1.1 Table of Contents 1](#_Toc511732981)

[2 General Outline 4](#_Toc511732982)

[2.1 Purpose 4](#_Toc511732983)

[2.2 Scope of Document 4](#_Toc511732984)

[2.3 Out of Scope of Document 4](#_Toc511732985)

[3 Security Basics. 4](#_Toc511732986)

[3.1 Key Security Areas 5](#_Toc511732987)

[4 Designing and Manage Identity Security Best Practices 5](#_Toc511732988)

[4.1 Overview 5](#_Toc511732989)

[4.2 Importance of the identity: 5](#_Toc511732990)

[4.3 Authentication in the Public Cloud. 6](#_Toc511732991)

[4.4 Azure Active Directory. 6](#_Toc511732992)

[4.5 Azure Population and Authentication 6](#_Toc511732993)

[4.6 Azure AD SKUs (Stock Keeping Units or Versions) 7](#_Toc511732994)

[4.7 Azure AD Domain Services. 7](#_Toc511732995)

[4.8 Multifactor Authentication 7](#_Toc511732996)

[4.9 RBAC 8](#_Toc511732997)

[4.10 Azure AD Privileged Identity Management 8](#_Toc511732998)

[4.11 Azure Active Directory Identity Protection 8](#_Toc511732999)

[5 Azure network security best practices 9](#_Toc511733000)

[5.1 Overview 9](#_Toc511733001)

[5.2 Importance of network security 9](#_Toc511733002)

[5.3 Layers of security offered by Azure 10](#_Toc511733003)

[5.4 Virtual Network best practices 10](#_Toc511733004)

[5.5 Logically segment Subnets 11](#_Toc511733005)

[5.6 Deploy DMZs for security zoning 11](#_Toc511733006)

[5.6.1 Perimeter network requirements 12](#_Toc511733007)

[5.6.2 Questions to be asked when building network boundaries 12](#_Toc511733008)

[5.6.3 DMZ Examples 13](#_Toc511733009)

[5.6.3.1 Boundary Examples 13](#_Toc511733010)

[5.6.3.2 DMZ between Azure and the Internet 14](#_Toc511733011)

[5.6.3.3 DMZ between Azure and your on-premises datacentre 15](#_Toc511733012)

[5.7 Securing VNet’s using NSG 15](#_Toc511733013)

[5.7.1 Planning NSG 15](#_Toc511733014)

[5.7.2 NSG Best Practices 15](#_Toc511733015)

[5.8 Determine the use of virtual appliances and user-defined routes 16](#_Toc511733016)

[5.9 Disable RDP/SSH Access to Azure Virtual Machines 16](#_Toc511733017)

[5.10 Azure Network Validation 16](#_Toc511733018)

[5.10.1 Monitor VPN gateways with Network Watcher troubleshooting 16](#_Toc511733019)

[5.10.2 Configure Network Performance Monitor for ExpressRoute 17](#_Toc511733020)

[5.10.3 Monitor network connections using connection monitor and traffic analytics 17](#_Toc511733021)

[5.10.4 Enable Azure Security Centre 18](#_Toc511733022)

[6 Compute Security Best Practices 18](#_Toc511733023)

[6.1 Install Antimalware software at every Azure virtual machine 18](#_Toc511733024)

[6.2 Virtual machine disk should be encrypted 19](#_Toc511733025)

[6.3 We should ensure that all OS patches are applied 20](#_Toc511733026)

[6.4 Implement Hardware Security Modules 21](#_Toc511733027)

[6.5 Critical Virtual Machine should be backed up always 21](#_Toc511733028)

[6.6 Security policy management and reporting by Azure Security Center 21](#_Toc511733029)

[6.7 Complex password policy should be set at each Azure Virtual machine 22](#_Toc511733030)

[6.8 Block Server Message block version SMB v1 22](#_Toc511733031)

[6.9 Manage virtual machine access using just in time (preview) 22](#_Toc511733032)

[7 Storage Security Best Practices 23](#_Toc511733033)

[7.1 The storage account can be secured using Role-Based Access Control. 23](#_Toc511733034)

[7.2 Always encrypt virtual disks and disk storage. 24](#_Toc511733035)

[7.3 Azure Storage Service Encryption 24](#_Toc511733036)

[7.4 Using Storage Analytics 25](#_Toc511733037)

[7.5 Azure Client-Side Encryption 25](#_Toc511733038)

[7.6 Use SMB 3.0 Encryption for Azure file share 25](#_Toc511733039)

[7.7 Delegated access to the data objects in Azure Storage can be granted using Shared Access Signatures 25](#_Toc511733040)

[8 Azure Security Center 25](#_Toc511733041)

[8.1 What is Azure Security Center? 25](#_Toc511733042)

[8.2 Azure Security Centre – Why should I use it? 26](#_Toc511733043)

[8.3 Billing – Azure Security Center 26](#_Toc511733044)

[8.4 Which Azure resources are monitored by Azure Security Center? 26](#_Toc511733045)

[8.5 Set security policies in Azure Security Center 27](#_Toc511733046)

[8.6 Data collection in Azure Security Center 27](#_Toc511733047)

[8.7 Recommendation List – Based on Prevention 28](#_Toc511733048)

[8.8 Email Notification 29](#_Toc511733049)

[8.9 Prevention is better than cure 29](#_Toc511733050)

[8.10 Short Description on Azure Security Center Recommendation 29](#_Toc511733051)

[8.11 Detection 31](#_Toc511733052)

[8.12 What are custom alert rules? 32](#_Toc511733053)

[8.13 Threat Intelligence: 33](#_Toc511733054)

[9 Azure Operational Security 36](#_Toc511733055)

[9.1 Overview 36](#_Toc511733065)

[9.2 Importance of the Operational Security 36](#_Toc511733066)

[9.3 Monitor, Manage and Protect cloud infrastructure 37](#_Toc511733067)

[9.4 Manage identity and implement single sign-on 38](#_Toc511733068)

[9.5 Trace requests, analyse usage trends, and diagnose issues 39](#_Toc511733069)

[9.6 Monitoring services 40](#_Toc511733070)

[9.7 Prevent, detect, and respond to threats 43](#_Toc511733071)

[9.8 End-to-end scenario-based network monitoring 44](#_Toc511733072)

[9.9 Secure deployment using proven DevOps tools 45](#_Toc511733073)

[9.10 Azure Operational Security checklist 46](#_Toc511733074)

[11 Document Control 47](#_Toc511733076)

[11.1 Document Version Information 47](#_Toc511733077)

[11.2 Document Distribution 47](#_Toc511733078)

[11.3 Associated Documents 47](#_Toc511733079)

[11.4 Approvals 47](#_Toc511733080)

[12 Appendices 49](#_Toc511733081)

[12.1 Glossary 49](#_Toc511733082)

# General Outline

## Purpose

Cognizant Cloud services team will evaluate and emulate a predefined set of Microsoft Azure Cloud best practices that will contribute to designing and implementing customer’s cloud environment security effectively for Azure IaaS services like:

* Identity management
* Compute security
* Storage security
* Network security
* Operational security

Azure provides with a wide array of configurable security options and the ability to control them so, that we can customize security to meet the unique requirements of customer’s deployments. This document helps you understand how Azure security capabilities can help you fulfil these requirements.

## 

## Scope of Document

Provide the security best practices for Azure IaaS services like Identity and Access Management, Compute, Storage, Network and Operational security.

## Out of Scope of Document

* Anything out the topics mentioned in Scope.
* List of any tools

# Security Basics.

In today's world, security must always be top of mind and no solution should be architected without security front and center, using the cloud does not change this.

* Every company has some level of security requirement that stretches across almost every element of the business.
* It's important to think of security in layers rather than a single protection element.

Layer upon layer upon layer, if first layer is compromised there should be some alerting.

* It's also important to ensure security while not crippling the businesses ability to operate.

It should not be secure and out of business, you need to closely work between the architecture, security network etc.

* Make security a core step of any new project, of change control, of anything you do.

Don’t think about the security once a year, how do I secure if any think new comes up, we need to security at any condition, to avoid the virus, malware, etc.

* Microsoft has the best secure, physical, technical, Malware this comes over time.

## Key Security Areas

Considerations for the cloud are similar to those on-premises but some are amplified because it may be easier for people to expose systems where proper governance is not in place.

For eg: we are not much worried about creating the VMs, as we have separate networks for internet facing, we have firewalls between the internal and DMZ etc. In public cloud if I don’t have proper process in place this will put in trouble, there you need to make sure key things in place and they are as follows.

* Identity management
* Compute security and System Integrity.
* Storage security
* Network security
* Operational security

There are other security areas and we will be only concentration on these key areas.

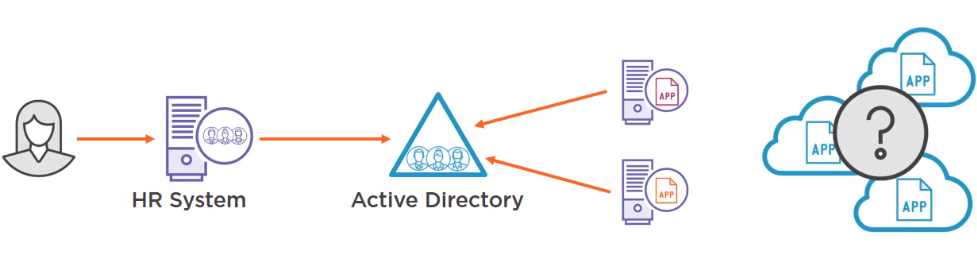
# Designing and Manage Identity Security Best Practices

## Overview

Microsoft identity and access management solutions help IT protect access to applications and resources across the corporate datacenters and into the cloud, enabling additional levels of validation such as multi-factor authentication and conditional access policies. Monitoring suspicious activity through advanced security reporting, auditing and alerting helps mitigate potential security issues.

## Importance of the identity:

Why it matters, how many identities we have and Azure AD key features and the problems with the passwords.



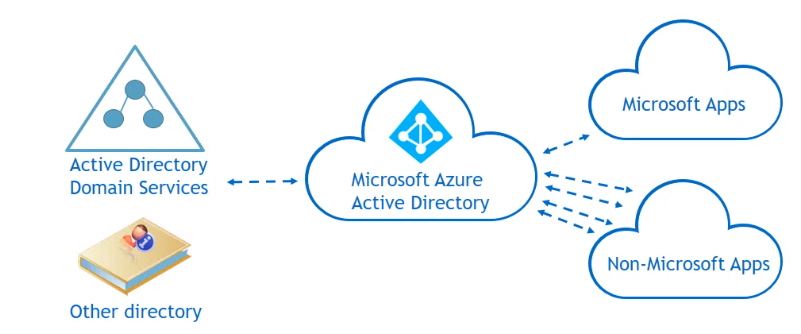
* It is critical that every user of a system can be uniquely and reliably identified.
* This ensures access and audits based on identity can be trusted.
* This means identity must be protected.
* Most organizations leverage a directory service with some source of truth, either the HR system and other systems may talk to the state of users of the company if user left what is the case etc.

## Authentication in the Public Cloud.

Authentication in the public cloud is a critical. In on-premises a client machine can be talking to active directory, client can talk on pretty much any port. That's not the case in the public cloud.

* Communication over the public cloud has to be focused on protocols company available lots of things are block when we talk to internet then it should http or https.
* HTTP and HTTPS with HTTPS preferred and often required because it is encrypted with SSL.
* Authentication commonly used are:
* Oauth is an open protocol provides a process for end users to authorize third party access to their servers resources, without actually having to share their credentials.
* Oauth 2 delegated the security to the HTTPS protocol which is used by Azure AD
* SAML is an XML based protocol open standard data format for exchange in the authentication and authorization data between parties, typically between an identity provider and service provided.
* So the solution for the public cloud really needs to be based on one of these types of authentication, I can't just use AD and join things to internet.

