**ELC - Azure Monitoring and Logging - Proof of Concept (POC)**

**Initial Draft version v1.1**

**Submitted to**

Text, logo

Description automatically generated

**By**

A logo with colorful dots

Description automatically generated

**Wipro Technologies**

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date of Revision** | **Description of Change** | **Reason for Change** | **Reviewed By** |
| 1.1 | 31-Oct-23 | Initial Draft | NA | Kannan & Felix |
|  |  |  |  |  |
|  |  |  |  |  |

**Author/Reviewer/Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Designation** | **Responsibility** | **Date** |
| Ameet Desai | Consultant | Author | 07-Oct-23 |
| Kannan Kuppusamy | Technical Lead | Review | 31-Oct-23 |
| Felix Jebamani | Lead Consultant | Review | 31-Oct-23 |
| Jamshid Abedi | ELC ED, Global Head of Security Engineer | Approval | 00-Oct-23 |

**Table of Contents**

**Objective of the Document…………………….………….………………………………………****…..…………………………….4**

**Executive Summary……………………………………………………………………………****…..…………………………………….4**

[Objective of the Document 3](#_Toc569786176)

[Executive Summary 3](#_Toc1954780259)

[1. Best Practice 01 Activity log should be retained for at least one year. 3](#_Toc253900803)

[1.1 Description 3](#_Toc1943214756)

[1.2 Control Domain 4](#_Toc1124263916)

[1.3 Non-Compliance Message 4](#_Toc1877261563)

[1.4 Policy Definition 4](#_Toc218054458)

[1.5 Error Details 5](#_Toc38566748)

[1.6 Exceptions 5](#_Toc123805321)

[2. Best practice 02 Azure subscriptions should have a log profile for Activity Log. 6](#_Toc787471390)

[2.1 Description 6](#_Toc698977106)

[2.2 Control Domain 6](#_Toc1202081840)

[2.3 Non-Compliance Message 7](#_Toc991776815)

[2.4 Policy Definition 7](#_Toc1716808439)

[2.5 Error Details 8](#_Toc951489992)

[2.6 Exceptions 8](#_Toc1994562015)

[3. Best Practice 03 Azure Monitor should collect activity logs from all regions. 9](#_Toc958898588)

[3.1 Description 9](#_Toc1222418877)

[3.2 Control Domain 9](#_Toc1811100940)

[3.3 Non-Compliance Message 9](#_Toc2096654616)

[3.4 Policy Definition 10](#_Toc782743324)

[3.5 Error Details 16](#_Toc667863361)

[3.6 Exceptions 17](#_Toc887348083)

[4. Scenario 04 Azure Monitor log profile should collect logs for categories 'write,' 'delete,' and 'action'. 18](#_Toc1110389417)

[4.1 Description 18](#_Toc528192419)

[4.2 Control Domain 18](#_Toc250059354)

[4.3 Non-Compliance Message 18](#_Toc2069157383)

[4.5 Error Details 20](#_Toc1300378052)

[4.6 Exceptions 20](#_Toc1190491253)

[5. Best practice 05 Storage account containing the container with activity logs must be encrypted with BYOK. 21](#_Toc1457892908)

[5.1 Description 21](#_Toc904151046)

[5.2 Control Domain 22](#_Toc629303309)

[5.3 Non-Compliance Message 22](#_Toc1843345224)

[5.4 Policy Definition 22](#_Toc1925892257)

[5.5 Error Details 23](#_Toc1729259639)

[5.6 Exceptions 23](#_Toc513404705)

[6. Best practice 06 Log Analytics agent should be installed on your virtual machine for Azure Security Centre monitoring. 24](#_Toc708935834)

[6.1 Description 24](#_Toc1245919645)

[6.2 Control Domain 24](#_Toc1277433333)

[6.3 Non-Compliance Message 24](#_Toc798534614)

[6.4 Policy Definition 25](#_Toc304736920)

[6.5 Error Details 26](#_Toc567027554)

[6.6 Exceptions 26](#_Toc805159336)

[7. Best practice 07 Resource logs in IoT Hub should be enabled. 27](#_Toc631130381)

[7.1 Description 28](#_Toc1822890369)

[7.2 Control Domain 28](#_Toc94373685)

[7.3 Non-Compliance Message 28](#_Toc1322092516)

[7.4 Policy Definition 28](#_Toc1283727653)

[7.5 Error Details 30](#_Toc1396107127)

[7.6 Exceptions 30](#_Toc261468088)

[8. Best practice 08 Resource logs in Logic Apps should be enabled. 31](#_Toc78133655)

[8.1 Description Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised 32](#_Toc1409472826)

[8.2 Control Domain 32](#_Toc1787972200)

[8.3 Non-Compliance Message 32](#_Toc1739824856)

[8.4 Policy Definition 32](#_Toc1669731452)

[8.5 Error Details 34](#_Toc2125869485)

[8.6 Exceptions 34](#_Toc643022234)

[9. Best practice 09 Resource logs in Key Vault should be enabled. 36](#_Toc2070184577)

[9.1 Description 36](#_Toc1239558664)

[9.2 Control Domain 36](#_Toc1309664156)

[9.3 Non-Compliance Message 36](#_Toc639697312)

[9.4 Policy Definition 36](#_Toc113976353)

[9.5 Error Details 39](#_Toc1376454970)

[9.6 Exceptions 39](#_Toc84193625)

[10. Best practice 10 Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring. 40](#_Toc227157862)

[10.1 Description 41](#_Toc470493870)

[10.2 Control Domain 41](#_Toc43712582)

[10.3 Non-Compliance Message 41](#_Toc1407768051)

[10.4 Policy Definition 41](#_Toc1818262076)

[10.5 Error Details 42](#_Toc171874698)

[10.6 Exceptions 42](#_Toc1387692600)

[11.0 Appendix 43](#_Toc969796405)

[11.1 Abbreviations 43](#_Toc1950800284)

[12.0 Reference Document links 44](#_Toc786025514)

**Objective of the Document**

In accordance with the Global Information Security Policy, Monitoring and Logging procedure will ensure that Estee Lauder Companies Inc. (ELC) is able to capture and analyse activity within the Azure cloud environment effectively and efficiently. It also helps in, the sufficient detection and identification capabilities needed to support information security. This procedure enables the technology controls and processes needed to ensure transparency and auditability across the technology environment, which will empower ELC’s ability to perform investigations, regulatory audits, and incident and problem management...etc.

**Executive Summary**

In any IT industry Monitoring and Logging play’s significant role. Every day there are new ways to steal, or valuable data gets compromised. To overcome this, we should build and configure strong monitoring and Logging in our environment to address everyday challenges we are facing in securing our corporate information. There are several tools and technologies available and making use of them to safeguard our data and information integrity. In this document we are focussing on Azure policy service to monitor our Azure resources and its logs.

# **1. Best Practice 01 Activity log should be retained for at least one year.**

**1.1 Description** This policy audits the activity log if the retention is not set for 365 days or forever (retention days set to 0).

**1.2 Control Domain** CIS Microsoft Azure Foundations Benchmark recommendation 5.1.2, CMMC L3 SI.2.217.

**1.3 Non-Compliance Message** In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended that Activity log should be retained for at least one year. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **1.4 Policy Definition**

{

"properties": {

"displayName": "Activity log should be retained for at least one year",

"policyType": "BuiltIn",

"mode": "All",

"description": "This policy audits the activity log if the retention is not set for 365 days or forever (retention days set to 0).",

"metadata": {

"version": "1.0.0",

"category": "Monitoring"

},

"parameters": {

"effect": {

"type": "String",

"metadata": {

"displayName": "Effect",

"description": "Enable or disable the execution of the policy"

},

"allowedValues": [

"AuditIfNotExists",

"Disabled"

],

"defaultValue": "AuditIfNotExists"

}

},

"policyRule": {

"if": {

"field": "type",

"equals": "Microsoft.Resources/subscriptions"

},

"then": {

"effect": "[parameters('effect')]",

"details": {

"type": "Microsoft.Insights/logProfiles",

"existenceCondition": {

"anyOf": [

{

"allOf": [

{

"field": "Microsoft.Insights/logProfiles/retentionPolicy.enabled",

"equals": "true"

},

{

"field": "Microsoft.Insights/logProfiles/retentionPolicy.days",

"equals": "365"

}

]

},

{

"allOf": [

{

"field": "Microsoft.Insights/logProfiles/retentionPolicy.enabled",

"equals": "false"

},

{

"field": "Microsoft.Insights/logProfiles/retentionPolicy.days",

"equals": "0"

}

]

}

]

}

}

}

}

},

"id": "/providers/Microsoft.Authorization/policyDefinitions/b02aacc0-b073-424e-8298-42b22829ee0a",

"type": "Microsoft.Authorization/policyDefinitions",

"name": "b02aacc0-b073-424e-8298-42b22829ee0a"

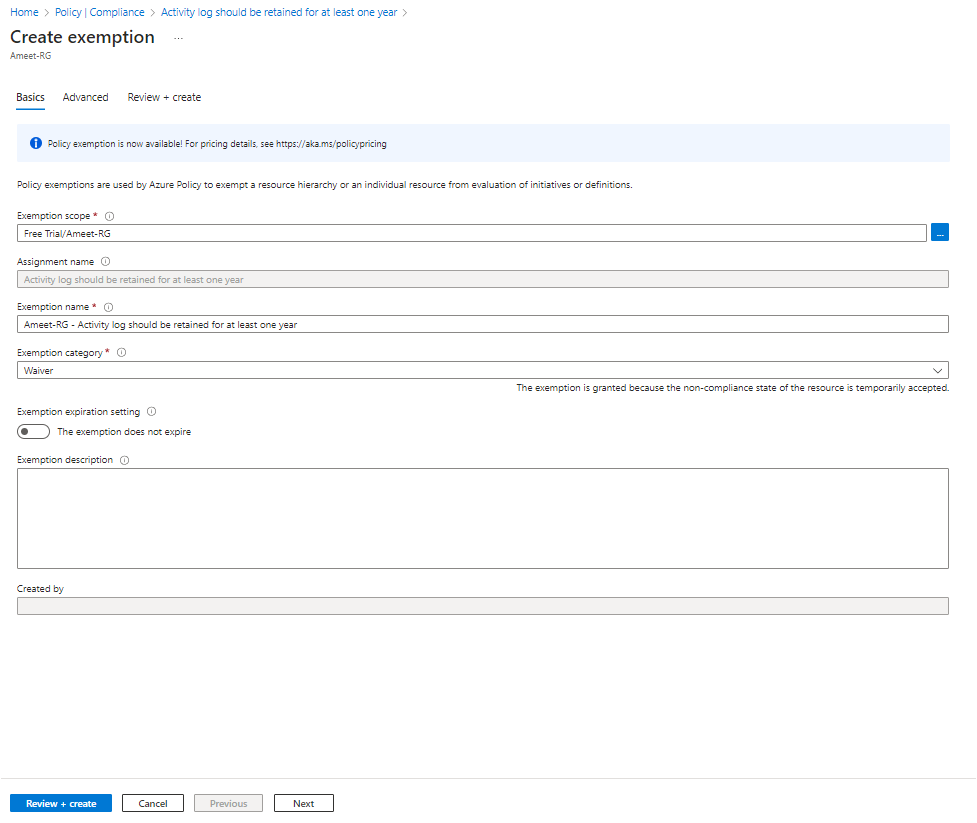
}

**1.5 Error Details** The location of the error details depends on what aspect of Azure Policy you are working with & error summary details.

**1.6 Exceptions** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

A screenshot of a computer

Description automatically generatedFigure 2 Select the policy, Click on Create Exemption.

Figure 3 Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **2. Best practice 02 Azure subscriptions should have a** **log profile for Activity Log.**

**2.1 Description** This policy ensures if a log profile is enabled for exporting activity logs. It audits if there is no log profile created to export the logs either to a storage account or to an event hub.

**2.2 Control Domain** CIS Microsoft Azure Foundations Benchmark recommendation 5.1.1, CMMC L3 AU.2.041, CMMC L3 CM.2.065, CMMC L3 SI.2.217.

