

Microsoft Azure Cloud Adoption Framework Server Migration Security Policy

**MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.**

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation. Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers. © 2016 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

**TABLE OF Contents**

[1 Introduction 3](#_Toc42625059)

[2 Target Audience 3](#_Toc42625060)

[3 Azure Server Migration Scenarios 3](#_Toc42625061)

[4 Azure Server Migration Architecture 3](#_Toc42625062)

[5 Requirements 4](#_Toc42625063)

[5.1 Operational Requirements 4](#_Toc42625064)

[6 Azure Security Policy 5](#_Toc42625065)

[6.1 How to run JSON Policy Script 5](#_Toc42625066)

[6.2 Major Azure Policy for security 8](#_Toc42625067)

[7 Appendix A 12](#_Toc42625068)

# Introduction

This document is a major deliverable on securing the Azure Server Migration and provide real-time compliance data while performing audit the environment. This will also help in reduce the number of external approval process by implementing policies at the core of the Azure platform for increased developer productivity. Control and optimize the cloud spend to get more value from your investment.

# Target Audience

This document is Level 400+ technical migration guide primarily intended for Azure Specialists, Cloud Solution Architects, Migration experts, System Administrators & anyone else who are going to be hands-on in executing the on-premise to Azure migrations. It is assumed that the audience has deep insights into their on-premise workload architectures, storage & networking capabilities along with the interdependencies across multiple services/components involved like Active Directory, RDS deployments, Microsoft Azure and its core services (compute, storage & Network).

Please note that this document will primarily focus on the detailed migration process and is NOT a primer for the technologies afore mentioned.

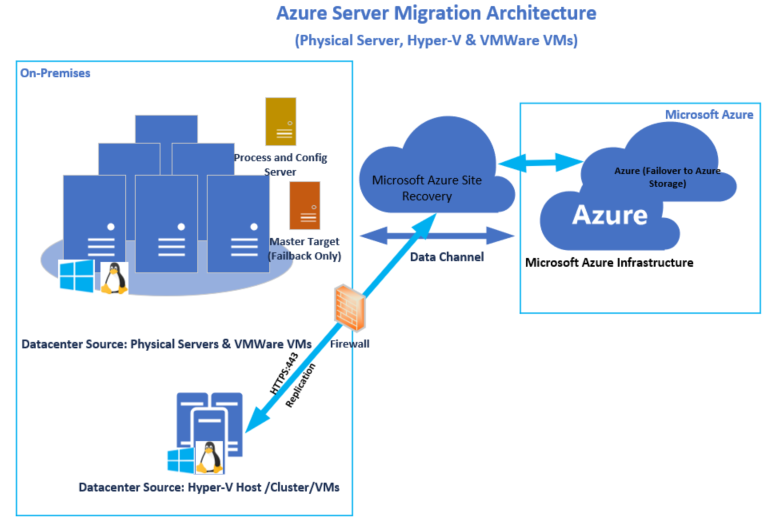
# Azure Server Migration Scenarios

Server migration to Azure covers the below 3 major scenarios.

| Scenarios | Tools | Notes |
| --- | --- | --- |
| Physical Servers | Azure Migrate: Server Assessment Tool | Discover Physical Server  Collect machine metadata and performance metadata and migrate to Azure |
| Hyper-V VMs | Azure Migrate: Server Assessment Tool | Discover Hyper-V Vms  Collect Machine metadata and performance metadata and migrate |
| VMWare VMs | Azure Migrate: Server Assessment Tool | Discover VMWare Vms  Collect Machine metadata and performance metadata and migrate |

# Azure Server Migration Architecture

Below architecture diagram defines 3 scenarios that covers the Physical to Azure Migration, Hyper-V to Azure Migration and VMWare to Azure Migration also includes Windows and Linux Operating System.



# Requirements

Below is a list of requirements for various configurations needed for the deployment of the Migration Process.