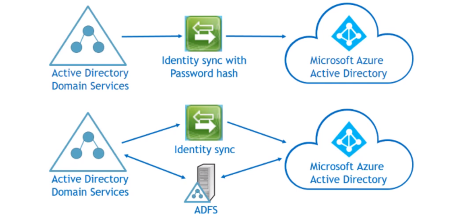
## Azure Active Directory.



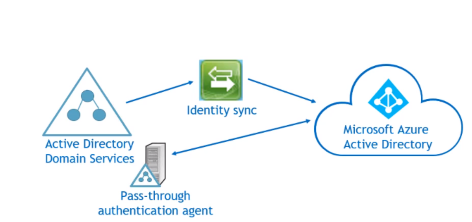
* Azure Active Directory is a flat structure allowing users and groups to be created. Basic directory service features.
* Azure AD Domain Services enable limited machine membership and policy application for Azure Service.
* By default, no Kerberos. That is not good fit for an Internet based service where communications are generally limited to HTTPS and HTTP.

## Azure Population and Authentication

* Azure AD is typically populated using a component called Azure AD Connect ADDS.
* The authentication can be performed by Azure AD if Azure AD has the user’s password
* Users provisioned in Azure AD (cloud account)
* Password replicated from on-premises.



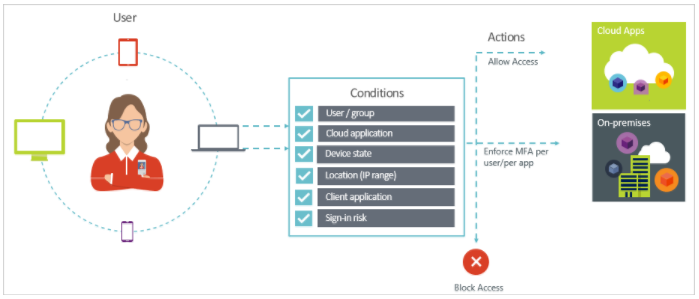
* Authentication can be performed using on-prem AD, if Azure AD connect pass-through authentication is utilized.



## Azure AD SKUs (Stock Keeping Units or Versions)

* We have difference AD licenses per user (three types) with in a single AD tenant. Which are Free, Basic and Premium(P1/P2), Scale and features vary by SKUs.
* Azure AD identity protection. It has privileged identity management and conditional access based on a user risk analysis this comes with Azure AD Premium 2.
* With Free and Basic SKUs we can register up to 10 app only. Azure AD SKUs can be assigned per user hence we can have mix and match according to the customer requirements.
* Premium SKUs included with other suites eg. Enterprise Mobility Security and Secure Productive Enterprise.

Azure AD Conditional Access:



## Azure AD Domain Services.

* Aimed for deployments without active directory domain services.
* Applications within the configured virtual networks can leverage Azure AD in a similar way to AD DS (LDAP, join domain, Kerberos, NTLM)

## Multifactor Authentication

* Azure AD Premium includes MFA and is available once license is assigned to users.
* Can also separately create MFA providers billed on a per user or per auth basis.
* Azure MFA has a number of configurable options.
* Users are then enabled or enforced for MFA
* Utilizes mobile devices either via application, text message or phone call
* App passwords are available for applications/services that don’t support MFA.

## RBAC

* Restricting access based on the need to know and least privilege security principles is imperative for organizations that want to enforce security policies for data access. Azure Role-Based Access Control (RBAC) can be used to assign permissions to users, groups, and applications at a certain scope. The scope of a role assignment can be a subscription, a resource group, or a single resource.
* You can leverage built in RBAC roles in Azure to assign privileges to users. Consider using Storage Account Contributor for cloud operators that need to manage storage accounts and Classic Storage Account Contributor role to manage classic storage accounts. For cloud operators that needs to manage VMs and storage account, consider adding them to Virtual Machine Contributor role.
* Organizations that do not enforce data access control by leveraging capabilities such as RBAC may be giving more privileges than necessary to their users. This can lead to data compromise by allow users access to certain types of types of data (e.g., high business impact) that they shouldn’t have in the first place.

## Azure AD Privileged Identity Management

With Azure Active Directory (AD) Privileged Identity Management, you can manage, control, and monitor access within your organization. This includes access to resources in Azure AD, Azure Resources (Preview), and other Microsoft Online Services like Office 365.

Organizations want to minimize the number of people who have access to secure information or resources, because that reduces the chance of a malicious user getting that access, or an authorized user inadvertently impacting a sensitive resource. However, users still need to carry out privileged operations in Azure AD, Azure, Office 365, or SaaS apps. Organizations can give users privileged access to Azure resources like Subscriptions, and Azure AD. There is a need for oversight for what those users are doing with their admin privileges. Azure AD Privileged Identity Management helps to mitigate the risk of excessive, unnecessary or misused access rights.

Azure AD Privileged Identity Management helps your organization:

* See which users are assigned privileged roles to manage Azure resources (Preview), as well as which users are assigned administrative roles in Azure AD
* Enable on-demand, "just in time" administrative access to Microsoft Online Services like Office 365 and Intune, and to Azure resources (Preview) of subscriptions, resource groups, and individual resources such as Virtual Machines
* See a history of administrator activation, including what changes administrators made to Azure resources (Preview)
* Get alerts about changes in administrator assignments
* Require approval to activate Azure AD privileged admin roles (Preview)
* Review membership of administrative roles and require users to provide a justification for continued membership

## Azure Active Directory Identity Protection

With Azure Active Directory Identity Protection, in your environment, you can use the same protection systems Microsoft uses to secure identities.

The vast majority of security breaches take place when attackers gain access to an environment by stealing a user’s identity. Over the years, attackers have become increasingly effective in leveraging third party breaches and using sophisticated phishing attacks. As soon as an attacker gains access to even low privileged user accounts, it is relatively easy for them to gain access to important company resources through lateral movement.

Azure Active Directory Identity Protection is a feature of the Azure AD Premium P2 edition that enables you to:

* Detect potential vulnerabilities affecting your organization’s identities
* Configure automated responses to detected suspicious actions that are related to your organization’s identities
* Investigate suspicious incidents and take appropriate action to resolve them.

# Azure network security best practices

## Overview

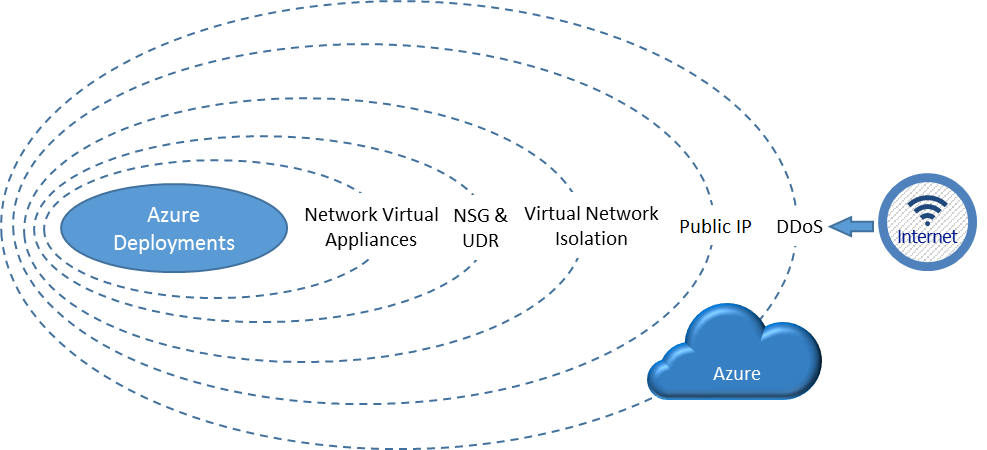
Azure Virtual Network is a secure, logical network that provides network isolation and security controls that you treat like your on-premises network. Each customer creates their own structure by using: subnets—they use their own private IP address range, configure route tables, network security groups, access control lists (ACLs), gateways, and virtual appliances to run their workloads in the cloud. Azure has a rich set of networking mechanisms that customers can use to secure their workloads.

## Importance of network security

[Network security](http://www.nutmegtech.com/enterprise-network-management) is the any protection of access, misuse, and hacking of files and directories in a computer network system. Some of the most common threats to a network include viruses, worms, spyware, adware and identity theft. One of the most important aspects of network [security](http://info.nutmegtech.com/it-insider-blog/10-information-security-mistakes-small-businesses-make) is the multiple layers of security. Azure offers multiple layers of security.

By having network security in place, your company will experience business benefits. Your company is protected against business disruption; this helps keep employees productive. Network security helps your company meet mandatory regulations. Because network security helps protect your customers' data, it reduces the risk of legal action from data theft.

## Layers of security offered by Azure



* Azure DDoS helps protect against large-scale attacks against Azure.
* DDoS attack – It’s an attack to make some legitimate resource or system unavailable by sending uncountable fake requests which may cost huge.
* DDoS protection is a layer of the Azure physical network that protects the Azure platform itself from large-scale Internet-based attacks.
* Azure has a robust DDoS protection mesh on all inbound, outbound, and Cross-Azure region connectivity.
* This DDoS protection layer has no user configurable attributes and is not accessible to the customer. The DDoS protection layer protects Azure as a platform from large-scale attacks, it also monitors out-bound traffic and Cross-Azure region traffic.
* It's critical to note that Azure DDoS is only looking for large-scale attacks. It is possible that your specific service could be overwhelmed before the platform level protection thresholds are exceeded.
* The Public IP Address endpoint uses Network Address Translation (NAT) to route traffic to the internal address and port on the Azure virtual network.
* This path is the primary way for external traffic to pass into the virtual network. The Public IP addresses are configurable to determine which traffic is passed in, and how and where it's translated on to the virtual network.
* Traffic isolation refers only to traffic inbound to the virtual network. By default, outbound traffic from the VNet to the internet is allowed, but can be prevented if desired by NSGs.
* NSG allows customers to create rules (ACLs) at the desired level of granularity: network interfaces, individual VMs, or virtual subnets.
* UDR and IP Forwarding allow customers to define the communication paths between different tiers within a virtual network.
* Deploy a firewall, IDS/IPS, and other virtual appliances, and route network traffic through these security appliances for security boundary policy enforcement, auditing, and inspection.

## Virtual Network best practices

* Determine address spaces as per your requirement.
* The private IP address spaces available are in the Class A (10.0.0.0/8), Class B (172.16.0.0/12), and Class C (192.168.0.0/16) ranges.
* The IP address range should not overlap with other connected VNet’s.
* Considering future growth plan your virtual network address spaces.
* Don’t create multiple VNet’s unnecessarily.
* You should consider creating multiple VNets in the following scenarios:
* VMs that need to be placed in different Azure locations. VNets in Azure are regional. They cannot span locations. Therefore, you need at least one VNet for each Azure location you want to host VMs in.
  + Workloads that need to be completely isolated from one another. You can create separate VNets, that even use the same IP address spaces, to isolate different workloads from one another. (Isolate Non-prod and Prod networks)
  + Keep in mind the azure VNet limits per region and per subscription before you design.
* Azure assigns virtual machines the addresses of DNS servers by DHCP. DNS servers can be: Azure provided or custom (Provided by you). Update the DNS Server details at VNet level.

## Logically segment Subnets

* Subnet address ranges should be with VNet address range. The smallest subnet supported is a /29 and the largest is a /8 (using CIDR subnet definitions).
* There are two types of subnets in a VNet, a gateway subnet and a virtual machine-hosting subnet.
* The Azure gateway subnet is needed by Azure to host the two virtual machines of your Azure gateway. Specify an address space with at least a 29-bit prefix length  A 28-bit or smaller prefix length is recommended, especially if you are planning to use ExpressRoute.
* Virtual machine-hosting subnets are where you place Azure virtual machines, which you can do according to typical on-premises guidelines, such as a common role or tier of an application or for subnet isolation.
* Give extra address spaces for the subnet considering future growth.
* Routing will happen automatically and you no need to configure any route tables.
* If you want to restrict access within the subnet use NSG’s or route tables.