**2.3 Non-Compliance Message** In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended that Azure subscriptions should have a log profile for Activity Log. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **2.4 Policy Definition**

{

"properties": {

"displayName": "Azure subscriptions should have a log profile for Activity Log",

"policyType": "BuiltIn",

"mode": "All",

"description": "This policy ensures if a log profile is enabled for exporting activity logs. It audits if there is no log profile created to export the logs either to a storage account or to an event hub.",

"metadata": {

"version": "1.0.0",

"category": "Monitoring"

},

"parameters": {

"effect": {

"type": "String",

"metadata": {

"displayName": "Effect",

"description": "Enable or disable the execution of the policy"

},

"allowedValues": [

"AuditIfNotExists",

"Disabled"

],

"defaultValue": "AuditIfNotExists"

}

},

"policyRule": {

"if": {

"field": "type",

"equals": "Microsoft.Resources/subscriptions"

},

"then": {

"effect": "[parameters('effect')]",

"details": {

"type": "Microsoft.Insights/logProfiles",

"existenceCondition": {

"field": "Microsoft.Insights/logProfiles/categories",

"exists": "true"

}

}

}

}

},

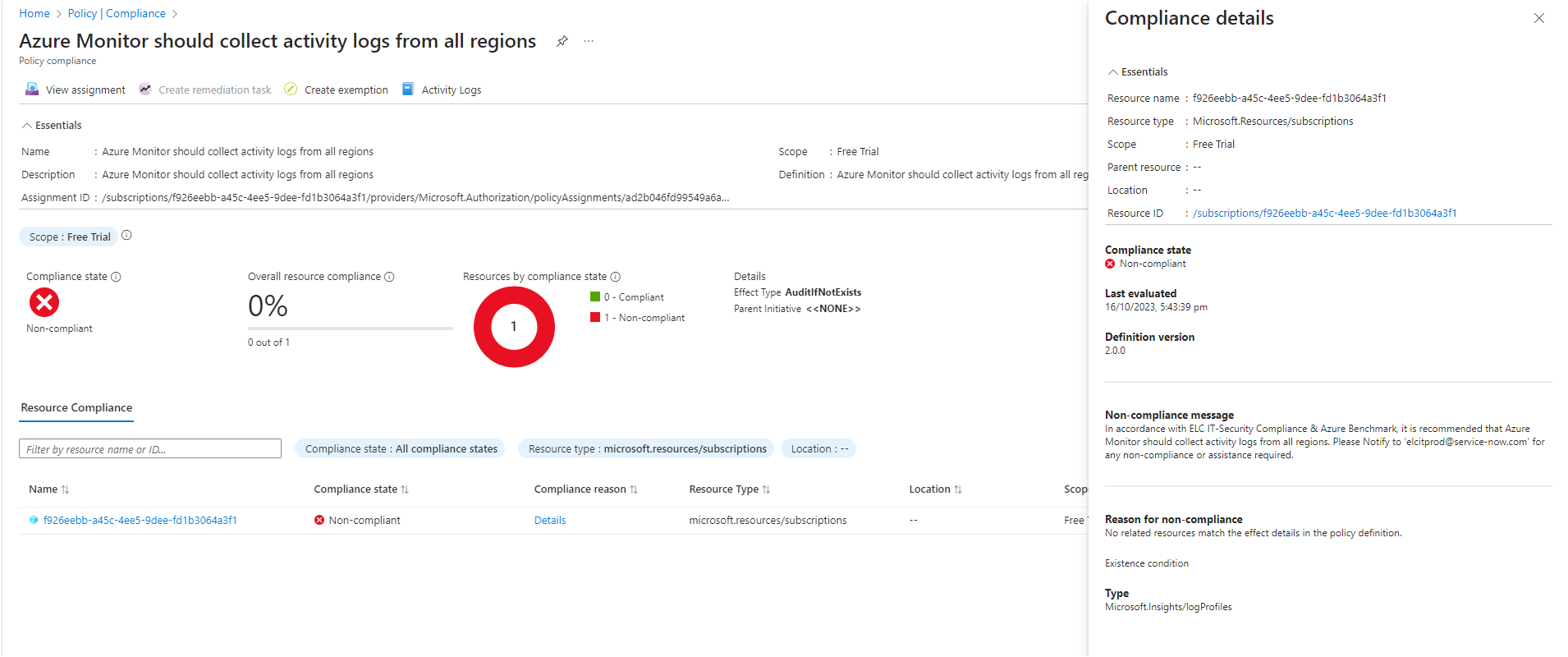
"id": "/providers/Microsoft.Authorization/policyDefinitions/7796937f-307b-4598-941c-67d3a05ebfe7",

"type": "Microsoft.Authorization/policyDefinitions",

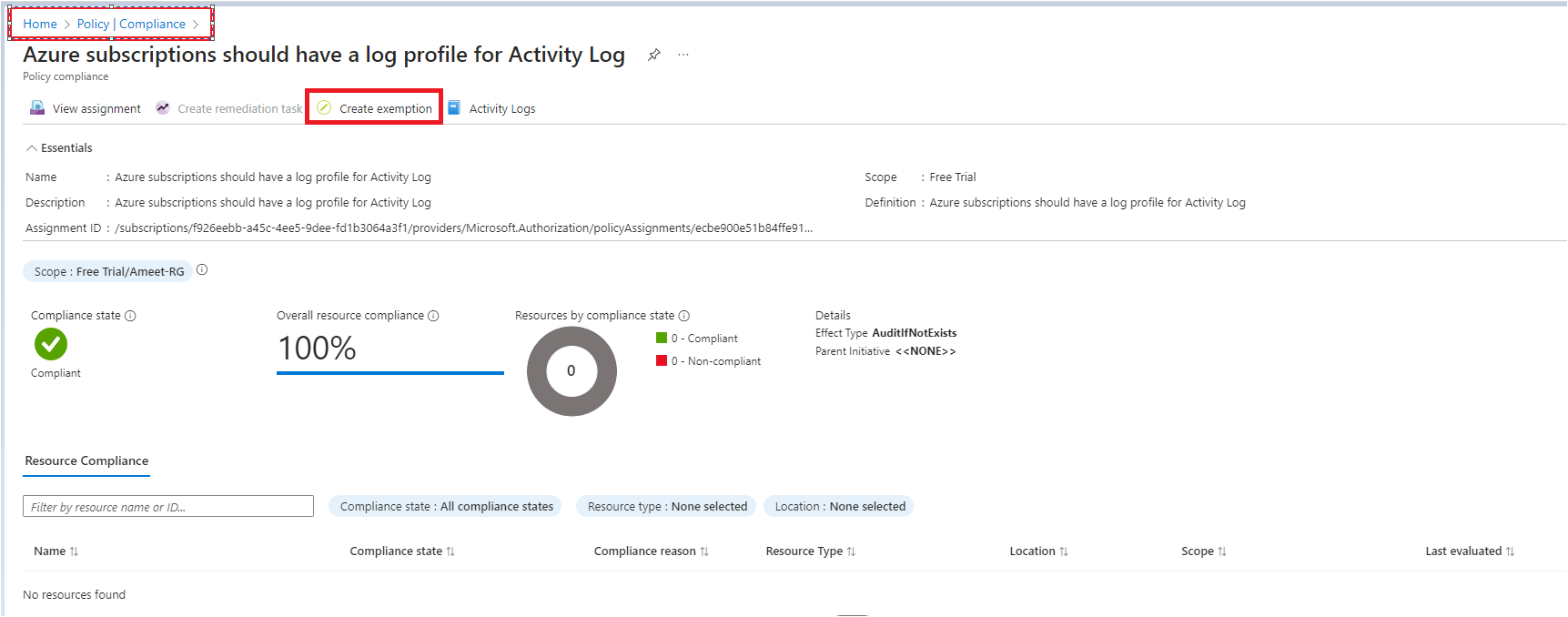
"name": "7796937f-307b-4598-941c-67d3a05ebfe7"

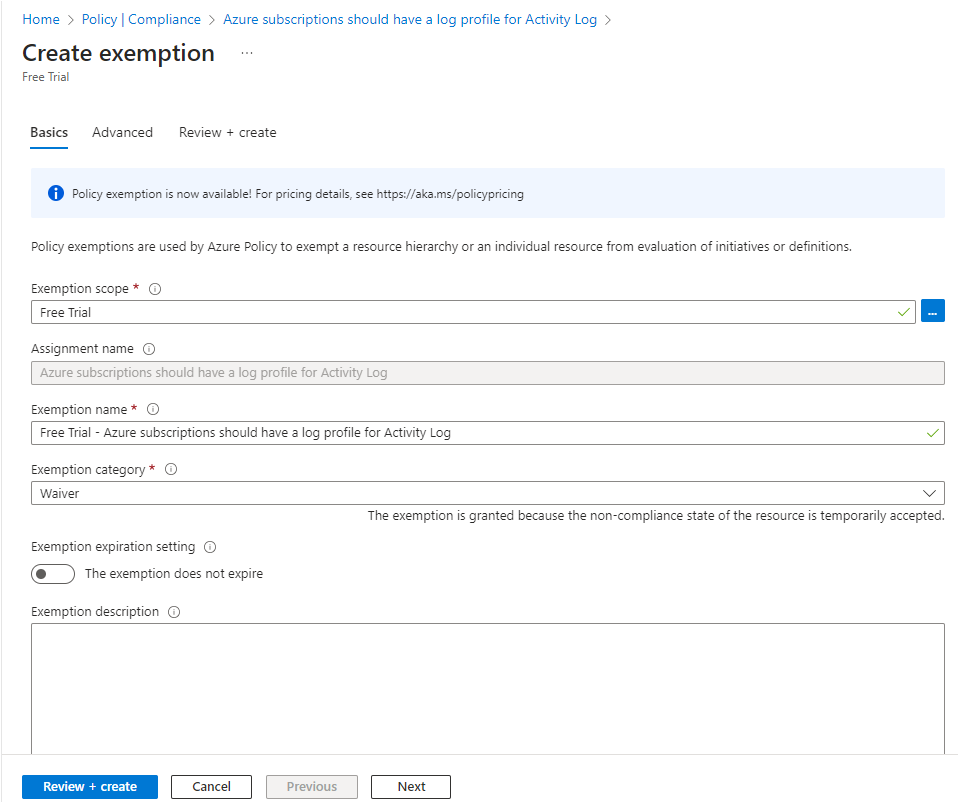
}

**2.5 Error Details** The location of the error details depends on what aspect of Azure Policy you are working with & error summary details.

Figure 1 – Error details

**2.6 Exceptions** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/Resource.

Figure 2 - Select the policy, Click on Create Exemption.

Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **3. Best Practice 03 Azure Monitor should collect activity logs from all regions.**

**3.1 Description** This policy audits the Azure Monitor log profile which does not export activities from all Azure supported regions including global.

**3.2 Control Domain** CIS Microsoft Azure Foundations Benchmark recommendation 5.1.4, CMMC L3 AU.2.041, CMMC L3 CM.2.065, Azure Policy built-in policy definitions.

