FOR INTERNAL USE

Cloud Operation Services with Azure

Low Level Design v1.3

OWNER: Capgemini Cloud Operation Services

Table of Contents

[Table of Contents 3](#_Toc93493227)

[About This Template 4](#_Toc93493228)

[Template History 4](#_Toc93493229)

[1. Document Control 5](#_Toc93493230)

[1.1 Version History 5](#_Toc93493231)

[1.2 Document Contributors 5](#_Toc93493232)

[1.3 Document Reviewers 6](#_Toc93493233)

[1.4 Document Approvals 6](#_Toc93493234)

[2. Overview 7](#_Toc93493235)

[2.1. Introduction 7](#_Toc93493236)

[2.2. Purpose of this Document 7](#_Toc93493237)

[2.3. Scope 7](#_Toc93493238)

[2.4. Referenced Documents 8](#_Toc93493239)

[3. Abbreviations, Acronyms and Glossary of Terms 9](#_Toc93493240)

[4. Solution Design 10](#_Toc93493241)

[4.1. Baseline Architecture 10](#_Toc93493242)

[4.2. Target Architecture 10](#_Toc93493243)

[4.3. Design Principles & Standards 10](#_Toc93493244)

[4.4. Design Decisions 10](#_Toc93493245)

[4.5. Risks/ Assumptions/ Issues/ Dependencies 11](#_Toc93493246)

[5. Target Architecture 12](#_Toc93493247)

[5.1. Network 12](#_Toc93493248)

[5.2. Integrations 18](#_Toc93493249)

[5.3. Backup & Recovery 19](#_Toc93493250)

[5.4. Operational Monitoring and Logging with ServiceNow integration 27](#_Toc93493251)

[5.5. Update Management 45](#_Toc93493252)

[5.6. Security 54](#_Toc93493253)

[5.7. Automation 63](#_Toc93493254)

[5.8. Governance 64](#_Toc93493255)

[5.9. Dashboards 68](#_Toc93493256)

[5.10. Reports 76](#_Toc93493257)

[5.11. Cost Management 77](#_Toc93493258)

[6. Environment Considerations 81](#_Toc93493259)

[7. Software Licensing 82](#_Toc93493260)

[8. Hardware and Software Components 83](#_Toc93493261)

About This Template

Guidance notes are written in a red font throughout the body of this template. They are designed to be deleted once taken into consideration. The font color should be returned to the standard (red: 236, green: 236, blue: 236).

Sections that are not relevant to the design should remain in the document with an ‘N/A’ in the subtext.

Comments and suggestions on the template are welcome. Please contact Leanne OLeary.

## Template History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Name** | **Changes** | **Date** | **Status** |
| V0.1 | Leanne O’Leary | Initial creation | 09/2019 | Draft |
| V0.2 | Leanne O’Leary | Rework to align with HLD template | 09/2019 | Draft |
| V1.0 | Leanne O’Leary | Input from security, updated reviewers/approvers | 10/2019 | Final |

1. Document Control

|  |  |
| --- | --- |
| Source File Location | [Temporary Link](https://capgemini.sharepoint.com/:f:/r/sites/CCPNative/Shared%20Documents/General/LLD?csf=1&web=1&e=lufEpW) |
| Confidentiality Level | Company Confidential |
| Version | Version 1.1 |
| Date | 19/01/2022 |
| Change Control Owner | Jakub Chwala |

## Version History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Name** | **Changes** | **Date** | **Status** |
| V0.1 | Jakub Chwala | Initial draft of document | 02/2021 | Draft |
| V0.2 | Tomasz Cebula, Jakub Chwala | Monitoring and Patching added | 03/2021 | Draft |
| V0.3 | Tomasz Cebula, Jakub Chwala | Backup and Logging Added | 04/2021 | Draft |
| V0.4 | Jakub Chwala | Role Based Access Control | 05/2021 | Draft |
| V0.5 | Jakub Chwala | Deployment and automation added | 06/2021 | Draft |
| V0.6 | Jakub Chwala | Policies | 06/2021 | Draft |
| V0.7 | Michal Hutnik | Workbooks | 06/2021 | Draft |
| V0.8 | Jakub Chwala | Design Decisions | 06/2021 | Draft |
| V0.9 | Jakub Chwala | Cost Management + Security | 07/2021 | Draft |
| V1.0 | Jakub Chwala | Security Approval | 08/2021 | Final |
| V1.1 | Jakub Chwala | Reports + Repository update | 11/2021 | Final |
| V1.2 | Miroslaw Rozek | Identity & Access Management update | 01/2022 | Final |
| V1.3 | Miroslaw Rozek | Governance update – added Initiatives | 01/2022 | Final |

## Document Contributors

|  |  |
| --- | --- |
| **Name** | **Role** |
| Tomasz Cebula | Microsoft Azure Architect |
| Jakub Chwala | Microsoft Azure Architect |
| Michal Hutnik | Microsoft Azure SME |
| Mirosław Rożek | Microsoft Azure Architect |

## Document Reviewers

Delete/add/amend as appropriate. Include version and date reviewed.

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Name** | **Role** | **Date** |
|  | Luke Harrigan | Business Owner |  |
|  | Guy Sidford | Lead Architect |  |
|  | Paul Bargiel | Network Architect |  |
|  | Steven Allen | Security Architect |  |
|  | Kasia Sulowska | Programme Manager |  |
|  | Thomas De Vita | Global Cloud Solution Team Lead |  |
|  | Niels Lemmens | Product Owner |  |
|  | Leanne OLeary | General Architect |  |
|  | Reagan Lewis | Run Owner |  |

## Document Approvals

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Name** | **Role/Title** | **Date** |
|  | Luke Harrigan | Business Owner |  |
|  | Niels Lemmens | Product Owner |  |

1. Overview
   1. Introduction

Cloud Operation Services is the Capgemini Cloud Platform (CCP) native offer for Infrastructure as a Service (IaaS) solutions. This document provides a breakdown of the various components necessary to provide IaaS management using cloud native tooling. It illustrates the relationship between the components and provides detailed information on the use and process flow for each component.

* 1. Purpose of this Document

This document is intended to be used as a design reference point for deploying Cloud Operation Services with Azure and for management of Infrastructure as a Service. Its intended audience is for internal CCP technical staff who require more detail in the interaction and setup of the overall Cloud Native design.

* 1. Scope

This document is focused on the definition of the cloud native components and relationships between them. At time of writing the scope for this project is limited to the following management functions for Azure Public Cloud VM’s:

* Identity: Azure AD Integration, RBAC
* Networking
* Update Management
* Backup
* Monitoring and Alerting to ServiceNow
* Logging
* Security
* Dashboards
* Cost Management
* Reports
  1. Referenced Documents

|  |  |  |  |
| --- | --- | --- | --- |
| **Item No.** | **Document Title/Collateral Description** | **Author** | **Version** |
| 1 | CCP IaaS Proof of Concept | David Wansell, Jakub Chwala | V0.2 |
| 2 | CCP Security HLD | Steven Allen | V2.1 |
| 3 | COS HLD | Guy Sidford, Tomasz Cebula | V1.0 |
| 4 | Azure Direct federation with CCP ADFS for CCP users (SAML) |  |  |
| 5 | CCP Networking HLD | Waseem Akhtar | V1.10 |
| 6 | CCP Image Deployment and Testing HLD | Leanne OLeary | V1.2 |
| 7 | CCP Proposed Changes to Azure Monitoring | Tomasz Cebula |  |
| 8 | Cloud Operation Services with Azure and AWS Reference Architecture | Sylvain Roby |  |
| 9 | Cloud Operation Services with Azure and AWS Service Descriptions | Lukasz Lacniak |  |
| 10 | Cloud Operation Services SOW | Lukasz Lacniak |  |
| 11 | Cloud Security Services Offering - Cloud Security Posture Management - Service Description | Michal Malec | V1.0 |
| 12 | Cloud Security Services Offering Service Description | Michal Gawor | V1.0 |
| 13 | Cloud Security Posture Management Solution Guidance | Michal Malec | V1.0 |
| 14 | Cloud Security Service Offering - Cloud Workload Protection Platform Solutioning Document | Michal Gawor | V1.0 |

1. Abbreviations, Acronyms and Glossary of Terms

Below are appropriate for the template. Delete/add/amend as necessary. Ensure this is in alphabetical order.

|  |  |
| --- | --- |
| **Term** | **Definition** |
| API | Application Programming Interface |
| APT | Advanced Persistent Threat |
| AV | Antivirus |
| CCP | Capgemini Cloud Platform |
| CIS | Cloud Infrastructure Service |
| CMO | Current Mode of Operation |
| DDoS | Distributed Denial of Service |
| DLP | Data Leakage Prevention |
| EU | European Union |
| FIM | File Integrity Management |
| FMO | Future Mode of Operation |
| GBL | Global Business Line |
| GDPR | General Data Protection Regulation |
| IDAM | Identity & Access Management |
| IDS | Intrusion Detection Systems |
| IEC | International Electrotechnical Commission |
| ISO | International Standards Organisation |
| IPS | Intrusion Prevention Systems |
| LLD | Low Level Design |
| MVP | Minimum Viable Product |
| N/A | Not Applicable |
| NIS | Network and Information Systems (cybersecurity legislation) |
| OS | Operating System |
| PAM | Privileged Access Management |
| PAYG | Pay as You Go |
| POV | Proof of Value |
| RAID | Risks, Assumptions, Issues & Dependencies |
| SIEM | Security Information and Event Management |

Table 1 Abbreviations, Acronyms and Glossary of Terms

1. Solution Design
   1. Baseline Architecture

Please refer to Cloud Operations Services HLD Document

* 1. Target Architecture

Please refer to Cloud Operations Services HLD Document

* 1. Design Principles & Standards

COS design principles:

* Based on Cloud Native Services
* Automation first approach
* Infrastructure as Code and version controlled as standard
* Reuse of existing investment and capability
* OS builds scripted across all platforms
* Integration into client catalogue
* Meets the requirements of the wider Capgemini GBLs
  1. Design Decisions

|  |  |
| --- | --- |
| ID | Decision |
| 1 | Primary goal of Cloud Operation Services (COS) offer is to use native solutions available within each Public Cloud provider, in this case – Microsoft Azure. |
| 2 | Each component of COS Solution can be deployed individually based on customer needs. For example, if customer has any Backup solution already deployed than it is possible to exclude COS Backup solution upon deployment phase. |
| 3 | Access to customer environment/workloads must be done via SAM Jump Hosts which enforces MFA and VPN, however if customer uses their own method for connecting to their environment and that solution is on par with security level offered by Capgemini’s SAM, than customer’s solution can be used. Solution has to be documented on Project phase and accepted by customer and Capgemini Group Security |

* 1. Risks/ Assumptions/ Issues/ Dependencies

|  |  |  |
| --- | --- | --- |
| **RAID ID**  (R.1, A.1, I.1, D.1 etc.) | **RAID Detail:**   * Description * Impact * Mitigating actions | **Supporting Comments:**   * Owners * Approvers * Internal/External * Open/Closed |
| A1 | Solution is region specific. Must be deployed to each client region requiring VM instance management.  If customer has multiple subscriptions in the same region within one Tenant there is no need to deploy solution to multiple subscriptions. |  |
| D1 | Solution depends on CCP SAM for accessing customer Virtual Machines and CCP Active Directory as Identity Provider unless customer has its own solution for VM access. |  |
| A2 | VMs have outbound access to Azure network over port 443 for Update Management purpose |  |
| A3 | Firewall Rules must allow traffic to Microsoft’s Update URLs listed in Firewall Prerequisites under Update Management section |  |
| A4 | As a default Public Repositories are used to patch Linux and Windows Virtual Machines |  |
| A4 | For initial deployment of COS, Capgemini Project Team must receive Azure AD Service Principle Identity with sufficient RBAC to deploy the solution. Minimum RBAC are listed within each solution. |  |

1. Target Architecture
   1. Network

Network setup is highly dependent on customer environment and necessary integrations. High Level Design documents of each Integration provide more details on network requirements for each tool.

This document contains the network requirements necessary only for native services to operate.

* + 1. Topology

Network Topology depends on customer environment. If CCP Federated access is not allowed by the client a jump server will be provisioned into the client account and the client will provide roles. The jump server will be accessed via SAM light. (Customer needs to provide access to customer SAM Citrix)

If customer prefers Capgemini’s SAM as a method of accessing Virtual Machines than SAM Network prerequisites should be met. Please refer to SAM documentation for more details.

If customer has its own method of accessing Virtual Machines, Capgemini personnel can use that method as well, however it must be clearly stated in the beginning of each project.

* + 1. User Connectivity

If a customer does not have a solution for accessing their workloads in secure manner, Capgemini support will use SAM.

SAM requires Virtual Network and VPN Gateway within a customer account to connect with SAM DC on AWS.

The client can provide their own solution, or a jump server will be provisioned into the client account and the client will provide roles. The jump server will be accessed via SAM light.

* + - 1. Capgemini Access

SAM is Capgemini’s primary means for accessing customer workloads. If a customer would like to use their own solution, it needs to be agreed with project team. More details can be found within SAM HLD document listed in the beginning of this document.

As the solution progresses the approach is to automate away as many day-to-day interactions that drive the need for Operations staff to log into a virtual machine.

Where this is not possible the intention is to leverage Azure Bastion or Run Command feature to facilitate access to all machines that have Azure Agent running on them. Both Azure Bastion and Run Command activities are being logged within Azure Activity Log and can be retrieved later in case of any misconfiguration issues. Activity Logs also contains information about user who Run Command on Virtual Machine

Subsequent phases of the project will refine how this can be used, gain agreement that the solution meets the appropriate security requirements with the aim to remove the need to support direct SSH & RDP access to customer workloads.

If CCP Federated access is not allowed by the client a jump server will be provisioned into the client account and the client will provide roles. The jump server will be accessed via SAM light.

* + - 1. External

Access for customer networks and users is considered on a case-by-case basis and it is not within the scope of this document.

External users can access customer Azure Tenant via the Azure Portal. Access must be granted by customer and must include RBAC assignment at minimum level for task to be executed.

Capgemini can act as advisor while granting RBAC to any external users. External users can only use AWS Azure Bastion Server to access customer VMs. Accessing VMs via SAM is not possible as SAM is dedicated for Capgemini personnel only.

* + 1. Traffic Flows

Every feature of Cloud Operation Services is native and is deployed within Customer Azure Tenant. Thanks to that approach Traffic flows are limited to below:

* + - 1. ServiceNow Integration

|  |  |
| --- | --- |
| Tool | Azure App Function |
| Source | Azure Datacenter |
| Destination | iPaaS |
| Direction | Unidirectional |
| Purpose | Automated Incident creation in Service Now for issues with customer resources |
| How is it protected? | App Function requires access to the key vault to store iPaaS ClientID, Client Secret and Barer Token to make HTTPS API POST request to iPaaS |
| Does it contain customer personal data? | No |
| What does it contain? | Azure Resource ID, Alert Description, Company Name and severity of the alert. |
| Who has access? | COS Operations |

* + - 1. Reports

|  |  |
| --- | --- |
| Tool | Azure |
| Source | Azure Datacenter |
| Destination | Delegated User |
| Direction | Unidirectional |
| Purpose | Automated Performance, Availability, Backup, Alerts and Patching reports |
| How is it protected? | Delegated User can access the storage account container and download the reports, and it will be sent to action group. |
| Does it contain customer personal data? | No |
| What does it contain? | Azure Resource IDs from Customer Tenant, Subscriptions, Tags |
| Who has access? | COS Operations |

* + - 1. CMDB – Need to check with Splunk team

|  |  |
| --- | --- |
| Tool | Azure Logic App |
| Source | Azure Datacenter |
| Destination | Rundeck server |
| Direction | Unidirectional |
| Purpose | Automated Update of CMDB |
| How is it protected? | Azure Function App uploads CSV with list of resources to storage blob. Rundeck job downloads file from storage blob. |
| Does it contain customer personal data? | No |
| What does it contain? | Azure Resource ID, Subscription, Tags |
| Who has access? | COS Run Ops Team |

* + 1. Firewall Rules

Customer may choose to use one or multiple of Native Solutions described within this document, hence Firewall requirements are listed within each section separately.

* + 1. Network Components

Network components deployed with Cloud Operation Services varies on solutions, integrations, and way of accessing customer Virtual Machines. As a minimum Network Security Groups must be deployed to block inbound and outbound internet traffic over VM management ports.

Azure Firewall is optional component of Azure Security Center which can be enabled and configured based on customer requirements. Azure Firewall is part of Cyber Security offer.

For customers using Capgemini’s SAM, please see SAM network requirements within SAM HLD document listed in the beginning of this document.

For scenarios with Azure Bastion AzureBastionSubnet with minimum /27 range must be deployed within each customer VNet.

Global endpoints for patching and monitoring needs to be enabled for 80 and 443 ports in customer environment.

* + - 1. Network Security Groups

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

In greenfield environment whitelisting Azure IPs will be included as a part of network security group configuration.

|  |  |
| --- | --- |
| Property | Explanation |
| Name | A unique name within the network security group. |
| Priority | A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops. As a result, any rules that exist with lower priorities (higher numbers) that have the same attributes as rules with higher priorities are not processed. |
| Source or destination | Any, or an individual IP address, classless inter-domain routing (CIDR) block (10.0.0.0/24, for example), service tag, or application security group. If you specify an address for an Azure resource, specify the private IP address assigned to the resource. Network security groups are processed after Azure translates a public IP address to a private IP address for inbound traffic, and before Azure translates a private IP address to a public IP address for outbound traffic. . Specifying a range, a service tag, or application security group, enables you to create fewer security rules. The ability to specify multiple individual IP addresses and ranges (you cannot specify multiple service tags or application groups) in a rule is referred to as augmented security rules. Augmented security rules can only be created in network security groups created through the Resource Manager deployment model. You cannot specify multiple IP addresses and IP address ranges in network security groups created through the classic deployment model. |
| Protocol | TCP, UDP, ICMP, ESP, AH, or Any. |
| Direction | Whether the rule applies to inbound, or outbound traffic. |
| Port range | You can specify an individual or range of ports. For example, you could specify 80 or 10000-10005. Specifying ranges enables you to create fewer security rules. Augmented security rules can only be created in network security groups created through the Resource Manager deployment model. You cannot specify multiple ports or port ranges in the same security rule in network security groups created through the classic deployment model. |
| Action | Allow or deny |

Network security group security rules are evaluated by priority using the 5-tuple information (source, source port, destination, destination port, and protocol) to allow or deny the traffic. You may not create two security rules with the same priority and direction. A flow record is created for existing connections. Communication is allowed or denied based on the connection state of the flow record. The flow record allows a network security group to be stateful. If you specify an outbound security rule to any address over port 80, for example, it's not necessary to specify an inbound security rule for the response to the outbound traffic. You only need to specify an inbound security rule if communication is initiated externally. The opposite is also true. If inbound traffic is allowed over a port, it's not necessary to specify an outbound security rule to respond to traffic over the port.

Existing connections may not be interrupted when you remove a security rule that enabled the flow. Traffic flows are interrupted when connections are stopped and no traffic is flowing in either direction, for at least a few minutes.

* + - 1. Default security rules
         1. Inbound Rules

AllowVNetInBound

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Priority | Source | Source ports | Destination | Destination ports | Protocol | Access |
| 65000 | VirtualNetwork | 0-65535 | VirtualNetwork | 0-65535 | Any | Allow |

AllowAzureLoadBalancerInBound

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Priority | Source | Source ports | Destination | Destination ports | Protocol | Access |
| 65001 | AzureLoadBalancer | 0-65535 | 0.0.0.0/0 | 0-65535 | Any | Allow |

DenyAllInbound

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Priority | Source | Source ports | Destination | Destination ports | Protocol | Access |
| 65500 | 0.0.0.0/0 | 0-65535 | 0.0.0.0/0 | 0-65535 | Any | Deny |

* + - * 1. Outbound Rules

AllowVnetOutBound

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Priority | Source | Source ports | Destination | Destination ports | Protocol | Access |
| 65000 | VirtualNetwork | 0-65535 | VirtualNetwork | 0-65535 | Any | Allow |

AllowInternetOutBound

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Priority | Source | Source ports | Destination | Destination ports | Protocol | Access |
| 65001 | 0.0.0.0/0 | 0-65535 | Internet | 0-65535 | Any | Allow |

DenyAllOutBound

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Priority | Source | Source ports | Destination | Destination ports | Protocol | Access |
| 65500 | 0.0.0.0/0 | 0-65535 | 0.0.0.0/0 | 0-65535 | Any | Deny |

In the Source and Destination columns, VirtualNetwork, AzureLoadBalancer, and Internet are service tags, rather than IP addresses. In the protocol column, Any encompasses TCP, UDP, and ICMP. When creating a rule, you can specify TCP, UDP, ICMP or Any. 0.0.0.0/0 in the Source and Destination columns represents all addresses. Clients like Azure portal, Azure CLI, or PowerShell can use \* or any for this expression.