## Deploy DMZs for security zoning

* A DMZ or “perimeter network” is a physical or logical network segment that is designed to provide an additional layer of security between your assets and the Internet.
* DMZs are useful because you can focus your network access control management, monitoring, logging and reporting on the devices at the edge of your Azure Virtual Network.

Some of the characteristics of a good perimeter network are as follows:

* Internet-facing:
  + The perimeter network subnet itself is Internet-facing, directly communicating with the Internet.
  + Public IP addresses, VIPs, and/or service endpoints pass Internet traffic to the front-end network and devices.
  + Inbound traffic from the Internet passes through security devices before other resources on the front-end network.
  + If outbound security is enabled, traffic passes through security devices, as the final step, before passing to the Internet.
* Protected network:
  + There is no direct path from the Internet to the core infrastructure.
  + Channels to the core infrastructure must traverse through security devices such as NSGs, firewalls, or VPN devices.
  + Other devices must not bridge Internet and the core infrastructure.
  + Security devices on both the Internet-facing and the protected network facing boundaries of the perimeter network.
* Other common practices and constraints:
  + Workloads must not store business critical information.
  + Access and updates to perimeter network configurations and deployments are limited to only authorized administrators.

## 5.6.1 Perimeter network requirements

**Subnet Architecture:**

* Specify the virtual network such that an entire subnet is dedicated as the perimeter network, separated from other subnets in the same virtual network.
* This separation ensures the traffic between the perimeter network and other internal or private subnet tiers flows through a firewall or IDS/IPS virtual appliance.
* User-defined routes on the boundary subnets are required to forward this traffic to the virtual appliance.

**NSG:**

* Minimize the network surfaces exposed to the Internet.
* Allow access to only ports or protocols that are required.

**Route table:**

* The perimeter network subnet itself should be able to communicate to the Internet directly, but should not allow direct communication to and from the back end or on-premises networks without going through a firewall or security appliance.

**Security appliance configuration:**

* To route and inspect packets between the perimeter network and the rest of the protected networks, the security appliances such as firewall, IDS, and IPS devices may be multi-homed.
* The NICs in the perimeter network communicate directly to and from the Internet, with the corresponding NSGs and the perimeter network routing table.
* The NICs connecting to the back-end subnets have more restricted NSGs and routing tables of the corresponding back-end subnets.

## 5.6.2 Questions to be asked when building network boundaries

1. **How many boundaries are needed?**

The first decision point is to decide how many security boundaries are needed in a given scenario:

* A single boundary: One on the front-end perimeter network, between the virtual network and the Internet.
* Two boundaries: One on the Internet side of the perimeter network, and another between the perimeter network subnet and the back-end subnets in the Azure virtual networks.
* Three boundaries: One on the Internet side of the perimeter network, one between the perimeter network and back-end subnets, and one between the back-end subnets and the on-premises network.
* N boundaries: A variable number. Depending on security requirements, there is no limit to the number of security boundaries that can be applied in a given network.

The number and type of boundaries needed vary based on a company’s risk tolerance and the specific scenario being implemented.

1. **Where are the boundaries located?**

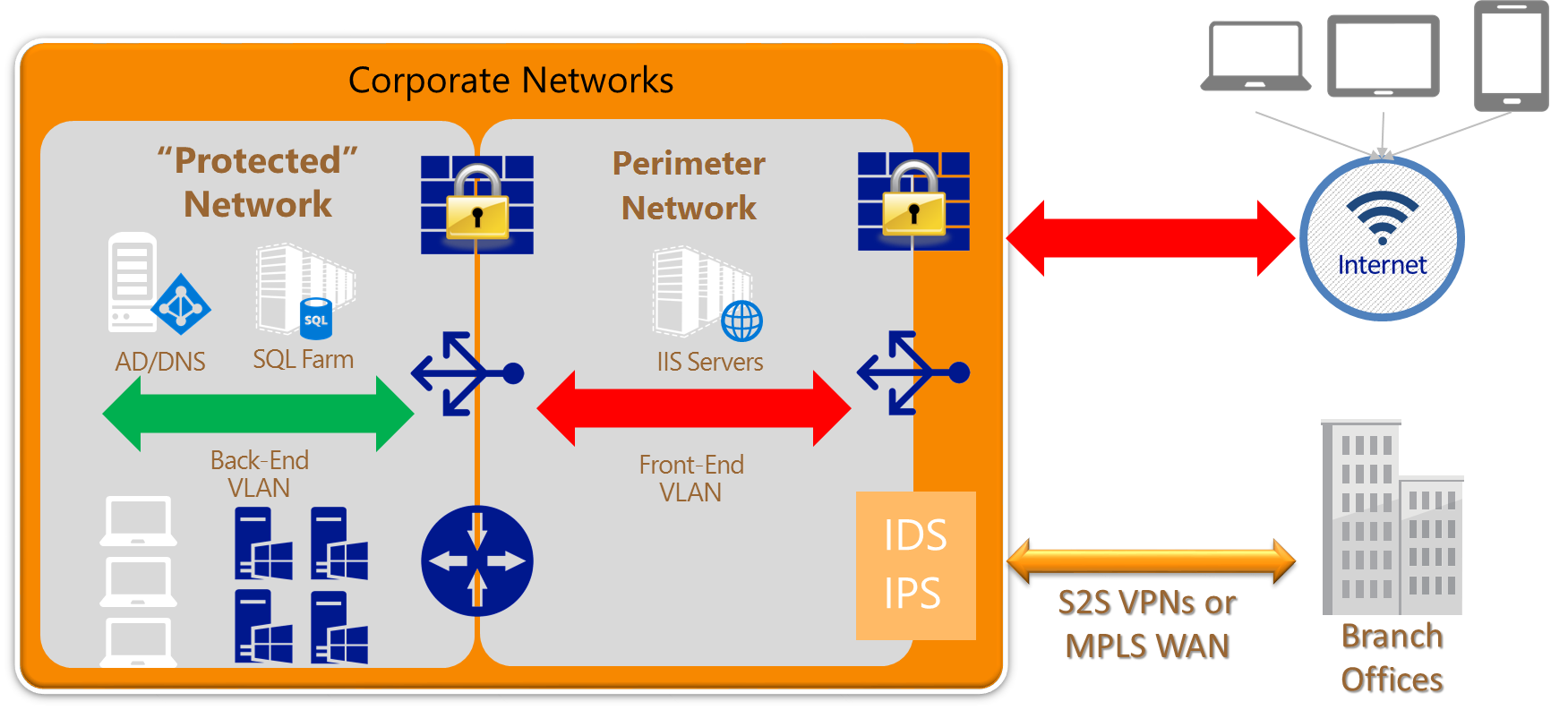
* There are generally three choices:
  + Using an Internet-based intermediary service (for example, a cloud-based Web application firewall, which is not discussed in this document)
  + Using native features and/or network virtual appliances in Azure
  + Using physical devices on the on-premises network
* On purely Azure networks, the options are native Azure features (for example, Azure Load Balancers) or network virtual appliances from the rich partner ecosystem of Azure (for example, Check Point firewalls).
* If a boundary is needed between Azure and an on-premises network, the security devices can reside on either side of the connection (or both sides). Thus a decision must be made on the location to place security gear.

1. **How are the boundaries implemented?**

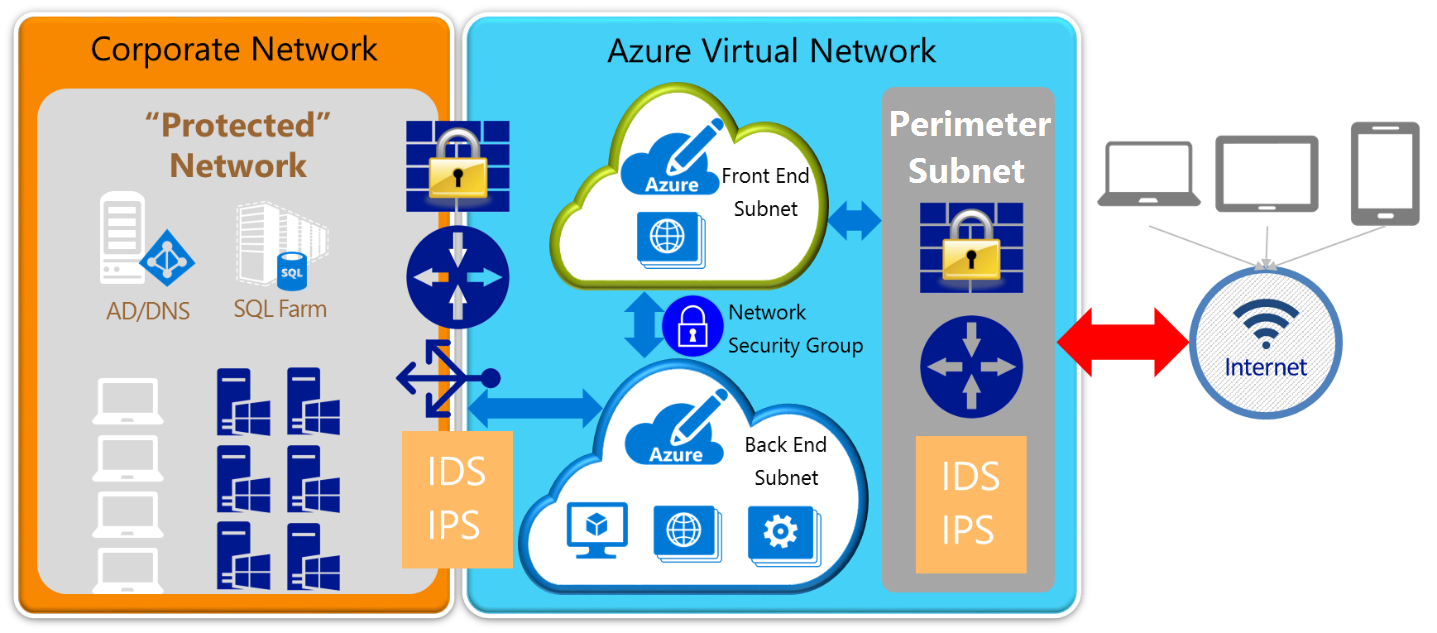
* You can use IDS and firewall rules on the Internet side of the perimeter network, but only ACLs between the perimeter network and back-end subnet. Deciding on which device (or how many devices) to use depends on the scenario and security requirements.

## 5.6.3 DMZ Examples

## 5.6.3.1 Boundary Examples

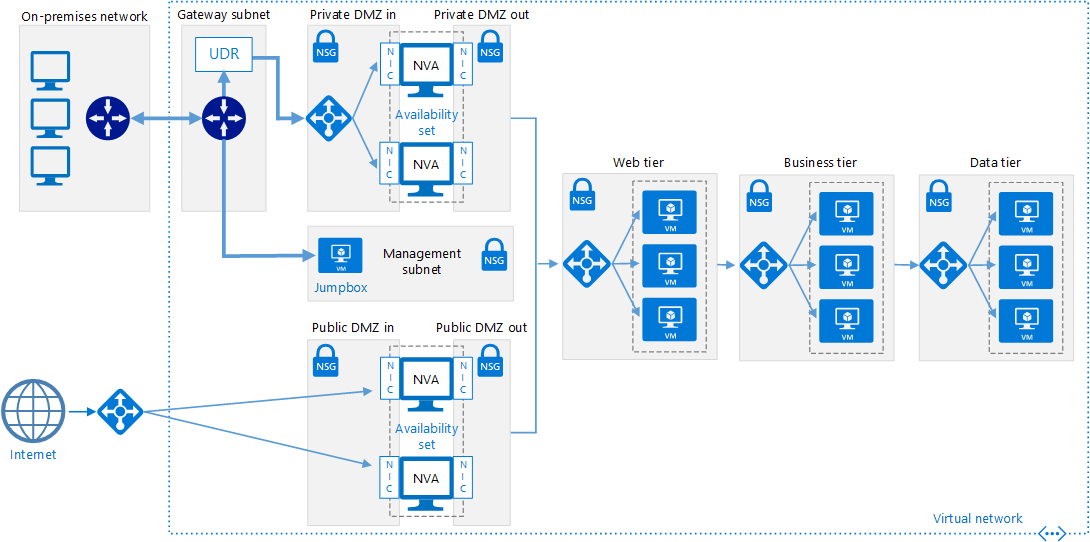


1. The preceding figure shows an example of a single subnet perimeter network in a corporate network, with two security boundaries.



