

**ELC – Virtual Machine- Proof of Concept
(POC)**

Initial Draft version v1.1

Submitted to

**ESTÉE
LAUDER
COMPANIES**

By



Wipro Technologies

Revision History

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

Author/Reviewer/Approvals

Name	Designation	Responsibility	Date
Arun Kumar V	Consultant	Author	31-Oct-23
Kannan Kuppusamy	Technical Lead	Reviewer	01-Nov-23
Felix Jebamani	Lead Consultant	Reviewer	01-Nov-23
Jamshid Abedi	ELC ED, Global Head of Security Engineer	Approver	00-Oct-23

Table of Contents

Overview	4
Purpose and Scope	4
1.0 Best Practice 01 - Azure Backup should be enabled for linux Virtual Machines.....	5
1.1 Description	5
1.2 Control Domain	5
1.3 Non-Compliance Message.....	5
1.4 Policy Definition.....	5
1.5 Error Details.....	6
1.6 Exceptions.....	7
2.0 Best Practice 02 - Linux machines that have accounts without passwords.	8
2.1 Description	8
2.2 Control Domain	8
2.3 Non-Compliance	8
2.4 Policy Definition.....	8
2.5 Error Details.....	11
2.6 Exceptions.....	12
3.0 Best practice 03 - Authentication to Linux machines should require SSH keys.	13
3.1 Description	13
3.2 Control Domain	13
3.3 Non-Compliance Message.....	13
3.4 Policy Definition.....	13
3.5 Error Details.....	18
3.6 Exceptions.....	18
4.0 Best practice 04 - Boot Diagnostics should be enabled on Linux virtual machines.	19
4.1 Description	19
4.2 Control Domain	19
4.3 Non-Compliance Message.....	19
4.4 Policy Definition.....	19
4.5 Error Details.....	20
4.6 Exceptions.....	21
5.0 Best practice 05 - A managed identity should be enabled on your machine.	22
5.1 Description	22
5.2 Control Domain	22

5.3	Non-Compliance Message.....	22
5.4	Policy Definition.....	22
5.5	Error Details.....	23
5.6	Exceptions.....	24
6.0	Appendix	25
6.1	Abbreviations.....	25
7.0	Reference Document links	25

Overview

Azure Virtual Machines (VMs) are a key component of Microsoft Azure's Infrastructure as a Service (IaaS) offering. They provide on-demand computing resources in the form of virtualized hardware, allowing you to run Windows or Linux-based applications and workloads in the cloud. Here's an overview of Azure Virtual Machines. The best practice of Azure Policy will ensure the ELC Cloud operations team to adhere to the ELC Global information security policy guidelines respect to the Cloud Security and follow the Azure Virtual machine Security policy. 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 to make sure the best practices are followed adhered as per the regulatory standards.

Purpose and Scope

As per the ELC's Global Information Security, Adopting the Azure Security benchmarks and the Azure Security Policy framework to Secure ELC Cloud services by creating and implementing strong Azure security policies in the Azure services for Virtual machines in the cloud environment through the Azure security policy to protect and secure the instances, workload running through the VM. Azure Security benchmarks can be referred in the Appendix.

1.0 Best Practice 01 - Azure Backup should be enabled for linux Virtual Machines.

1.1 Description

Ensure protection of your Azure Virtual Machines by enabling Azure Backup. Azure Backup is a secure and cost-effective data protection solution for Azure.

1.2 Control Domain

NIST_SP_800-53_R5, CMMC Level 3

1.3 Non-Compliance Message

In accordance with ELC IT-Security Compliance & Azure Benchmark, it is recommended to enable the Azure Backup for Virtual Machines. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