* Physical Servers and VMs: List any VMs or servers included in the Assessment workload.
* Storage: List of all the storage configured for servers and capacity included in the workload
* Applications: List any applications included in this Assessment workload.
* Operating Systems: List of any operating systems included in the Assessment workload.
* Dependencies: List any asset dependencies not included in the Assessment workload.

## Operational Requirements

The following is a list of operational requirements:

* The Servers to be migrated are Supported by the deployment method and Healthy
* Active Directory installed and healthy
* ExpressRoute S2S connectivity from On-premises to Azure
* Coordination with Customer on outage is necessary
* Each Application is tested and certified on the utilized resources (Azure)

# Azure Security Policy

Azure Security policy can be configured in 2 ways, one is by deploying the build-in migration security policy and another way is to configure customized policy based on the Infrastructure requirement.

Below is a list of various configurations needed for the deployment of the Security Policy Process.

* Physical Servers and VMs: List any VMs or servers included in the Assessment workload.
* Storage: List of all the storage configured for servers and capacity included in the workload
* Applications: List any applications included in this Assessment workload.

Azure policy reduces the time needed to audit your environments by maintaining all your compliance data in a centralized place. Set guardrails throughout your resources to help ensure cloud compliance and avoid misconfigurations. The security policy implementation helps to automate the external approval process and maintain in core of the Azure Platform. Also, it maintains the cloud spending cost and provide high valuable for investment.

**Security Baseline Policy:** Security Baseline policy should support the cloud adoption design decisions to ensure compliance with governance efforts.

**Asset classification**: All deployed assets must be categorized by criticality and data classification. Classifications must be reviewed by the Cloud Governance team and the application owner before deployment to the cloud.

**Network isolation**: Network subnets containing protected data must be isolated from any other subnets. Network traffic between protected data subnets is to be audited regularly.

**Secure on-premises connectivity**: All connections between the on-premises and cloud networks must take place either through a secure encrypted VPN connection or a dedicated private WAN link.