1. The preceding figure shows a high-level view of a three security boundary network. The boundaries are between the perimeter network and the Internet, the Azure front-end and back-end private subnets, and the Azure back-end subnet and the on-premises corporate network.

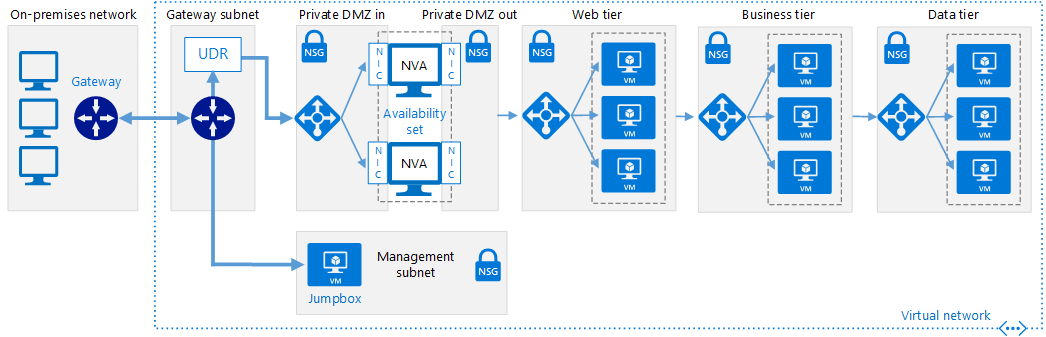
## 5.6.3.2 DMZ between Azure and the Internet



Deployment template for the reference architecture can be found in the below URL

<https://github.com/mspnp/reference-architectures/tree/master/dmz/secure-vnet-dmz>

## 5.6.3.3 DMZ between Azure and your on-premises datacentre



Deployment template for the reference architecture can be found in the below URL

<https://github.com/mspnp/reference-architectures/tree/master/dmz/secure-vnet-hybrid>

## Securing VNet’s using NSG

## 5.7.1 Planning NSG

Before implementing NSGs, you need to answer the following questions:

1. What types of resources do you want to filter traffic to or from? You can connect resources such as NICs (Resource Manager), VMs (classic), Cloud Services, Application Service Environments, and VM Scale Sets.
2. Are the resources you want to filter traffic to/from connected to subnets in existing VNets?

## 5.7.2 NSG Best Practices

* NSG’s can be associated to Subnets or NIC.
* Binding NSG to VM’s (NIC level) is powerful and you may lose complexity of your deployment since it would be hard to track and maintain.
* If you want to use NSG to specific VM then bind it at VM level. If you want to bind NSG to multiple VM’s in same subnet, bind NSG at subnet.
* Priority must be unique within each set (inbound and outbound).
* There are default rules that are created when you create NSG (VirtualNetwork, AzureLoadBalancer, Internet)
* The default rules cannot be deleted, but because they are assigned the lowest priority, they can be overridden by the rules that you create.
* You can associate the same NSG to as many resources you want.
* Don’t block 168.63.129.16. Basic infrastructure services such as DHCP, DNS, and health monitoring are provided through this virtualized host IP address.
* Don’t block outbound request to port 1688. It’s used for windows licensing; a request is sent to the Key Management Service host servers that handle such queries.
* Don’t apply NSG to GatewaySubnet. If you do so, cross-VNet or cross-premises connectivity may fail.
* Routes configured for virtual appliances or on-premises traffic. Internet traffic can be redirected to on-premises via forced-tunneling. An RDP/SSH connection from the Internet to your VM may not work with this setting, depending on how the on-premises network hardware handles this traffic.
* If there are no NSGs associated with the NIC or subnet and you have a public IP address assigned to your VM, all ports will be open for inbound and outbound access. If the VM has a public IP address, applying NSGs to the NIC or subnet is strongly recommended.
* Diagnostic logs are only available for NSGs deployed through the Azure Resource Manager deployment model. Enable NSG logs at network watcher.

## Determine the use of virtual appliances and user-defined routes

* Forced tunneling must be associated with a VNet that has a dynamic routing VPN gateway (not a static gateway).
* If there are no Internet-facing workloads in your virtual networks, you also can apply forced tunneling to the entire virtual networks.
* Create default route tables with the default route that uses VNet gateway as in next-hop address and associate the route table to the subnets.
* Use UDR at GatewaySubnet and control the incoming and outgoing traffic.
* Place security appliances in dedicated subnet.
* Enable IP forwarding for the NIC of virtual appliance that is involved in the routing.
* Use multiple NIC’s for the virtual appliances, to RDP, to control the routing within the VNet (between subnets) and to control routing between the VNet’s.
* Use application gateways for protecting web applications from common web vulnerabilities and exploits.
* Use Application gateway WAF to run in detection mode to observe traffic for malicious patterns.
* Use Application Gateway WAF to monitor web applications against attacks using a real-time WAF log that is integrated with [Azure Monitor](https://docs.microsoft.com/azure/monitoring-and-diagnostics/monitoring-overview) and [Azure Security Center](https://azure.microsoft.com/services/security-center/) to track WAF alerts and easily monitor trends.
* Don’t place any VM’s in the security appliances subnet.

## Disable RDP/SSH Access to Azure Virtual Machines

* Disable direct RDP and SSH access to your Azure Virtual Machines from the Internet. After direct RDP and SSH access from the Internet is disabled, you have other options you can use to access these virtual machines for remote management:
  + Point-to-site VPN (Connect a single computer to a virtual network)
  + Site-to-site VPN (Connect on-premise network to azure virtual network over a public internet)
  + ExpressRoute (Connect on-premise network to azure virtual network using a dedicated WAN link)

## Azure Network Validation

## 5.10.1 Monitor VPN gateways with Network Watcher troubleshooting

* Gaining deep insights on your network performance is critical to provide reliable services to customers. It is therefore critical to detect network outage conditions quickly and take corrective action to mitigate the outage condition.
* Azure Automation enables you to implement and run a task in a programmatic fashion through runbooks.
* Using Azure Automation creates a perfect recipe for performing continuous and proactive network monitoring and alerting.

**Reference Link**

<https://docs.microsoft.com/en-in/azure/network-watcher/network-watcher-monitor-with-azure-automation>

## 5.10.2 Configure Network Performance Monitor for ExpressRoute

* Network Performance Monitor (NPM) is a cloud-based network monitoring solution that monitors connectivity between Azure cloud deployments and on-premises locations (Branch offices, etc.).
* NPM is part of Microsoft Operations Management Suite (OMS).
* NPM now offers an extension for ExpressRoute that lets you monitor network performance over ExpressRoute circuits that are configured to use Private Peering.
* When you configure NPM for ExpressRoute, you can detect network issues to identify and eliminate.
* You can:
* Monitor loss and latency across various VNets and set alerts
* Monitor all paths (including redundant paths) on the network
* Troubleshoot transient and point-in-time network issues that are difficult to replicate
* Help determine a specific segment on the network that is responsible for degraded performance
* Get throughput per virtual network (If you have agents installed in each VNet)
* See the ExpressRoute system state from a previous point in time

**Reference Link**

<https://docs.microsoft.com/en-us/azure/expressroute/how-to-npm>

## 5.10.3 Monitor network connections using connection monitor and traffic analytics

* + Use connection monitor to monitor network connectivity between an azure vm and an ip address.

**Reference Link**

<https://docs.microsoft.com/en-in/azure/network-watcher/connection-monitor>

* Use Traffic analytics, a cloud-based solution that provides visibility into user and application traffic on your cloud networks is in public preview.

**Reference Link**

<https://azure.microsoft.com/en-us/blog/traffic-analytics-in-preview/>

## 5.10.4 Enable Azure Security Centre

* Azure Security Center helps you optimize and monitor network security by:
  + - Providing network security recommendations
    - Monitoring the state of your network security configuration
    - Alerting you to network based threats both at the endpoint and network levels

# Compute Security Best Practices

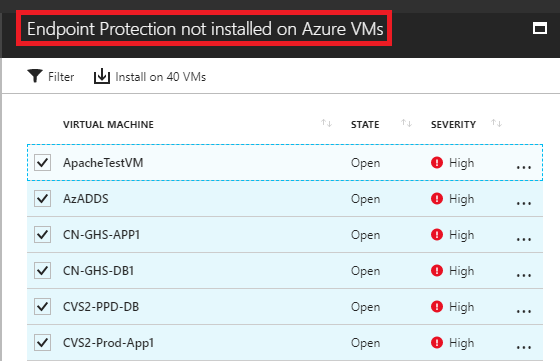
In most infrastructure as a service (IaaS) scenarios, Azure virtual machines (VMs) are the main workload for organizations that use cloud computing. This fact is especially evident in hybrid scenarios where organizations want to slowly migrate workloads to the cloud. In such scenarios, follow the general security considerations for IaaS, and apply security best practices to all your VMs.

**Following points describe Compute Security Best Practices**

## Install Antimalware software at every Azure virtual machine

We can use antimalware software from security vendors such as Microsoft, Symantec, Trend Micro, and Kaspersky to protect your Azure/On premise virtual machines from malicious files, adware, and other threats.

It is identified from **Azure Security Center**



**Microsoft Antimalware:**

Microsoft Antimalware for Azure Cloud Services and Virtual Machines is a real-time protection capability that helps identify and remove viruses, spyware, and other malicious software

**Solution Code Snippet is available here:**

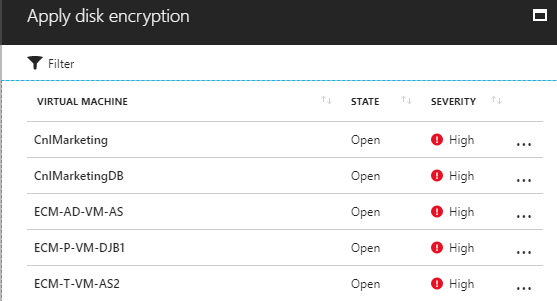
<https://blogs.technet.microsoft.com/ukplatforms/2017/07/31/azure-resource-manager-arm-automate-installation-of-vm-extensions-using-powershell-and-json/>

## Virtual machine disk should be encrypted

Azure Disk Encryption uses the industry standard BitLocker feature of Windows and the dm-crypt feature of Linux to provide volume encryption for the OS and the data disks. It encrypts entire hard drive. Our sensitive data, operating system, software programs, temporary files, etc. are all encrypted. By encrypting the entire drive, in the event of drive being lost, stolen, or improperly decommissioned, the data that raised on the drive is inaccessible.

It is identified from **Azure Security Center**





**Solution PS Code Snippet is available here:**

<https://docs.microsoft.com/en-us/azure/virtual-machines/scripts/virtual-machines-windows-powershell-sample-encrypt-vm>

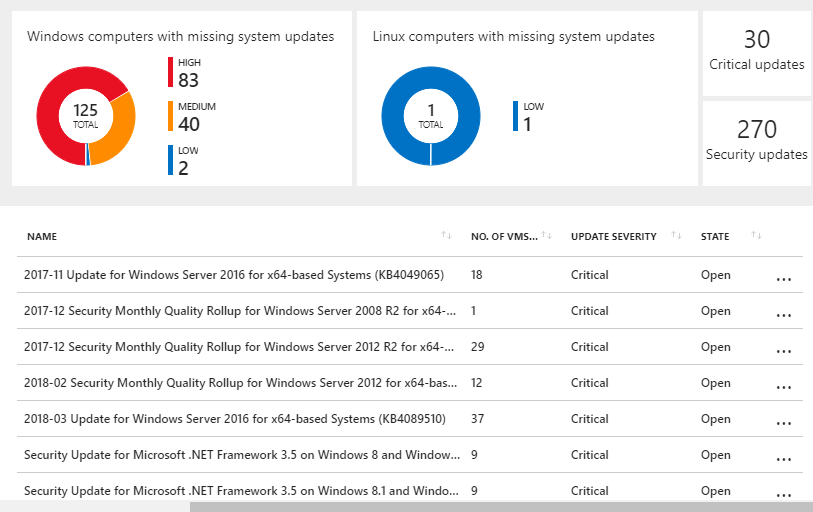
## Ensure latest OS patches are applied

Vendors like Microsoft, Apple and RedHat (Applying updates to an encrypted Azure IaaS Red Hat VM using Yum Update) periodically release hotfixes, service packs and security patches to correct known defects in their operating systems. These patches cover the security holes, keeping hackers from further exploiting the security flaws.