You cannot remove the default rules, but you can override them by creating rules with higher priorities.

* + 1. IP Addressing

IP Addressing is addressed on a client-by-client basis and not in scope for this document.

* 1. Integrations

Depends on customer requirements Cloud Operation Services may integrate with below tools:

|  |  |  |
| --- | --- | --- |
| System to Integrate with | Purpose of Integration | Method of Integration |
| CCP On Prem Active Directory + DUO MFA (optional) | To avoid islands of identity and to utilize existing SSO available on CCP Active Directory and to allow further integration with SAM | Azure Direct Federation SAML integration |
| Capgemini SAM (optional) | Jump Hosts to access customer workloads and CCP 3rd party tools. | Citrix |
| CSEM (optional) | Cost Management | Azure App Registration |
| ServiceNow | ITSM | Standard CIS MSP ServiceNow instance for service management. Azure Function App sends alerts from Azure Monitor via iPaaS. |
| Customer Hardened Images | To provide CIS Hardened cloud native OS Images | Azure App Registration |
| Splunk (optional) | AI Operations an alert generated from Azure monitor.  Excluding metrics, SIEM and non-alerting functions of Splunk. | Monitoring Alert correlation, suppression |
|  |  |  |

* 1. Backup & Recovery

Azure Backup allows to backup the data, machine state, and Azure virtual machine (VM) instances. With use of backup policy, customers can edit a policy, associate more virtual machines to a policy, and delete unnecessary policies to meet their compliance requirements. Azure Backup stores backed-up data in vaults - Recovery Services vaults and Backup vaults. A vault is an online-storage entity in Azure that's used to hold data, such as backup copies, recovery points, and backup policies.

Microsoft Azure Backup offers three levels of redundancy:

* Locally-redundant storage (LRS) – COS default
* Zone-redundant storage (ZRS) - optional
* Geo-redundant storage (GRS) - optional

When deciding which redundancy option is best for customer scenario, consider the tradeoffs between lower costs and higher availability. Within this document LRS and GRS Backup are used as an example during deployment process. **Please note that decision on redundancy level must be made before first VM will be added to the solution.**

* + 1. Backup prerequisites
       1. Access requirements

Minimum role requirements for Azure Recovery Vault Creation:

|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure role required | Scope required |
| Create Recovery Services vault | Backup Contributor | Resource group containing the vault |

Minimum role requirements for Backup Policy Creation/Modification/Deletion:

|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure role required | Scope required |
| Create backup policy for Azure VM backup | Backup Contributor | Recovery Services vault |
| Modify backup policy of Azure VM backup | Backup Contributor | Recovery Services vault |
| Delete backup policy of Azure VM backup | Backup Contributor | Recovery Services vault |

Minimum role requirements for Backup Restoration:

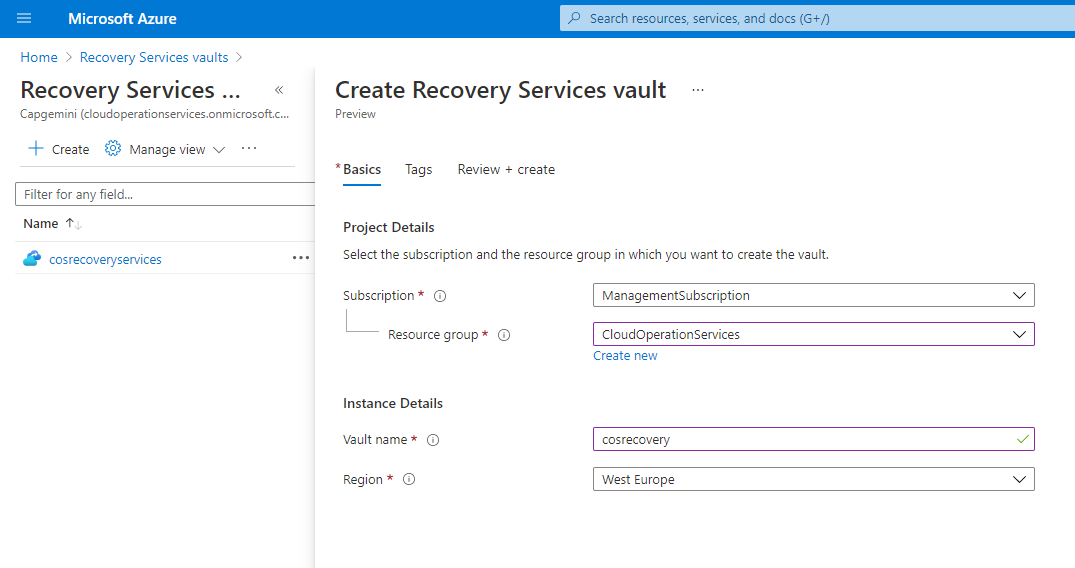
|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure role required | Scope required |
| Restore VM | Backup Operator | Recovery Services vault |
| Contributor | Resource group in which VM will be deployed |
| Virtual Machine Contributor | Source VM that got backed up |
| Restore unmanaged disks VM backup | Backup Operator | Recovery Services vault |
| Virtual Machine Contributor | Source VM that got backed up |
| Storage Account Contributor | Storage account resource where disks are going to be restored |
| Restore managed disks from VM backup | Backup Operator | Recovery Services vault |
| Virtual Machine Contributor | Source VM that got backed up |
| Storage Account Contributor | Temporary Storage account selected as part of restore to hold data from vault before converting them to managed disks |
| Contributor | Resource group to which managed disk(s) will be restored |
| Restore individual files from VM backup | Backup Operator | Recovery Services vault |
| Virtual Machine Contributor | Source VM that got backed up |
| Cross region restore | Backup Operator | Subscription of the recovery Services vault |

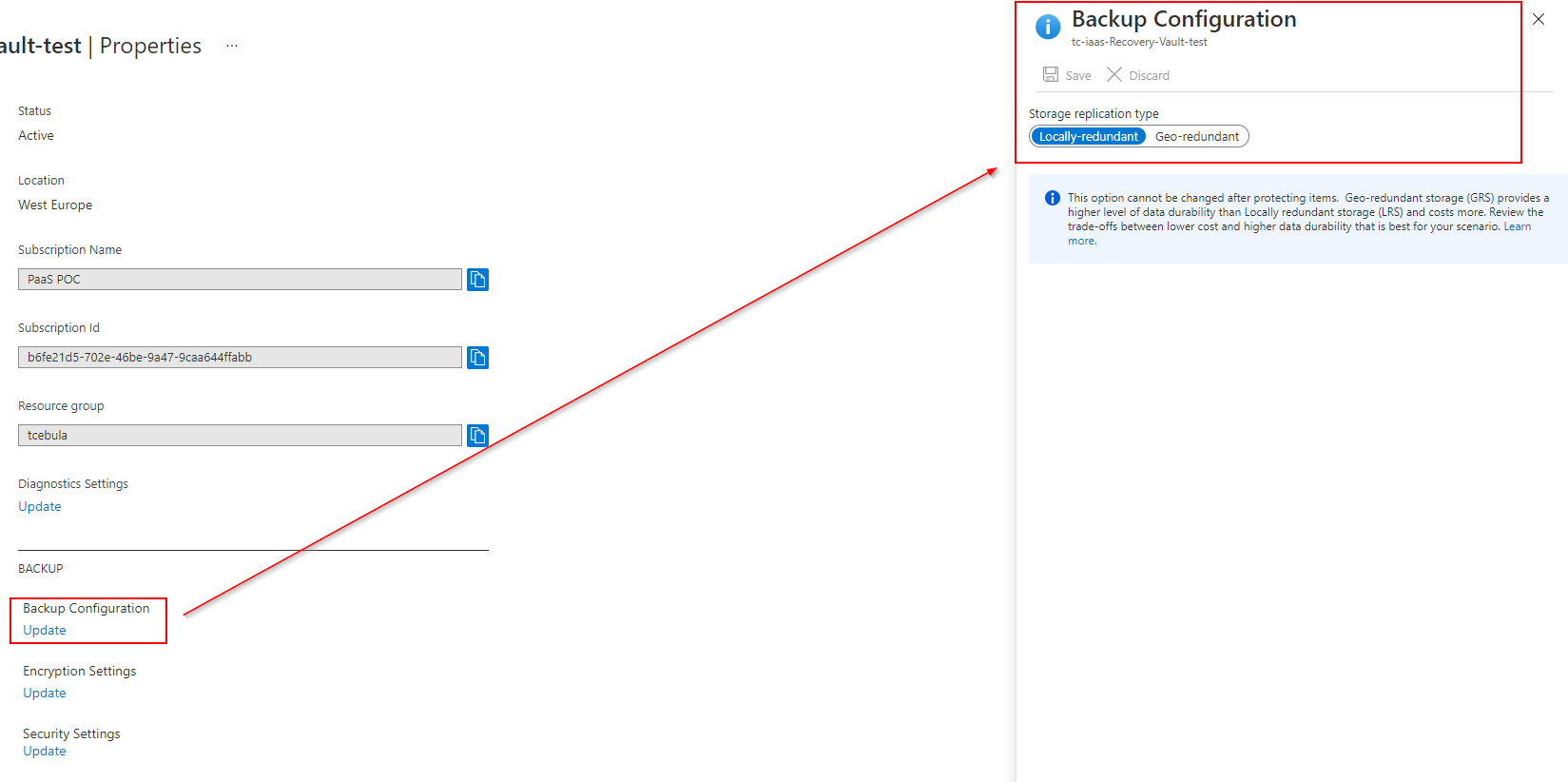
* + 1. Azure Backup – One Time Setup

During the initial setup of Cloud Operation Services - Azure Backup Solution following components must be created to ensure VM backup, automatic VM onboarding to backup solution and backup monitoring:

* Recovery Services Vault
* Azure Backup Policy
* Alerts
* Azure Policy to onboard VMs to backup based on Tags

A Recovery Services vault is an entity that stores the backups and recovery points created over time. The Recovery Services vault also contains the backup policies that are associated with the protected virtual machines. Below screenshot presents Creation of Recovery Services Vault from the Azure Portal. (For automated deployment steps – please refer to Automation section within this document).





Once Recovery Services Vault is created the Backup Policies can be defined.

* + 1. Backup Policy creation/modification

Backup Policies allow to define daily or weekly schedule and retention period for retaining snapshot locally to reduce backup and restore time (Instant Restore). This default value is given between 1 to 5 days.

The delay can be expected in backup start time from the scheduled backup time set in backup policy, scheduled backup will be triggered within 2 hours of the scheduled backup time. For example, if we have up to 100 VM’s and start time setup at 1:00 AM then by 3:00 AM all the VM’s job should be in progress. When performing initial backup we can observe an extended time window required for completion, this is because the first backup is always a full backup and the total backup time might be more than 24 hours, whereas that might not be the case for the incremental backups. Mentioned delays should be taken into consideration when planning maintenance window.

Following Backup Policy has been defined as standard:

|  |  |
| --- | --- |
| Backup schedule | |
| Frequency | Customer requirement |
| Time | Customer requirement |
| Timezone | As per customer Time zone |

|  |  |
| --- | --- |
|  |  |

Below screenshot presents creation and modification of Azure Backup Policy from Azure Portal. (For automated deployment steps – please refer to Automation section within this document).

* + 1. Backup Retention Policy

Retention range can be defined in days, retention of weekly \ monthly \ yearly backup point, when the recovery point expires, it either gets deleted or merged.

Following retention Policies have been defined upon policy creation and are considered within Cloud Operation Services as standard:

|  |  |
| --- | --- |
| Retention range | Backup Retention period |
| Daily backup | Customer requirement |
| Weekly backup | Customer requirement |
| Monthly backup | Customer requirement |
| Yearly backup | Customer requirement |

* + 1. Restoration Policy

Azure Backup can keep most recent backups on fast storage available for instant recovery. Instant Restore Policy can be set between 1 and 5 days. Azure Backup service creates a separate resource group to store the instant recovery points of managed virtual machines. The default naming format of resource group created by Azure Backup service is AzureBackupRG\_{Geo}\_{n}. It is optional to customize the name as per customer requirement.

|  |  |
| --- | --- |
| Azure Backup Resource Group (Optional) | |
| Retain instant recovery snapshot(s) | AzureBackupRG\_{Geo}\_{n} - Default one  AzureBackupRG\_canadacentral\_1 |

Following Restoration Policy has been defined upon policy creation and are considered within Cloud Operation Services as standard:

|  |  |
| --- | --- |
| Instant Restore | |
| Retain instant recovery snapshot(s) for | Customer Requirement |

* + 1. Backup & Restoration Testing

There are several options to restore Azure VM data from the recovery points stored in Azure Backup Recovery Services Vaults. Below table presents few scenarios.

|  |  |
| --- | --- |
| Restore Option | Details |
| Create a new VM | Quickly creates and gets a basic VM up and running from a restore point.  You can specify a name for the VM, select the resource group and virtual network (VNet) in which it will be placed, and specify a storage account for the restored VM. The new VM must be created in the same region as the source VM.  If a VM restore fails because an Azure VM SKU wasn't available in the specified region of Azure, or because of any other issues, Azure Backup still restores the disks in the specified resource group. |
| Restore disk | Restores a VM disk, which can then be used to create a new VM.  Azure Backup provides a template to help you customize and create a VM.  The restore job generates a template that you can download and use to specify custom VM settings, and create a VM.  The disks are copied to the Resource Group you specify.  Alternatively, you can attach the disk to an existing VM, or create a new VM using PowerShell.  This option is useful if you want to customize the VM, add configuration settings that weren't there at the time of backup, or add settings that must be configured using the template or PowerShell. |
| Replace existing | You can restore a disk, and use it to replace a disk on the existing VM.  The current VM must exist. If it's been deleted, this option can't be used.  Azure Backup takes a snapshot of the existing VM before replacing the disk, and stores it in the staging location you specify. Existing disks connected to the VM are replaced with the selected restore point.  The snapshot is copied to the vault, and retained in accordance with the retention policy.  After the replace disk operation, the original disk is retained in the resource group. You can choose to manually delete the original disks if they aren't needed.  Replace existing is supported for unencrypted managed VMs, including VMs created using custom images. It's unsupported for classic VMs, unmanaged VMs, and generalized VMs.  If the restore point has more or less disks than the current VM, then the number of disks in the restore point will only reflect the VM configuration.  Replace existing is also supported for VMs with linked resources, like user-assigned managed-identity or Key Vault. |
| Cross Region (secondary region) | Cross Region restore can be used to restore Azure VMs in the secondary region, which is an Azure paired region.  You can restore all the Azure VMs for the selected recovery point if the backup is done in the secondary region.  During the backup, snapshots aren't replicated to the secondary region. Only the data stored in the vault is replicated. So secondary region restores are only vault tier restores. The restore time for the secondary region will be almost the same as the vault tier restore time for the primary region.  This feature is available for the options below:  Create a VM  Restore Disks  We don't currently support the Replace existing disks option. |

* + 1. Backup Monitoring & Alerting

Backup status is available within Azure Portal in Monitoring section of Recovery Services as well as logged in Azure Log Analytics Workspace.

Azure Alert Rules with custom KQL queries presented below are used to trigger Alerts for: Warning and Critical events from Recovery Service Vault as well as any Backup Job Failures.

Below table presents Backup Alerts and custom Kusto queries which are conditions of each Alert Rule: (for details on how to create Alert Rule please refer to Monitoring section within this document)

|  |  |
| --- | --- |
| Alert rule name | Kusto query |
| Recovery Service Vault – Critical Alert | AddonAzureBackupAlerts  | where AlertSeverity contains "Critical"  | summarize AggregatedValue = count() by AlertUniqueId, bin(TimeGenerated, 10m), AlertRaisedOn, AlertStatus, AlertSeverity, AlertType, Category, BackupItemUniqueId, BackupManagementType |
| Recovery Service Vault - Warning Alert | AddonAzureBackupAlerts  | where AlertSeverity contains "Warning"  | summarize AggregatedValue = count() by AlertUniqueId, bin(TimeGenerated, 10m), AlertRaisedOn,AlertStatus,AlertSeverity,AlertType,Category,BackupItemUniqueId,BackupManagementType |
| Recovery Service Vault - Failed Backup Job | AddonAzureBackupJobs  | where JobOperation=="Backup"  | summarize arg\_max(TimeGenerated,\*) by JobUniqueId  | where JobStatus=="Failed"  | summarize AggregatedValue = count() by BackupItemUniqueId, bin(TimeGenerated, 10m), JobFailureCode, BackupManagementType, ProtectedContainerUniqueId,\_ResourceId |

* + 1. Automatic VM onboarding to Backup solution via Azure Policy

Azure Policy Service is used to automatically enable Backup on Azure VMs based on predefined Tags. Below table presents Tags required on a VM to be automatically onboarded to Backup solution.

|  |  |
| --- | --- |
| Tags assigned to VMs | |
| Tag Key | cos\_customername\_sub\_env\_backup |
| Key Value | {region name} (i.e. canadacentral) |

Following Azure Policy has to be Deployed to customer subscription and assigned on a Subscription level: **Iaas\_Policy\_to\_onboard\_VM\_to\_Backup.json.** Code of the Policy can be found on Cloud Operation Services Repository which is listed in Automation section.

Upon Policy Assignment Azure will create System assigned Managed Identity with **Virtual Machine Contributor** and **Backup Contributor** roles. That Identity is managed by Azure and used only for Backup deployment on new Virtual Machines. That Identity will be automatically deleted along with Policy.

Minimum role requirements for Azure Policy Deployment and Assignment: (due to the fact that Policy assignment require minimum role of Owner on Subscription level we suggest to use custom Role with below permissions instead)

- Contributor without Delete permissions

- Microsoft.Authorization/policySetDefinitions/write

- Microsoft.Authorization/policyAssignments/write

- Microsoft.Authorization/policyDefinitions/\*

- Microsoft.Authorization/\*/read

* + 1. Business Continuity/Disaster Recovery

Disaster Recover is an optional component and is delivered for each customer individually taking into consideration customer environment and requirements. While planning any Business Continuity and Disaster Recovery solution, testing should be considered as one of its key elements and should be embedded into solution.

* 1. Operational Monitoring and Logging with ServiceNow integration

Azure Monitor is Azure native solution for Monitoring and Logging. It uses Log Analytics Workspace as logical storage where log data is collected, stored, retained, and queried. It is used to collect logs from Windows and Linux Virtual Machines.

* + 1. Monitoring Prerequisites
       1. ServiceNow Integration Prerequisites

|  |
| --- |
| Note |
| Before deploying ServiceNow integration please read CCP Proposed Changes to Azure Monitoring document listed in the beginning of this document. Key requirements listed there are cliendID, clientSecret and company name. It is not possible to deploy integration without those details. |

* + - 1. Access requirements

Service Principle or User must have at least below Roles assigned to deploy Monitoring solution. Those can be granted only for deployment purpose and revoked after.