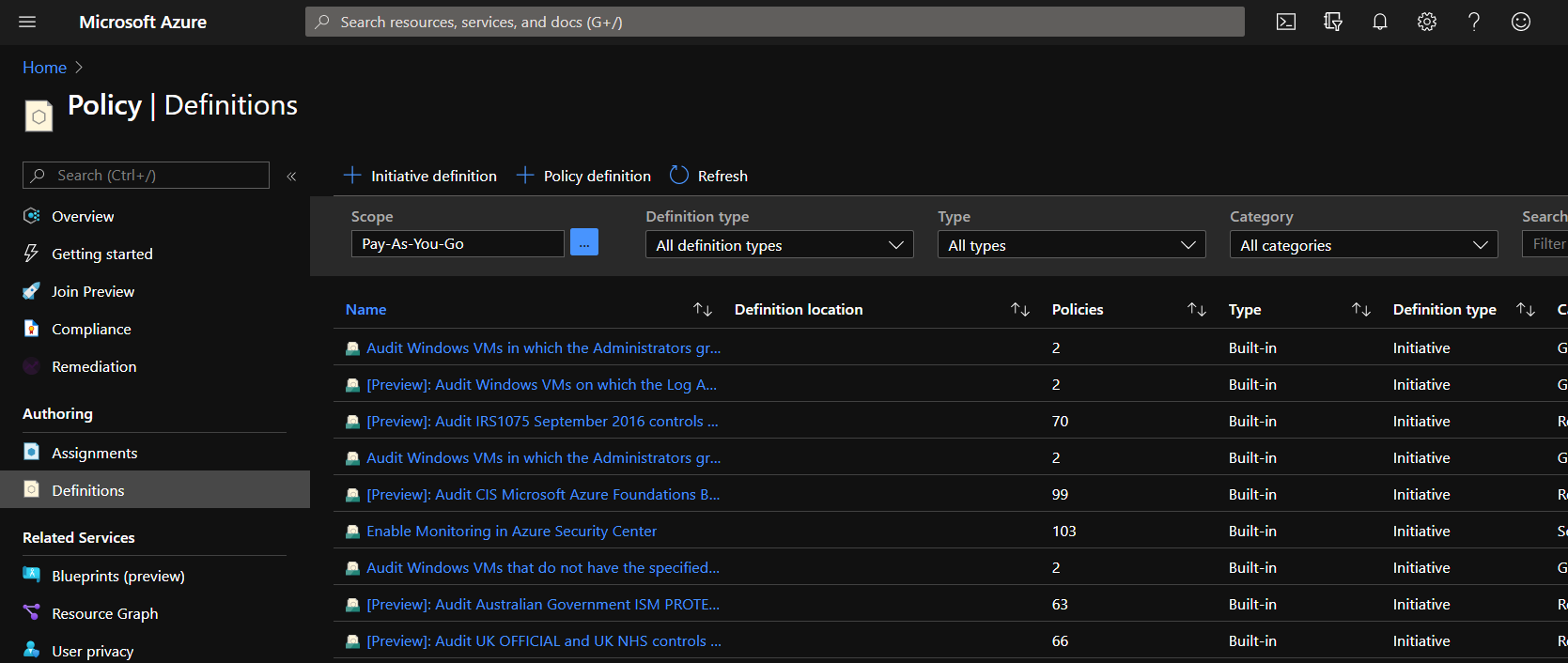
## How to run JSON Policy Script

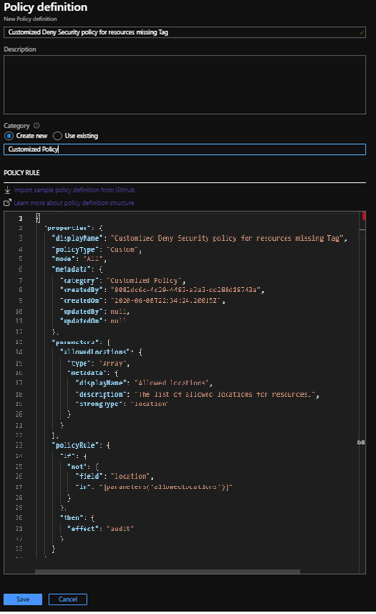
The custom script executes on Azure Virtual machines can be used post deployment and it require custom script extension. Scripts can be downloaded from Azure Storage or GitHub or provided to the Azure portal at extension run time.

The custom script extension integrates with Azure resources manager templates, and can be run using the Azure CLI, Powershell, Azure Portal, or the Azure Virtual Machine REST API.

Policy can be used from the Built-In policy that was already defined in the Azure portal or can be customized by using the existing JSON policy.

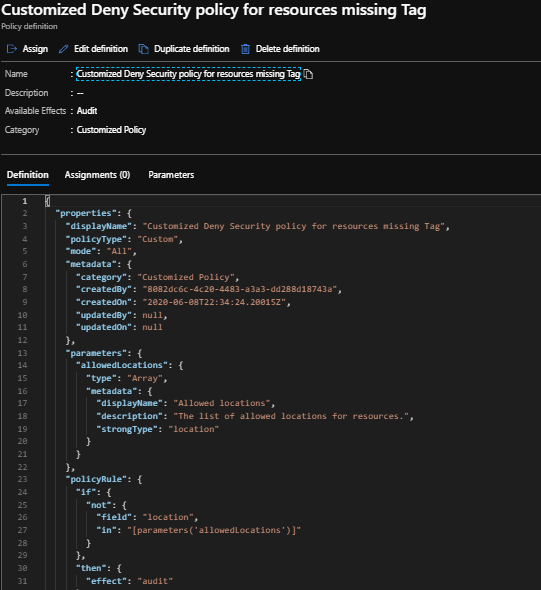
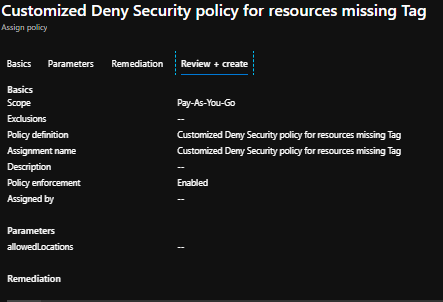
Below is the steps to apply the customized policy in Azure Portal,



Go to the Policy Definitions and click the policy definition

Define the customized policy, Type the Name of the Policy and the Category and click Save. You can also import the policy from GitHub by clicking the Import policy option shown in the above screen.