**3.3 Non-Compliance Message** In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended that Azure Monitor should collect activity logs from all regions. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **3.4 Policy Definition**

{

"properties": {

"displayName": "Azure Monitor should collect activity logs from all regions",

"policyType": "BuiltIn",

"mode": "All",

"description": "This policy audits the Azure Monitor log profile which does not export activities from all Azure supported regions including global.",

"metadata": {

"version": "2.0.0",

"category": "Monitoring"

},

"parameters": {

"effect": {

"type": "String",

"metadata": {

"displayName": "Effect",

"description": "Enable or disable the execution of the policy"

},

"allowedValues": [

"AuditIfNotExists",

"Disabled"

],

"defaultValue": "AuditIfNotExists"

}

},

"policyRule": {

"if": {

"field": "type",

"equals": "Microsoft.Resources/subscriptions"

},

"then": {

"effect": "[parameters('effect')]",

"details": {

"type": "Microsoft.Insights/logProfiles",

"existenceCondition": {

"allOf": [

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "australiacentral"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "australiacentral2"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "australiaeast"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "australiasoutheast"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "brazilsouth"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "brazilsoutheast"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "canadacentral"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "canadaeast"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "centralindia"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "centralus"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "eastasia"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "eastus"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "eastus2"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "francecentral"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "francesouth"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "germanynorth"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "germanywestcentral"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "japaneast"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "japanwest"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "jioindiawest"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "koreacentral"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "koreasouth"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "northcentralus"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "northeurope"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "norwayeast"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "norwaywest"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "southafricanorth"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "southafricawest"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "southcentralus"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "southeastasia"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "southindia"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "switzerlandnorth"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "switzerlandwest"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "uaecentral"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "uaenorth"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "uksouth"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "ukwest"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "westcentralus"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "westeurope"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "westindia"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "westus"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "westus2"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "westus3"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/locations[\*]",

"notEquals": "global"

}

}

]

}

}

}

}

},

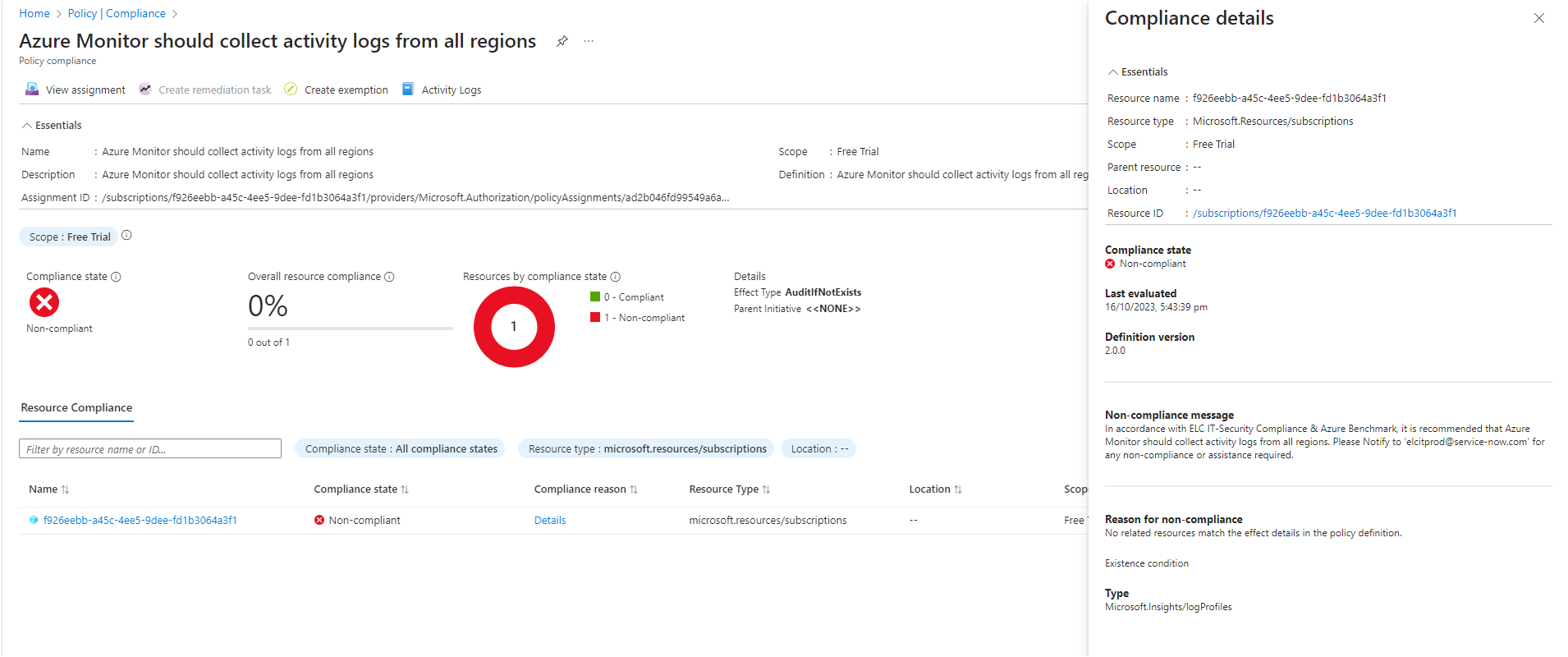
"id": "/providers/Microsoft.Authorization/policyDefinitions/41388f1c-2db0-4c25-95b2-35d7f5ccbfa9",

"type": "Microsoft.Authorization/policyDefinitions",

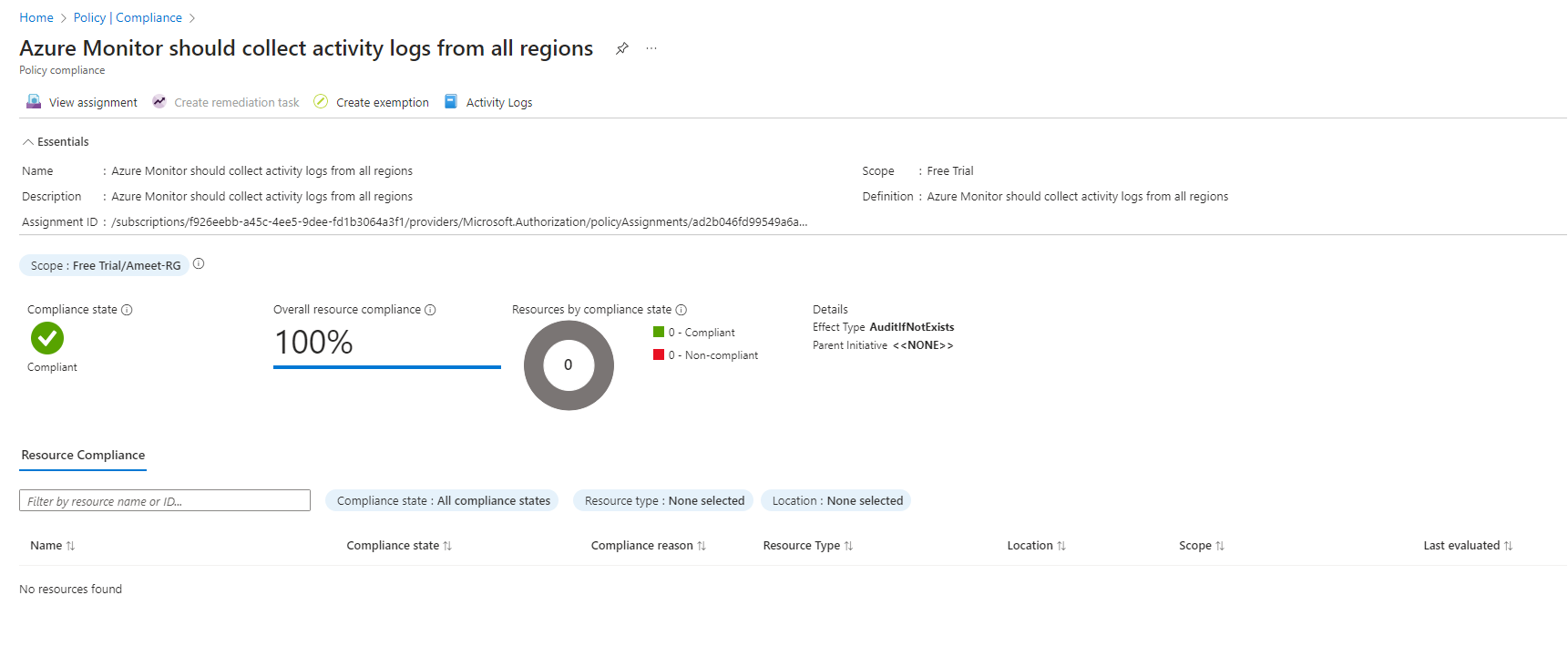
"name": "41388f1c-2db0-4c25-95b2-35d7f5ccbfa9"

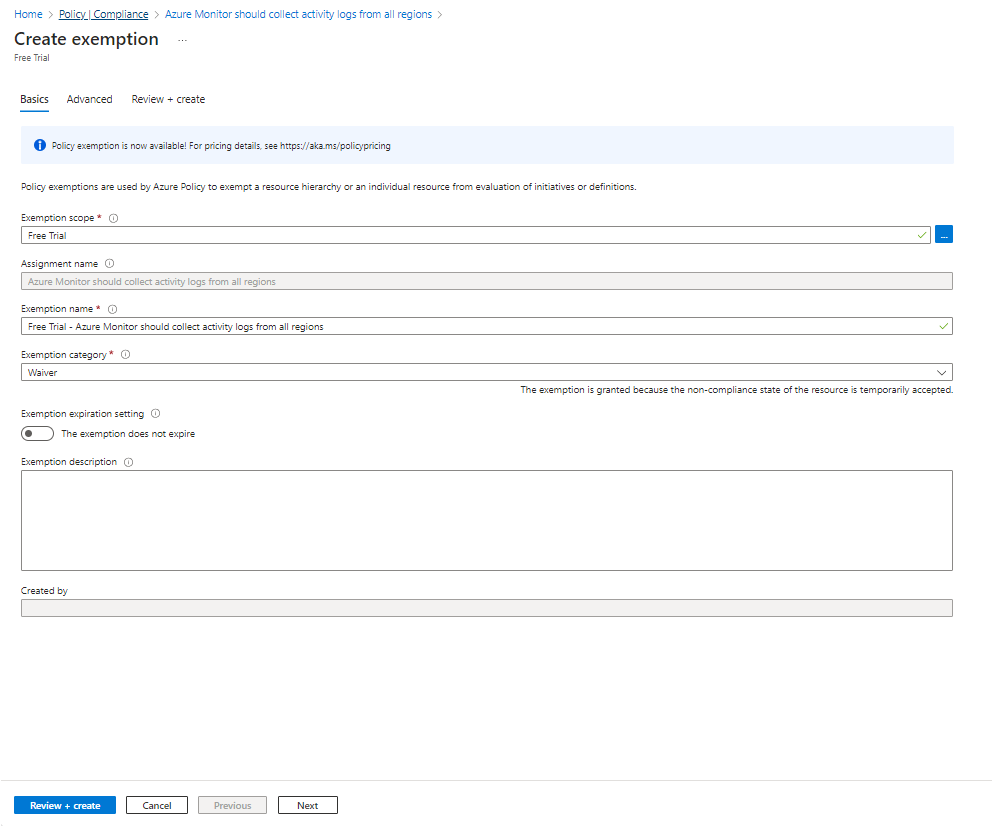
}

**3.5 Error Details** The location of the error details depends on what aspect of Azure Policy you are working with & error summary details.

Figure 1 Error details

**3.6 Exceptions** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/Resource.

Figure 2 Select the policy, Click on Create Exemption.

Figure 3 Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **4. Scenario 04 Azure Monitor log profile should collect logs for categories 'write,' 'delete,' and 'action'.**

**4.1 Description** This policy ensures that a log profile collects logs for categories 'write,' 'delete,' and 'action'.

**4.2 Control Domain** CIS Microsoft Azure Foundations Benchmark recommendation 5.1.3, CMMC L3 SI.2.217, 1219.09ab3System.10-09.ab(HIPAA HITRUST 9.2).