Minimum role requirements for Azure Action Group Creation:

|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure permission required | Scope required |
| Creating a Action Group in the Azure portal | Microsoft.Resources/deployments/\*  Monitoring Contributor | These permissions need to be granted at resource group or subscription level |

Minimum role requirements for Azure Function App Creation:

|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure permission required | Scope required |
| Creating a Azure Function App in the Azure portal | Microsoft.Resources/deployments/\* | These permissions need to be granted at resource group or subscription level |
| Creating storage account to store splunk integration function | Storage Account Contributor | COS Dedicated Storage Account |
| Reading the function from the blob uploaded in storage account | Storage Blob Data Reader | COS Dedicated Storage Account |
| Reading Keys stored within KeyVault | Key Vault Administrator | COS dedicated KeyVault |

Minimum role requirements for Azure Key Vault Creation:

|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure permission required | Scope required |
| Creating a Azure KeyVault in the Azure portal | Microsoft.Resources/deployments/\*  Key Vault Contributor | These permissions need to be granted at resource group or subscription level and COS dedicated KeyVault |
| Reading Keys stored within KeyVault | Key Vault Administrator | COS dedicated KeyVault |

Minimum role requirements for Azure Alert Rule Creation:

|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure permission required | Scope required |
| Creating Azure Alert Rule in the Azure portal | Microsoft.Resources/deployments/\*  Monitoring Contributor  Log Analytics Reader | These permissions need to be granted at resource group or subscription level |

Minimum role requirements for Log Analytics Creation and setup:

|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure permission required | Scope required |
| Create new deployment | Microsoft.Resources/deployments/\* | Subscription |
| Create new resource group | Microsoft.Resources/subscriptions/resourceGroups/write | Subscription |
| Create new Data Collection Rule | Microsoft.Insights/dataCollectionRules/\* | Data Collection Rule |
| Associate Data collection Rules | Microsoft.Insights/dataCollectionRuleAssociations/\* | Data Collection Rule |
| AutomationOnboarding blade - Create new workspace | Microsoft.OperationalInsights/workspaces/write | Resource group |
| AutomationOnboarding blade - read solution | Microsoft.OperationalInsights/workspaces/intelligencepacks/read | Solution |
| AutomationOnboarding blade - read workspace | Microsoft.OperationalInsights/workspaces/intelligencepacks/read | Workspace |
| Create link for workspace and Account | Microsoft.OperationalInsights/workspaces/write | Workspace |
| Create/edit saved search | Microsoft.OperationalInsights/workspaces/write | Workspace |
| Create/edit scope config | Microsoft.OperationalInsights/workspaces/write | Workspace |
| Register the Log Analytics provider | Microsoft.Insights/register/action | Subscription |
| VMOnboarding blade - Create MMA extension | Microsoft.Compute/virtualMachines/write | Virtual Machine |
| Create / edit saved search | Microsoft.OperationalInsights/workspaces/write | Workspace |
| Create / edit scope config | Microsoft.OperationalInsights/workspaces/write | Workspace |
| Creating a Action Group in the Azure portal | Microsoft.Resources/deployments/\*  Monitoring Contributor | These permissions need to be granted at resource group or subscription level |

Minimum role requirements for Azure Policy Deployment and Assignment: (since Policy assignment require Owner built-in role on Subscription level we suggest using more limited, custom Role with below permissions instead):

|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure permission required | Scope required |
| Azure Policy Deployment and Assignment | Contributor without Delete permissions  Microsoft.Authorization/policySetDefinitions/write  Microsoft.Authorization/policyAssignments/write  Microsoft.Authorization/policyDefinitions/\*  Microsoft.Authorization/\*/read | These permissions need to be granted at resource group or subscription level |

* + 1. Monitoring – One Time Setup

|  |
| --- |
| Note |
| Cloud Operation Services requires Log Analytics Workspace to be deployed in each region within customer Tenant.  If Customer has multiple subscriptions in one region within the same Tenant, it is possible to deploy only one Log Analytics Workspace for monitoring solution and Update Management.  Deploying Log Analytics Workspace into multiple subscriptions located in the same region is also possible, however it requires more effort during deployment phase and is harder to manage in the future. Although there might be scenarios where such setup is preferred, for example if customer would like to keep logs and metrics from Production systems separate from Development and Test ones. |

Once deployed COS Monitoring Solution enables following features for Azure Virtual Machines:

* VM Monitoring
* VM Inventory
* VM Logging
* Alert delivery to ServiceNow
* Automatic VM onboarding to monitoring solution
* Change Tracking and File Integrity Monitoring

During COS Monitoring solution following resources will be deployed to customer’s Azure Subscription:

* Log Analytics Workspace + Data Collection Rule + VM insights
* Azure Function App and KeyVault and Storage Account+ Action Group for ServiceNow integration
* Azure Policies to onboard VMs to monitoring based on Tags
* Alert Rules

To deploy whole monitoring, logging, and alerting solution following steps must be followed:

1. Deployment of Log Analytics Workspace and Data Collection Rule
2. Deployment of Alert Rules
3. Deployment of ServiceNow integration
4. Deployment of Azure Policies

All four steps have been automated with Terraform.

* + - 1. Alert Rule Creation

Alerts in Azure Monitor are using data collected in Log Analytics Workspace by VM insights.

VM insights relies on the following components to deliver its experience:

• A Log Analytics workspace, which stores monitoring data from VMs and other sources.

• A collection of performance counters configured in the workspace. The collection updates the monitoring configuration on all VMs connected to the workspace.

• VMInsights, which is a monitoring solution configured in the workspace. This solution updates the monitoring configuration on all VMs connected to the workspace.

• AzureMonitoringAgent and GuestAgent, which are Azure VM extensions. These extensions collect and send data to the workspace.

Alert Rules can be created from Azure Portal manually or with Terraform. To avoid any misconfiguration, it is highly recommended to use Terraform located within Cloud Operation Services Repository.

Below Tables presents Alert Rules which must be deployed during initial setup of Cloud Operation Services Monitoring Solution:

|  |  |
| --- | --- |
| Alert rule name | All Disks Free space |
| Alert Scope | Log Analytics Workspace |
| Alert Condition | Search query:  InsightsMetrics  | where Origin == "vm.azm.ms"  | where Namespace == "LogicalDisk" and Name == "FreeSpacePercentage"  | extend Disk=tostring(todynamic(Tags)["vm.azm.ms/mountId"])  | summarize AggregatedValue = avg(Val) by bin(TimeGenerated, 5m), Computer, \_ResourceId, Disk  Alert Logic:   |  |  |  | | --- | --- | --- | | Based on | Operator | Threshold Value | | Metric measurement | Less than | 10 |   Trigger Alert Based On:   |  |  |  | | --- | --- | --- | | Total breaches | Greater than | 0 |   Aggregate on:   |  | | --- | | Computer |   Evaluated based on:   |  |  | | --- | --- | | Period (in minutes) | Frequency (in minutes) | | 5 | 5 | |
| Action group | Notification:   * Email Azure Resource Manager Role * Email/SMS message/Push/Voice   Actions:   * Automation Runbook * Azure Function * ITSM * Function App * Secure Webhook * Webhook |
| Rules details | Description: All Disks Free space less than 10%  Save alert rule to resource group: *resource group name*  Severity:  0 - Critical  1 – Error  2 - Warning  3 - Informational  **4 – Verbose – default setup** |
| Suppress alerts | Suppress alerts (in minutes) |

|  |  |
| --- | --- |
| Alert rule name | Available Memory in percentage |
| Alert Scope | Log Analytics Workspace |
| Alert Condition | Search query:  InsightsMetrics  | where Origin == "vm.azm.ms"  | where Namespace == "Memory" and Name == "AvailableMB"  | extend TotalMemory = toreal(todynamic(Tags)["vm.azm.ms/memorySizeMB"])  | extend AvailableMemoryPercentage = (toreal(Val) / TotalMemory) \* 100.0  | summarize AggregatedValue = avg(AvailableMemoryPercentage) by bin(TimeGenerated, 5m), Computer, \_ResourceId  Alert Logic:   |  |  |  | | --- | --- | --- | | Based on | Operator | Threshold Value | | Metric measurement | Greater than | 95 |   Trigger Alert Based On:   |  |  |  | | --- | --- | --- | | Total breaches | Greater than | 6 |   Aggregate on:   |  | | --- | | Computer |   Evaluated based on:   |  |  | | --- | --- | | Period (in minutes) | Frequency (in minutes) | | 5 | 5 | |
| Action group | Notification:   * Email Azure Resource Manager Role * Email/SMS message/Push/Voice   Actions:   * Automation Runbook * Azure Function * ITSM * Function App * Secure Webhook * Webhook |
| Rules details | Description: Available Memory in percentage greater than 95%  Save alert rule to resource group: *resource group name*  Severity:  0 - Critical  1 – Error  2 - Warning  3 - Informational  **4 – Verbose – default setup** |
| Suppress alerts | Suppress alerts (in minutes) |

|  |  |
| --- | --- |
| Alert rule name | CPU alert per resource |
| Alert Scope | Log Analytics Workspace |
| Alert Condition | Search query:  InsightsMetrics  | where Origin == "vm.azm.ms"  | where Namespace == "Processor" and Name == "UtilizationPercentage"  | summarize AggregatedValue = avg(Val) by bin(TimeGenerated, 15m), Computer, \_ResourceId  Alert Logic:   |  |  |  | | --- | --- | --- | | Based on | Operator | Threshold Value | | Metric measurement | Greater than | 95 |   Trigger Alert Based On:   |  |  |  | | --- | --- | --- | | Total breaches | Greater than | 6 |   Aggregate on:   |  | | --- | | Computer |   Evaluated based on:   |  |  | | --- | --- | | Period (in minutes) | Frequency (in minutes) | | 5 | 5 | |
| Action group | Notification:   * Email Azure Resource Manager Role * Email/SMS message/Push/Voice   Actions:   * Automation Runbook * Azure Function * ITSM * Logic App * Secure Webhook * Webhook |
| Rules details | Description: CPU utilization greater than 95%  Save alert rule to resource group: *resource group name*  Severity:  0 - Critical  1 – Error  2 - Warning  3 - Informational  **4 – Verbose – default setup** |
| Suppress alerts | Suppress alerts (in minutes) |

|  |  |
| --- | --- |
| Alert rule name | Heartbeat – VM not responding |
| Alert Scope | Log Analytics Workspace |
| Alert Condition | Search query:  Heartbeat  | where TimeGenerated > ago(10m)  | summarize LastCall = max(TimeGenerated) by Computer, \_ResourceId  | where LastCall < ago(5m)  Alert Logic:   |  |  |  | | --- | --- | --- | | Based on | Operator | Threshold Value | | Number of results | Greater than | 0 |   Trigger Alert Based On:   |  |  |  | | --- | --- | --- | |  |  |  |   Aggregate on:   |  | | --- | |  |   Evaluated based on:   |  |  | | --- | --- | | Period (in minutes) | Frequency (in minutes) | | 10 | 5 | |
| Action group | Notification:   * Email Azure Resource Manager Role * Email/SMS message/Push/Voice   Actions:   * Automation Runbook * Azure Function * ITSM * Logic App * Secure Webhook * Webhook |
| Rules details | Description: VM not responding  Save alert rule to resource group: *resource group name*  Severity:  0 - Critical  1 – Error  2 - Warning  3 - Informational  **4 – Verbose – default setup** |
| Suppress alerts | Suppress alerts (in minutes) |

|  |  |
| --- | --- |
| Alert rule  name | Syslog service stopped |
|  |  |
| Alert Scope | Log Analytics Workspace |
| Alert Condition | Search query:  ConfigurationChange  | where ConfigChangeType == "Daemons" and SvcName contains "rsyslog" and SvcState == "Running"  Alert Logic:   |  |  |  | | --- | --- | --- | | Based on | Operator | Threshold Value | | Number of results | Greater than | 0 |   Evaluated based on:   |  |  | | --- | --- | | Period (in minutes) | Frequency (in minutes) | | 5 | 5 | |
| Action group | Notification:   * Email Azure Resource Manager Role * Email/SMS message/Push/Voice   Actions:   * Automation Runbook * Azure Function * ITSM * Logic App * Secure Webhook * Webhook |
| Rules details | Description: Syslog service stopped  Save alert rule to resource group: resource group name  Severity:  0 - Critical  1 – Error  2 - Warning  3 - Informational  **4 – Verbose – default setup** |
| Suppress alerts | Suppress alerts (in minutes) |

|  |  |
| --- | --- |
| Alert rule name | SSH service stopped |
| Alert Scope | Log Analytics Workspace |
| Alert Condition | Search query:  ConfigurationChange  | where ConfigChangeType == "Daemons" and SvcName contains "ssh" and SvcState != "Running"  Alert Logic:   |  |  |  | | --- | --- | --- | | Based on | Operator | Threshold Value | | Number of results | Greater than | 0 |   Evaluated based on:   |  |  | | --- | --- | | Period (in minutes) | Frequency (in minutes) | | 5 | 5 | |
| Action group | Notification:   * Email Azure Resource Manager Role * Email/SMS message/Push/Voice   Actions:   * Automation Runbook * Azure Function * ITSM * Logic App * Secure Webhook * Webhook |
| Rules details | Description: SSH service stopped  Save alert rule to resource group: resource group name  Severity:  0 - Critical  1 – Error  2 - Warning  3 - Informational  **4 – Verbose – default setup** |
| Suppress alerts | Suppress alerts (in minutes) |

|  |  |
| --- | --- |
| Alert rule name | Microsoft Azure Linux service stopped |
| Alert Scope | Log Analytics Workspace |
| Alert Condition | Search query:  ConfigurationChange  | where ConfigChangeType == "Daemons" and SvcName contains "walinuxagent" and SvcState == "Running"  Alert Logic:   |  |  |  | | --- | --- | --- | | Based on | Operator | Threshold Value | | Number of results | Greater than | 0 |   Evaluated based on:   |  |  | | --- | --- | | Period (in minutes) | Frequency (in minutes) | | 5 | 5 | |
| Action group | Notification:   * Email Azure Resource Manager Role * Email/SMS message/Push/Voice   Actions:   * Automation Runbook * Azure Function * ITSM * Logic App * Secure Webhook * Webhook |
| Rules details | Description: Microsoft Azure Linux service stopped  Save alert rule to resource group: resource group name  Severity:  0 - Critical  1 – Error  2 - Warning  3 - Informational  **4 – Verbose – default setup** |
| Suppress alerts | Suppress alerts (in minutes) |

|  |  |
| --- | --- |
| Alert rule name | Windows Remote Management WS-Management service stopped |
| Alert Scope | Log Analytics Workspace |
| Alert Condition | Search query:  ConfigurationChange  | where ConfigChangeType == "WindowsServices" and SvcDisplayName == "Windows Remote Management (WS-Management)" and SvcState == "Stopped  Alert Logic:   |  |  |  | | --- | --- | --- | | Based on | Operator | Threshold Value | | Number of results | Greater than | 0 |   Evaluated based on:   |  |  | | --- | --- | | Period (in minutes) | Frequency (in minutes) | | 5 | 5 | |
| Action group | Notification:   * Email Azure Resource Manager Role * Email/SMS message/Push/Voice   Actions:   * Automation Runbook * Azure Function * ITSM * Logic App * Secure Webhook * Webhook |
| Rules details | Description: Windows Remote Management WS-Management service stopped  Save alert rule to resource group: resource group name  Severity:  0 - Critical  1 – Error  2 - Warning  3 - Informational  **4 – Verbose – default setup** |
| Suppress alerts | Suppress alerts (in minutes) |

|  |  |
| --- | --- |
| Alert rule name | Windows Azure Network Agent stopped |
| Alert Scope | Log Analytics Workspace |
| Alert Condition | Search query:  ConfigurationChange  | where ConfigChangeType == "WindowsServices" and SvcDisplayName == "Windows Azure Network Agent" and SvcState == "Stopped  Alert Logic:   |  |  |  | | --- | --- | --- | | Based on | Operator | Threshold Value | | Number of results | Greater than | 0 |   Evaluated based on:   |  |  | | --- | --- | | Period (in minutes) | Frequency (in minutes) | | 5 | 5 | |
| Action group | Notification:   * Email Azure Resource Manager Role * Email/SMS message/Push/Voice   Actions:   * Automation Runbook * Azure Function * ITSM * Logic App * Secure Webhook * Webhook |
| Rules details | Description: Windows Azure Network Agent service stopped  Save alert rule to resource group: resource group name  Severity:  0 - Critical  1 – Error  2 - Warning  3 - Informational  **4 – Verbose – default setup** |
| Suppress alerts | Suppress alerts (in minutes) |

|  |  |
| --- | --- |
| Alert rule name | Windows Azure Guest service stopped |
| Alert Scope | Log Analytics Workspace |
| Alert Condition | Search query:  ConfigurationChange  | where ConfigChangeType == "WindowsServices" and SvcDisplayName == "Windows Azure Guest Agent" and SvcState == "Stopped  Alert Logic:   |  |  |  | | --- | --- | --- | | Based on | Operator | Threshold Value | | Number of results | Greater than | 0 |   Evaluated based on:   |  |  | | --- | --- | | Period (in minutes) | Frequency (in minutes) | | 5 | 5 | |
| Action group | Notification:   * Email Azure Resource Manager Role * Email/SMS message/Push/Voice   Actions:   * Automation Runbook * Azure Function * ITSM * Logic App * Secure Webhook * Webhook |
| Rules details | Description: Windows Azure Guest service stopped  Save alert rule to resource group: resource group name  Severity:  0 - Critical  1 – Error  2 - Warning  3 - Informational  **4 – Verbose – default setup** |
| Suppress alerts | Suppress alerts (in minutes) |

|  |  |
| --- | --- |
| Alert rule name | Microsoft Monitoring Agent Azure VM Extension Heartbeat Service stopped |
| Alert Scope | Log Analytics Workspace |
| Alert Condition | Search query:  ConfigurationChange  | where ConfigChangeType == "WindowsServices" and SvcDisplayName == “Microsoft Monitoring Agent Azure VM Extension Heartbeat Service" and SvcState == "Stopped  Alert Logic:   |  |  |  | | --- | --- | --- | | Based on | Operator | Threshold Value | | Number of results | Greater than | 0 |   Evaluated based on:   |  |  | | --- | --- | | Period (in minutes) | Frequency (in minutes) | | 5 | 5 | |
| Action group | Notification:   * Email Azure Resource Manager Role * Email/SMS message/Push/Voice   Actions:   * Automation Runbook * Azure Function * ITSM * Logic App * Secure Webhook * Webhook |
| Rules details | Description: Microsoft Monitoring Agent Azure VM Extension Heartbeat Service stopped  Save alert rule to resource group: resource group name  Severity:  0 - Critical  1 – Error  2 - Warning  3 - Informational  **4 – Verbose – default setup** |
| Suppress alerts | Suppress alerts (in minutes) |

|  |  |
| --- | --- |
| Alert rule name | Microsoft Monitoring Agent service stopped |
| Alert Scope | Log Analytics Workspace |
| Alert Condition | Search query:  ConfigurationChange  | where ConfigChangeType == "WindowsServices" and SvcDisplayName == "Microsoft Monitoring Agent " and SvcState == "Stopped  Alert Logic:   |  |  |  | | --- | --- | --- | | Based on | Operator | Threshold Value | | Number of results | Greater than | 0 |   Evaluated based on:   |  |  | | --- | --- | | Period (in minutes) | Frequency (in minutes) | | 5 | 5 | |
| Action group | Notification:   * Email Azure Resource Manager Role * Email/SMS message/Push/Voice   Actions:   * Automation Runbook * Azure Function * ITSM * Logic App * Secure Webhook * Webhook |
| Rules details | Description: Microsoft Monitoring Agent service stopped  Save alert rule to resource group: resource group name  Severity:  0 - Critical  1 – Error  2 - Warning  3 - Informational  **4 – Verbose – default setup** |
| Suppress alerts | Suppress alerts (in minutes) |

|  |  |
| --- | --- |
| Alert rule name | Microsoft Dependency Agent service stopped |
| Alert Scope | Log Analytics Workspace |
| Alert Condition | Search query:  ConfigurationChange  | where ConfigChangeType == "WindowsServices" and SvcDisplayName == "Microsoft Dependency Agent " and SvcState == "Stopped  Alert Logic:   |  |  |  | | --- | --- | --- | | Based on | Operator | Threshold Value | | Number of results | Greater than | 0 |   Evaluated based on:   |  |  | | --- | --- | | Period (in minutes) | Frequency (in minutes) | | 5 | 5 | |
| Action group | Notification:   * Email Azure Resource Manager Role * Email/SMS message/Push/Voice   Actions:   * Automation Runbook * Azure Function * ITSM * Logic App * Secure Webhook * Webhook |
| Rules details | Description: Microsoft Dependency Agent service stopped  Save alert rule to resource group: resource group name  Severity:  0 - Critical  1 – Error  2 - Warning  3 - Informational  **4 – Verbose – default setup** |
| Suppress alerts | Suppress alerts (in minutes) |

* + - 1. Log Analytics Workspace + Automation Account creation (DCR)

Log Analytics Workspace is the core component of Monitoring, Patching, Logging and Reporting solutions. Taking that into consideration it must be deployed using Terraform. Terraform scripts are located within COS Monitoring Repository.

Preferred way of deployment is via a terraform vm. It also enables logging of System Logs on Windows Virtual Machines and Syslog on Linux Virtual Machines.

Although automated deployment is preferred way of deploying Monitoring solution it can be done manually too. Please refer to sections 5.5.2.1 and 5.5.2.2 for details on manual deployment.