Assigning the customized policy to the Compute category /Deployed VMs.



Once the Customized policy is assigned, the policy will be enforced.

## Major Azure Policy for security

Microsoft provides security capabilities to protect enterprise Azure subscriptions, Cloud Security’s shared responsibilities model require Azure customers to deliver security in Azure Server Migration. There are 7 major critical areas of security in Azure that customers must follow to ensure their Azure workloads are secure:

1. Security Policy

2. Identify and Access Management

3. Storage Accounts

4. SQL Services

5. Networking

6. Virtual Machines

7. Miscellaneous

1. **Security Policy**

|  |  |  |
| --- | --- | --- |
| Policy Name | Description | Future Policy |
| OS Vulnerabilities is set to ON | Enable OS vulnerabilities recommendations for virtual machines. When this setting is enabled, it analyzes operating system configurations daily to determine issues that could make the virtual machine vulnerable to attack. The policy also recommends configuration changes to correct these vulnerabilities. | [Inbuilt\_OS Vulnerability set to ON Script](https://github.com/Azure/azure-policy/blob/d4a47a82f895c438ed2895c84c1d7f386e904234/built-in-policies/policySetDefinitions/Security%20Center/AzureSecurityCenter.json) |
| Endpoint Protection is set to ON | Enable endpoint protection recommendations for virtual machines. When this setting is enabled, Azure Security Center recommends endpoint protection be provisioned for all Windows virtual machines to help identify and remove viruses, spyware, and other malicious software. | [Inbuilt\_Endpoint Protection Set to ON Script](https://github.com/Azure/azure-policy/blob/d4a47a82f895c438ed2895c84c1d7f386e904234/built-in-policies/policySetDefinitions/Security%20Center/AzureSecurityCenter.json) |
| JIT network access is set to ON | Enable JIT network access for virtual machines. When this setting is enabled, the Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic should be locked down. Just-in-time VM access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed. | [JIT Network Access Set to ON](https://github.com/Azure/azure-policy/blob/d4a47a82f895c438ed2895c84c1d7f386e904234/built-in-policies/policySetDefinitions/Security%20Center/AzureSecurityCenter.json) |

Business Risk for Security Baseline Policy:

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Description | Indicators | Resolution |
| Data breach | Inadvertent exposure or loss of sensitive cloud-hosted data can lead to losing customers, contractual issues, or legal consequences. | Current | Policy statements enforced |
| Service disruption | Outages and other performance issues due to insecure infrastructure interrupts normal operations and can result in lost productivity or lost business. | Mission-critical workloads deployed | Policy statements drafted but not enforced |

1. **Identity & Asset management Baseline Policy**

|  |  |  |
| --- | --- | --- |
| Policy Name | Description | Future Policy |
| Ensure that for all users, MFA is enabled | Enable multi-factor authentication for all user credentials who have write access to Azure resources. Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk. | [Inbuilt\_Ensure all user MFA enabled Script](https://github.com/Azure/azure-policy/blob/d4a47a82f895c438ed2895c84c1d7f386e904234/built-in-policies/policySetDefinitions/Security%20Center/AzureSecurityCenter.json) |
| Ensure that restrict access to Azure AD administration portal is set to yes | Restrict access to Azure AD administration portal to administrators only. Azure AD administrative portal has sensitive data. You should restrict all non-administrators from accessing any Azure AD data in the administration portal to avoid exposure. | [BuiltIn\_Access to Azure AD Script](https://github.com/Azure/azure-policy/blob/d4a47a82f895c438ed2895c84c1d7f386e904234/built-in-policies/policySetDefinitions/Security%20Center/AzureSecurityCenter.json) |