**4.3 Non-Compliance Message** In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended that Azure Monitor log profile should collect logs for categories 'write,' 'delete,' and 'action'. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

**4.4 Policy Definition**

{

"properties": {

"displayName": "Azure Monitor log profile should collect logs for categories 'write,' 'delete,' and 'action'",

"policyType": "BuiltIn",

"mode": "All",

"description": "This policy ensures that a log profile collects logs for categories 'write,' 'delete,' and 'action'",

"metadata": {

"version": "1.0.0",

"category": "Monitoring"

},

"parameters": {

"effect": {

"type": "String",

"metadata": {

"displayName": "Effect",

"description": "Enable or disable the execution of the policy"

},

"allowedValues": [

"AuditIfNotExists",

"Disabled"

],

"defaultValue": "AuditIfNotExists"

}

},

"policyRule": {

"if": {

"field": "type",

"equals": "Microsoft.Resources/subscriptions"

},

"then": {

"effect": "[parameters('effect')]",

"details": {

"type": "Microsoft.Insights/logprofiles",

"existenceCondition": {

"allOf": [

{

"not": {

"field": "Microsoft.Insights/logProfiles/categories[\*]",

"notEquals": "Write"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/categories[\*]",

"notEquals": "Delete"

}

},

{

"not": {

"field": "Microsoft.Insights/logProfiles/categories[\*]",

"notEquals": "Action"

}

}

]

}

}

}

}

},

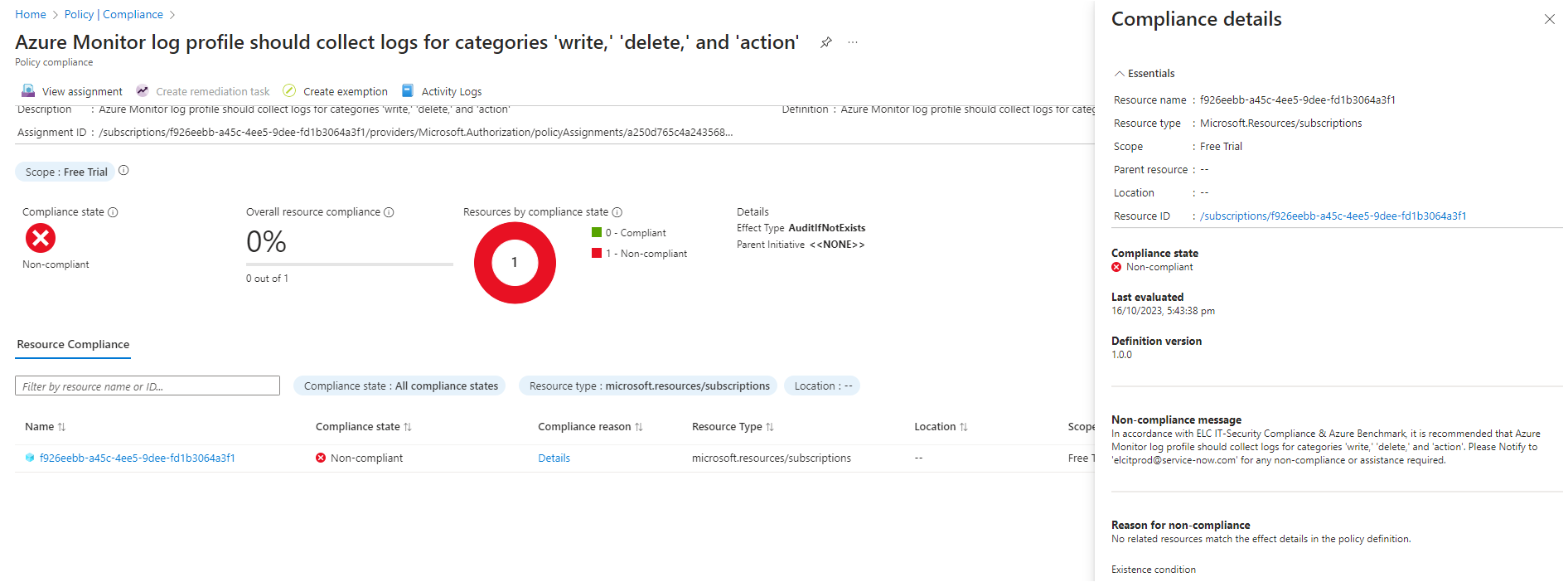
"id": "/providers/Microsoft.Authorization/policyDefinitions/1a4e592a-6a6e-44a5-9814-e36264ca96e7",

"type": "Microsoft.Authorization/policyDefinitions",

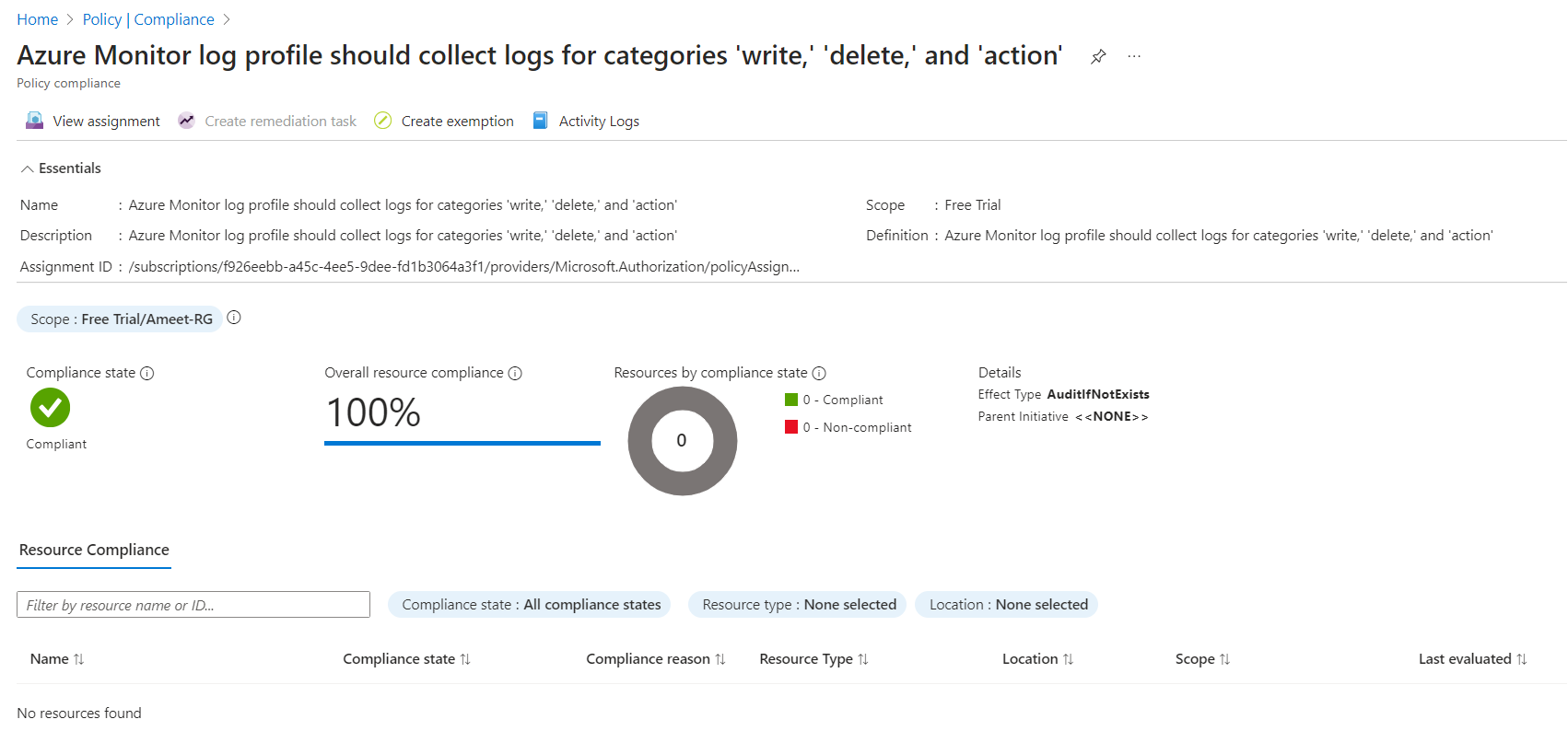
"name": "1a4e592a-6a6e-44a5-9814-e36264ca96e7"

}

**4.5 Error Details** The location of the error details depends on what aspect of Azure Policy you are working with & error summary details.

Figure 1 Error details

**4.6 Exceptions** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/Resource.

Figure 2 Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generated Figure 3 Select the Exemption Scope (Subscription/ Resource Group / Resource).

# 5. **Best practice 05 Storage account containing the container with activity logs must be encrypted with** **BYOK.**

**5.1 Description** This policy audits if the Storage account containing the container with activity logs is encrypted with BYOK. The policy works only if the storage account lies on the same subscription as activity logs by design. More information on Azure Storage encryption at rest can be found here https://aka.ms/azurestoragebyok.

**5.2 Control Domain** CIS Microsoft Azure Foundations Benchmark recommendation 5.1.6, CIS Microsoft Azure Foundations Benchmark recommendation 5.1.4, NZISM Security Benchmark AC-19, RMiT 10.53.

**5.3 Non-Compliance Message** In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended that Storage account containing the container with activity logs must be encrypted with BYOK. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **5.4 Policy Definition**

{

"properties": {

"displayName": "Storage account containing the container with activity logs must be encrypted with BYOK",

"policyType": "BuiltIn",

"mode": "All",

"description": "This policy audits if the Storage account containing the container with activity logs is encrypted with BYOK. The policy works only if the storage account lies on the same subscription as activity logs by design. More information on Azure Storage encryption at rest can be found here https://aka.ms/azurestoragebyok. ",

"metadata": {

"version": "1.0.0",

"category": "Monitoring"

},

"parameters": {

"effect": {

"type": "String",

"metadata": {

"displayName": "Effect",

"description": "Enable or disable the execution of the policy"

},

"allowedValues": [

"AuditIfNotExists",

"Disabled"

],

"defaultValue": "AuditIfNotExists"

}

},

"policyRule": {

"if": {

"allOf": [

{

"field": "type",

"equals": "Microsoft.Insights/logProfiles"

},

{

"field": "Microsoft.Insights/logProfiles/storageAccountId",

"exists": "true"

}

]

},

"then": {

"effect": "[parameters('effect')]",

"details": {

"type": "Microsoft.Storage/storageAccounts",

"existenceScope": "subscription",

"existenceCondition": {

"allOf": [

{

"value": "[contains(field('Microsoft.Insights/logProfiles/storageAccountId'), subscription().Id)]",

"equals": "true"

},

{

"field": "name",

"equals": "[last(split(field('Microsoft.Insights/logProfiles/storageAccountId'),'/'))]"

},

{

"field": "Microsoft.Storage/storageAccounts/encryption.keySource",

"equals": "Microsoft.Keyvault"

}

]

}

}

}

}

},

"id": "/providers/Microsoft.Authorization/policyDefinitions/fbb99e8e-e444-4da0-9ff1-75c92f5a85b2",

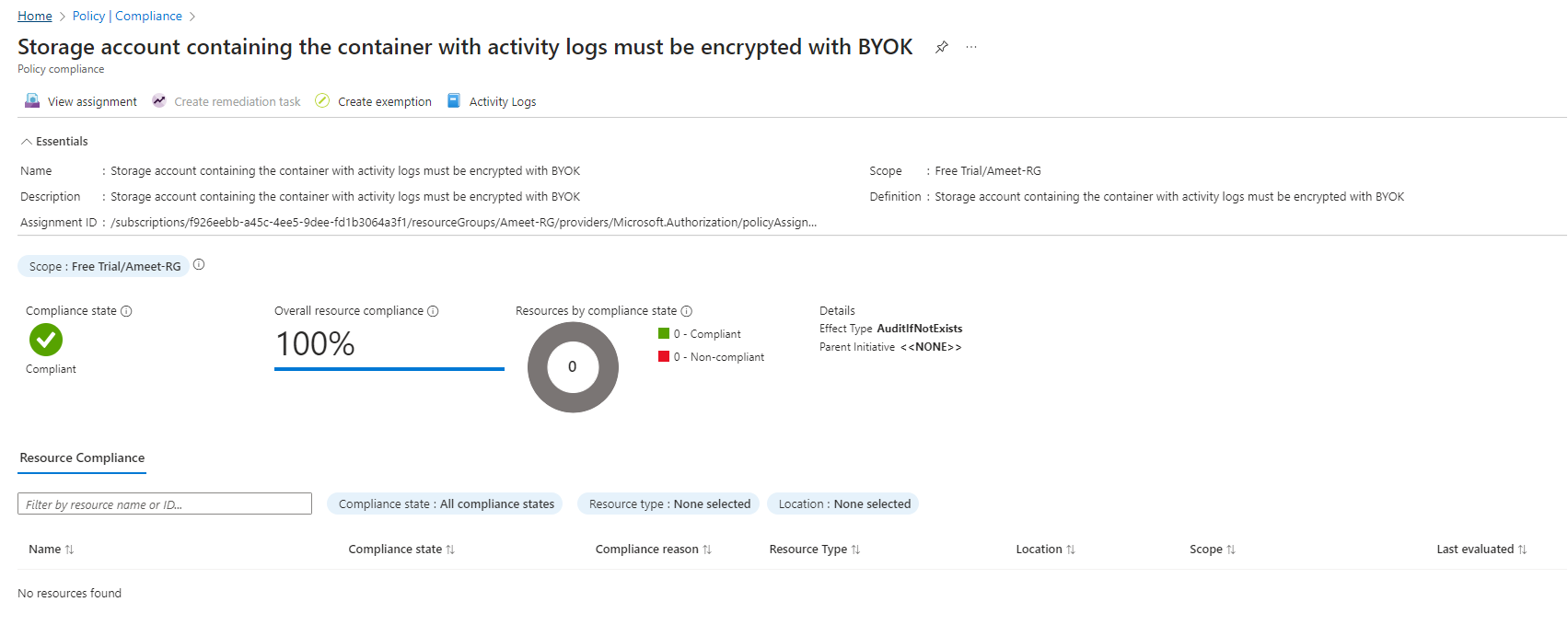
"type": "Microsoft.Authorization/policyDefinitions",

"name": "fbb99e8e-e444-4da0-9ff1-75c92f5a85b2"

}

**5.5 Error Details** The location of the error details depends on what aspect of Azure Policy you are working with & error summary details.