It is identified from **Azure Security Center**



Following screen-shot is displaying some of the example system updates



## Implement Hardware Security Modules

You can simplify the management and security of your critical secrets and keys by storing them in Azure Key Vault. Key Vault provides the option to store your keys in hardware security modules (HSMs) certified to FIPS 140-2 Level 2 standards.

## Critical Virtual Machine should be backed up always

Azure Backup is a scalable solution that protects your application data with zero capital investment and minimal operating costs. Application errors can corrupt your data, and human errors can introduce bugs into your applications. With Azure Backup, your virtual machines running Windows and Linux are protected.

**Solution Code Snippet is available here:**

<https://docs.microsoft.com/en-us/azure/backup/scripts/backup-powershell-sample-backup-encrypted-vm>

## Security policy management and reporting by Azure Security Center

Azure Security Center helps you optimize and monitor virtual machine security by providing virtual machine security recommendations such as apply system updates, configure ACLs endpoints, enable antimalware, enable network security groups, and apply disk encryption. Monitoring the state of your virtual machines

## Complex password policy should be set at each Azure Virtual machine

a. Enforce Password History

b. Maximum Password Age

c. Minimum Password Age

d. Minimum Password Length

e. Passwords Must Meet Complexity Requirements

* Passwords must have at least six characters.
* Passwords can’t contain the user name or parts of the user’s full name, such as his first name.
* Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.

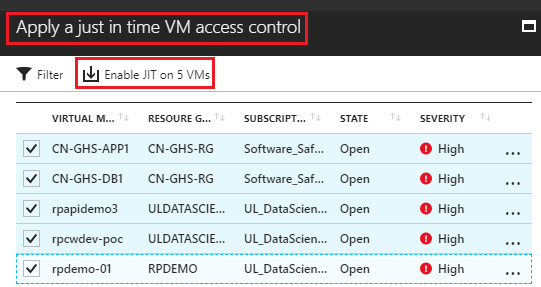
## Block Server Message block version SMB v1

Many of our Windows customers have recently had to deal with the threat of ransomware attacks due to issues with the Server Message Block version 1 (SMB v1) protocol. For this reason, the Azure security team has made the decision to disable SMB v1 by default on all Windows operating system images available in the Azure Marketplace for creating new Azure Virtual Machines, effective August 2017.

## Manage virtual machine access using just in time (preview)

Brute force attacks commonly target management ports as a means to gain access to a VM. If successful, an attacker can take control over the VM and establish a foothold into your environment. **One way to reduce exposure to a brute force attack is to limit the amount of time that a port is open**. Management ports do not need to be open at all times. They only need to be open while you are connected to the VM, for example to perform management or maintenance tasks. When just in time is enabled Security Center uses Network Security Group (NSG) rules, which restrict access to management ports so they cannot be targeted by attackers.

It is identified from **Azure Security Center**



**Solution Code Snippet is available here:**

<http://www.brainscale.com/enabling-just-time-vm-access/>

# Storage Security Best Practices

In many cases, the focus of IT security has been on the network and the data traveling over it. The security of stored data, especially backup data, has received less attention. The SAN has been presumed to be secure because it uses Fibre Channel instead of TCP/IP. But is this complacency justified? What are the security threats associated with data that's stored off-site? In this article, we'll take a look at these questions and the reason organizations need to become more security-aware when it comes to storage strategies.

## The storage account can be secured using Role-Based Access Control.

For example, you can authorize someone to manage Storage Accounts, but not to the blobs or tables within a Storage Account.

**Solution Code Snippet**

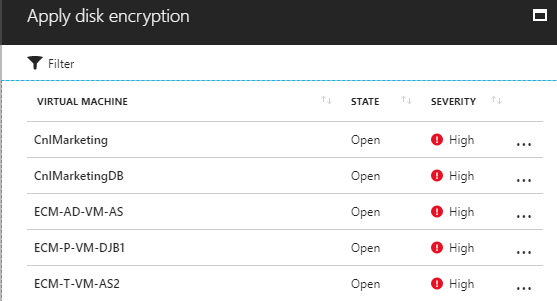
* Get-AzureRmRoleAssignment -SignInName "username@domain.com"
* Get-AzureRmRoleAssignment -SignInName "username@domain.com" -ExpandPrincipalGroups
* **# Scope and object ID can be collected from any of the above two commands**
* Get-AzureRmRoleAssignment -scope "/subscriptions/f0675ec9-480d-4c2a-982a-ed97983af390" | select displayname
* New-AzureRmRoleAssignment -ObjectId "74b007ea-ab34-4209-981e-c538200fe251" ‑RoleDefinitionName "Virtual Machine Contributor" -Scope "/subscriptions/f0675ec9-480d-4c2a-982a-ed97983af390"
* Remove-AzureRmRoleAssignment -ObjectId "74b007ea-ab34-4209-981e-c538200fe251" -RoleDefinitionName "Virtual Machine Contributor" -Scope "/subscriptions/f0675ec9-480d-4c2a-982a-ed97983af390"

## Always encrypt virtual disks and disk storage.

Azure Disk Encryption eliminates data theft risk or the exposure to unauthorized access. Disk Encryption uses BitLocker on Windows and DM-Crypt on Linux to encrypt the operating system and data drives. Azure Disk Encryption is integrated with Key Vault to control and manage encryption keys (It is available for standard virtual machines and virtual machines with premium storage.).

It is identified from **Azure Security Center**





Solution Code Snippet is available here:

<https://docs.microsoft.com/en-us/azure/virtual-machines/scripts/virtual-machines-windows-powershell-sample-encrypt-vm>

## Azure Storage Service Encryption

The Azure Storage Services encryption helps protect data at rest. It is activated at the storage account level. It encrypts the data in Azure as it is written and then decrypted automatically when the user wishes to access it.

## Using Storage Analytics

The authentication method used by someone when they access storage can be tracked using Storage analytics. It will help us for further auditing.

## Azure Client-Side Encryption

It is functionality to help developers encrypt their data inside client applications before uploading to Azure Storage, and also to decrypt it

## Use SMB 3.0 Encryption for Azure file share

To encrypt data in transit with Azure File Storage, you can use SMB 3.x with Windows 8, 8.1, and 10 and with Windows Server 2012 R2 and Windows Server 2016. When you are using the Azure Files service, any connection without encryption fails when "Secure transfer required" is enabled.

## Delegated access to the data objects in Azure Storage can be granted using Shared Access Signatures

SAS or Shared Access Signature grants the restricted access rights to Azure Storage resources. You can grant them access to the resource for a specific period time. Service – Level SAS delegates access to multiple storage services like the blob, files, tables, and queues.

Solution Code Snippet

<https://social.technet.microsoft.com/wiki/contents/articles/35988.azure-file-storage-implementing-restricted-access-with-powershell-and-net.aspx>

# Azure Security Center

## What is Azure Security Center?

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. With Security Center, you can apply security policies across your workloads, limit your exposure to threats, and detect and respond to attacks.

## Azure Security Centre – Why should I use it?

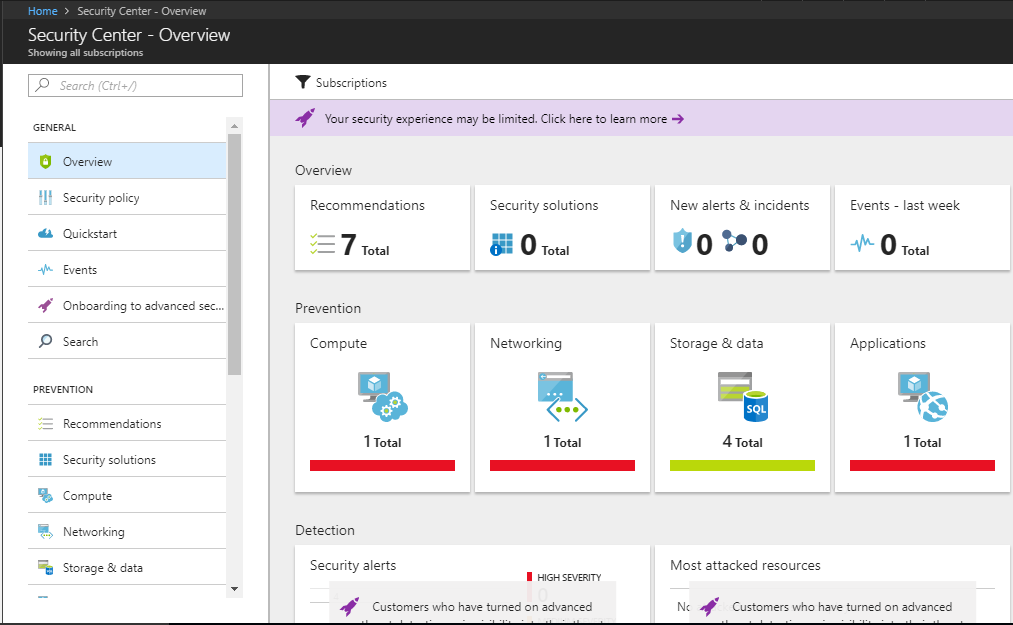
* Monitor security across on-premises and cloud workloads
* Apply policy to ensure compliance with security standards
* Find and fix vulnerabilities before they can be exploited
* Use access and application controls to block malicious activity
* Leverage advanced analytics and threat intelligence to detect attacks
* Simplify investigation for rapid threat response

## Billing – Azure Security Center

* Security Center is offered in two tiers.
* The Free tier provides visibility into the security state of your Azure resources, basic security policy, security recommendations, and integration with security products and services from partners.
* The Standard tier adds advanced threat detection capabilities, including threat intelligence, behavioural analysis, anomaly detection, security incidents, and threat attribution reports. The Standard tier is free for the first 60 days. Should you choose to continue to use the service beyond 60 days, we automatically start to charge for the service. To upgrade, select Pricing Tier in the security policy.