1.4 Policy Definition

```
{
  "properties": {
    "displayName": "Azure Backup should be enabled for linux Virtual Machines",
    "policyType": "Custom",
    "mode": "Indexed",
    "description": "Ensure protection of your Azure Virtual Machines by enabling Azure Backup. Azure Backup is a",
    "metadata": {
      "category": "",
      "createdBy": "829e58c3-742e-4964-aba4-58334c64fa42",
      "createdOn": "2023-10-11T01:07:41.4549694Z",
      "updatedBy": null,
      "updatedOn": null
    },
    "parameters": {
      "effect": {
        "type": "String",
        "metadata": {
          "displayName": "Effect",
          "description": "Enable or disable the execution of the policy"
        },
        "allowedValues": [
          "AuditIfNotExists",
          "deny",
          "Disabled"
        ],
        "defaultValue": "deny"
      }
    }
  },
}
```

```

    "if": {
      "allOf": [
        {
          "field": "type",
          "equals": "Microsoft.Compute/virtualMachines"
        },
        {
          "field": "id",
          "notContains": "/resourceGroups/databricks-rg-"
        },
        {
          "field": "Microsoft.Compute/imagePublisher",
          "notEquals": "azureopenshift"
        },
        {
          "field": "Microsoft.Compute/imagePublisher",
          "notEquals": "AzureDatabricks"
        }
      ]
    },
    "then": {
      "effect": "[parameters('effect')]",
      "details": {
        "type": "Microsoft.RecoveryServices/backupprotecteditems"
      }
    }
  },
  "id": "/subscriptions/9073e58b-15b4-4cfe-8ce0-b09f430f15c6/providers/Microsoft.Authorization/policyDefinitions",
  "type": "Microsoft.Authorization/policyDefinitions",
  "name": "74014943-51da-4644-93c1-cbf5f08db789",

```

1.5 Error Details

The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.

The screenshot displays the Azure portal interface for creating a virtual machine. A red banner at the top indicates a 'Validation failed' error. The error details pane on the right provides the following information:

- Summary:** Resource 'test' was disallowed by policy. (Code: RequestDisallowedByPolicy)
- Policy:** Azure Backup should be enabled for linux Virtual Machines
- Reason:** Error: Please enable the azure backup.

Below the error details, there are links for 'Troubleshooting Options', 'Check Usage', 'Quota', and 'New Support Request'.

Figure 1 - Validation Failed error summary details.

1.6 Exceptions

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

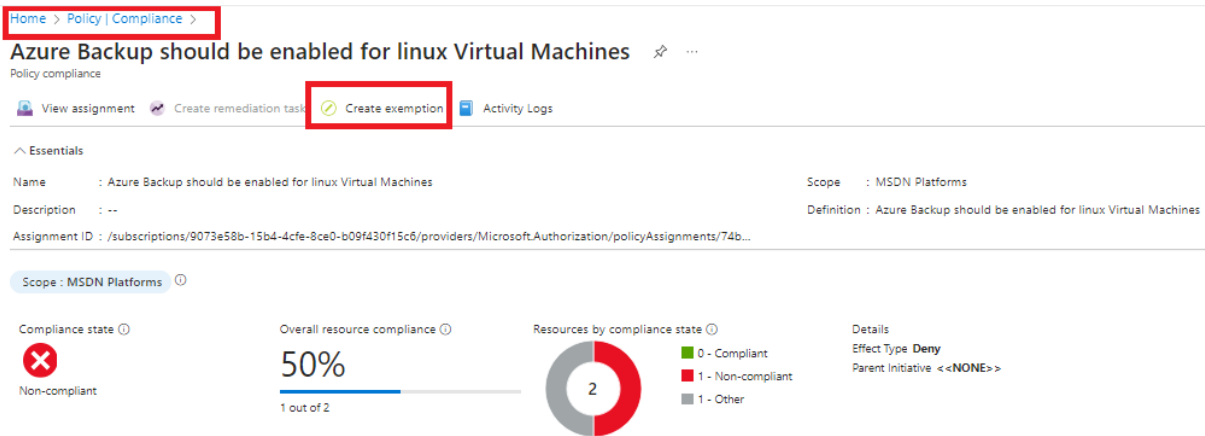


Figure 2 - Select the policy, Click on Create Exemption.