**5.6 Exceptions** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/Resource.

Figure 2 - Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generatedFigure 3 Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **6.** **Best practice 06 Log Analytics agent should be installed on your virtual machine for Azure Security Centre monitoring.**

**6.1 Description** This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Centre uses to monitor for security vulnerabilities and threats.

**6.2 Control Domain** Microsoft cloud security benchmark LT-5,

**6.3 Non-Compliance Message** In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended that Log Analytics agent should be installed on your virtual machine for Azure Security Centre monitoring. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **6.4 Policy Definition**

{

 "properties": {

    "displayName": "Log Analytics agent should be installed on your virtual machine for Azure Security Center monitoring",

    "policyType": "BuiltIn",

    "mode": "All",

    "description": "This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Center uses to monitor for security vulnerabilities and threats",

    "metadata": {

      "version": "1.0.0",

      "category": "Security Center"

    },

    "parameters": {

      "effect": {

        "type": "String",

        "metadata": {

          "displayName": "Effect",

          "description": "Enable or disable the execution of the policy"

        },

        "allowedValues": [

          "AuditIfNotExists",

          "Disabled"

        ],

        "defaultValue": "AuditIfNotExists"

      }

    },

    "policyRule": {

      "if": {

        "field": "type",

        "in": [

          "Microsoft.ClassicCompute/virtualMachines",

          "Microsoft.Compute/virtualMachines"

        ]

      },

      "then": {

        "effect": "[parameters('effect')]",

        "details": {

          "type": "Microsoft.Security/assessments",

          "name": "d1db3318-01ff-16de-29eb-28b344515626",

          "existenceCondition": {

            "field": "Microsoft.Security/assessments/status.code",

            "in": [

              "NotApplicable",

              "Healthy"

            ]

          }

        }

      }

    }

  },

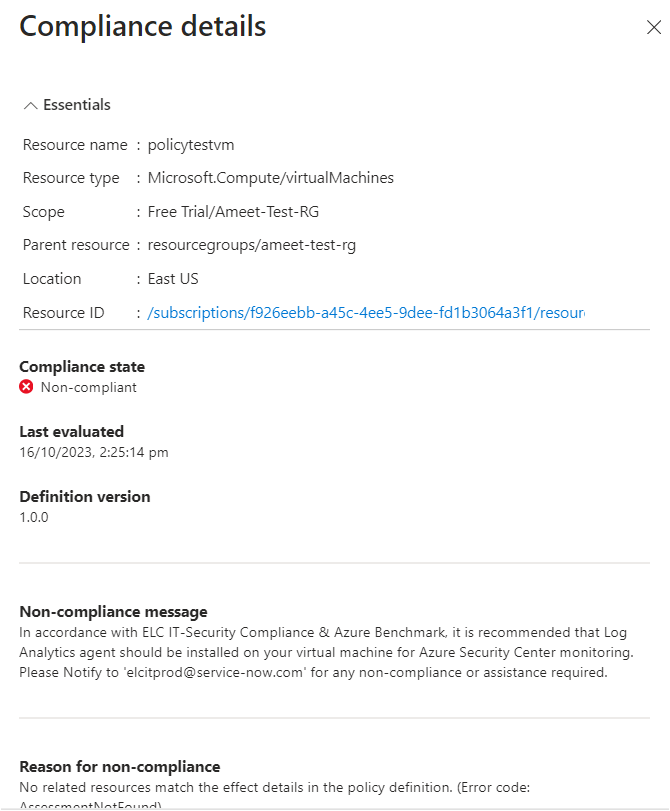
  "id": "/providers/Microsoft.Authorization/policyDefinitions/a4fe33eb-e377-4efb-ab31-0784311bc499",

  "type": "Microsoft.Authorization/policyDefinitions",

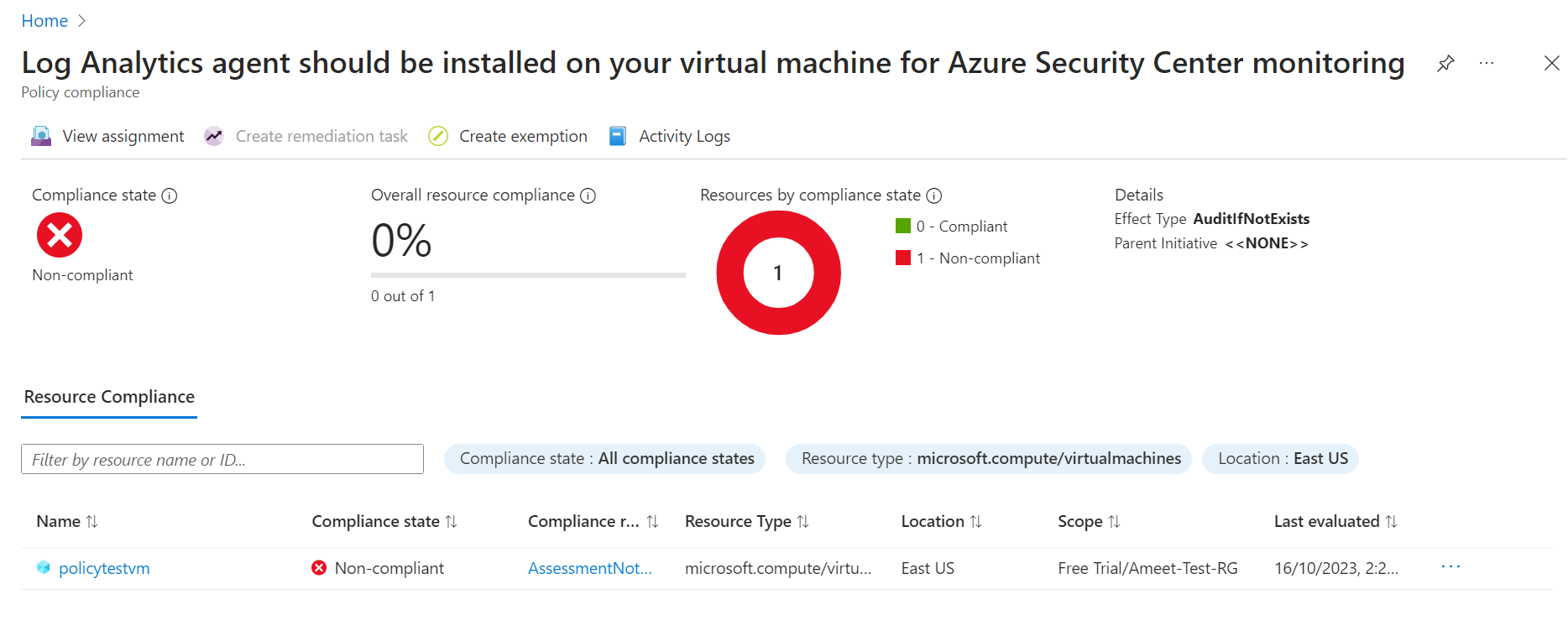
  "name": "a4fe33eb-e377-4efb-ab31-0784311bc499"

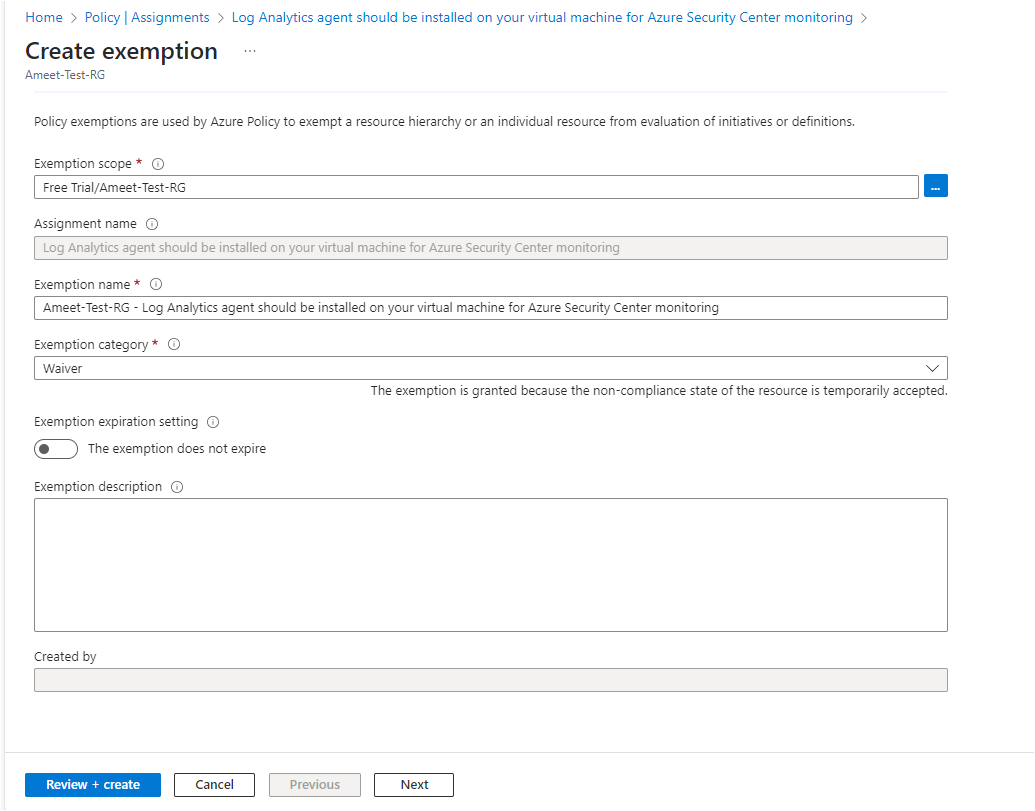
}

**6.5 Error Details** The location of the error details depends on what aspect of Azure Policy you are working with & error summary details.

Figure 1 Error details

**6.6 Exceptions** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

Figure 2 Select the policy, Click on Create Exemption.