## Which Azure resources are monitored by Azure Security Center?

* Virtual machines (VMs) (including Cloud Services)
* Azure Virtual Networks
* Azure SQL service
* Azure Storage account
* Azure Web Apps (in App Service Environment)
* Partner solutions integrated with your Azure subscription such as a web application firewall on VMs and on App Service Environment



## Set security policies in Azure Security Center

**Step** 1: Data collection in Azure Security Center

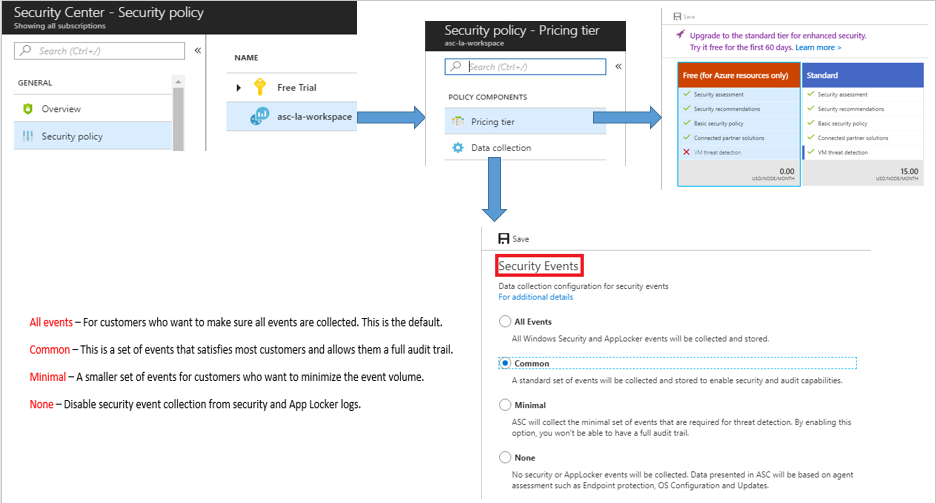
**Step** 2: Enable/Disable Available security policy definitions

**Step** 3: Provide security contact details in Azure Security Center

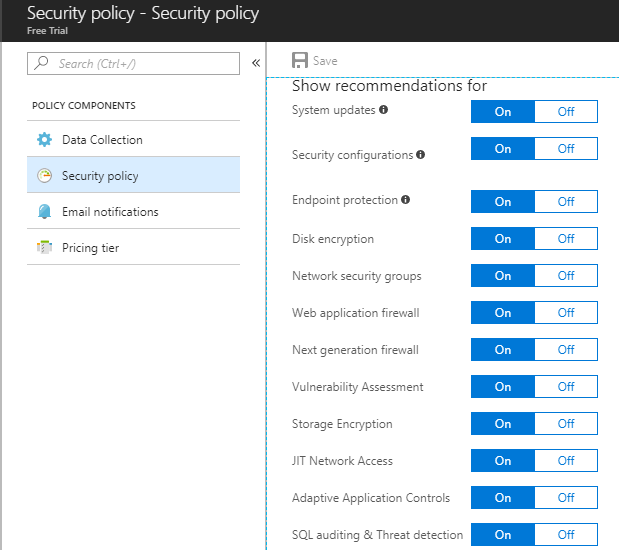
**Step** 4: Upgrade to Security Center Standard tier for enhanced security

## Data collection in Azure Security Center

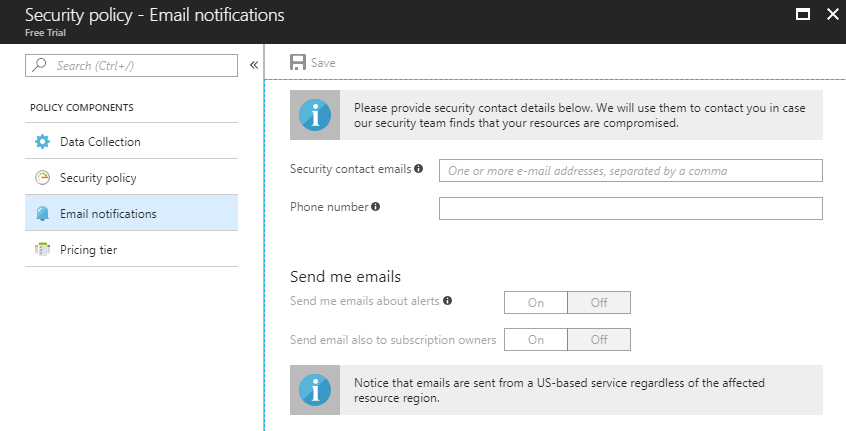
* Security Center collects data from your Azure virtual machines (VMs) and non-Azure computers to monitor for security vulnerabilities and threats. Data is collected using the Microsoft Monitoring Agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis.
* Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, logged in user, and tenant ID. The Microsoft Monitoring Agent also copies crash dump files to your workspace
* Security Center uses Microsoft Monitoring Agent to collect Security Data from Azure Virtual Machine
* When data collection is enabled, Microsoft Monitoring Agent is automatically provisioned on all the existing and new supported virtual machines that are deployed as a subscription



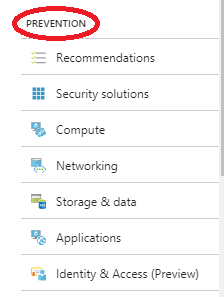
## Recommendation List – Based on Prevention

****

## Email Notification

****

## Prevention is better than cure

****

## Short Description on Azure Security Center Recommendation

* **System updates: –**

Retrieves a daily list of available security and critical updates from Windows Update or Windows Server Update Services. The retrieved list depends on the service that's configured for your virtual machines, and it recommends that missing updates be applied.

For Linux systems, the policy uses the distro-provided package-management system to determine packages that have available updates. It also checks for security and critical updates from Azure Cloud Services virtual machines.

* **Endpoint protection: –**

Recommends that endpoint protection be set up for all Windows virtual machines (VMs) to help identify and remove viruses, spyware, and other malicious software.

* **Disk encryption –**

Recommends enabling disk encryption in all virtual machines to enhance data protection at rest.

* **Network security groups –**

Recommends that network security groups be configured to control inbound and outbound traffic to VMs that have public endpoints. Network security groups that are configured for a subnet are inherited by all virtual-machine network interfaces unless otherwise specified. In addition to checking to see whether a network security group has been configured, this policy assesses inbound security rules to identify rules that allow incoming traffic.

* **Web application firewall-**

Recommends that a web application firewall be set up on virtual machines when either of the following is true.

An instance-level public IP is used, and the inbound security rules for the associated network security group are configured to allow access to port 80/443.

A load-balanced IP is used, and the associated load balancing and inbound network address translation (NAT) rules are configured to allow access to port 80/443. For more information, see Azure Resource Manager support for Load Balancer.

* **Next generation firewall-**

Extends network protections beyond network security groups, which are built into Azure. Security Center discovers deployments for which a next generation firewall is recommended, and then you can set up a virtual appliance.

* **SQL auditing and threat detection-**

Recommends that auditing of access to your SQL database be enabled for both compliance and advanced threat detection, for investigation purposes.

* **SQL encryption-**

Recommends that encryption at rest be enabled for your SQL database, associated backups, and transaction log files. Even if your data is breached, it is not readable.

* **Vulnerability assessment-**

Recommends that you install a vulnerability assessment solution on your VM.

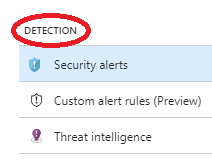
* **Storage encryption-**

Currently, this feature is available for blobs and Azure Files. After you enable Storage Service Encryption, only new data is encrypted, and any existing files in this storage account remain unencrypted.

* **JIT network access-**

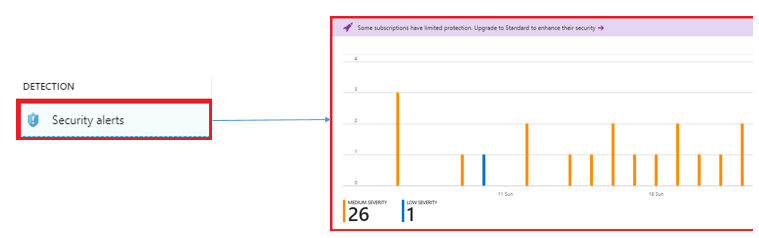
When just-in-time network access is enabled, Security Center locks down inbound traffic to your Azure VMs by creating a network security group rule. You select the ports on the VM to which inbound traffic should be locked down

## Detection

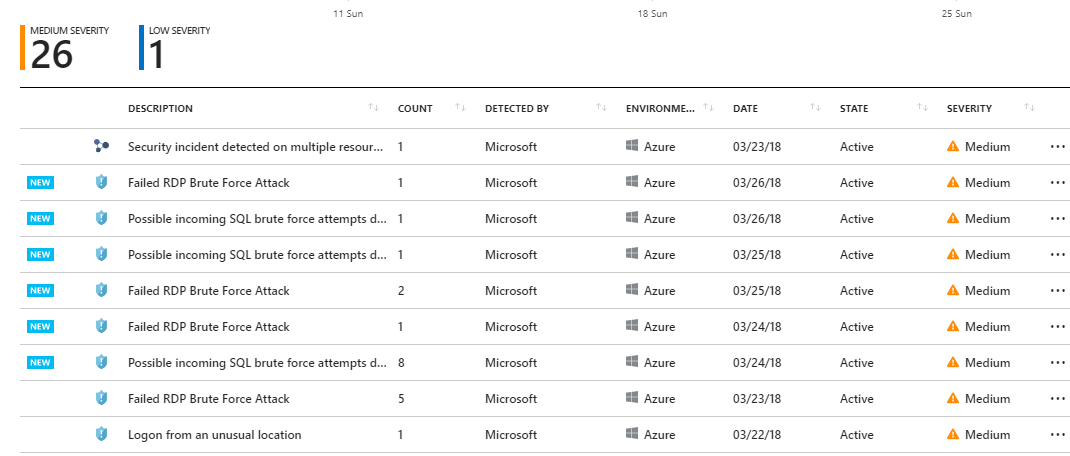
****

* **Security Alerts**

Security Center automatically collects, analyses, and integrates log data from your Azure resources, the network, and connected partner solutions, like firewall and endpoint protection solutions

****

* **Some of the Examples**

****

## What are custom alert rules?

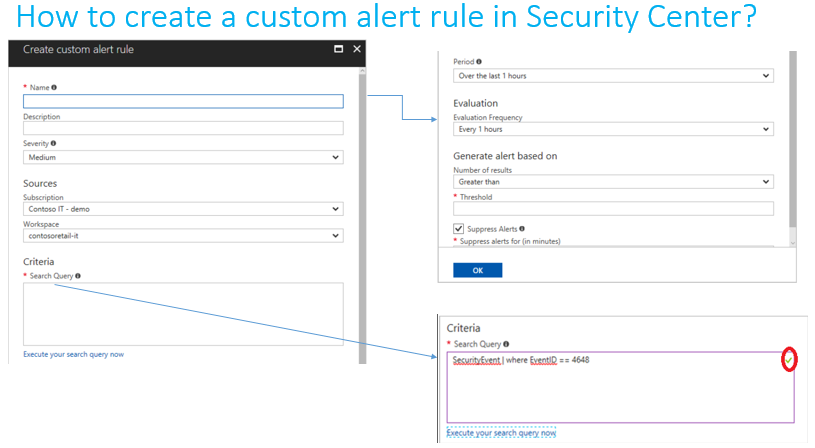
Custom alert rules allow you to define new security alerts based on data that is already collected from your environment. You can turn any search query result into alert rule to detect custom behaviours

.

The queries can use computers security events, partner's security solution logs or data ingested using APIs.

* **How custom alert rules work?**

Each time custom alert rule is defined, a special Azure Monitoring alert is created. When the alert rule is triggered, it is processed together with the other security alerts just like the built-in analytics.



## Threat Intelligence:

By using the threat intelligence option available in Security Center, IT administrators can identify security threats against the environment.