* + - 1. ServiceNow Integration

|  |
| --- |
| Note |
| Please note that there is new release of ServiceNow Integration planned which will incorporate Splunk into whole solution. Splunk will be integrated between iPaaS and ServiceNow allowing smart Alert correlation. |
| Following ServiceNow integration is for service monitoring only. |
|  |

To send alerts from Azure to ServiceNow following workflow has been developed:

**Azure Alert Rule > Azure Action Group > Azure Function App > iPaaS > ServiceNow**

That is a standard for sending alerts from Azure to ServiceNow within Capgemini. That process has been documented in detail within CCP Proposed Changes to Azure Monitoring document.

Deployment process includes:

* Action Group creation
* App Service Plan creation
* Function App creation
* KeyVault creation

It is advised to deploy the solution using ARM templates available within Cloud Operation Services Repository. Please check the ServiceNow prerequisites mentioned in prerequisites section of Monitoring solution.

* + - 1. Configure VM Onboarding

Onboarding of Virtual Machines is done via Azure Policy. This solution is applicable for greenfield as well as brownfield deployments. Once Policies have been assigned on Subscription level within customer environment, they run every 24hrs or on every updated resource.

Policies are configured to deploy Dependency Agent and Log Analytics Agent on all virtual machines with below tags applied:

|  |  |  |
| --- | --- | --- |
| TAG Key | TAG Value | Use |
| cos\_managed | yes | Indicate which systems are billable by COS.  Used to allow both managed and unmanaged systems within the same environment. |

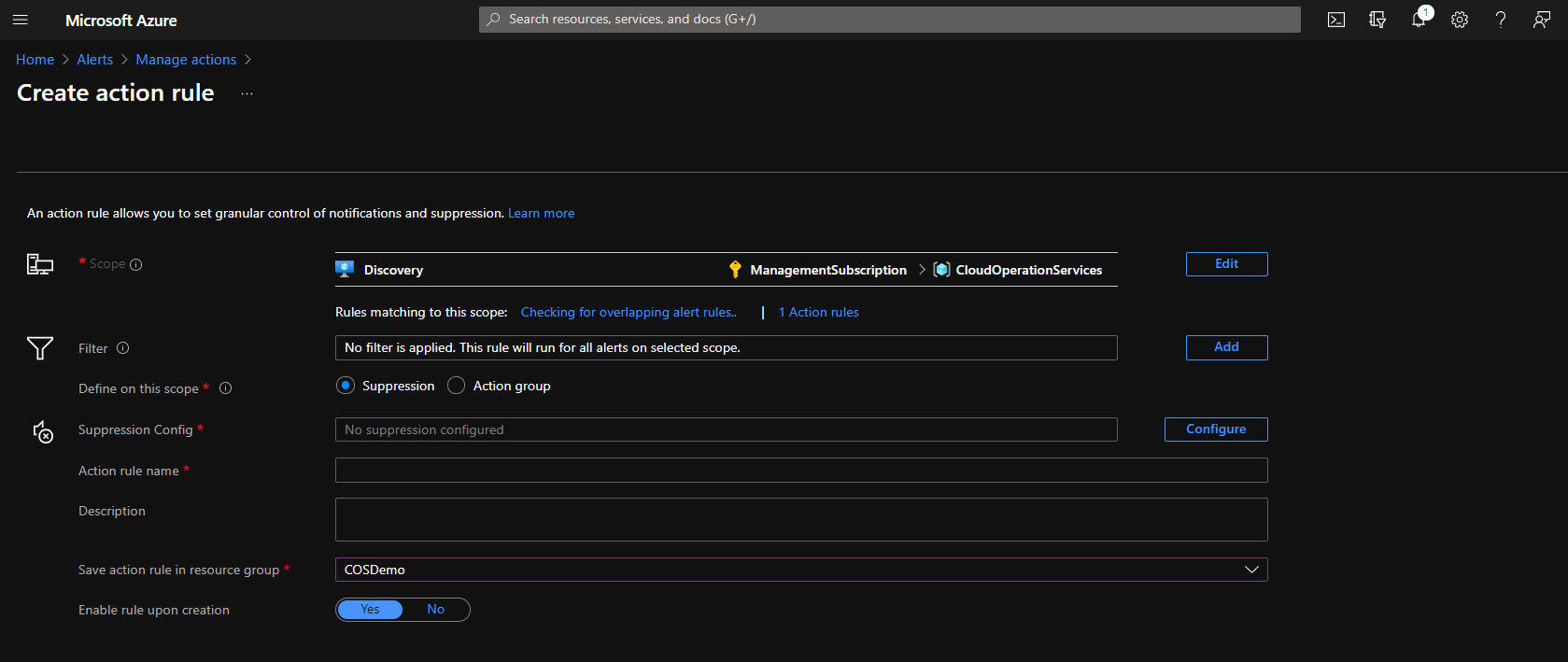
Below policies for agent deployment have been created and uploaded to COS Repository:

|  |  |  |
| --- | --- | --- |
| COS Custom Policy Name | Effect | Managed Identity RBAC |
| COS Dependency agent for Linux virtual machines | deployIfNotExists | Log Analytics Contributor |
| COS Dependency agent for Windows virtual machines | deployIfNotExists | Log Analytics Contributor |
| COS Azure Monitor agent for Linux virtual machines | deployIfNotExists | Log Analytics Contributor |
| COS Azure Monitor agent for Windows virtual machines | deployIfNotExists | Log Analytics Contributor |

* + - 1. Maintenance Mode/Action Rule

To avoid false alerting from Virtual Machines during patching activity, the native Azure maintenance mode functionality – Action Rule can be used.

To create Action Rule from portal go to Alerts > Manage actions > Create Action Rule

****

* 1. Update Management

Azure Update Management is native Azure solution for patching of Virtual Machines. You can use Update Management in Azure Automation to manage operating system updates for your Windows and Linux virtual machines in Azure, in on-premises environments, and in other cloud environments. You can quickly assess the status of available updates on all agent machines and manage the process of installing required updates for servers.

|  |
| --- |
| Note |
| Update Management does not offer any patch rollback option. You should have a separate rollback plan for critical servers, such as restoring from latest Azure Backup. |
| By default, updates are downloaded from Internet. However, you can also configure local update repository if outbound Internet is blocked for client machines |
| Update management is dependant on Log Analytics Agent and Dependency Agent installed on Windows VMs and OMS Agent and Dependency Agent installed on Linux VMs. Both Agents can be easily deployed to Virtual Machines using Azure Policy which can be found within COS Repository mentioned in Automation section. Please note that during Policy Deployment/Assignment Log Analytics Workspace ID must be provided. If Monitoring solution has been already deployed, than Workspace ID can be obtained from already deployed Log Analytics. What is more – there is no need to follow below Update Management – One Time Setup if Monitoring solution has been deployed. |

* + 1. Update Management Prerequisites

Before you deploy Update Management solution, make sure that you meet the Network, Firewall and Access requirements.

* + - 1. Network and Firewall

1. To properly report to the service, Update Management requires Virtual Machines to be able to communicate to below URLs over port 443 (the traffic flows via Azure backbone network):

|  |
| --- |
| Azure Public |
| \*.ods.opinsights.azure.com |
| \*.oms.opinsights.azure.com |
| \*.blob.core.windows.net |
| \*.azure-automation.net |

1. For Windows VMs to download updates from Windows Update servers, certain URLs need to be accessible from source VMs. So below URLs need to be whitelisted in Firewall. It would be wise to revisit below list of URLs in future and check whether non https URLs are still needed.

|  |
| --- |
| Windows Updates |
| http://windowsupdate.microsoft.com |
| http://\*.windowsupdate.microsoft.com |
| https://\*.windowsupdate.microsoft.com |
| http://\*.update.microsoft.com |
| https://\*.update.microsoft.com |
| http://\*.windowsupdate.com |
| http://download.windowsupdate.com |
| https://download.microsoft.com |
| http://\*.download.windowsupdate.com |
| http://wustat.windows.com |
| http://ntservicepack.microsoft.com |

1. For Red Hat Linux, below IP addresses need to be whitelisted so that Linux VMs can download updates from Red Hat Update Infrastructure (RHUI)

|  |
| --- |
| Red Hat Linux Updates |
| 13.91.47.76 |
| 40.85.190.91 |
| 52.187.75.218 |
| 52.174.163.213 |
| 52.237.203.198 |

* + - 1. Update Source

In case you are planning to use local patch repository for Windows and Linux VMs instead of Internet repository, your network and firewall planning will be changed significantly.

For example, you might want to use WSUS as the local patch repository for your Windows Servers. In that case, all Windows Servers need to approach the WSUS servers to download updates and patches, rather than downloading from Internet. As a result, many of the network and firewall requirements which we have mentioned in the previous sections would need to be re-considered.

* + - 1. Workspace Mapping

Update Management requires following Azure Services to work:

* Azure Log Analytics Workspace
* Azure Automation Account.

At the time of writing this document Automation Account and Log Analytics Workspace can be linked together only according to bellow region mapping table:

|  |  |
| --- | --- |
| Log Analytics workspace region | Azure Automation region |
| US |  |
| EastUS1 | EastUS2 |
| EastUS22 | EastUS |
| WestUS | WestUS |
| WestUS2 | WestUS2 |
| CentralUS | CentralUS |
| SouthCentralUS | SouthCentralUS |
| WestCentralUS | WestCentralUS |
| Canada |  |
| CanadaCentral | CanadaCentral |
| Asia Pacific |  |
| AustraliaEast | AustraliaEast |
| AustraliaSoutheast | AustraliaSoutheast |
| EastAsia | EastAsia |
| SoutheastAsia | SoutheastAsia |
| CentralIndia | CentralIndia |
| ChinaEast23 | ChinaEast2 |
| JapanEast | JapanEast |
| Europe |  |
| NorthEurope | NorthEurope |
| FranceCentral | FranceCentral |
| UKSouth | UKSouth |
| WestEurope | WestEurope |
| SwitzerlandNorth | SwitzerlandNorth |

* + - 1. Access Requirements

Service Principle or User must have at least below Roles assigned to deploy Update Management solution. Those can be granted only for deployment purpose and revoked after.

Minimum role requirements needed for deployment of the Update Management solution:

|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure permission required | Scope required |
| Create new deployment | Microsoft.Resources/deployments/\* | Subscription |
| Create new resource group | Microsoft.Resources/subscriptions/resourceGroups/write | Subscription |
| AutomationOnboarding blade - Create new workspace | Microsoft.OperationalInsights/workspaces/write | Resource group |
| AutomationOnboarding blade - read linked workspace | Microsoft.Automation/automationAccounts/read | Automation account |
| AutomationOnboarding blade - read solution | Microsoft.OperationalInsights/workspaces/intelligencepacks/read | Solution |
| AutomationOnboarding blade - read workspace | Microsoft.OperationalInsights/workspaces/intelligencepacks/read | Workspace |
| Create link for workspace and Account | Microsoft.OperationalInsights/workspaces/write | Workspace |
| Write account for shoebox | Microsoft.Automation/automationAccounts/write | Account |
| Create/edit saved search | Microsoft.OperationalInsights/workspaces/write | Workspace |
| Create/edit scope config | Microsoft.OperationalInsights/workspaces/write | Workspace |
| Register the Log Analytics provider | Microsoft.Insights/register/action | Subscription |
| VMOnboarding blade - Create MMA extension | Microsoft.Compute/virtualMachines/write | Virtual Machine |
| Create / edit saved search | Microsoft.OperationalInsights/workspaces/write | Workspace |
| Create / edit scope config | Microsoft.OperationalInsights/workspaces/write | Workspace |
|  |  |  |

* + 1. Update Management – One Time Setup

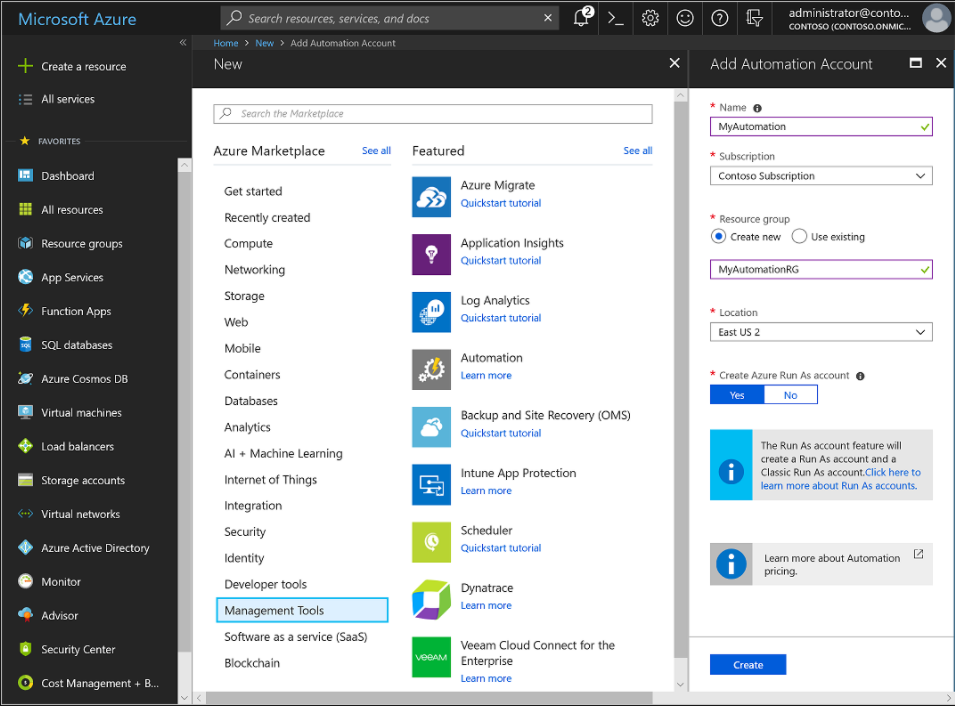
|  |
| --- |
| Note |
| Cloud Operation Services requires Log Analytics Workspace to be deployed in each region within customer Tenant. If customer has both: Update Management Solution and Monitoring Solution deployed within the same region, only one Log Analytics must be deployed. |

During automated deployment process of Update Management Log Analytics Workspace and Automation Account are deployed and linked together. ARM templates for Update Management Solution deployment can be found on COS Repository, please see Automation section within this document for more details. Automated deployment is the quickest and preferred method of deployment.

Deployment can be also performed from Azure Portal, please follow below manual steps:

* + - 1. Create Automation Account

1. Choose a name for your Azure account. Automation account names are unique per region and resource group. Names for Automation accounts that have been deleted might not be immediately available.
2. Click the Create a resource button found in the upper left corner of Azure portal.
3. Select IT & Management Tools, and then select Automation.
4. Enter the account information, including the selected account name. For Create Azure Run As account, choose Yes so that the artifacts to simplify authentication to Azure are enabled automatically. When the information is complete, click Create to start the Automation account deployment.

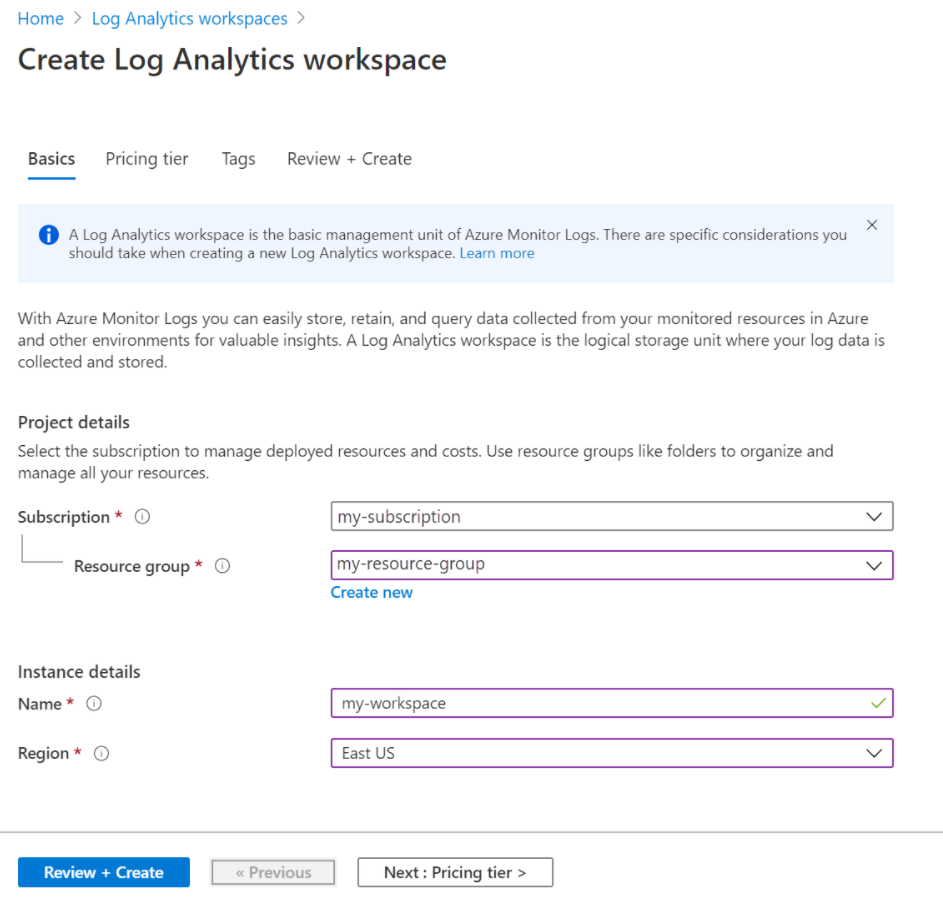


* + - 1. Create Log Analytics Workspace

|  |
| --- |
| Note |
| Make sure you are creating the Log Analytics Workspace in the correct region, so that you can link it to the Automation Account which you have created in previous step. |

1. In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.
2. Click Add, and then provide values for the following options:

* Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate.
* For Resource Group, choose to use an existing resource group already setup or create a new one.
* Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. This name must be unique per resource group.
* Select an available Region. For more information, see which regions Log Analytics is available in and search for Azure Monitor from the Search for a product field.
* Select appropriate Pricing Tier. If there are no specific requirements from customer, you can stick to Pay-as-you go Tier



Once you create the workspace, you can note down the workspace ID and workspace Key. You will get this information in the Advanced Settings > Connected Source section of Log Analytics Workspace. You will need this information in future, especially if you onboard VMs through Azure Policy.

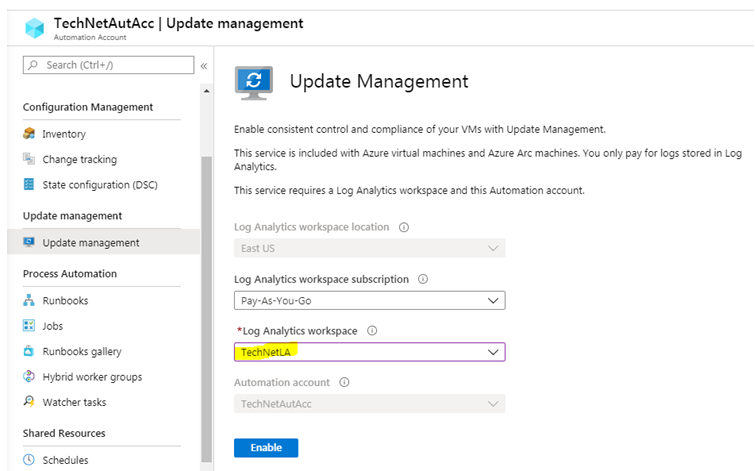
* + - 1. Enable Update Management Solution

NOTE: While deploying solution with Azure DevOps, Devops Pipeline covers enablement of Update Management and no manual steps are required.

To use the Update management solution for the first time, you need to enable the solution from Azure Portal.

While enabling the solution, you will get the option of selecting Log Analytics Workspace. Make sure you select the correct Log Analytics Workspace, which you have planned to use with this Automation Account.

Once you are done, just click Enable, and update management solution will be enabled.



Once you enable Update Management, the Automation Account and The Log Analytics Workspace will be linked with each other. You can validate it with Linked Workspace section under Automation Account.

In case you have created the Log Analytics Workspace but it is not showing here in the drop down menu, you have probably created in the wrong region which does not support linking. You can refer to the Workspace Mapping table which we have discussed earlier.