Figure 3 Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **7.** **Best practice 07** **Resource logs in IoT Hub should be enabled.**

**7.1 Description** Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised.

**7.2 Control Domain** CMMC L3 AU.3.048, 1204.09aa1System.3-09.aa, NZISM Security Benchmark AC-17.

**7.3 Non-Compliance Message** In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended Resource logs in IoT Hub should be enabled. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **7.4 Policy Definition**

{

"properties": {

"displayName": "Resource logs in IoT Hub should be enabled",

"policyType": "BuiltIn",

"mode": "Indexed",

"description": "Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised",

"metadata": {

"version": "3.1.0",

"category": "Internet of Things"

},

"parameters": {

"effect": {

"type": "String",

"metadata": {

"displayName": "Effect",

"description": "Enable or disable the execution of the policy"

},

"allowedValues": [

"AuditIfNotExists",

"Disabled"

],

"defaultValue": "AuditIfNotExists"

},

"requiredRetentionDays": {

"type": "String",

"metadata": {

"displayName": "Required retention (days)",

"description": "The required resource logs retention in days"

},

"defaultValue": "365"

}

},

"policyRule": {

"if": {

"field": "type",

"equals": "Microsoft.Devices/IotHubs"

},

"then": {

"effect": "[parameters('effect')]",

"details": {

"type": "Microsoft.Insights/diagnosticSettings",

"existenceCondition": {

"count": {

"field": "Microsoft.Insights/diagnosticSettings/logs[\*]",

"where": {

"anyOf": [

{

"allOf": [

{

"field": "Microsoft.Insights/diagnosticSettings/logs[\*].retentionPolicy.enabled",

"equals": "true"

},

{

"anyOf": [

{

"field": "Microsoft.Insights/diagnosticSettings/logs[\*].retentionPolicy.days",

"equals": "0"

},

{

"value": "[padLeft(current('Microsoft.Insights/diagnosticSettings/logs[\*].retentionPolicy.days'), 3, '0')]",

"greaterOrEquals": "[padLeft(parameters('requiredRetentionDays'), 3, '0')]"

}

]

},

{

"field": "Microsoft.Insights/diagnosticSettings/logs.enabled",

"equals": "true"

}

]

},

{

"allOf": [

{

"not": {

"field": "Microsoft.Insights/diagnosticSettings/logs[\*].retentionPolicy.enabled",

"equals": "true"

}

},

{

"field": "Microsoft.Insights/diagnosticSettings/logs.enabled",

"equals": "true"

}

]

}

]

}

},

"greaterOrEquals": 1

}

}

}

}

},

"id": "/providers/Microsoft.Authorization/policyDefinitions/383856f8-de7f-44a2-81fc-e5135b5c2aa4",

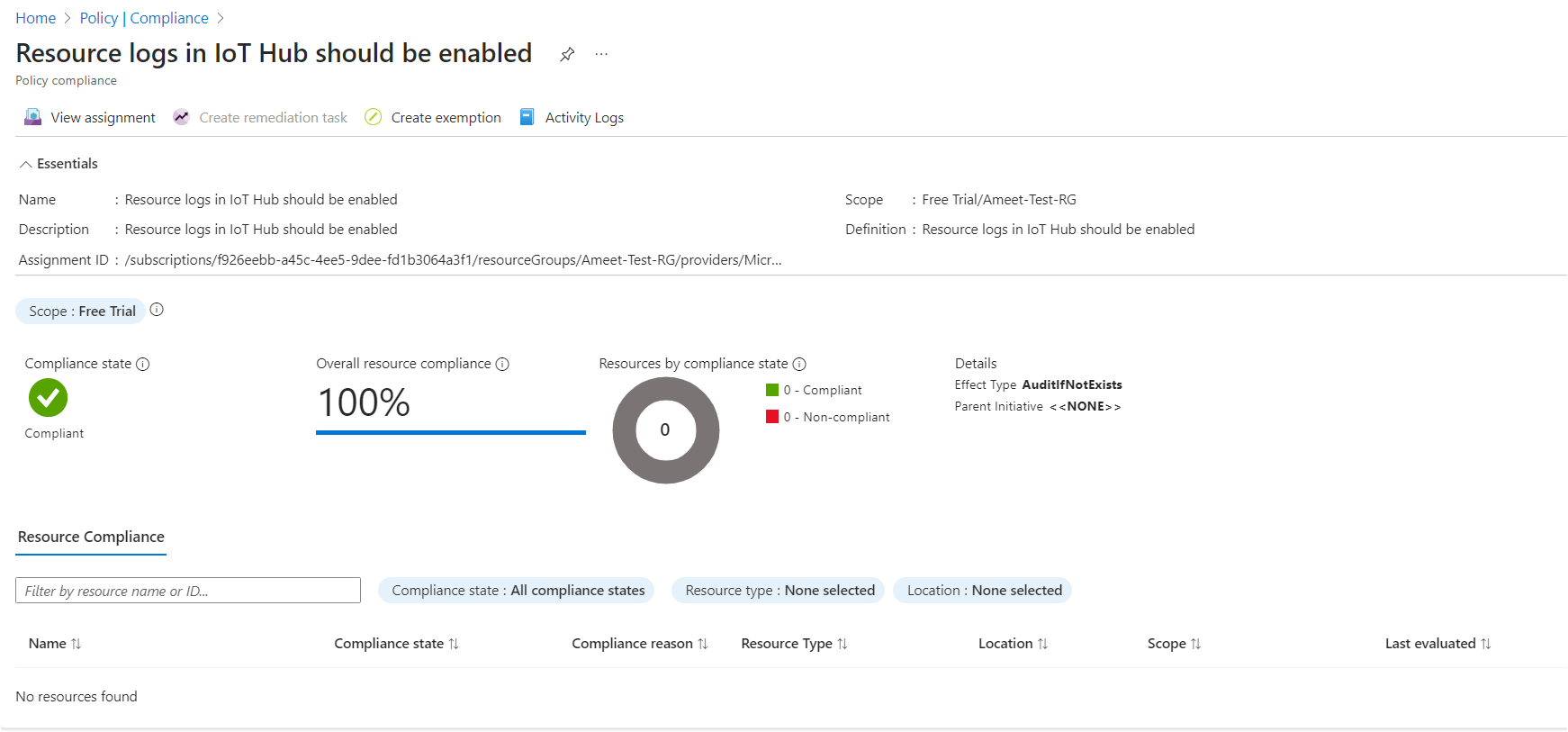
"type": "Microsoft.Authorization/policyDefinitions",

"name": "383856f8-de7f-44a2-81fc-e5135b5c2aa4"

}

**7.5 Error Details** The location of the error details depends on what aspect of Azure Policy you are working with & error summary details.

**7.6 Exceptions** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

Figure 2 Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generatedFigure 3 Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **8. Best practice 08 Resource logs in Logic Apps should be enabled.**

**8.1 Description** Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised.

**8.2 Control Domain** NZISM Security Benchmark AC-17, NIST SP 800-53 Rev. 4 AU-12, CIS Microsoft Azure Foundations Benchmark recommendation 5.3, Microsoft cloud security benchmark LT-3.

**8.3 Non-Compliance Message** In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended that Resource logs in Logic Apps should be enabled. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **8.4 Policy Definition**

{

"properties": {

"displayName": "Resource logs in Logic Apps should be enabled",

"policyType": "BuiltIn",

"mode": "Indexed",

"description": "Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised",

"metadata": {

"version": "5.1.0",

"category": "Logic Apps"

},

"parameters": {

"effect": {

"type": "String",

"metadata": {

"displayName": "Effect",

"description": "Enable or disable the execution of the policy"

},

"allowedValues": [

"AuditIfNotExists",

"Disabled"

],

"defaultValue": "AuditIfNotExists"

},

"requiredRetentionDays": {

"type": "String",

"metadata": {

"displayName": "Required retention (days)",

"description": "The required resource logs retention in days"

},

"defaultValue": "365"

}

},

"policyRule": {

"if": {

"field": "type",

"equals": "Microsoft.Logic/workflows"

},

"then": {

"effect": "[parameters('effect')]",

"details": {

"type": "Microsoft.Insights/diagnosticSettings",

"existenceCondition": {

"count": {

"field": "Microsoft.Insights/diagnosticSettings/logs[\*]",

"where": {

"anyOf": [

{

"allOf": [

{

"field": "Microsoft.Insights/diagnosticSettings/logs[\*].retentionPolicy.enabled",

"equals": "true"

},

{

"value": "[padLeft(current('Microsoft.Insights/diagnosticSettings/logs[\*].retentionPolicy.days'), 3, '0')]",

"greaterOrEquals": "[padLeft(parameters('requiredRetentionDays'), 3, '0')]"

},

{

"field": "Microsoft.Insights/diagnosticSettings/logs.enabled",

"equals": "true"

}

]

},

{

"allOf": [

{

"field": "Microsoft.Insights/diagnosticSettings/logs.enabled",

"equals": "true"

},

{

"anyOf": [

{

"field": "Microsoft.Insights/diagnosticSettings/logs[\*].retentionPolicy.enabled",

"notEquals": "true"

},

{

"field": "Microsoft.Insights/diagnosticSettings/storageAccountId",

"exists": false

}

]

}

]

}

]

}

},

"greaterOrEquals": 1

}

}

}

}

},

"id": "/providers/Microsoft.Authorization/policyDefinitions/34f95f76-5386-4de7-b824-0d8478470c9d",

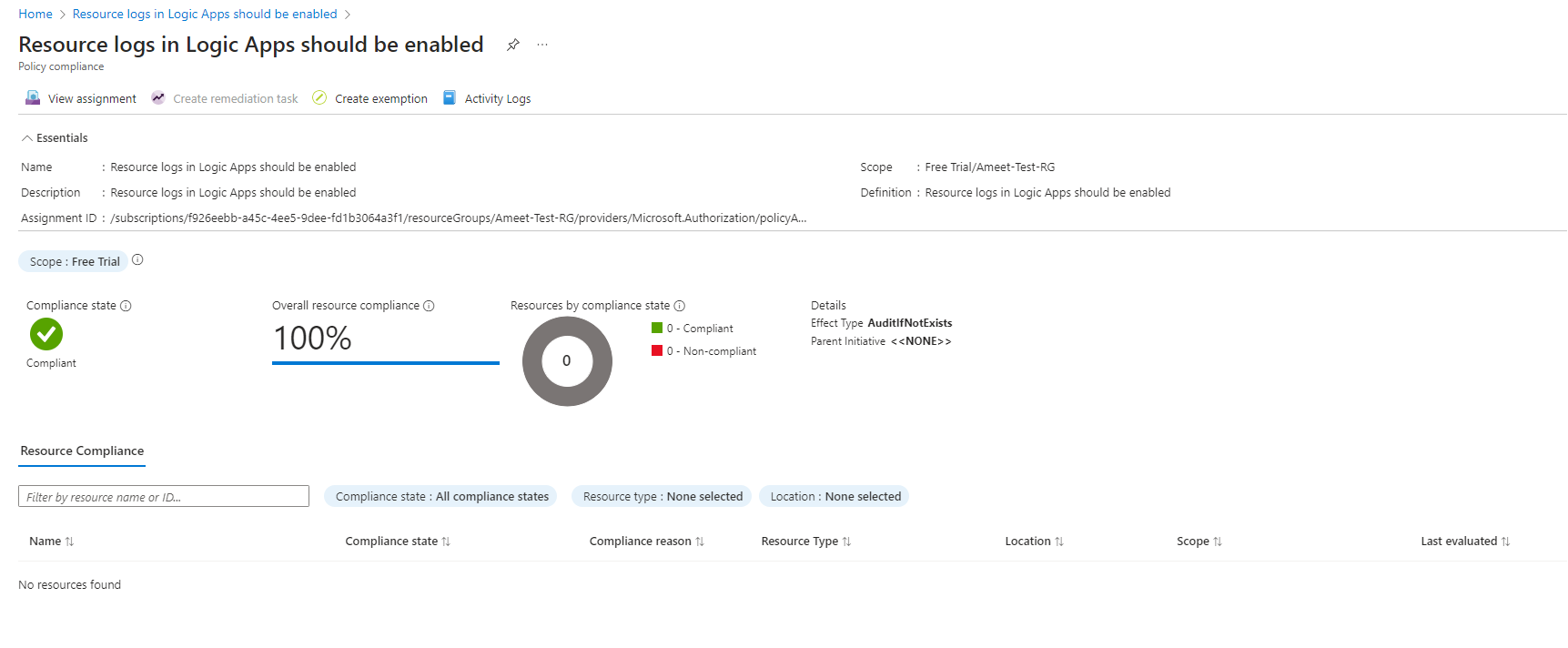
"type": "Microsoft.Authorization/policyDefinitions",

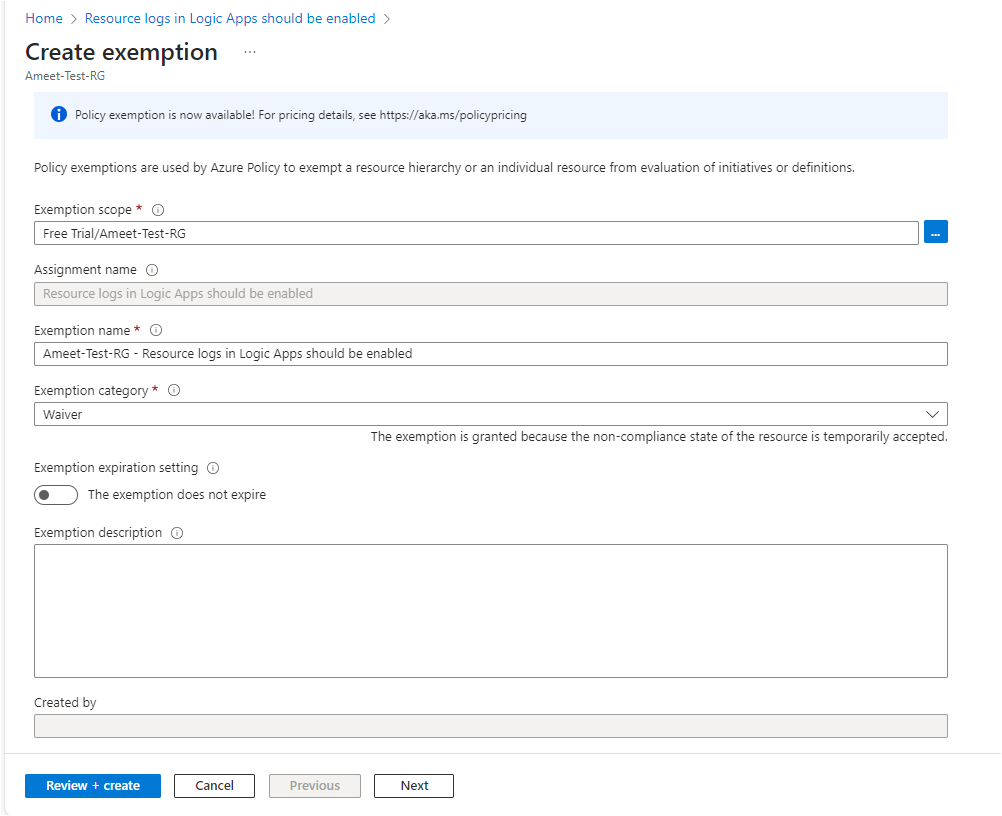
"name": "34f95f76-5386-4de7-b824-0d8478470c9d"

}

**8.5 Error Details** The location of the error details depends on what aspect of Azure Policy you are working with & error summary details.