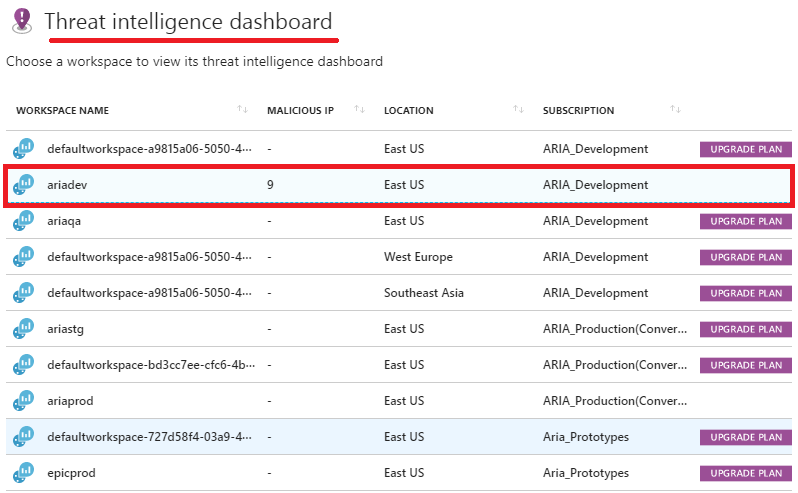
* **Threat intelligence pane is composed of three major options:**

Detected threat types

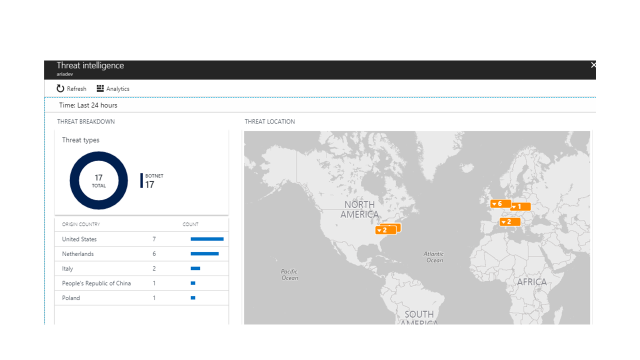
Threat origin

Threat intelligence map

* **Click on Workspace Name**

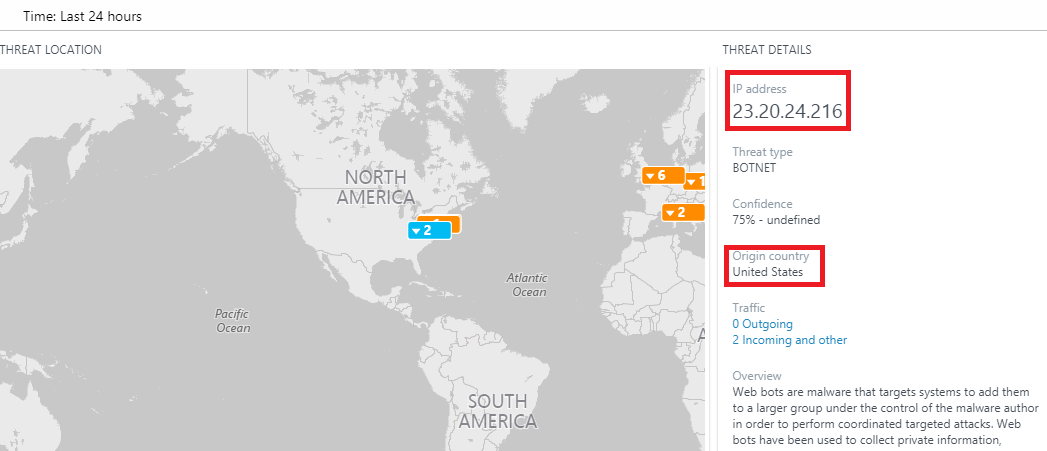
****

Cutting edge technologies like AI and Machine Learning to actually analyse all the data traffics that is going on around to all end points we have, in return it makes it available in front of you

****

* **Threat Location and Threat Details**

Example: malicious IP is displaying here

****

# Azure Operational Security



## Overview

It is a method or technique to understand how Azure Operational Security that protects data, applications and other assets of users by means of Azure Operational Security Services. It also helps to understand unique capabilities of Microsoft includes, Microsoft Security Development Lifecycle (SDL), Microsoft Security Response Center program, and deep awareness of the cyber security threat

Following benefits could be realized post-successful usage of the checklist document of Operational Security best practice

* Monitor, manage, and protect cloud infrastructure
* Manage identity and implement single sign-on (SSO)
* Trace requests, analyze usage trends, and diagnose issues
* Monitoring services with a centralized monitoring solution
* Prevent, detect, and respond to threats
* End-to-end scenario-based network monitoring
* Secure deployment using proven DevOps tool

## Importance of the Operational Security

It monitors your resources, Enables Single sign-on for users, Multi Factor Authentication gives additional level of protection for users, Avoid Data Loss, Business Protection. Unless you fail to enable Best practices, you might face Security issue, Unauthorized Access, Data leakage and that leads to Business Loss.

## Monitor, Manage and Protect cloud infrastructure

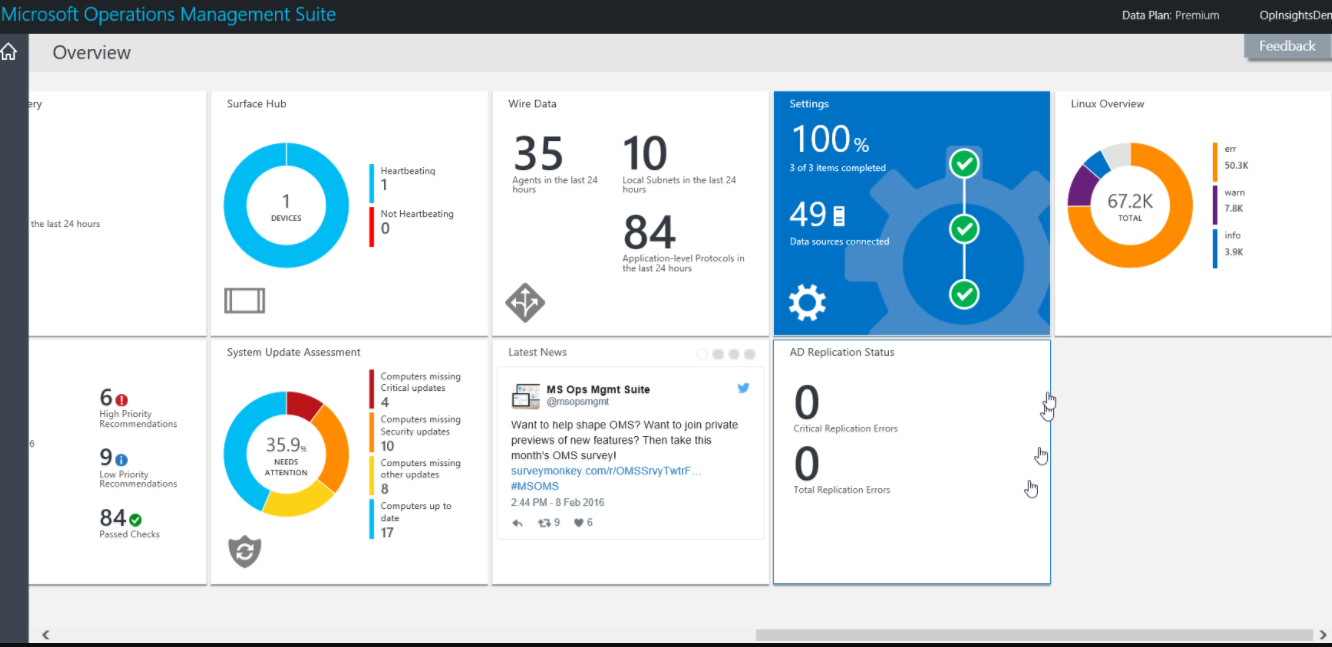
**Microsoft Operations Management Suite(OMS) for managing**

* It is collection of cloud-based services and protect your on-premises and cloud infrastructure
* Below are the services which helps to managing your cloud infrastructure.
  + **Log Analytics** - Monitor, analyze and performance of physical and virtual machine
  + **Automation** - Automate manual process
  + **Backup**  - Backup and restore critical data
  + **Site Recovery** - Provide high availability for critical applications

**OMS Security and Audit Solutions**

* It actively monitors all resources, which can help minimize the impact of security incidents
* Below are the services helps for monitoring purposes
  + **Security Domains** - track records of past and current events
  + **Notable issues** - identify the number of active and severity issues
  + **Detections** - identify attack patterns by visualizing security alerts take place against your resources
  + **Threat intelligence** - identify attack patterns of outbound malicious
  + **Common security queries** – Searching queries using Search blade on the dashboard page

**OMS Dashboard**



## Manage identity and implement single sign-on

Azure AD provides **Identity Management Service**, which identify vulnerabilities affecting your organization’s identities. It provides secure access to on-premises and cloud applications includes Microsoft Office 365, Non-Microsoft as a Service(SaaS)applications

* Detect Vulnerabilities - Calculating sign-in risk levels and user risk level
* Investigating risk events - sending notifications for risk events, provides basic workflow to track investigations
* Risk-based conditional access policies - Policy to block or secure risky/unauthorized user accounts

**Example**: You are trying to access a SaaS application like Gmail, you failed login in 1st attempt because you entered wrong password, to overcome this scenario we have a second layer of authentication like phone call, text message and so on...!

**Single sign-on** is a method to access all of your applications using single user account. It enables applications to redirect to Azure AD for user authentication instead of entering password in manual.

**Example** for Single Sign-on is Signing into your SaaS application like Google Apps, Office 365, One Cognizant etc., User authentications are stored in AD level

## Trace requests, analyse usage trends, and diagnose issues

**Azure Storage Analytics** performs logging and provides metrics data for a storage account. This data helps to identify, diagnose, and troubleshoot Azure Storage-related issues. Storage Analytics metrics are enabled by default for new storage accounts.

Azure Storage uses table storage to store the metrics for your storage account

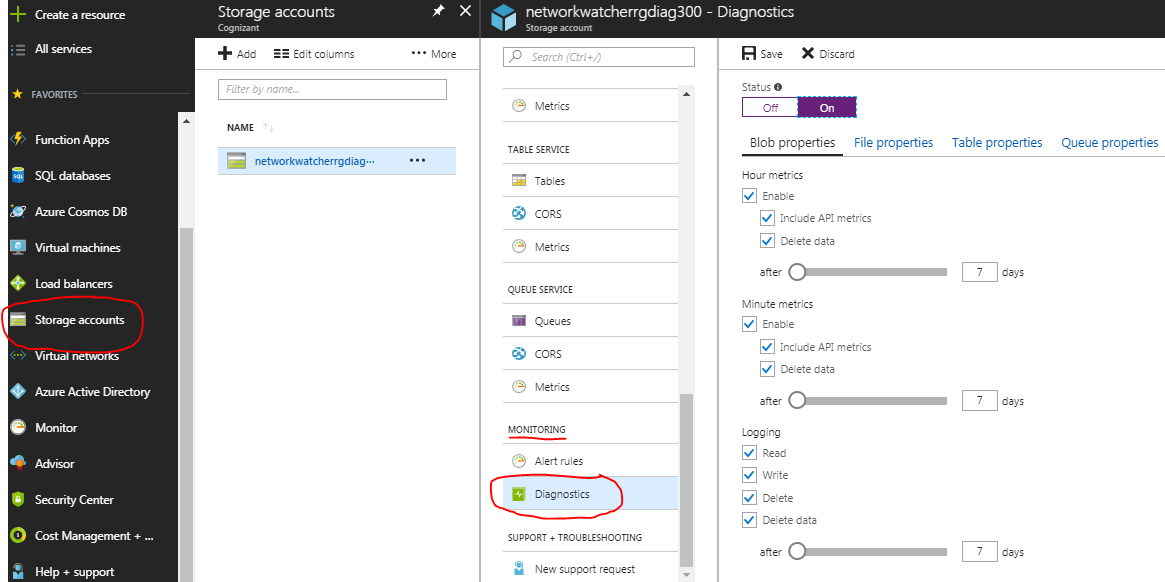
**How Metrics Are Stored**

All metrics data stored for storage services are stored in three tables

|  |  |
| --- | --- |
| **Table Name** | **Description** |
| 1. Hour Transaction Information | Request and response data |
| 2. Minute Transaction Information | Request and response data |
| 3. Capacity Information | Storage usage data which is used by Storage account in Blob Service |

**Configuring Metrics and Logging in azure portal**

In the [**Azure portal**](https://portal.azure.com/), select **Storage accounts**, then the storage account name to open the account dashboard



**Reference link to get logs and metrics using PowerShell**

<https://docs.microsoft.com/enus/powershell/module/azure.storage/?view=azurermps-5.4.0>

## Monitoring services

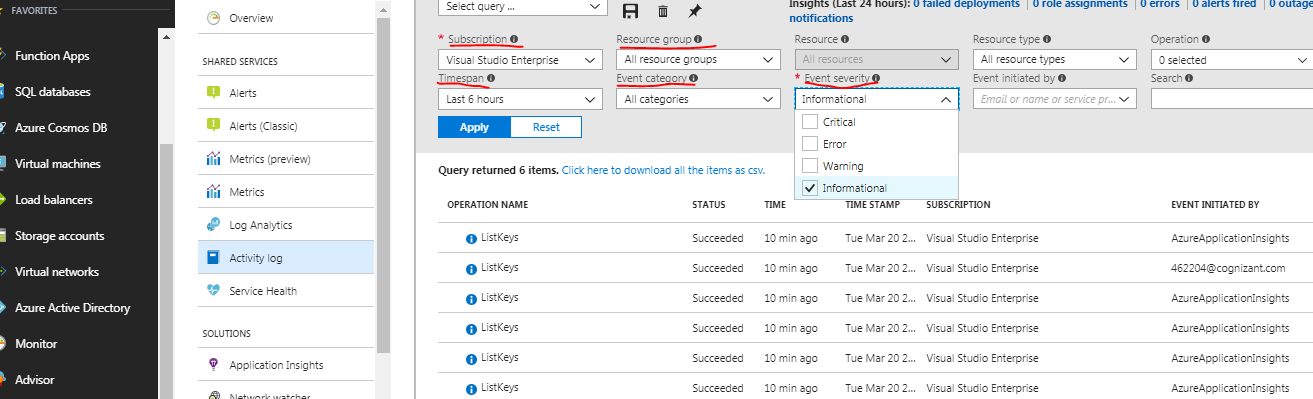
Azure Monitor helps to monitor your application stays up and running in a healthy state. Using monitoring, gain in-depth details of your application that helps to improve your application performance and maintainability where you lagging.