1. **Storage Account Policy**

|  |  |  |
| --- | --- | --- |
| Policy Name | Description | Future Policy |
| Secure transfer required is set to enabled | Enable data encryption is transit. The secure transfer option enhances the security of your storage account by only allowing requests to the storage account by a secure connection. For example, when calling REST APIs to access your storage accounts, you must connect using HTTPS. Any requests using HTTP will be rejected when ‘secure transfer required’ is enabled. When you are using the Azure files service, connection without encryption will fail, including scenarios using SMB 2.1, SMB 3.0 without encryption, and some flavors of the Linux SMB client. | [BuiltIn\_Secure Data Transfer Enable Script](https://github.com/Azure/azure-policy/blob/13cd1036e9faea260c2b1341375e7a76a6f8b41c/built-in-policies/policySetDefinitions/Regulatory%20Compliance/IRAP_Audit.json) |
| Storage service encryption is set to enabled | Enable data encryption at rest for blobs. Storage service encryption protects your data at rest. Azure storage encrypts your data as it’s written in its data centers, and automatically decrypts it for you as you access it. | [BuiltIn\_Storage Service Encryption Script](https://github.com/Azure/azure-policy/blob/d4a47a82f895c438ed2895c84c1d7f386e904234/built-in-policies/policySetDefinitions/Security%20Center/AzureSecurityCenter.json) |

1. **Application and SQL Services**

|  |  |
| --- | --- |
| **Policy Name** | **Future Policy** |
| Auditing is set to ON | [BuiltIn\_Audit ON Script](https://github.com/Azure/azure-policy/blob/d4a47a82f895c438ed2895c84c1d7f386e904234/built-in-policies/policySetDefinitions/Security%20Center/AzureSecurityCenter.json) |
| Thread detection is set to ON | [BuiltIn\_Thread Detection Script](https://github.com/Azure/azure-policy/blob/eac12cb8dd763315872d9f9a700908b7b61340a5/built-in-policies/policyDefinitions/SQL/DeployTdOnSqlServers_Deploy.json) |
| Data Encryption is set to ON | [BuiltIn\_Data Encryption Script](https://github.com/Azure/azure-policy/blob/eac12cb8dd763315872d9f9a700908b7b61340a5/built-in-policies/policyDefinitions/SQL/SqlDBEncryption_Deploy.json) |

1. **Network**

|  |  |  |
| --- | --- | --- |
| Policy Name | Description | Future Policy |
| Disable RDP | The potential security problem with using RDP over the Internet is that attackers can use various brute-force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use your virtual machine as a launch point for compromising other machines on your Azure Virtual Network or even attack networked devices outside of Azure. | [BuiltIn\_NSG\_RDPAccess\_Audit Script](https://github.com/Azure/azure-policy/blob/06063439b7eacacd638c653913700d96bafd00f9/built-in-policies/policyDefinitions/Network/NetworkSecurityGroup_RDPAccess_Audit.json) |
| Disable SSH | The potential security problem with using SSH over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use your virtual machine as a launch point for compromising other machines on your Azure Virtual Network or even attack networked devices outside of Azure. | [BuiltIn\_NSG\_SSHAccess Script](https://github.com/Azure/azure-policy/blob/06063439b7eacacd638c653913700d96bafd00f9/built-in-policies/policyDefinitions/Network/NetworkSecurityGroup_SSHAccess_Audit.json) |