**8.6 Exceptions** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

Figure 2 Select the policy, Click on Create Exemption.

Figure 3 Select the Exemption Scope (Subscription/ Resource Group / Resource).

# **9. Best practice 09 Resource logs in Key Vault should be enabled.**

**9.1 Description** Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes when a security incident occurs or when your network is compromised.

**9.2 Control Domain** CIS Microsoft Azure Foundations Benchmark recommendation 5.1.5, 1211.09aa3System.4-09.aa, Microsoft cloud security benchmark DP-8.

**9.3 Non-Compliance Message** In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended that Resource logs in Key Vault should be enabled. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **9.4 Policy Definition**

{

"properties": {

"displayName": "Resource logs in Key Vault should be enabled",

"policyType": "BuiltIn",

"mode": "Indexed",

"description": "Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes when a security incident occurs or when your network is compromised",

"metadata": {

"version": "5.0.0",

"category": "Key Vault"

},

"parameters": {

"effect": {

"type": "String",

"metadata": {

"displayName": "Effect",

"description": "Enable or disable the execution of the policy"

},

"allowedValues": [

"AuditIfNotExists",

"Disabled"

],

"defaultValue": "AuditIfNotExists"

},

"requiredRetentionDays": {

"type": "String",

"metadata": {

"displayName": "Required retention (days)",

"description": "The required resource logs retention in days"

},

"defaultValue": "365"

}

},

"policyRule": {

"if": {

"field": "type",

"equals": "Microsoft.KeyVault/vaults"

},

"then": {

"effect": "[parameters('effect')]",

"details": {

"type": "Microsoft.Insights/diagnosticSettings",

"existenceCondition": {

"count": {

"field": "Microsoft.Insights/diagnosticSettings/logs[\*]",

"where": {

"anyOf": [

{

"allOf": [

{

"field": "Microsoft.Insights/diagnosticSettings/logs[\*].retentionPolicy.enabled",

"equals": "true"

},

{

"anyOf": [

{

"field": "Microsoft.Insights/diagnosticSettings/logs[\*].retentionPolicy.days",

"equals": "0"

},

{

"value": "[padLeft(current('Microsoft.Insights/diagnosticSettings/logs[\*].retentionPolicy.days'), 3, '0')]",

"greaterOrEquals": "[padLeft(parameters('requiredRetentionDays'), 3, '0')]"

}

]

},

{

"field": "Microsoft.Insights/diagnosticSettings/logs.enabled",

"equals": "true"

}

]

},

{

"allOf": [

{

"field": "Microsoft.Insights/diagnosticSettings/logs.enabled",

"equals": "true"

},

{

"anyOf": [

{

"field": "Microsoft.Insights/diagnosticSettings/logs[\*].retentionPolicy.enabled",

"notEquals": "true"

},

{

"field": "Microsoft.Insights/diagnosticSettings/storageAccountId",

"exists": false

}

]

}

]

}

]

}

},

"greaterOrEquals": 1

}

}

}

}

},

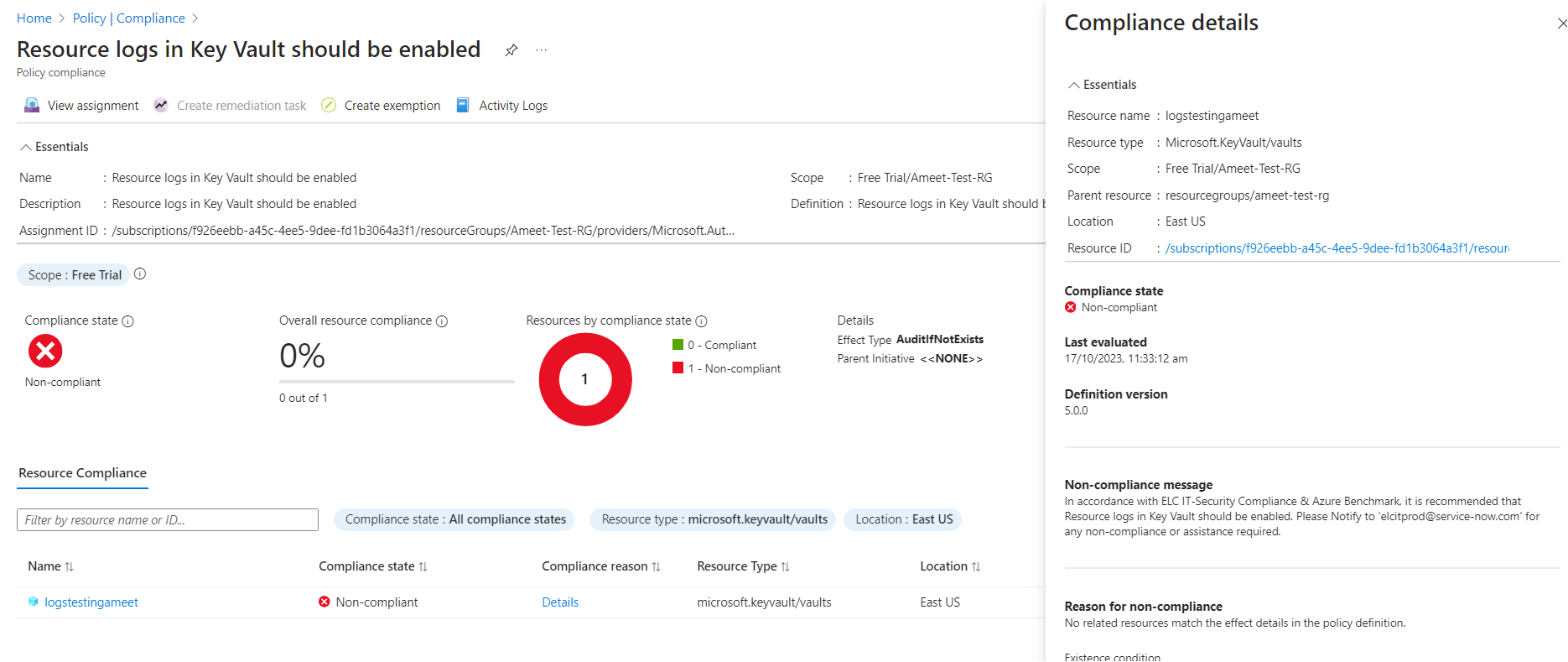
"id": "/providers/Microsoft.Authorization/policyDefinitions/cf820ca0-f99e-4f3e-84fb-66e913812d21",

"type": "Microsoft.Authorization/policyDefinitions",

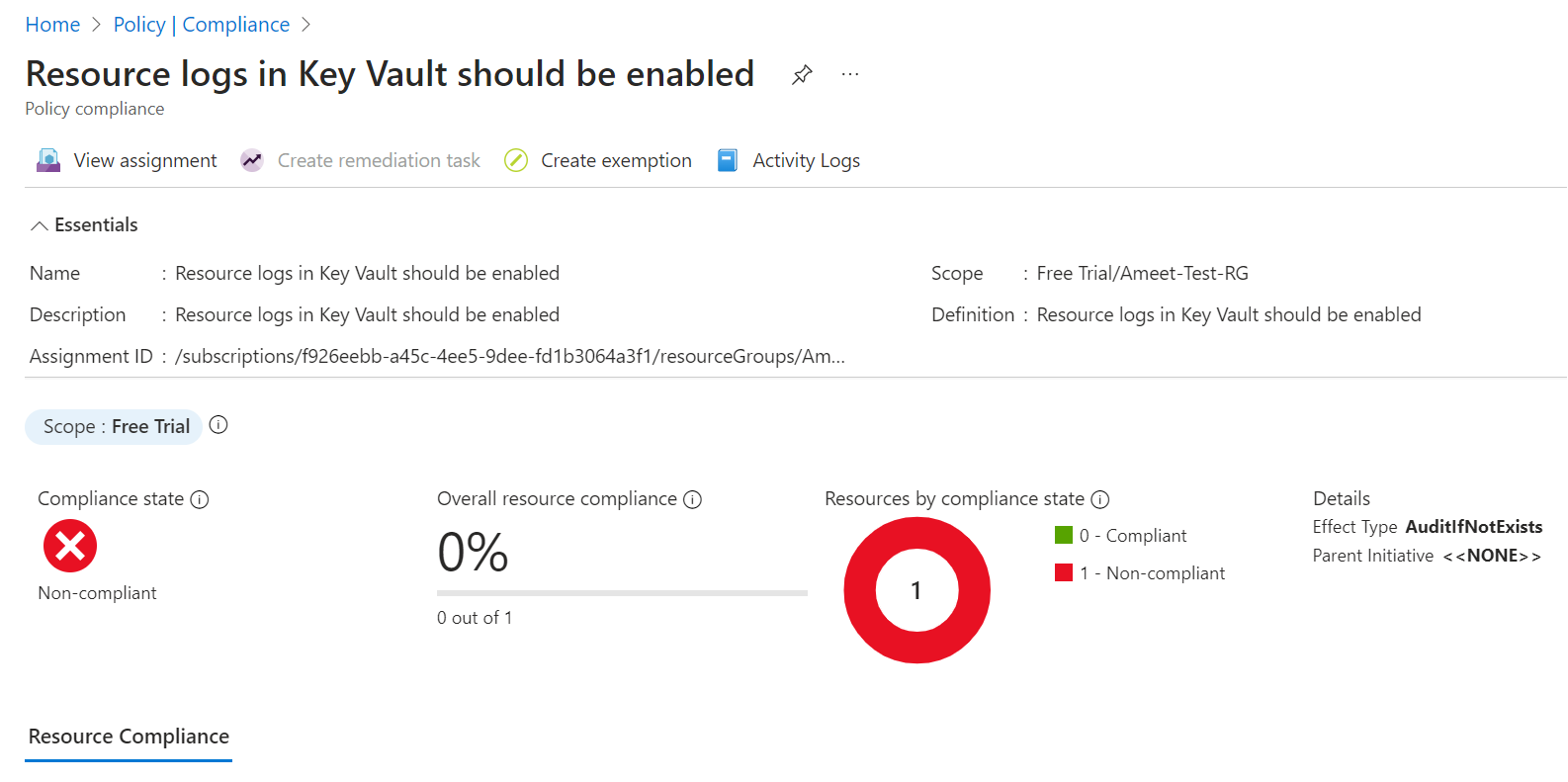
"name": "cf820ca0-f99e-4f3e-84fb-66e913812d21"

}

**9.5 Error Details** The location of the error details depends on what aspect of Azure Policy you are working with & error summary details.