* + - 1. Configure VM Onboarding

Onboarding process consists of two steps:

* Agent Deployment on VMs
* Update Management auto-enablement for VMs reporting to defined Log Analytics Workspace

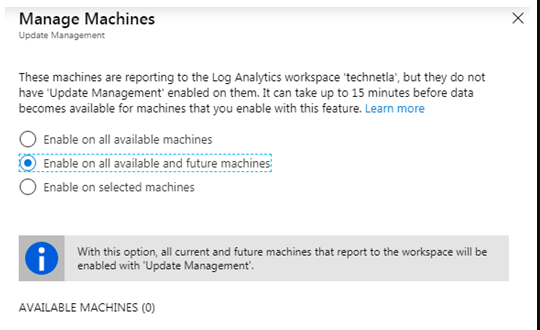
First step is done with Azure Policies, once Policies are deployed and assigned to Subscription and VMs have specific TAG added than VMs will have all necessary agents pointing to correct workspace installed.

Below policies for agent deployment have been created and uploaded to COS Repository:

|  |  |  |
| --- | --- | --- |
| COS Custom Policy Name | Effect | Managed Identity RBAC |
| COS Dependency agent for Linux virtual machines | deployIfNotExists | Log Analytics Contributor |
| COS Dependency agent for Windows virtual machines | deployIfNotExists | Log Analytics Contributor |
| COS Log Analytics agent for Linux virtual machines | deployIfNotExists | Log Analytics Contributor |
| COS Log Analytics agent for Windows virtual machines | deployIfNotExists | Log Analytics Contributor |

Second step requires enablement of automatic onboarding solution within Update Management for all available and future VMs. Please remember that this is a one-time setup. Once changed, this option will be greyed out and will no longer be available to change.

You will get this option in the Manage Machines section within Update Management console.



* + 1. Update Management - Create Deployment Schedule

Deployment Schedule is a key component of the Update Management Solution. An effective patch management solution depends on the effective deployment schedule strategy.

Usually, customers define the patching schedule of their Virtual Machines, and such activity is also supported by change request and customer approval. Once patching schedule is defined below steps should be executed to create deployment schedule:

Using Deployment schedule, you can define following parameters :

* When a group of VMs machines will be patched.
* Which machines will be patched (Static / Dynamic machine grouping).
* What Operating System Will be patched (Windows or Linux but not both).
* What type of updates will be deployed (Ex: Critical, Security etc).
* Whether any update need to be excluded.
* System reboot option after update installation depending on tags.
* Maintenance Window (Minimum is 90 minutes, We can adjust the window as per the requirement from the client). And Schedule settings can be tweaked as per the customer’s requirements.

Within COS following patching schedule has been defined as standard:

|  |  |  |
| --- | --- | --- |
|  | Windows | Linux |
| Items to Update | Target Group based on Tags | Target Group based on Tags |
| Update Classification | Security and Critical | Security and Critical |
| Exclude updates | Option (not set) | Option (not set) |
| Schedule Settings | As per the customer requirement | As per the customer requirement |
| Maintenance Window | 90 minutes | 90 minutes |
| Reboot option | Depending on dependency type selected | Depending on dependency type selected |

For machine grouping, we recommend to use Dynamic Grouping approach. In this approach, you will not statically attach any VM to any deployment schedule, rather you will define some criteria in the deployment schedule. Within COS solution we have defined Tags which can be utilized for Dynamic Grouping.

Once you define the criteria and save it, Azure will create a query. During the deployment, it will run that query and will apply the patches to those machines which are generated by the query result.

Dynamic Grouping supports few additional criteria in addition to TAGs:

• Subscription(s)

• Resource Group(s)

• Location(s)

The above points will be covering in coming points.

* + - 1. Access Requirements

Service Principle or User must have at least below Roles assigned to deploy Update Management solution. Those can be granted only for deployment purpose and revoked after.

Minimum role requirements needed for deployment of the Update Management solution:

|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure permission required | Scope required |
| Deploying Maintenance Configuration | **Contributor Role** | Subscription |
| Deploying Policies | **Resource Policy Contributor Role** | Subscription |
| Assigning policies | **Managed Identity Operator** | Subscription |

**Prerequisites for VM Patching**

**VM Configuration Requirements**

To ensure proper VM patching, all provisioned virtual machines must have the following options enabled:

patch\_assessment\_mode = "AutomaticByPlatform"

patch\_mode = "AutomaticByPlatform"

bypass\_platform\_safety\_checks\_on\_user\_schedule\_enabled = "AutomaticByPlatform"

provision\_vm\_agent = "AutomaticByPlatform"

If any of these configurations are missing, tagging functionality may not work as expected. Having these settings in place ensures that Patch Orchestration falls under **Customer Managed Schedule**, with periodic assessments enabled. If any of the above settings are missing, you must run the patch\_config module from GitHub that will update the Virtual Machine to switch its Patch Orchestration from **Image Default or Azure** to **Customer Managed**.

**Viewing Pending Updates**

Once these configurations are applied, you can view pending updates in the **Update Status** section. If any of the required parameters are missing, the update status will appear **grayed out**, indicating that no updates are available. In such cases, you need to run patch\_config to correct the settings.

A screenshot of a computer

AI-generated content may be incorrect.

Second Option: You can do it manually by following below steps:

Manual Steps : you need to click on VM from update management portal, then update settings. Choose Customer Managed Schedule and save.

A screenshot of a computer

AI-generated content may be incorrect.

**VM Tagging Requirements**

It is essential to tag the respective VMs based on their dependency type. The following four tags are available for patching, depending on client requirements:

|  |  |  |  |
| --- | --- | --- | --- |
| |  | | --- | | **Tag Name** | | |  | | --- | |  |   **Description** |
| **prod\_dependency\_server** | Enables **"Never Reboot"** option for production servers while patching. |
| **prod\_non\_dependency\_server** | Enables **"Always Reboot"** option for production servers while patching. |
| **nonprod\_dependency\_server** | |  |  | | --- | --- | |  | Enables **"Never Reboot"** option for non-production servers while patching. | |
| **nonprod\_non\_dependency\_server** | Enables **"Always Reboot"** option for non-production servers while patching. |

Within COS following patching schedule has been defined as standard:

**Tag Auto-Generation Logic**

When selecting tags, you must choose **two tags**: one for the **environment** and one for its **dependency type**. Based on these selections, a **third tag** will be automatically generated, combining the first two. The logic for this is defined in the **Azure Policy** named **"enforce-prod-non-dependency-tag"** and their dependencies respectively.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

This automatically generated tag is then attached to the respective **Maintenance Configuration Name**.

**Dynamic Scope Validation**

Once the VMs are tagged correctly, follow these steps to validate the **dynamic scope** under the respective **Maintenance Configuration**:

1. Navigate to the **Maintenance Configuration** section.
2. Verify that all necessary attributes such as **Subscription ID, Resource Group, and associated Tags** are automatically generated via Terraform code.
3. Click **OK** to confirm the selection.
4. Ensure that all VMs with the same tag are correctly listed.
5. Click **Save** to finalize the configuration.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

By following these steps, you ensure seamless patching with automated orchestration, reducing manual overhead and potential misconfigurations.

* 1. Security

Design, implementation, configuration, and support of all security features within Cloud Operation Services is delivered by Cyber Security Team. This chapter lists Security features used within Cyber Security solution. Detailed solution guidance and service description can be found within below documents:

[CWPP Azure Solution Document 1.0 - 02112021](https://g-port.capgemini.com/file/40144?fileName=CybersecurityDefendServices_CloudSecurityServiceOffering_Explain_SolutionDeepDiveWorkshopKit_CwppAzureSolutionDocument10-02112021_03052021)

[CWPP Azure Service Description 1.0 - 02112021](https://g-port.capgemini.com/file/40143?fileName=CybersecurityDefendServices_CloudSecurityServiceOffering_Explain_SolutionDeepDiveWorkshopKit_CwppAzureServiceDescription10-02112021_03052021)

[CSPM Azure Solution Document 1.0 - 02172021](https://g-port.capgemini.com/file/40142?fileName=CybersecurityDefendServices_CloudSecurityServiceOffering_Explain_SolutionDeepDiveWorkshopKit_CspmAzureSolutionDocument10-02172021_03052021)

[CSPM Azure Service Description 1.0 - 02172021](https://g-port.capgemini.com/file/40141?fileName=CybersecurityDefendServices_CloudSecurityServiceOffering_Explain_SolutionDeepDiveWorkshopKit_CspmAzureServiceDescription10-02172021_03052021)

Remediation of Vulnerabilities discovered on Virtual Machines by Cyber Security will be handled by COS Run team based on insights received from Cyber Security team.

* + 1. Azure Security Center

Azure Security Center strengthen security posture of Azure Infrastructure. This means it helps to identify and perform the hardening tasks recommended as security best practices and implement them across virtual machines, data services, and apps. This includes managing and enforcing security policies, and making sure customer’s Azure virtual machines, and Azure PaaS services are compliant. Security Center provides the tools organization needs to have a bird's eye view on its workloads.

* + - 1. Azure Security Center – Prerequisites

To enable Azure Defender and Security Center features described within COS Security Solution Azure Security Center Standard Tier must be enabled prior to any further configurations.

Network Security Groups must allow following traffic from Virtual Machines:

Ensure the target machines can communicate with Qualys' cloud service by adding the following IPs to your allow lists (via port 443 - the default for HTTPS):

64.39.104.113 - Qualys' US data center

154.59.121.74 - Qualys' European data center

|  |
| --- |
| Note |
| Thanks to partnership between Microsoft and Qualys there is no additional cost involved for Qulays assessment. Qualys comes for free for all VMs with Azure Defender enabled. |

Minimum role-based access control to enable Azure Security Center and Azure Defender:

|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure role required | Scope required |
| Enable Security Center on Azure Subscription | Subscription Contributor or Security Admin | Subscription |
| Enable Azure Defender on Azure Subscription | Subscription Contributor or Security Admin | Subscription |
| Enable Security Center on Azure Subscription | Log Analytics Contributor | Existing Log Analytics Used for Monitoring or Patching |

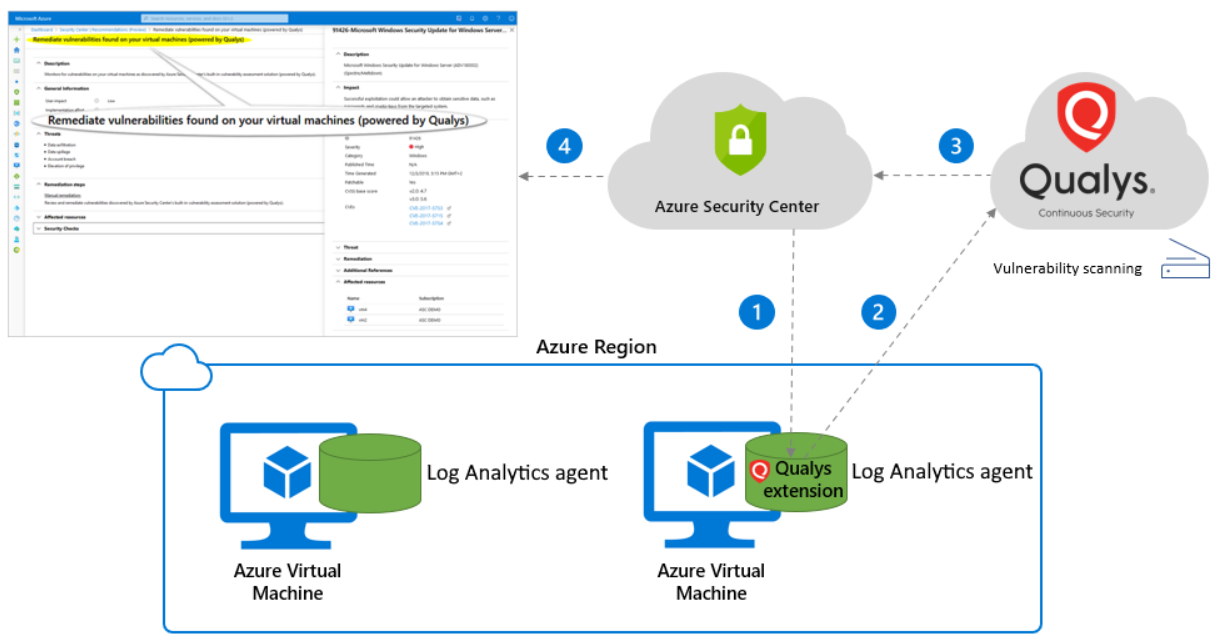
|  |
| --- |
| Note |
| At this point Linux Virtual Machines doesn’t support multihoming, which means each Linux VM can be connected to only one Log Analytics Workspace. Project Team responsible for COS deployment need to work together with Cyber Security team during deployment of Security solutions to agree on which Log Analytics Workspace will be used for Linux Virtual Machines |

* + - 1. Vulnerability Management

The vulnerability scanner included with Azure Security Center is powered by Qualys.

The vulnerability scanner extension works as follows:

1. Deploy - Azure Security Center monitors your machines and provides recommendations to deploy the Qualys extension on your selected machine/s.
2. Gather information - The extension collects artifacts and sends them for analysis in the Qualys cloud service in the defined region.
3. Analyze - Qualys' cloud service conducts the vulnerability assessment and sends its findings to Security Center.
4. Report - The findings are available in Security Center.



* + - 1. Remediate findings from vulnerability assessment solutions on your VMs

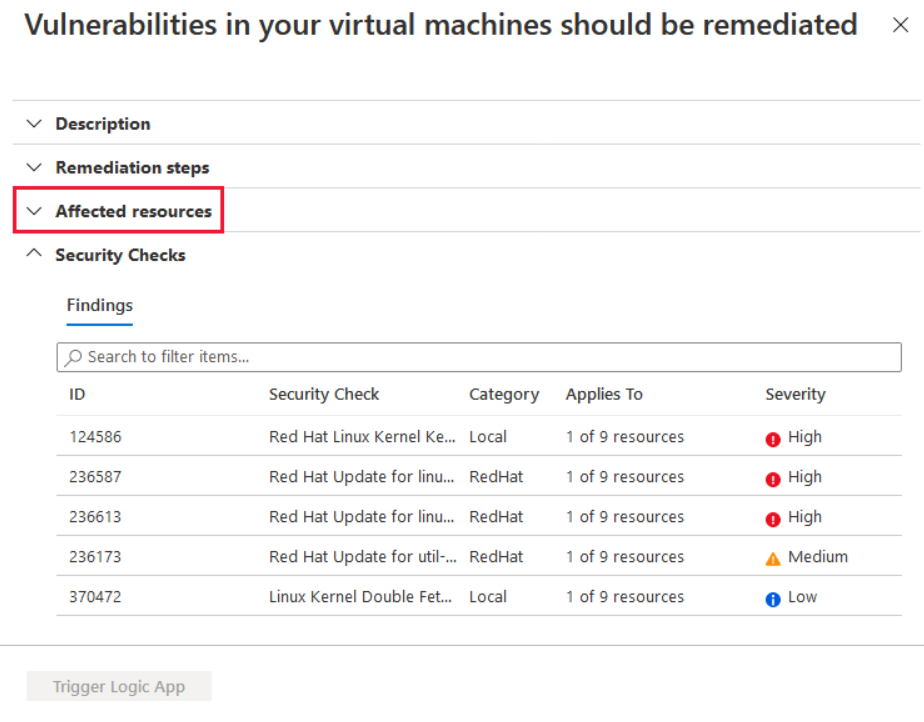
When your vulnerability assessment tool reports vulnerabilities to Security Center, Security Center presents the findings and related information as recommendations. In addition, the findings include related information such as remediation steps, relevant CVEs, CVSS scores, and more. You can view the identified vulnerabilities for one or more subscriptions, or for a specific VM.

Based on above information from Security Center and feedback from CyberSecurity Team Run COS Team will remediate vulnerabilities found on customer workloads.

To view vulnerability assessment findings (from all of your configured scanners) and remediate identified vulnerabilities:

1. Open Azure Security Center and go to the Recommendations page.
2. Select the recommendation Vulnerabilities in your virtual machines should be remediated.

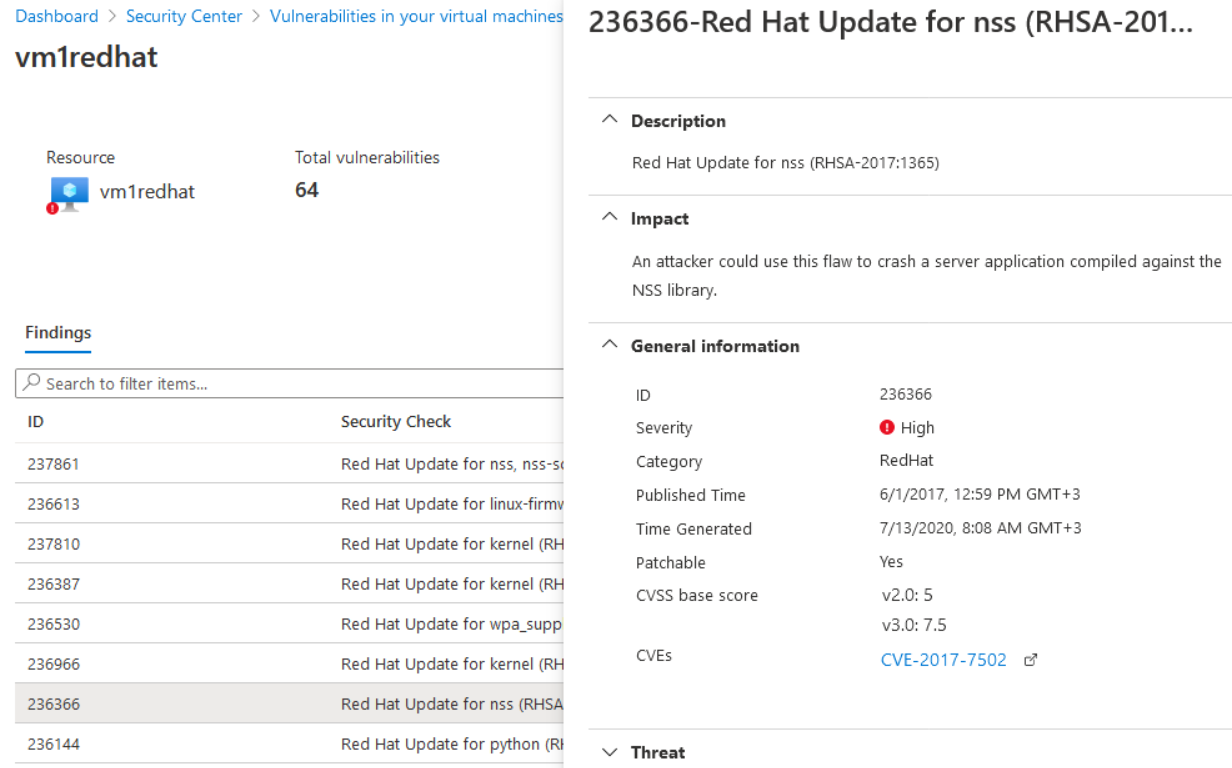
Security Center shows you all the findings for all VMs in the currently selected subscriptions. The findings are ordered by severity.



1. To filter the findings by a specific VM, open the "Affected resources" section and click the VM that interests you. Or you can select a VM from the resource health view, and view all relevant recommendations for that resource.

Security Center shows the findings for that VM, ordered by severity.

4. To learn more about a specific vulnerability, select it.



The details pane that appears contains extensive information about the vulnerability, including:

* Links to all relevant CVEs (where available)
* Remediation steps
* Any additional reference pages

5. To remediate a finding, follow the remediation steps from this details pane. Please note any remediation must be agreed with customer and conducted based on change order request.

* + - 1. Identity & Access Management (IDAM)

* + - * 1. Without Management Tenant. Customer managed Azure Active Directory

Management of customer’s Azure Active Directory is not in scope of Cloud Operation Services, but it is mandatory to setup features like conditional access and MFA on customer’s Azure Active Directory for scenarios where SAM is not implemented.

Conditional Access, feature of Azure Active Directory can limit logging to customer’s Azure Portal only to IP addresses from Capgemini’s networks. MFA is additional level of authentication.