1. **Compute (Virtual Machine)**

|  |  |  |
| --- | --- | --- |
| Policy Name | Description | Future Policy |
| Identify Missing Endpoint protection and Install for Virtual machines | Installing endpoint protection systems (antivirus/anti-malware) provides real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your Azure systems. | [BuiltIn\_Missing Endpoint Protection Script](https://github.com/Azure/azure-policy/blob/eac12cb8dd763315872d9f9a700908b7b61340a5/built-in-policies/policyDefinitions/Security%20Center/ASC_MissingEndpointProtection_Audit.json) |
| Enable latest OS patch updates for Virtual Machines | Ensure Latest OS Patches for virtual machines. Windows and Linux virtual machines should be kept updated to:  Address a specific bug or flaw  Improve an OS or application’s general stability  Fix a security vulnerability | [BuiltIn\_Automatic OS Patching on Virtual Machine Script](https://github.com/Azure/azure-policy/blob/eac12cb8dd763315872d9f9a700908b7b61340a5/built-in-policies/policyDefinitions/Compute/VMSSOSUpgradeHealthCheck_Deny.json) |
| Enforce disk encryption on Virtual machines | Ensure that data disks (non-boot volumes) are encrypted, where possible. Encrypting your IaaS VM’s data disks (non-boot volume) ensures that its entire content is fully unrecoverable without a key and protects the volume from unwarranted reads. | [BuiltIn\_Enforce Disk Encryption Script](https://github.com/Azure/azure-policy/blob/d4a47a82f895c438ed2895c84c1d7f386e904234/built-in-policies/policySetDefinitions/Security%20Center/AzureSecurityCenter.json) |
| Enable VM agent on virtual machines. | Install VM agent on virtual machines. The VM agent must be installed on Azure virtual machines (VMs) in order to enable Azure Security Center for data collection. Security Center collects data from your VMs to assess their security state, provide security recommendations, and alert you to threats. | [BuiltIn\_Azure monitor VM Script](https://github.com/Azure/azure-policy/blob/d4a47a82f895c438ed2895c84c1d7f386e904234/built-in-policies/policySetDefinitions/Monitoring/AzureMonitor_VM.json) |

1. **Miscellaneous (Other Services)**

|  |  |  |
| --- | --- | --- |
| Policy Name | Description | Future Policy |
| Secure the subscription | A secure Azure cloud subscription provides a core foundation upon which subsequent development and deployment activities can be conducted. An engineering team should have the capabilities to deploy and configure security in the subscription including elements such as alerts, ARM policies, RBAC, Security Center policies, JEA, Resource Locks, etc. Likewise, it should be possible to check that all settings are in conformance to a secure baseline. | [BuiltIn\_Secure Monitoring Subscription Script](https://github.com/Azure/azure-policy/blob/d4a47a82f895c438ed2895c84c1d7f386e904234/built-in-policies/policySetDefinitions/Security%20Center/AzureSecurityCenter.json) |
| Do not grant permissions to external accounts | Non-AD accounts (i.e. 123@hotmail.com) subject your cloud assets to undue risk. These accounts are not managed to the same standards as enterprise tenant identities. | [BuiltIn\_Security Baseline Configuration Script](https://github.com/Azure/azure-policy/blob/eac12cb8dd763315872d9f9a700908b7b61340a5/built-in-policies/policySetDefinitions/Guest%20Configuration/GuestConfiguration_AzureBaseline.json) |

Based on the requirement from the customer environment, we can apply built in Security policy and fine tune the requirement. Server Migration Built in security policy available in the [Link](https://microsoft.sharepoint.com/:x:/t/CAFEnablementKitDevelopment/ETUQnY3_0JRAhQA1xr5mn4gB0IMva6Q6c81sT4QQ-Cbucg?e=HcI1hW).

# Appendix A

|  |  |
| --- | --- |
| Reference | Description |
| [Azure RBAC](https://docs.microsoft.com/en-us/azure/role-based-access-control/) | Azure role-based access control (Azure RBAC) is a system that provides fine-grained access management of Azure resources. Using Azure RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. |
| [Microsoft-Cloud-Adoption-Framework-Strategy-and-Plan-Template](https://archcenter.blob.core.windows.net/cdn/fusion/readiness/Microsoft-Cloud-Adoption-Framework-Strategy-and-Plan-Template.docx) | Document decisions as you execute your cloud adoption strategy and plan. |