The screenshot shows the 'Create exemption' form in the Azure portal. The breadcrumb navigation is 'Home > Policy | Compliance > StorageTest >'. The form title is 'Create exemption'. The 'Exemption scope' is 'MSDN Platforms'. The 'Assignment name' is 'StorageTest'. The 'Exemption name' is 'MSDN Platforms - StorageTest'. The 'Exemption category' is 'Waiver'. The 'Exemption expiration setting' is 'The exemption does not expire'. The 'Exemption description' is empty. The 'Exemption scope' sidebar is open, showing the 'Subscription' as 'MSDN Platforms', 'Resource Group' as 'Optionally choose a Resource Group', and 'Resource' as 'Optionally choose a Resource'. The 'Review + create' button is highlighted.

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

2.0 Best Practice 02 - Linux machines that have accounts without passwords.

2.1 Description

Machines are non-compliant if Linux machines that have accounts without passwords.

2.2 Control Domain

NIST_SP_800-53_R5, ISO27001 – 2013, CMMC Level 3

2.3 Non-Compliance

Message In accordance with ELC IT-Security & Compliance, it is recommended to create a password for the virtual machine. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

2.4 Policy Definition

```
{
  "properties": {
    "displayName": "Linux machines that have accounts without passwords",
    "policyType": "Custom",
    "mode": "Indexed",
    "description": "Requires that prerequisites are deployed to the policy assignment scope. For details, visit",
    "metadata": {
      "version": "3.0.0",
      "requiredProviders": [
        "Microsoft.GuestConfiguration"
      ],
      "guestConfiguration": {
        "name": "PasswordPolicy_msid232",
        "version": "1.*"
      },
      "createdBy": "829e58c3-742e-4964-aba4-58334c64fa42",
      "createdOn": "2023-10-11T01:28:27.163312Z",
      "updatedBy": null,
      "updatedOn": null
    },
    "parameters": {
      "IncludeArcMachines": {
        "type": "String",
        "metadata": {
          "displayName": "Include Arc connected servers",
          "description": "By selecting this option, you agree to be charged monthly per Arc connected machine.",
          "portalReview": "true"
        },
        "allowedValues": [
          "true",
          "false"
        ]
      }
    }
  }
}
```



```

    },
    "effect": {
      "type": "String",
      "metadata": {
        "displayName": "Effect",
        "description": "Enable or disable the execution of this policy"
      },
      "allowedValues": [
        "AuditIfNotExists",
        "deny",
        "Disabled"
      ],
      "defaultValue": "deny"
    }
  },
  "policyRule": {
    "if": {
      "anyOf": [
        {
          "allOf": [
            {
              "field": "type",
              "equals": "Microsoft.Compute/virtualMachines"
            },
            {
              "anyOf": [
                {
                  "field": "Microsoft.Compute/imagePublisher",
                  "in": [
                    "microsoft-aks",
                    "qubole-inc",

```

```

                    "datastax",
                    "couchbase",
                    "scalegrid",
                    "checkpoint",
                    "paloaltonetworks",
                    "debian",
                    "credativ"
                  ],
                },
              ],
            },
          ],
        {
          "allOf": [
            {
              "field": "Microsoft.Compute/imagePublisher",
              "equals": "OpenLogic"
            },
            {
              "field": "Microsoft.Compute/imageSKU",
              "notLike": "6*"
            }
          ]
        },
        {
          "allOf": [
            {
              "field": "Microsoft.Compute/imagePublisher",
              "equals": "Oracle"
            },
            {
              "field": "Microsoft.Compute/imageSKU",
              "notLike": "6*"
            }
          ]
        }
      ],
    }
  }
}

```

```

    {
      "allOf": [
        {
          "field": "Microsoft.Compute/imagePublisher",
          "equals": "RedHat"
        },
        {
          "field": "Microsoft.Compute/imageSKU",
          "notLike": "6*"
        }
      ],
    },
    {
      "allOf": [
        {
          "field": "Microsoft.Compute/imagePublisher",
          "equals": "center-for-internet-security-inc"
        },
        {
          "field": "Microsoft.Compute/imageOffer",
          "notLike": "cis-windows*"
        }
      ],
    },
    {
      "allOf": [
        {
          "field": "Microsoft.Compute/imagePublisher",
          "equals": "Suse"
        },
        {
          "field": "Microsoft.Compute/imageSKU",
          "notLike": "11*"
        }
      ],
    }
  ],
}