Azure Monitor has three basic categories of monitoring data: The **activity log, metrics, and diagnostic logs**

* + 1. **Activity log** – it shows all operations performed on resources in your subscription. It helps to analysis Who, What and When they create, update and deletion of the resources. Logs are viewed based on the drop down of sub sections like subscription, resource group, timescan, category, event search on the right side.

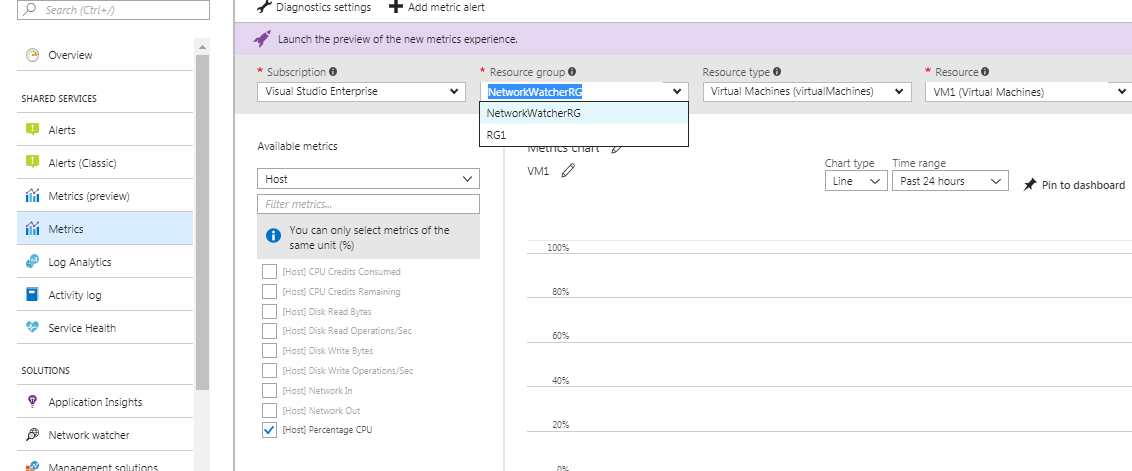
**For example**, If Virtual Machine stopped, Activity log shows who stopped and when they stopped it. Logs are stored according to time that we set at **Timespan** (below diagram I set to 6 hours so it gets an activity for last 6 hours)

**Activity log in Azure Portal**



* + 1. **Metrics** – Same like activity log, filtering and selecting resources in drop down to view the metrics. By default, once you selected your resource, all available metrics are listed in left blade. It represents in graph chart.

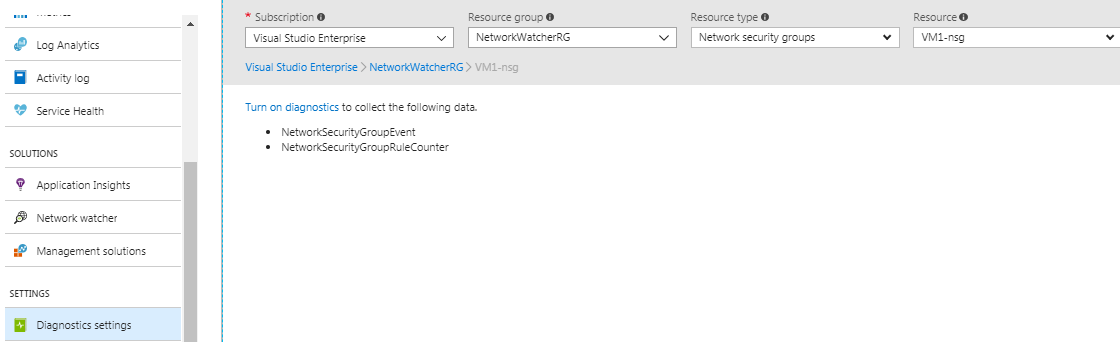
**For example**, in this below screenshot I have selected Percentage CPU metric for VM. Since this is a new VM, there is no utilization002E



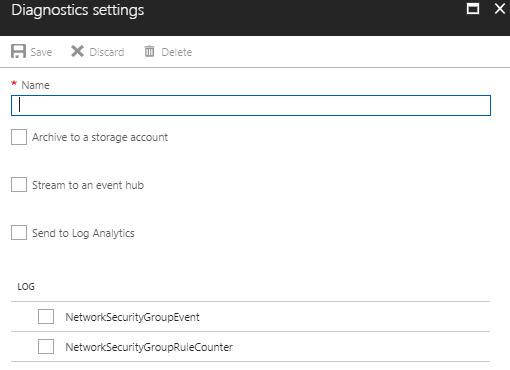
* + 1. **Diagnostic logs –** this logs are produced from resource that provide data about the resource.

Following steps shows how to enable diagnose logs for your resources.

Step 1: Select **Diagnostics settings** in left blade then filter and select drop downs on the right side to enable Diagnostic logs for the resource. Here I had chosen **NSG**.



Step 2:Network Security Group Rule Counters and Logic App Workflow Logs are both type of diagnostics logs. To store these logs in either of 3 in below screenshot.



**Reference link to monitoring azure resources using PowerShell :** <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-powershell-samples>

## Prevent, detect, and respond to threats

Security Center helps to prevent, detect respond to threats from azure resources, the networks and connected partner solutions. It gives overall view of the azure resources.

When you choose Security Center make sure you review all recommendations which is done by **Recommendations tile** or per resource **(Compute, Networking, Storage & data, Application)** Once you addressed all recommendations

* + 1. **Prevention** section should be green for all resources and preventing incidents.
    2. **Detection** section is about identifying threats early. Security Alerts shows graphical representation of detected threats found on each day and it is identified by different priorities like (Low, Medium, High). These are alerts regarding issues that are either taking place now, or occurred in the past.
    3. **Response** is about removing the attacker and restoring systems to reduce the impacts. Responding to threats have some key capabilities,
* **Understand cloud security state** – it gives you overall view to understanding of resources are configured correctly and controls are in place in security center. Here we can easily identify resources which required immediate attention.
* **Take control of cloud security** – Security policies have a control of your azure subscription. Policy are defined based on your work load and data sensitivity.
* **Easily deploy integrated cloud security solutions** – By enabling Security Solutions, Microsoft and its partners provides easy way of deployment in cloud. Even network changes are configured in network layer.
* **Detect threats and respond fast** – Security Center alert, give you attacked area, related events, impacted resources, suggest ways for improvement and quick recovery.

## End-to-end scenario-based network monitoring

**Network Watcher** is end-to-end scenario based network monitoring.

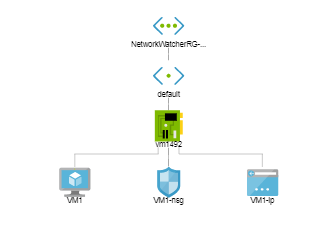
It monitors and diagnose data on all connected network resources like VNet, ExpressRoute, Application Gateway, Load balancers, Packet captures and more in Azure without logging in to VM.

It captures in and out packets of your VM and packets are stored in blob/local. Below are the features available in Network watcher

* Topology
* Packet capture
* IP flow verify
* Next hop
* Security group view
* NSG flow logging
* Virtual Network Gateway troubleshooting

To choose Network Watcher in portal, Choose **All Services - > Networking - > Network Watcher**

**For example**, User wants to view network interconnection of the resources in graphical, below diagram shows topology in azure network watcher for single VM. It shows the flow graph of subset/interconnected networking components.



## Secure deployment using proven DevOps tools

Below are some DevOps tools testing performances in app and improve the quality of the deployment to make sure application is always up and available.

* + 1. **Infrastructure as Code (IaC)**

It reduces burden facing by IT pros in daily basis. It provides template to IT pros to build and maintain their environment. Like ARM, we are deploying many resources in a single template.

* + 1. **Continuous Integration and Deployment:**

Visual Studio Online automatically deploys the binaries after doing a build to Azure after every code check-in

* + 1. **Release Management**

It helps in managing and automate our release process easily, quickly.

* + 1. **App Performance Monitoring**

Detect issues, solve problems, and continuously improve your applications performance.

* + 1. **Load Testing & Auto scale**

Testing performance problems in our app to improve deployment quality and to make sure our app is always up or available.

## Azure Operational Security checklist

Before deploying cloud application in production it’s a good practice to have a checklist. It evaluates your application against a list of essential and recommendation given by you/customer.

At last, it helps you to build a secure cloud migration and good operation strategy for your organization

Below are check list category

|  |  |
| --- | --- |
| **Check List Category** | **Description** |
| Security Roles & Access Control | Using **RBAC**, we can provide secure permissions to users, groups and applications |
| Data Collection & Storage | Data collected and stored in your storage are automatically encrypted using **Storage Service Encryption (SSE)**  OS and Data disks using by VM’s are encrypted using **Azure Disk Encryption** |
| Security Policies & Recommendations | Policies are defined at **Security Center** for your Azure subscription based on your Workload and Data Sensitivity. |
| Identity & Access Management | **Azure AD** helps to identify sign-in and user level risk  Enable **Multi Factor Authentication**, it provides 2nd layer of authentication for users to access your application  Use **Single Sign-on**, users to access multiple applications using single credentials |
| Ongoing Security Monitoring | **Identity and Access** provides Live monitoring like,  No of failed or successful logged on attempts, password change/reset for user accounts, accounts that were locked out.  **Log analytics**, produce the reports of antimalware protection of your infrastructure. |
| Azure Security Center Detection capabilities | With help of **Detect capability**, we canidentify active threat that targeting your Azure resources. |
| Developer Operations (DevOps) | Here we have different operations like automation and integration to develop the performance of the application. At last, successfully releasing application at right time. |



# Document Control

## Document Version Information

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Document Version Information | | | | |
| Date | **Change Reference** | **Author** | **Version** | **Sections Affected** |
|  |  |  |  |  |
|  |  |  |  |  |

## Document Distribution

|  |  |  |
| --- | --- | --- |
| Document Distribution | |  |
| Name | **Responsibility** | **Action/Information/**  **Approval** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Associated Documents

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Associated Documents | | | | |
| No. | **Type** | **Version** | **Link** | |
|  |  |  |  | |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Approvals

|  |  |  |  |
| --- | --- | --- | --- |
| Approvals |  |  |  |
| Type | **Function** | **Reviewer(s)** | **Date** |
|  |  |  |  |
|  |  |  |  |

## 