* + - 1. Advanced Persistent Threat (APT) Detection

Please refer to below Cyber Security documentation for more details:

[CWPP Azure Solution Document 1.0 - 02112021](https://g-port.capgemini.com/file/40144?fileName=CybersecurityDefendServices_CloudSecurityServiceOffering_Explain_SolutionDeepDiveWorkshopKit_CwppAzureSolutionDocument10-02112021_03052021)

[CWPP Azure Service Description 1.0 - 02112021](https://g-port.capgemini.com/file/40143?fileName=CybersecurityDefendServices_CloudSecurityServiceOffering_Explain_SolutionDeepDiveWorkshopKit_CwppAzureServiceDescription10-02112021_03052021)

[CSPM Azure Solution Document 1.0 - 02172021](https://g-port.capgemini.com/file/40142?fileName=CybersecurityDefendServices_CloudSecurityServiceOffering_Explain_SolutionDeepDiveWorkshopKit_CspmAzureSolutionDocument10-02172021_03052021)

[CSPM Azure Service Description 1.0 - 02172021](https://g-port.capgemini.com/file/40141?fileName=CybersecurityDefendServices_CloudSecurityServiceOffering_Explain_SolutionDeepDiveWorkshopKit_CspmAzureServiceDescription10-02172021_03052021)

* + - 1. Antivirus (AV)

Microsoft Antimalware for Azure is a real-time protection that helps identify and remove viruses, spyware, and other malicious software. It generates alerts when known malicious or unwanted software tries to install itself or run on your Azure systems.

Enablement of Antimalware is delivered by Cyber Security Team via Azure Policy assigned to Subscription level during Security Center Standard Tier enablement.

* + - 1. Encryption – At Rest

Azure Managed Disks are encrypted at rest by default using Azure Storage Service

Encryption where the encryption keys are Microsoft managed keys in Azure.

Customer managed keys can be used as an option.

* + - 1. Encryption – In Transit
         1. Data-link Layer encryption in Azure

Whenever Azure Customer traffic moves between datacenters-- outside physical boundaries not controlled by Microsoft (or on behalf of Microsoft) -- a data-link layer encryption method using the IEEE 802.1AE MAC Security Standards (also known as MACsec) is applied from point-to-point across the underlying network hardware. The packets are encrypted and decrypted on the devices before being sent, preventing physical “man-in-the-middle” or snooping/wiretapping attacks. Because this technology is integrated on the network hardware itself, it provides line rate encryption on the network hardware with no measurable link latency increase. This MACsec encryption is on by default for all Azure traffic traveling within a region or between regions, and no action is required on customers’ part to enable.

* + - * 1. TLS encryption in Azure

Microsoft gives customers the ability to use Transport Layer Security (TLS 1.2) protocol to protect data when it’s traveling between the cloud services and customers. Microsoft datacenters negotiate a TLS connection with client systems that connect to Azure services. TLS 1.2 provides strong authentication, message privacy, and integrity (enabling detection of message tampering, interception, and forgery), interoperability, algorithm flexibility, and ease of deployment and use.

Perfect Forward Secrecy (PFS) protects connections between customers’ client systems and Microsoft cloud services by unique keys. Connections also use RSA-based 2,048-bit encryption key lengths. This combination makes it difficult for someone to intercept and access data that is in transit.

* + - * 1. Azure Storage transactions

When you interact with Azure Storage through the Azure portal, all transactions take place over HTTPS. You can also use the Storage REST API over HTTPS to interact with Azure Storage. You can enforce the use of HTTPS when you call the REST APIs to access objects in storage accounts by enabling the secure transfer that's required for the storage account.

Shared Access Signatures (SAS), which can be used to delegate access to Azure Storage objects, include an option to specify that only the HTTPS protocol can be used when you use Shared Access Signatures. This approach ensures that anybody who sends links with SAS tokens uses the proper protocol.

Client-side encryption encrypts the data before it’s sent to your Azure Storage instance, so that it’s encrypted as it travels across the network.

* + - * 1. RDP sessions

For scenarios where Capgemini SAM is a method of accessing customer workloads it is possible to

connect to a VM by using the Remote Desktop Protocol (RDP) from a SAM Jumphost. Domain credentials must be provided for COS Team members to access to customer Virtual Machines.

* + - * 1. Secure access to Linux VMs with SSH

For scenarios where Capgemini SAM is a method of accessing customer workloads it is possible to

connect to a VM by using the Secure Shell (SSH). It is the default connection protocol for Linux VMs hosted in Azure. By using SSH keys for authentication, you eliminate the need for passwords to sign in. SSH uses a public/private key pair (asymmetric encryption) for authentication. To utilize public/private key pair for authentication Capgemini’s Hashicorp Vault integration should be implemented.

* + - 1. Encryption Key Management

By default, all Azure Managed Disks are encrypted with Azure Managed Keys. Users have no access to those keys.

* + - 1. Privileged Access Management (PAM)

Privileged Access Management is a feature of Azure Active Directory. Azure Active Directory support is not covered by standard COS offer.

* + - 1. Admin Access

Capgemini personnel will not have admin access within customer environment. It is up to customer to create and manage accounts for Capgemini personnel and external contractors.

* + - 1. Firewalls

Network Security Groups are utilized within Cloud Operation Services to manage inbound and outbound connection to Virtual Machines. If more advanced solution is needed than Azure Firewall can be configured additionally by Cyber Security Team.

Setup of Azure Firewall must be done based on customer network requirements.

* + - 1. Intrusion Detection/Prevention Systems (IDS/IPS)

Not part of standard COS offer but can be provided additionally by Cyber Security.

IDS and IDP are supported by Azure Firewall and Azure Security Center. More details on IDS/IPS can be found within Cyber Security documentation:

[CWPP Azure Solution Document 1.0 - 02112021](https://g-port.capgemini.com/file/40144?fileName=CybersecurityDefendServices_CloudSecurityServiceOffering_Explain_SolutionDeepDiveWorkshopKit_CwppAzureSolutionDocument10-02112021_03052021)

[CWPP Azure Service Description 1.0 - 02112021](https://g-port.capgemini.com/file/40143?fileName=CybersecurityDefendServices_CloudSecurityServiceOffering_Explain_SolutionDeepDiveWorkshopKit_CwppAzureServiceDescription10-02112021_03052021)

[CSPM Azure Solution Document 1.0 - 02172021](https://g-port.capgemini.com/file/40142?fileName=CybersecurityDefendServices_CloudSecurityServiceOffering_Explain_SolutionDeepDiveWorkshopKit_CspmAzureSolutionDocument10-02172021_03052021)

[CSPM Azure Service Description 1.0 - 02172021](https://g-port.capgemini.com/file/40141?fileName=CybersecurityDefendServices_CloudSecurityServiceOffering_Explain_SolutionDeepDiveWorkshopKit_CspmAzureServiceDescription10-02172021_03052021)

* + - 1. Distributed Denial of Service (DDOS)

Not part of standard COS offer but can be provided additionally by Cyber Security.

* + - 1. Data Leakage Prevention (DLP)

Not part of standard COS offer but can be provided additionally by Cyber Security.

* + 1. Organization Control

N/A

* + - 1. Assurance
         1. Penetration Testing

Account team is responsible for arranging penetration testing.

* + - * 1. Code Verification

N/A

* + - 1. Compliance
         1. ISO/IEC 27001/27002

Currently CCP service delivery is ISO 27001 certified and all new COS processes etc. must maintain that certification.

* + 1. Personal Data & GDPR Compliance

The guide discusses how to use Microsoft products, services and administrative tools to help our controller customers find and act on personal data to respond to DSRs. Specifically, this includes how to find, access, and act on personal data that reside in the Microsoft cloud. Here's a quick overview of the processes outlined in this guide:

Discover: Use search and discovery tools to more easily find customer data that may be the subject of a DSR. Once potentially responsive documents are collected, you can perform one or more of the DSR actions described in the following steps to respond to the request. Alternatively, you may determine that the request doesn't meet your organization's guidelines for responding to DSRs.

Access: Retrieve personal data that resides in the Microsoft cloud and, if requested, make a copy of it that can be available to the data subject.

Rectify: Make changes or implement other requested actions on the personal data, where applicable.

Restrict: Restrict the processing of personal data, either by removing licenses for various Azure services or turning off the desired services where possible. You can also remove data from the Microsoft cloud and retain it on-premises or at another location.

Delete: Permanently remove personal data that resided in the Microsoft cloud.

Export/Receive (Portability): Provide an electronic copy (in a machine-readable format) of personal data or personal information to the data subject. Personal information under the CCPA is any information relating to an identified or identifiable person. There is no distinction between a person's private, public, or work roles. The defined term "personal information" roughly lines up with "personal data" under GDPR. However, the CCPA also includes family and household data. For more information about the CCPA, see the California Consumer Privacy Act and the California Consumer Privacy Act FAQ.

For more information on processing user data in Azure please go to Microsoft dedicated GDPR website: <https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-dsr-Azure?view=o365-worldwide>

* + 1. Key Management

Azure Key Vault is used for secure key and secret management within COS solution. COS deployment template deploys Key Vault during deployment of ServiceNow integration as ServiceNow/iPaaS keys are the only keys COS needs to work. Each time iPaaS team changes keys, the manual key rotation is required within Azure Key Vault to maintain alerting functionality.

* 1. Automation

Solution Deployment as well as Virtual Machines Onboarding to each solution has been automated.

Below two sections describes each automation process in detail.

* + 1. Solution deployment automation

Deployment Template of each solution has been written in JSON in form of an Azure native ARM Template. Those templates can be deployed from Azure Portal, using Powershell or with Azure DevOps.

On top of ARM Templated Azure DevOps Pipelines has been created to streamline the deployment process.

Both ARM Templates and Azure DevOps Pipelines can be copied to customer environment for further deployment.

* + 1. Configuration automation

When One Time Setup of COS is completed than each Virtual Machine needs only specific TAG applied to be managed. Azure Policy Service is running constantly in the background and scans customer’s subscription for new eligible Virtual Machines. Azure Policy run every 24h and upon each resource creation/modification. That makes solution perfect not only for greenfield, but also for brownfield deployments. For more information with regards to Azure Policy please see section 5.8.1 within this document.

* + 1. Repository

Cloud Operation Services code is stored within [Cloud Transformation Library Private GitHub Repository](https://github.com/Capgemini-Innersource/Cloud-Transformation-Library). To access that Repository you need to be member of [Capgemini Innersource Organisation](https://github.com/Capgemini-Innersource) on GitHub first. You can request membership to that Organization via GitHub. Please note CG World VPN or MobilePass Token is required to access that GitHub Organization.

Once you become a member then Azure COS Architect can grant you with access to [Cloud Transformation Library](https://github.com/Capgemini-Innersource/Cloud-Transformation-Library) where Cloud Operation Services code for Azure, AWS and GCP is stored.

* 1. Governance
     1. Azure Policies

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. These business rules, described in JSON format, are known as policy definitions. To simplify management, several business rules can be grouped together to form a policy initiative. Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources. The assignment applies to all resources within the Resource Manager scope of that assignment. Sub scopes can be excluded, if necessary. For more information, see Scope in Azure Policy.

Azure Policies play key role in Cloud Operation Services. Thanks to their remediation feature policies can deploy agents to Virtual Machines and connect them to correct Log Analytics Workspace for monitoring, patching and logging solutions.

Within COS we can differentiate custom policies created by COS development team and built-in policies which are available on Azure.

Following set of custom policies is deployed and assigned on Subscription or Management Group level during Cloud Operation Services enablement:

* COS Dependency agent for Linux virtual machines
* COS Dependency agent for Windows virtual machines
* COS Log Analytics agent for Linux virtual machines
* COS Log Analytics agent for Windows virtual machines
* COS Policy to assign Virtual Machines to Backup Policy
* COS Deploy Diagnostic Settings for Recovery Services Vault to Log Analytics workspace for resource specific categories by tags
* COS Adds ccp\_managed tag to Virtual Machine Resource

Policy Initiatives can be also used. With an initiative definition, you can group several policy definitions to achieve one overarching goal. Using initiatives greatly reduces the number of policy assignments you need to manage.

For example, when using tags to group your billing data. Typically, you may have around five tags which should be applied to figure out who is going to pay for that resources. Policies are a great tool to make sure these tags are applied and enforced.

Unfortunately, as your environment grows, you will have a lot of policy assignments. In case of five billing tags, you will have a total of 10 policy assignments (apply and enforce) for each scope (typically a resource group). This makes management of policies very hard. That’s where policy initiatives come in handy. Instead of assigning 10 policies to each resource group, you can now group these policies in an initiative (also known as policy set) and just assign the newly created assignment to your resource groups.

Following Microsoft recommended Policies will be assigned on Subscription or Management Group level:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Policy Name | Policy Description | Policy ID | Category | Effect | |
| Unattached disks should be encrypted | This policy audits any unattached disk without encryption enabled. | 2c89a2e5-7285-40fe-afe0-ae8654b92fb2 | Compute | Audit | |
| Virtual machines should be migrated to new Azure Resource Manager resources | Use new Azure Resource Manager for your virtual machines to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management | 1d84d5fb-01f6-4d12-ba4f-4a26081d403d | Compute | Audit |
| Microsoft Antimalware for Azure should be configured to automatically update protection signatures | This policy audits any Windows virtual machine not configured with automatic update of Microsoft Antimalware protection signatures. | c43e4a30-77cb-48ab-a4dd-93f175c63b57 | Compute | AuditIfNotExists | |
| Only approved VM extensions should be installed | This policy governs the virtual machine extensions that are not approved. | c0e996f8-39cf-4af9-9f45-83fbde810432 | Compute | Audit |
| Managed disks should disable public network access | Disabling public network access improves security by ensuring that a managed disk isn't exposed on the public internet. Creating private endpoints can limit exposure of managed disks. Learn more at: https://aka.ms/disksprivatelinksdoc. | 8405fdab-1faf-48aa-b702-999c9c172094 | Compute | Audit | |
| Audit VMs that do not use managed disks | This policy audits VMs that do not use managed disks | 06a78e20-9358-41c9-923c-fb736d382a4d | Compute | audit |
| Microsoft IaaSAntimalware extension should be deployed on Windows servers | This policy audits any Windows server VM without Microsoft IaaSAntimalware extension deployed. | 9b597639-28e4-48eb-b506-56b05d366257 | Compute | AuditIfNotExists | |
| Flow logs should be enabled for every network security group | Audit for flow log resources to verify if flow log status is enabled. Enabling flow logs allows to log information about IP traffic flowing through network security group. It can be used for optimizing network flows, monitoring throughput, verifying compliance, detecting intrusions and more. | 27960feb-a23c-4577-8d36-ef8b5f35e0be | Network | Audit |
| Virtual machines should be connected to an approved virtual network | This policy audits any virtual machine connected to a virtual network that is not approved. | d416745a-506c-48b6-8ab1-83cb814bcaa3 | Network | Audit | |
| SSH access from the Internet should be blocked | This policy audits any network security rule that allows SSH access from Internet | 2c89a2e5-7285-40fe-afe0-ae8654b92fab | Network | Audit |
| RDP access from the Internet should be blocked | This policy audits any network security rule that allows RDP access from Internet | e372f825-a257-4fb8-9175-797a8a8627d6 | Network | Audit | |
| Storage accounts should be migrated to new Azure Resource Manager resources | Use new Azure Resource Manager for your storage accounts to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management | 37e0d2fe-28a5-43d6-a273-67d37d1f5606 | Storage | Audit |

* + 1. Tagging

Customers may use their Tagging policy, but there are specific tags which are required for COS to work properly.

Following TAGs has been defined as minimum for Cloud Operation services to operate:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Cloud Operation Services Platform Tags | | | | |
| Tag Name | **Description** | **Key** | **Example Value** | **Required?** |
| VM Onboarding | Region specific tag which matches Azure Onboarding Policy to Deploy Monitoring Agent and Dependency Agent on VM. | cos\_customername\_sub\_env\_managed | {region name} | Yes |
| Patching | OS and Region specific default tag used to populate default Patch Group created during onboarding | cos\_customername\_sub\_env\_patchgroup | {os-region name} | Yes |
| Backup | Region specific default tag used to add VMs to default Backup Policy created during onboarding | cos\_customername\_sub\_env\_backup | {region name} | Yes |
| Monitoring | Tag can be used for maintenance functionality | cos\_customername\_sub\_env\_monitoring | {enabled} | Yes |
| Billing | Billing Purpose | cos\_managed | yes | Yes |

* 1. Dashboards

Dashboards are based on native Azure solution – Azure Workbooks which uses KQL queries to visualize all sorts of data collected within Log Analytics Workspace. The main purpose of those Workbooks is to help operations with their daily/weekly/monthly activities and to allow better observability of the environment.

* + 1. Operations Workbooks
       1. Operations Workbooks Prerequisites

Minimum role requirements for Azure Workbook creation:

Please note: In some cases, Log Analytics Workspace can be shared with different Solutions and different Teams. In such case, more restrict Roles can be applied down to Table level.

|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure permission required | Scope required |
| Creating Azure Workbook | Log Analytics Workspace Contributor | Desired Log Analytics Workspace |
| Creating Azure Workbook | Microsoft.Resources/deployments/\* | Resource Group or Subscription |
| Viewing Workbooks | Log Analytics Workspace Reader | Desired Log Analytics Workspace |

|  |
| --- |
| Note |
| For each workbook to work correctly corresponding solution must be deployed prior to Workbook creation. |
| Within Log Analytics Workspace, following Logs and Metrics must be collected from Virtual Machines  System (Windows event logs)  System(\*) (Linux Performance counter)  System\Uptime (Windows Performance counter)  LogicalDisk\% Free space (Windows Performance counter)  LogicaDisk(%) \Free Megabytres (Windows Performance counter)  Network Adapter(\*)\Packets sent (Windows Performance counter)  Network (Windows Performance counter)  Logical Disk(\*) (Linux Performance counter)  Memory(\*) (Linux Performance counter)  Network(\*) (Linux Performance counter)  System(\*) (Linux Performance counter)  Syslog (Syslog) |

* + - 1. Operations Workbooks - One Time Setup

Deployment of Azure Workbooks boils down to deployment of ARM Template with predefined KQL queries. ARM Templates can be found within COS Repository under Dashboard section.

ARM Template can be deployed from Azure Portal, with Powershell or using Azure DevOps.

* + - 1. Available Dashboards
         1. Update Management Dashboard

The Update Management Dashboard lists available updates for onboarded virtual machines and validates whether onboarded Virtual Machines have all patching prerequisites met. For example, before patching process is initiated, Virtual Machines should have enough free space on disk to download patches.

Update Management Dashboard consists of three Tabs:

* Compliance Summary
* VM Status
* Update Details

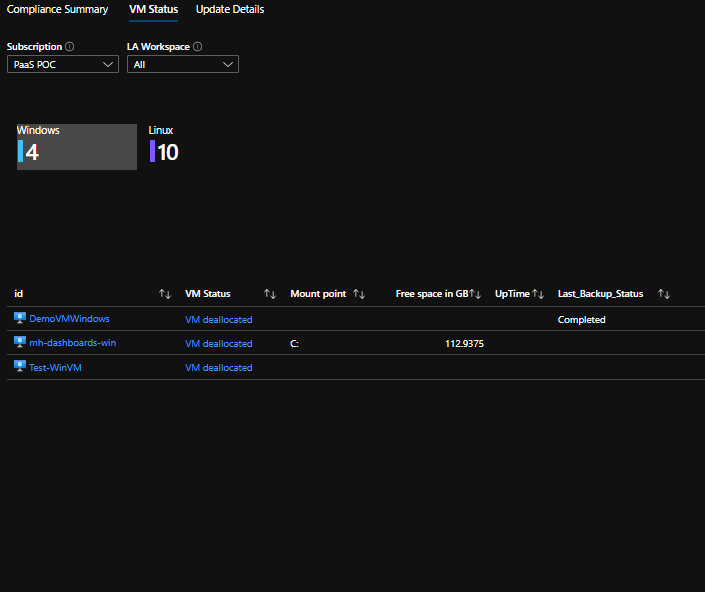
**Compliance Summary**

This tab is just a short summary about virtual machines. Under the sub-tab “overview” we can see a graph that describes how many patches virtual machine requires. If a tile’s color is different that green, it means that the virtual machine needs an attention. Under “Key metrics” tab we can see the following real time metrics: CPU utilization, total network in/out, total disk read/write. The virtual machines are grouped by subscription.