Figure 1 Error details

**9.6 Exceptions** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

Figure 2 Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generatedFigure 3 Select the Exemption Scope (Subscription/ Resource Group / Resource)

# **10. Best practice 10 Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring.**

**10.1 Description** Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.

**10.2 Control Domain** Microsoft cloud security benchmark LT-5.

**10.3 Non-Compliance Message** In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended that Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **10.4 Policy Definition**

{

"properties": {

"displayName": "Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring",

"policyType": "BuiltIn",

"mode": "All",

"description": "Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.",

"metadata": {

"version": "1.0.0",

"category": "Security Center"

},

"parameters": {

"effect": {

"type": "String",

"metadata": {

"displayName": "Effect",

"description": "Enable or disable the execution of the policy"

},

"allowedValues": [

"AuditIfNotExists",

"Disabled"

],

"defaultValue": "AuditIfNotExists"

}

},

"policyRule": {

"if": {

"field": "type",

"in": [

"Microsoft.Compute/virtualMachineScaleSets"

]

},

"then": {

"effect": "[parameters('effect')]",

"details": {

"type": "Microsoft.Security/assessments",

"name": "45cfe080-ceb1-a91e-9743-71551ed24e94",

"existenceCondition": {

"field": "Microsoft.Security/assessments/status.code",

"in": [

"NotApplicable",

"Healthy"

]

}

}

}

}

},

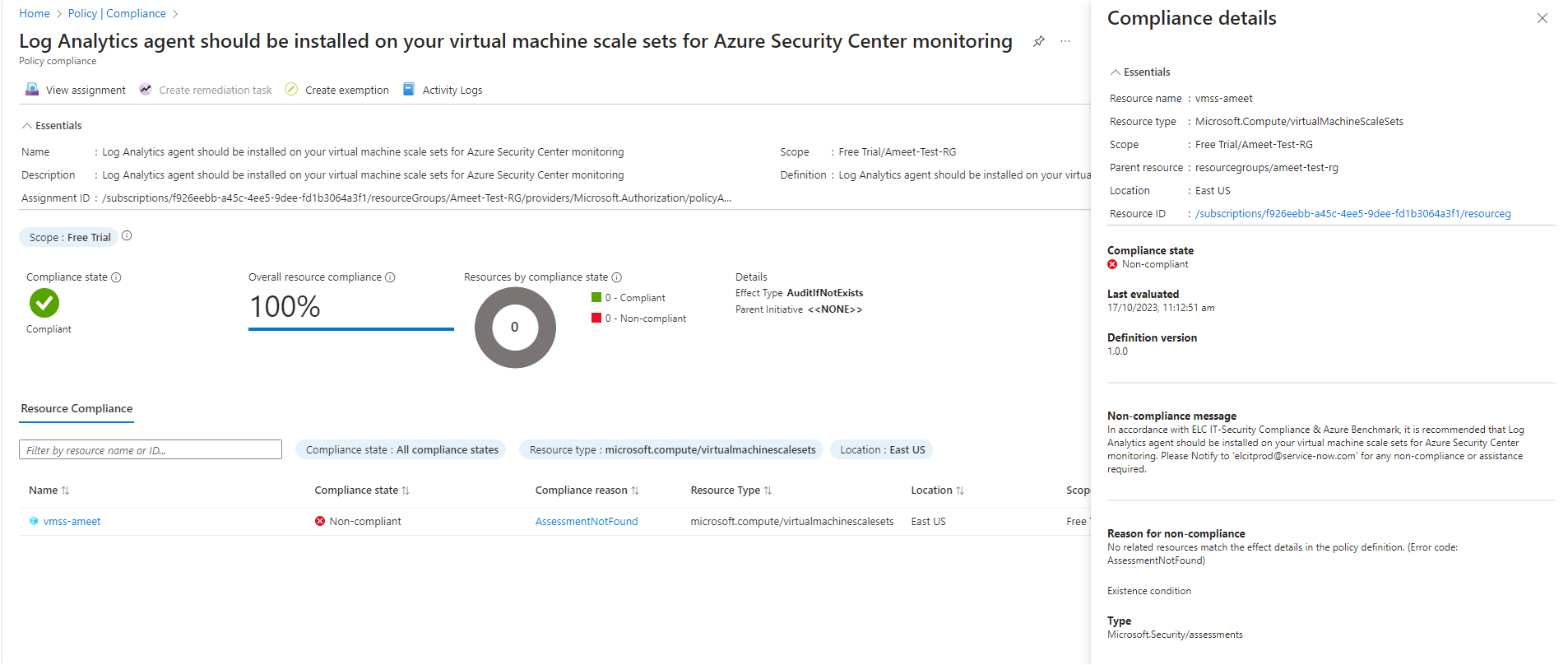
"id": "/providers/Microsoft.Authorization/policyDefinitions/a3a6ea0c-e018-4933-9ef0-5aaa1501449b",

"type": "Microsoft.Authorization/policyDefinitions",

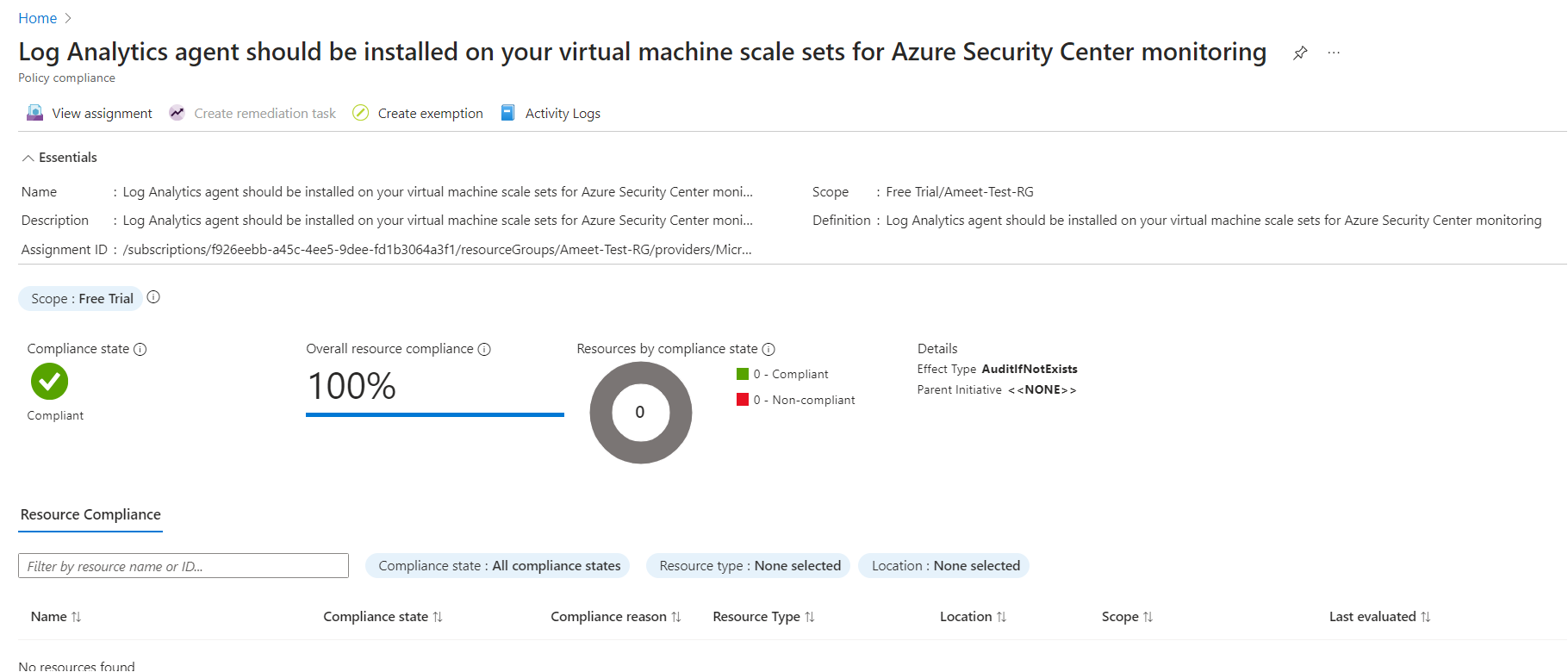
"name": "a3a6ea0c-e018-4933-9ef0-5aaa1501449b"

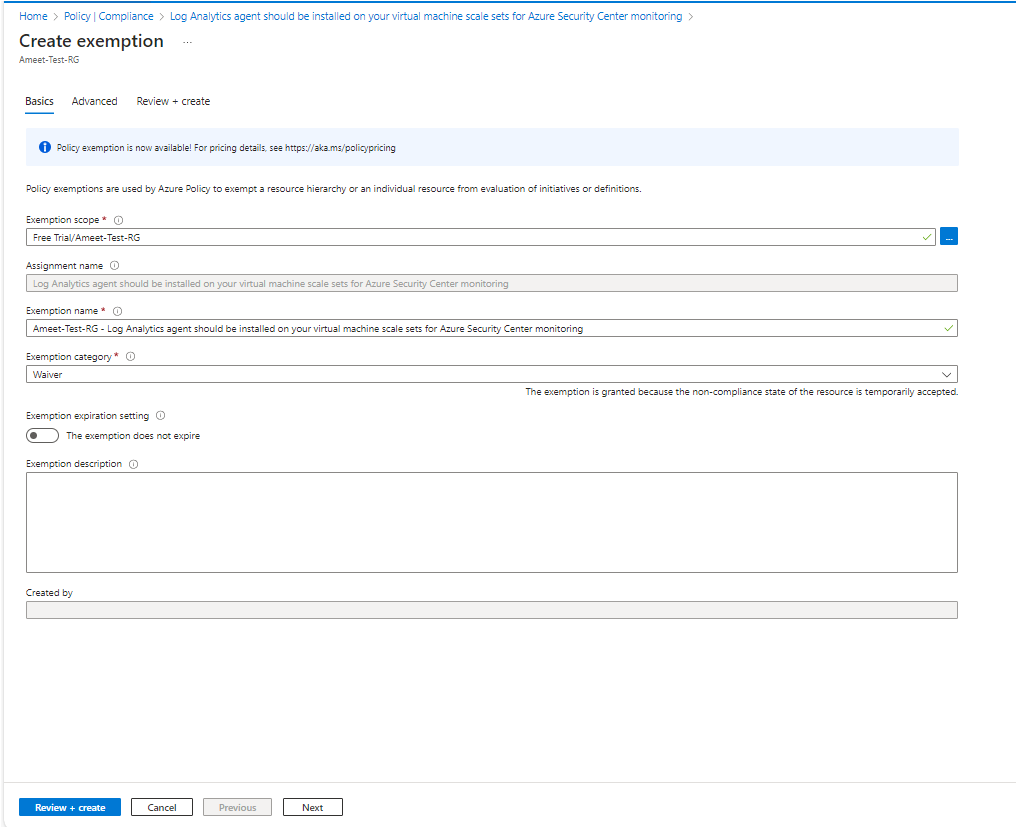
}

**10.5 Error Details** The location of the error details depends on what aspect of Azure Policy you are working with & error summary details.

Figure 1 – Error details

**10.6 Exceptions** While creating or after created the policy, We can Exclusions the Subscription/Resource Group/ Resource.

Figure 2 Select the policy, Click on Create Exemption.

Figure 3 Select the Exemption Scope (Subscription/ Resource Group / Resource).

**11.0** **Appendix**

**11.1** **Abbreviations**

|  |  |
| --- | --- |
| **Abbreviations** | **Descriptions** |
| **CIS** | Center for Internet Security |
| **CMMC** | Cybersecurity Maturity Model Certification |
| **HIPAA** | Health Insurance Portability and Accountability Act |
| **HITRUST** | Health Information Trust Alliance |
| **NZISM** | New Zealand Information Security Manual |
| **RMiT** | Royal Melbourne Institute of Technology |
| **VMs** | Virtual Machine/s |
| **IoT** | Internet of Things |
| **NIST** | National Institute of Standards and Technology |
| **BYOK** | Bring Your Own Key |
| **NA** | Not Applicable |

**12.0 Reference Document links**

Azure Security Benchmark 3.0

[Overview of the Azure Security Benchmark v3 | Microsoft Learn](https://learn.microsoft.com/en-us/security/benchmark/azure/overview-v3)

Regulatory Compliance

[Regulatory Compliance details for ISO 27001:2013 - Azure Policy | Microsoft Learn](https://learn.microsoft.com/en-us/azure/governance/policy/samples/iso-27001#compliance)