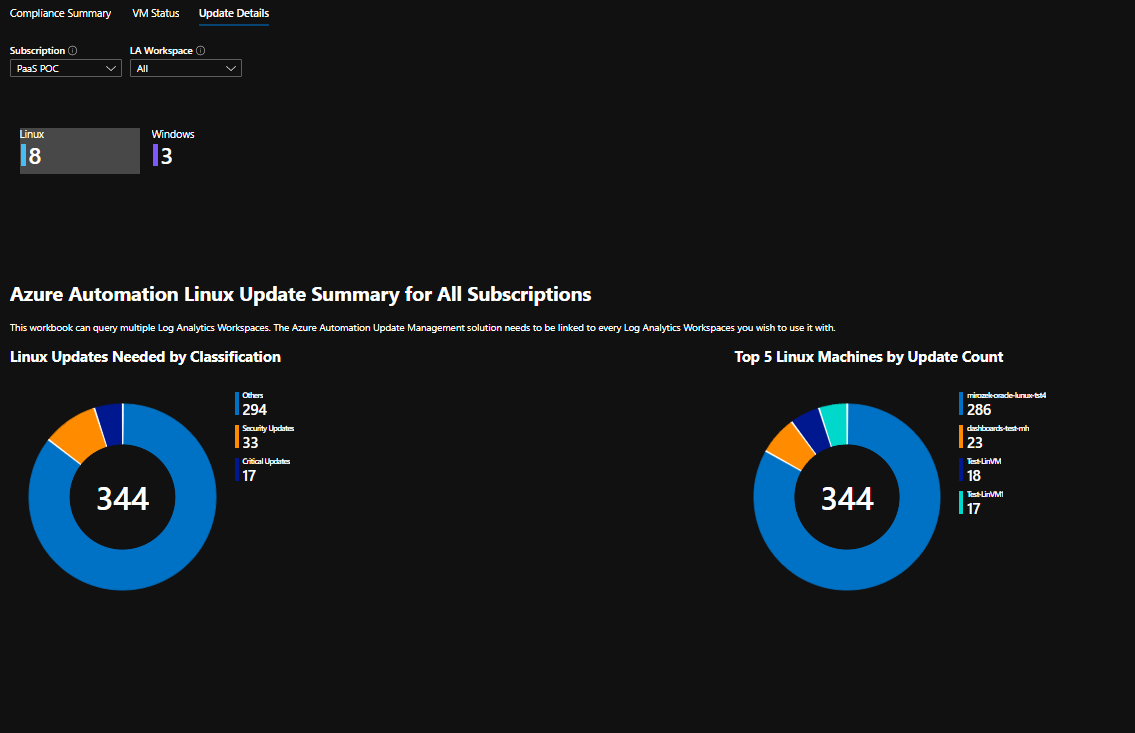
**VM Status**

This tab contains required information for assessing if a virtual machine can be patched. First, we are asked to choose a Log Analytics Workspace to fetch information from. Next, we are asked to choose an operating system. After that we can see a table of metrics with specific VMs, we can decide whether Virtual Machine is eligible for patching or not based on provided information.

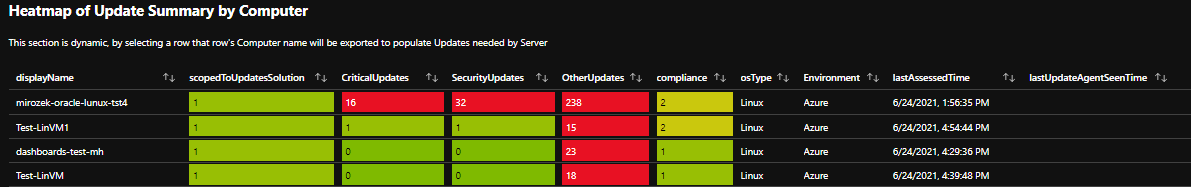


**Update Details**

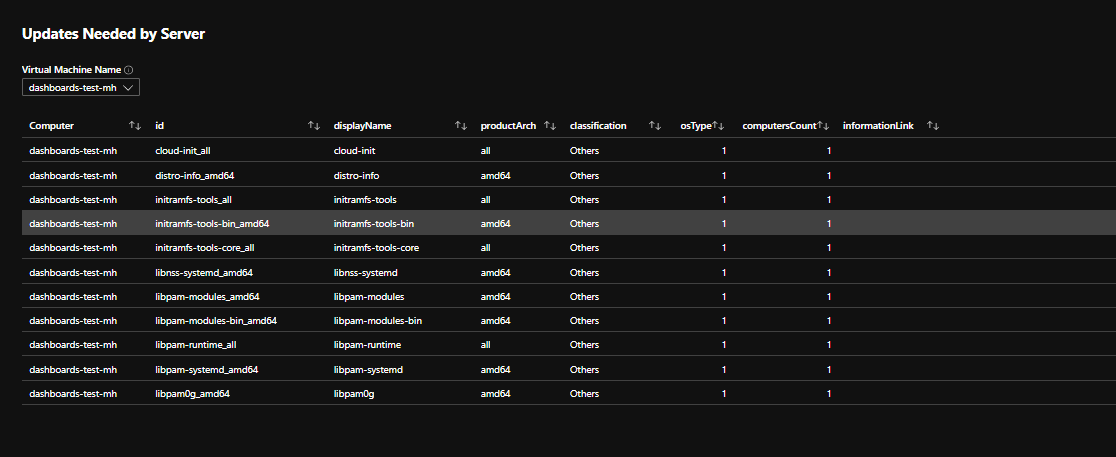
This tab contains the details about available updates. First pie chart describes number of updates grouped by category; second pie chart describes number of updates grouped by Virtual Machine.



Next chart is a summary of previous two charts, and displays list of virtual machine with number of required patches grouped by category.



Lastly - table containing details about specific update for specific virtual machine.



* + - * 1. Monitoring Dashboard

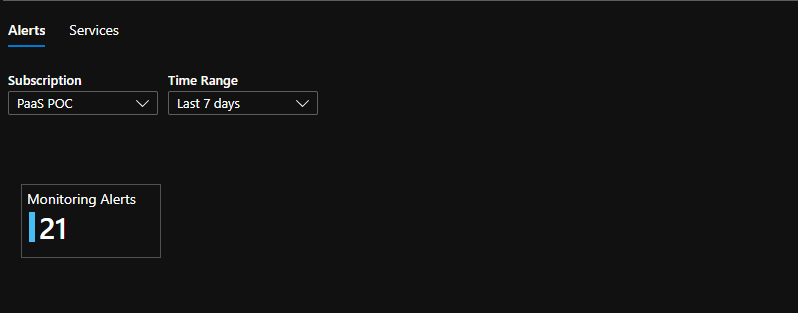
This dashboard contains information on alerts created based on Alert Rules deployed with Monitoring Solution.

Monitoring Dashboard consists of two Tabs:

* Alerts
* Services

**Alerts**

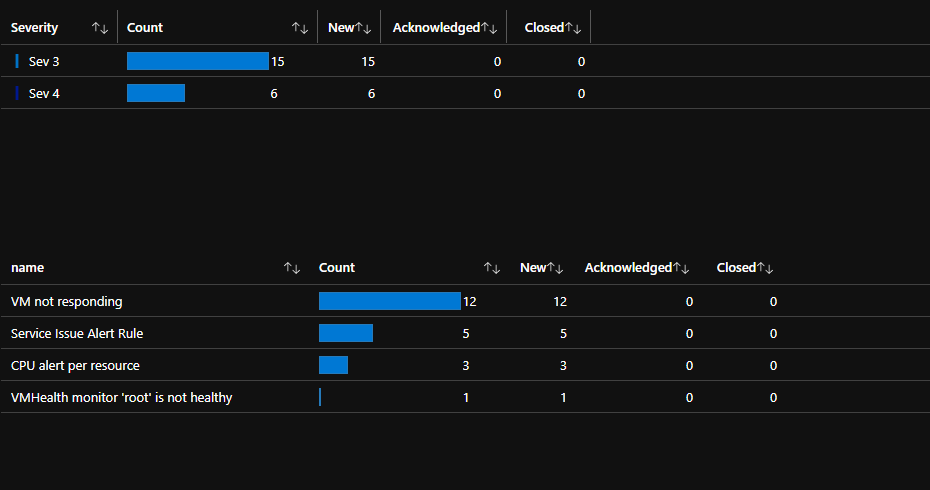
Alerts tab has clickable Tile with number of fired alerts during the period set in time range parameter. Clicking the Tile expands more data including Alert Category and Alert Severity.

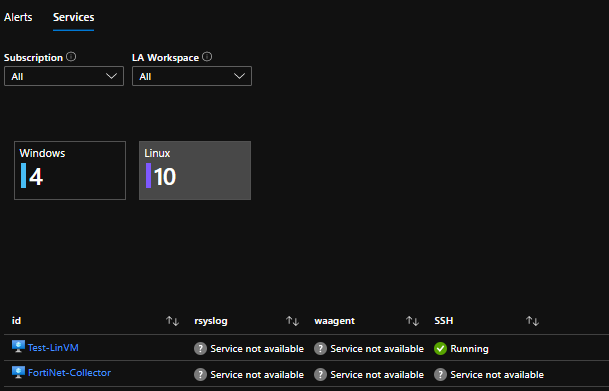


**Services**

Services tab has clickable Tiles (one per OS Category). Clicking each Tile provides status information on services running on Virtual Machines. If output returns “Service is not available” it may mean that:

* Change tracking is disabled
* There is no information about service in Change configuration table
* Virtual machine is not reporting to Log Analytics workspace
* Service isn’t deployed on specific VM



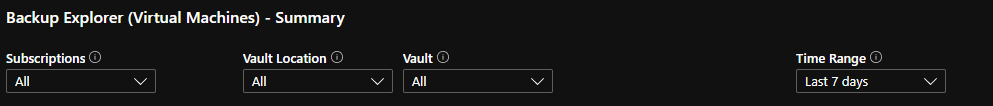


* + - * 1. Backup Dashboard

Backup dashboard contains details on state of backup of Virtual Machines and Recovery Vaults within selected Subscription. The dashboard is divided into six Tabs:

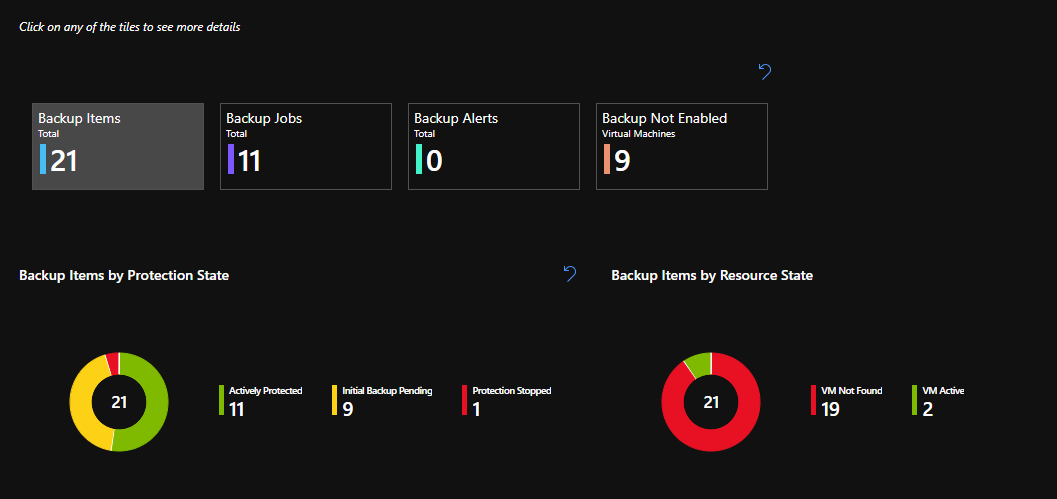
* Summary
* Backup Items
* Jobs
* Alert
* Policies
* Backup not enabled

It is possible to limit results by selecting parameters first:



**Summary**

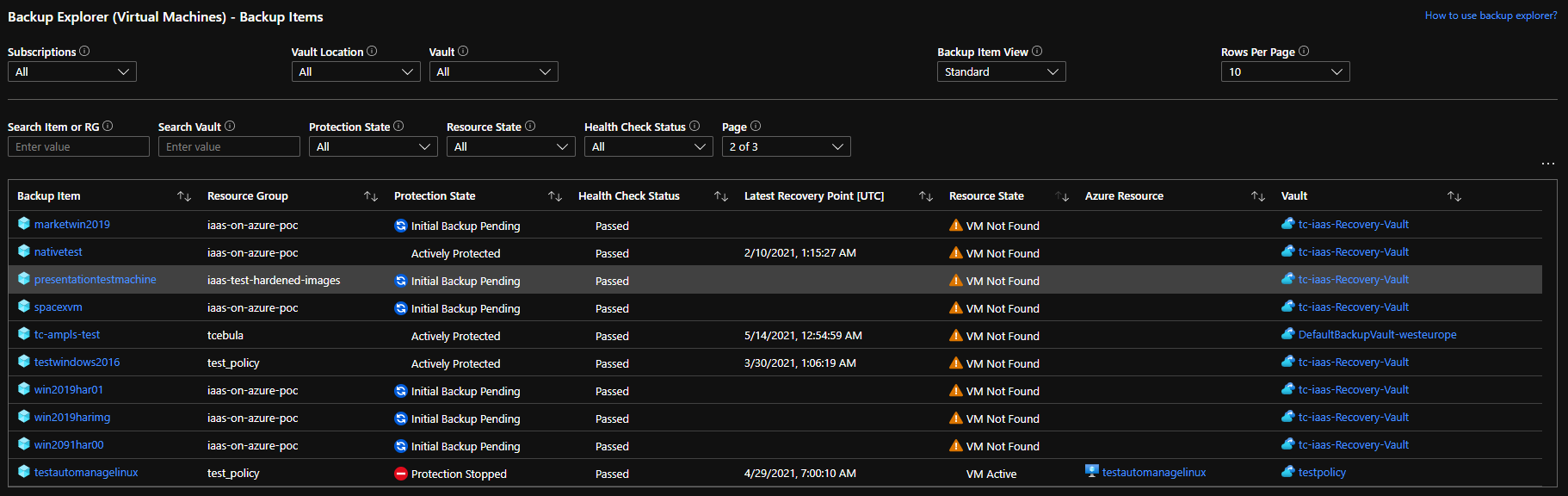
The summary tab provides general statistics about backup. It presents information about Backup Items, Backup Jobs, Backup Alerts, Backup not Enabled. By clicking each of those Tiles, more detailed information reviles.



**Backup Items**

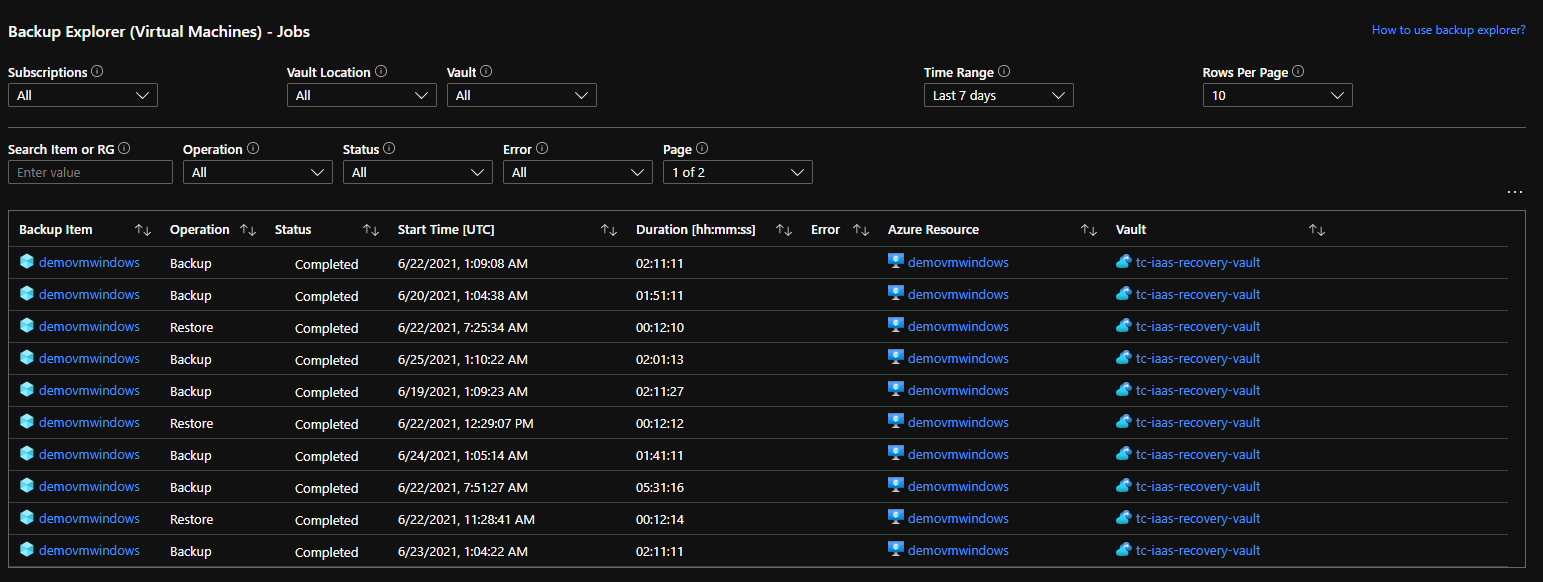
Returns details on backed up items. The table is divided into following sections:

* Backup items – name of backed up item
* Resource group – the group that backup item belongs to
* Protection state – state of backup item
* Health check status – information about backup status
* Last recovery point – last successful backup
* Resource state – column returns information if backed up item exists
* Azure resource – link to backed up resource
* Vault - recovery service vault that resource is connected to



**Jobs**

Jobs tab returns information about all kinds of vault jobs like: backup, restore, Configure Backup, Delete Backup Data with status: Completed, Completed With Warning, Failed, Cancelled, InProgress. The table below returns details about all kind of jobs. We can limit results to specific operation, status, or error.

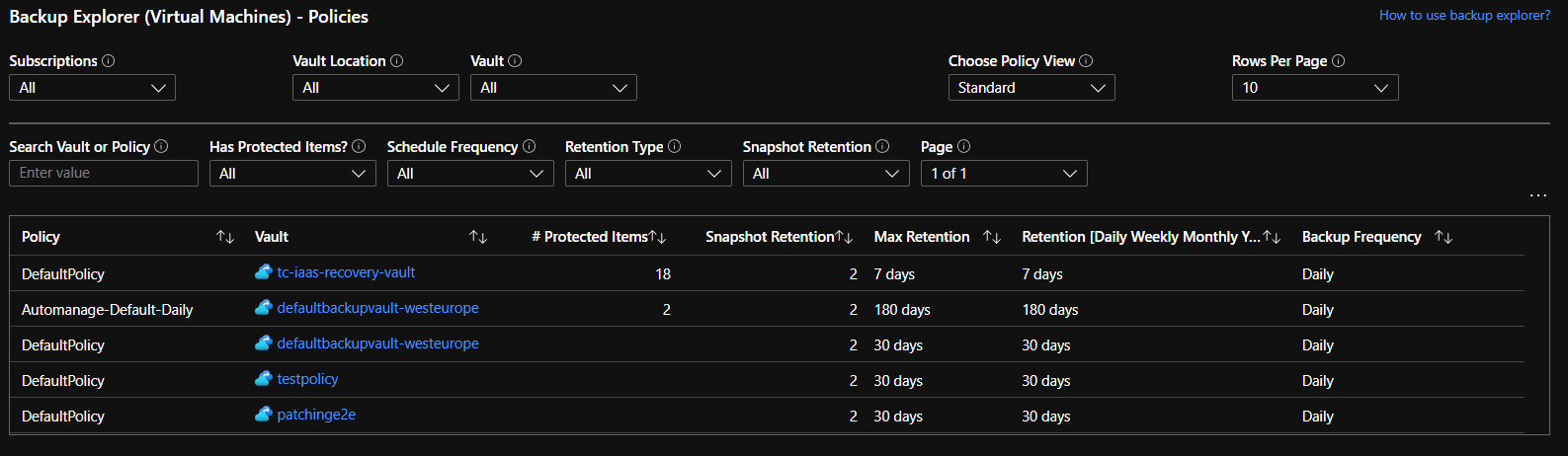


**Alerts**

Alerts tab displays information about alerts triggered for the scope of Recovery Service Vault.

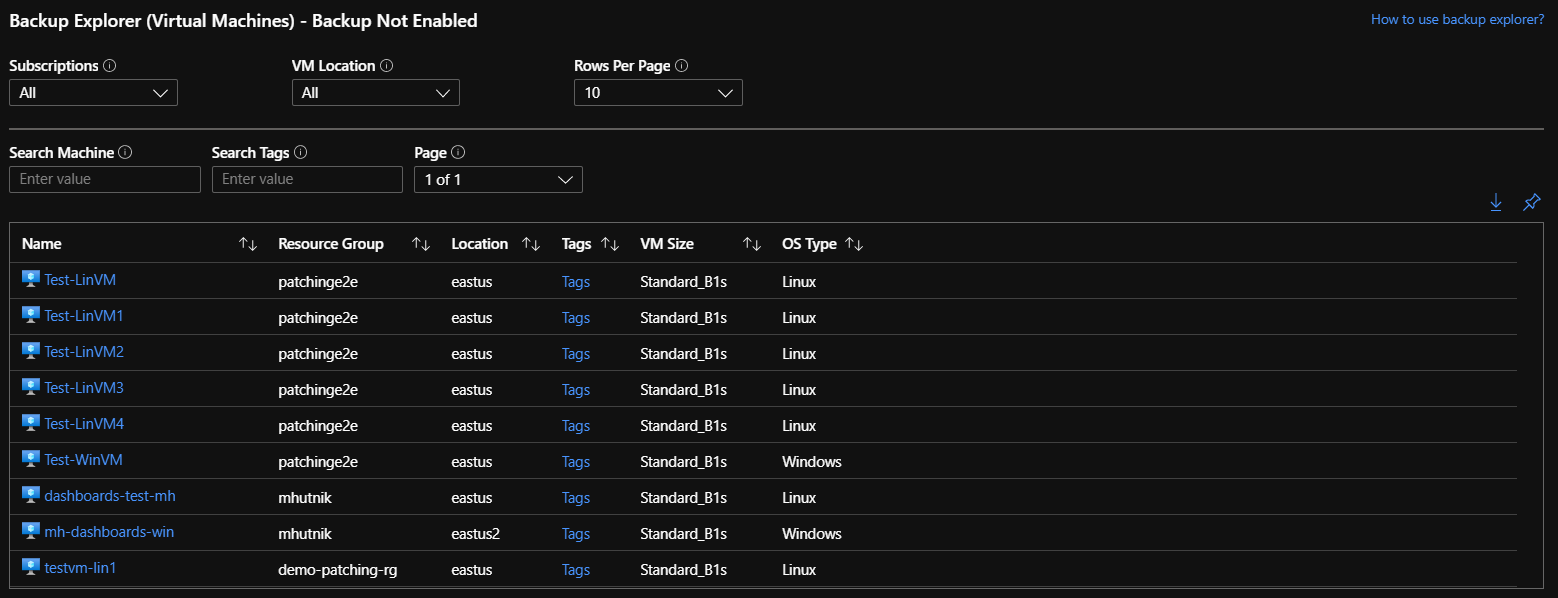
**Policies**

Policies tab displays information on Backup Policies created within each Recover Service Vault.



**Backup not enabled**

That tab lists Virtual Machines not connected to Recovery Service Vault.



* 1. Reports

Reporting functionality relies on data collected within Azure Log Analytics Workspace and data available in Azure Resource Graph. All Reports are automated and uploaded to Storage Account monthly. Deployment of report functionality is also fully automated with Azure DevOps Pipeline.

* + 1. Availability Report

Availability Report consist data from Log Analytics Workspace collected using Azure App Function and Kusto Query Language query.

* + 1. Performance Report

Performance Report consist data from Log Analytics Workspace and VM Insights collected using Azure App Function and Kusto Query Language query.

* + 1. Event Report

Event/Alert Report consist data from Azure Resource Graph collected using Azure App Function and Kusto Query Language query.

* + 1. Update Management Report

Update Management Report consist data from Log Analytics Workspace collected using Azure App Function and Kusto Query Language query.

As soon as Microsoft releases Update Center – replacement for Update Management - reports will be created using Update Center functionality and Azure Resource Graph.

* + 1. Backup Report

Backup Report consist data from Log Analytics Workspace collected using Backup Center Reporting functionality.

* 1. Cost Management

Cost control is a critical component to maximizing the value of your investment in the cloud. There are several scenarios where cost visibility, reporting, and cost-based orchestration are critical to continued business operations. Cloud Operation Services offers full support of Azure Cost Management solution, which includes:

* Costs Forecasts
* Budgets
* Cost Alerts
* Automated actions based on Budgets
  + 1. Cost Management – Prerequisites

Minimum role requirements for Cost Management:

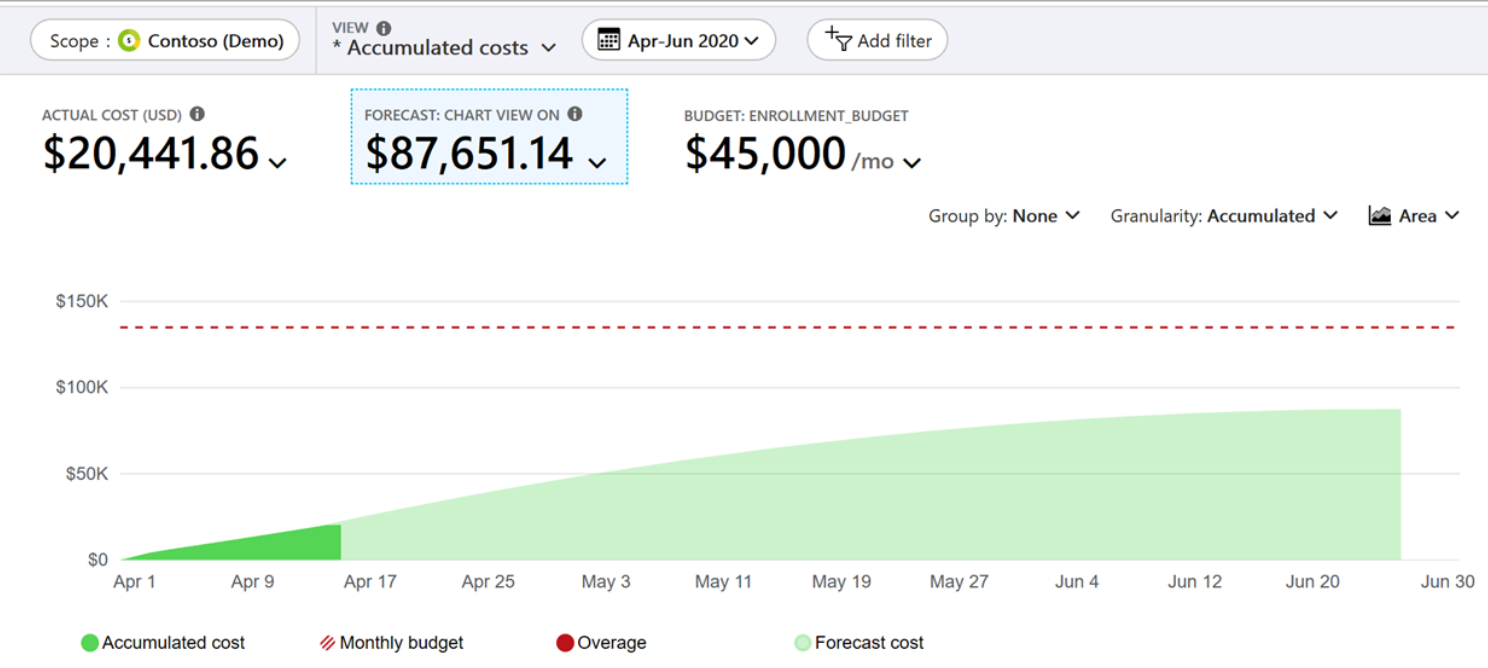
|  |  |  |
| --- | --- | --- |
| Management Operation | Minimum Azure permission required | Scope required |
| View costs, manage cost configuration, and view recommendations | Cost Management Contributor | Subscription or Management Group Level |
| Manage Action Groups and Alerting | Monitoring Contributor | Resource Group Level |

* + 1. Cost Management – Forecasts

Forecasted costs are shown in cost analysis areas for area and stacked column views. The forecast is based on customer’s historical resource use. Changes to your resource use affect forecasted costs.

In the Azure portal, navigate to cost analysis for desired scope. For example: Cost Management + Billing > Cost Management > Cost analysis.

In the default view, the top chart has the Actual/Amortized cost and forecasted cost sections. The solid colour of the chart shows your Actual/Amortized cost. The shaded colour shows the forecast cost.



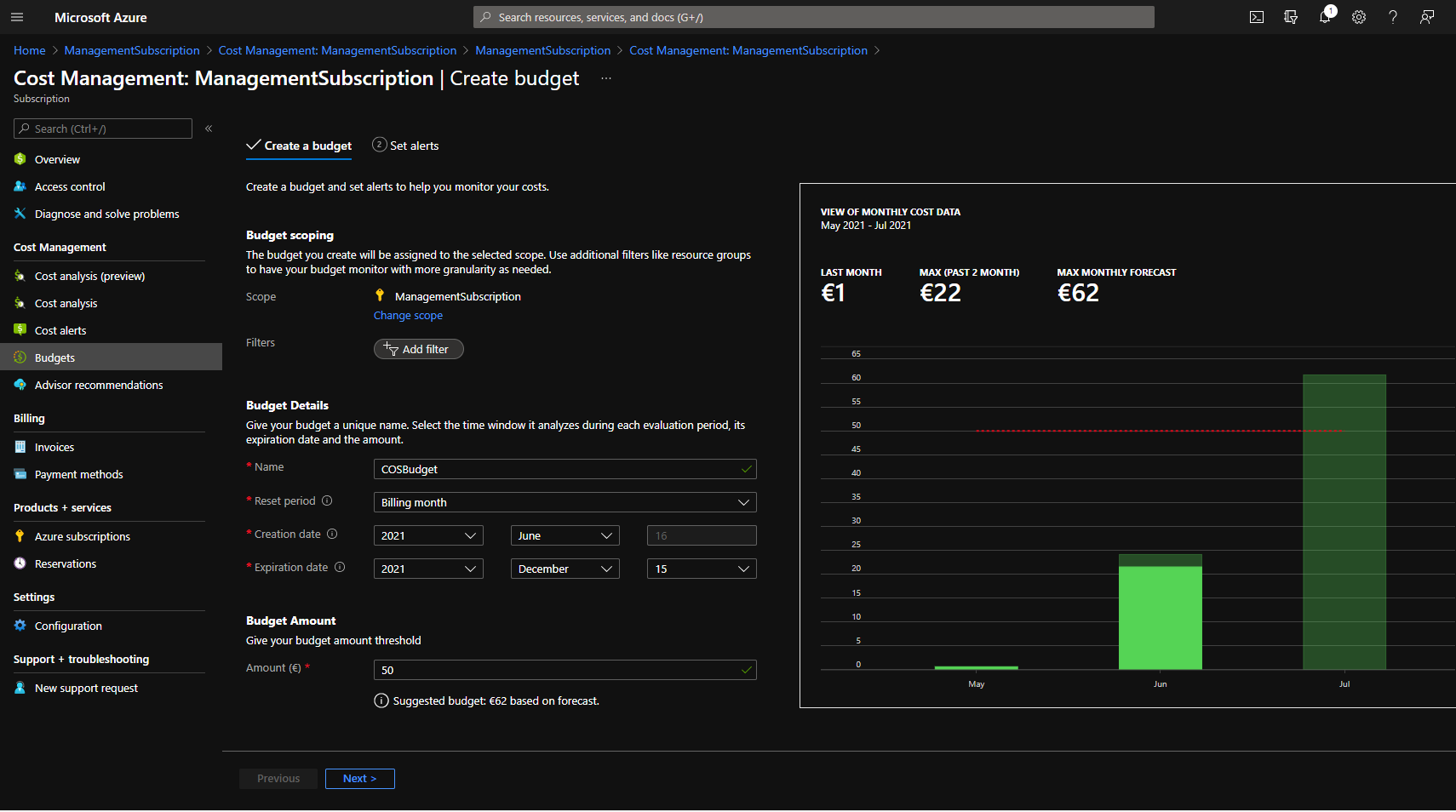
* + 1. Cost Management – Budgets

Budgets in Cost Management help you plan for and drive organizational accountability. They help you inform others about their spending to proactively manage costs, and to monitor how spending progresses over time. You can configure alerts based on your actual cost or forecasted cost to ensure that your spend is within your organizational spend limit. When the budget thresholds you've created are exceeded, only notifications are triggered. None of your resources are affected and your consumption isn't stopped. You can use budgets to compare and track spending as you analyze costs.

Cost and usage data is typically available within 8-24 hours and budgets are evaluated against these costs every 24 hours. Be sure to get familiar with Cost and usage data updates specifics. When a budget threshold is met, email notifications are normally sent within an hour of the evaluation.

Budgets reset automatically at the end of a period (monthly, quarterly, or annually) for the same budget amount when you select an expiration date in the future. Because they reset with the same budget amount, you need to create separate budgets when budgeted currency amounts differ for future periods. When a budget expires, it's automatically deleted.

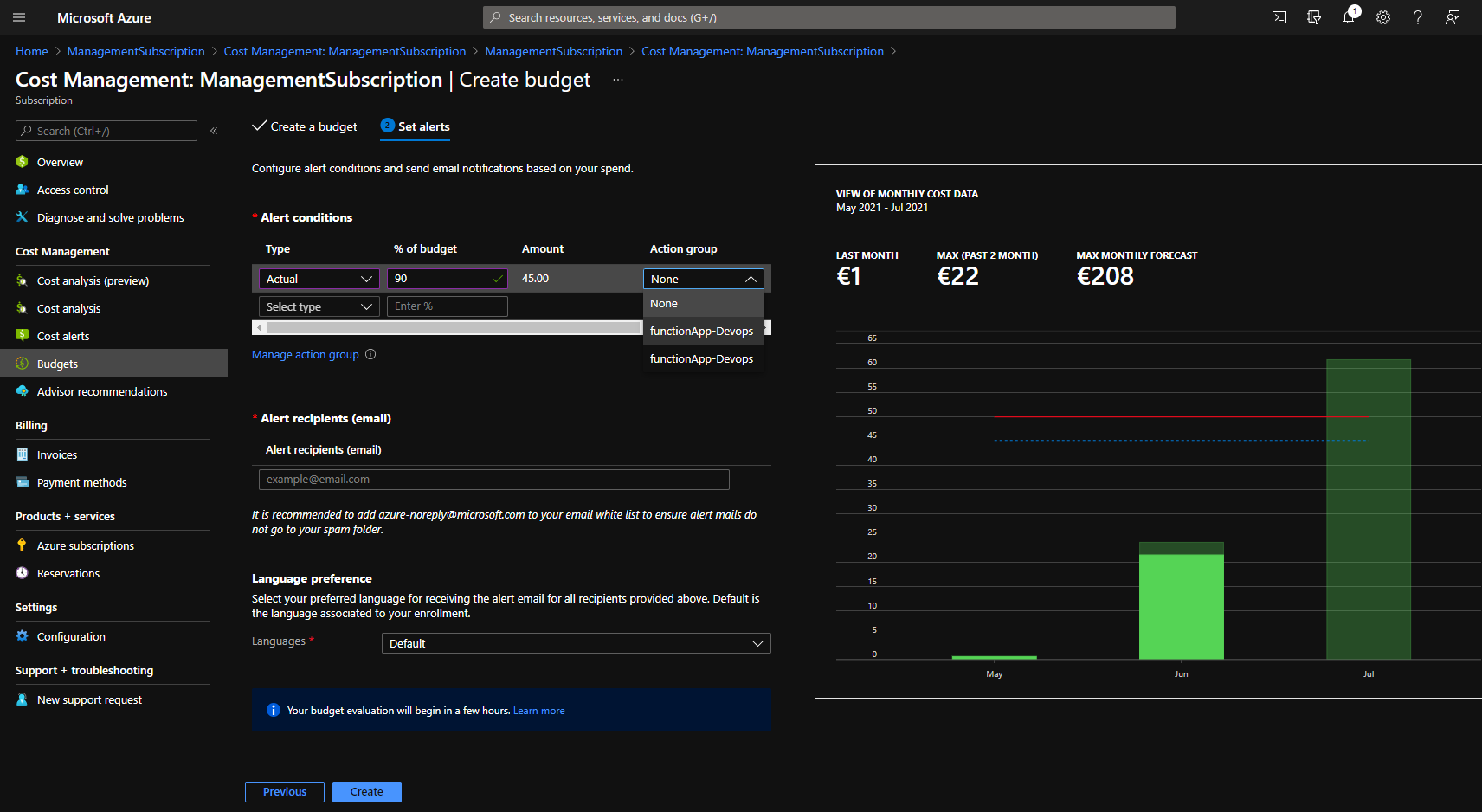
Below screenshot presents Budget creation from Azure Portal:



Next section presents Alert creation based on defined Budgets.

* + 1. Cost Management – Cost Alerts

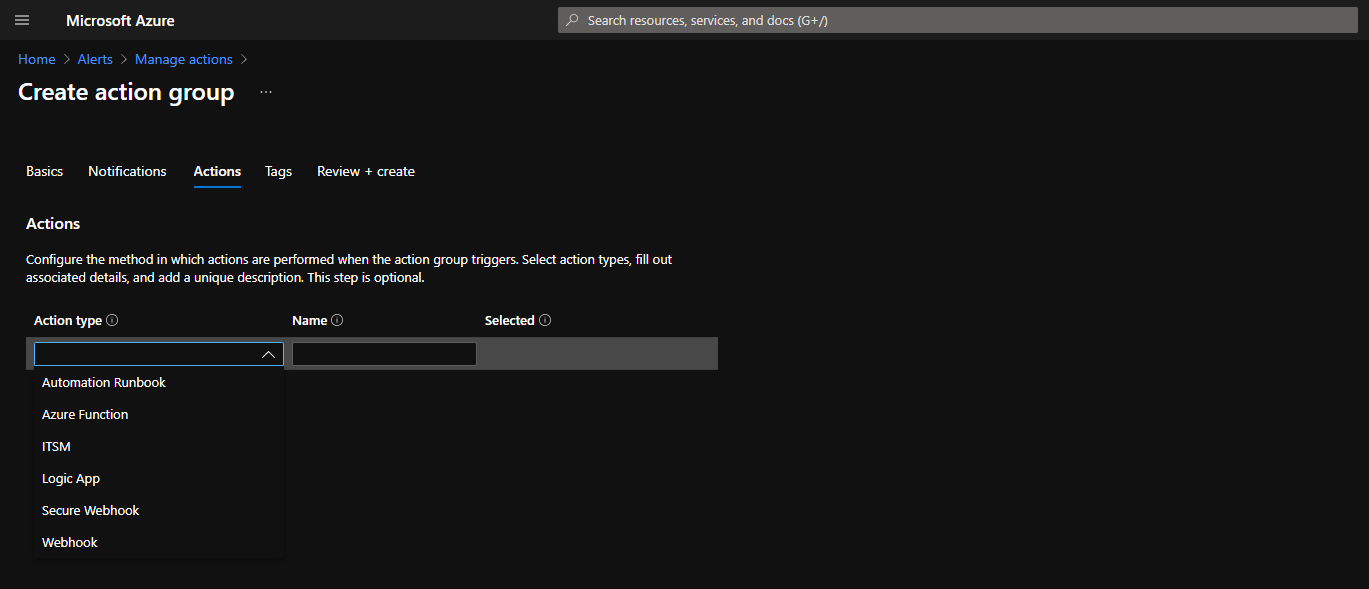
Budgets require at least one cost threshold (% of budget) and a corresponding email address. You can optionally include up to five thresholds and five email addresses in a single budget. When a budget threshold is met, email notifications are normally sent within an hour of the evaluation. Actual costs budget alerts are generated for the actual cost you've accrued in relation to the budget thresholds configured. Below screenshot presents Cost Alert creation within Azure Portal.



* + 1. Cost Management - Automated actions based on Budgets

When you create or edit a budget for a subscription or resource group scope, you can configure it to call an action group. The action group can perform various actions when your budget threshold is met. Below screenshot shows which action can be triggered via action group. That gives plenty options for automation. For example, it is possible to setup Budget to trigger Automation Runbook to shut down VMs when desired Budget is met.

Support of Azure Function allows sending incident to ServiceNow when Budget threshold is met.

Action Groups are currently only supported for subscription and resource group scopes.

1. Environment Considerations

N/A

1. Software Licensing

Customer is responsible for License Management within Cloud Operation Services.

Following Licenses might be required:

Azure Active Directory P1 License

Azure Security Center Standard Tier

Azure DevOps for automated deployment

1. Hardware and Software Components

N/A

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients’ opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.

Learn more about us at [www.capgemini.com](http://www.capgemini.com)



This document contains information that may be privileged or confidential and is the property of the Capgemini Group.  
Copyright © 2019 Capgemini. All rights reserved.