```

```

    "allof": [
      {
        "field": "Microsoft.Compute/imagePublisher",
        "equals": "Canonical"
      },
      {
        "field": "Microsoft.Compute/imageSKU",
        "notLike": "12*"
      }
    ],
  },
  {
    "allof": [
      {
        "field": "Microsoft.Compute/imagePublisher",
        "equals": "microsoft-dsvm"
      },
      {
        "field": "Microsoft.Compute/imageOffer",
        "notLike": "dsvm-win*"
      }
    ],
  },
  {
    "allof": [
      {
        "field": "Microsoft.Compute/imagePublisher",
        "equals": "cloudera"
      },
      {
        "field": "Microsoft.Compute/imageSKU",
        "notLike": "6*"
      }
    ],
  },

```

```

    "allof": [
      {
        "anyOf": [
          {
            "field": "Microsoft.Compute/virtualMachines/osProfile.linuxConfiguration",
            "exists": "true"
          },
          {
            "field": "Microsoft.Compute/virtualMachines/storageProfile.osDisk.osType",
            "like": "Linux*"
          }
        ]
      },
      {
        "anyOf": [
          {
            "field": "Microsoft.Compute/imagePublisher",
            "exists": "false"
          },
          {
            "field": "Microsoft.Compute/imagePublisher",
            "notIn": [
              "OpenLogic",
              "RedHat",
              "credativ",
              "Suse",
              "Canonical",
              "microsoft-dsvm",
              "cloudera",
              "microsoft-ads",
              "center-for-internet-security-inc",
              "Oracle",
              "AzureDatabricks",

```

```

    "then": {
      "effect": "[parameters('effect')]",
      "details": {
        "type": "Microsoft.GuestConfiguration/guestConfigurationAssignments",
        "name": "PasswordPolicy_msid232",
        "existenceCondition": {
          "field": "Microsoft.GuestConfiguration/guestConfigurationAssignments/complianceStatus",
          "equals": "Compliant"
        }
      }
    }
  },
  "id": "/subscriptions/9073e58b-15b4-4cfe-8ce0-b09f430f15c6/providers/Microsoft.Authorization/policyDefinition",
  "type": "Microsoft.Authorization/policyDefinitions",
  "name": "6fd489d6-087d-42c9-b3f7-9f2542bb77da",

```

2.5 Error Details

The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.

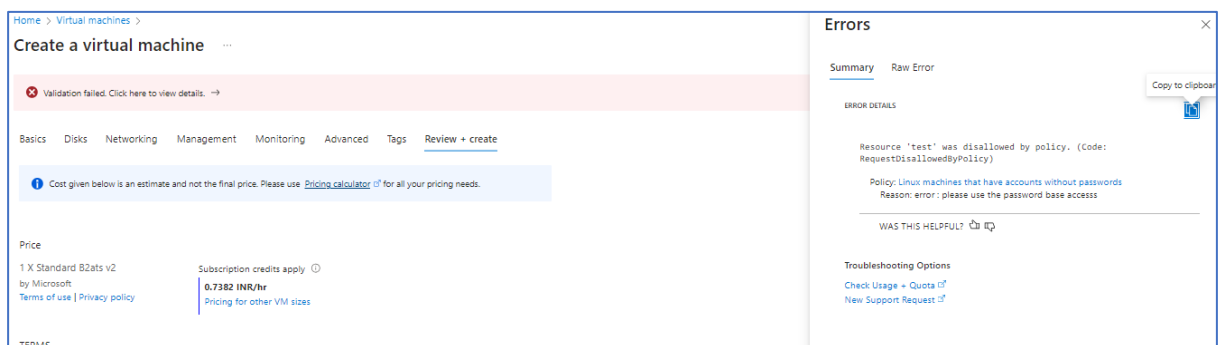


Figure 4 - Validation Failed error summary details.

2.6 Exceptions

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

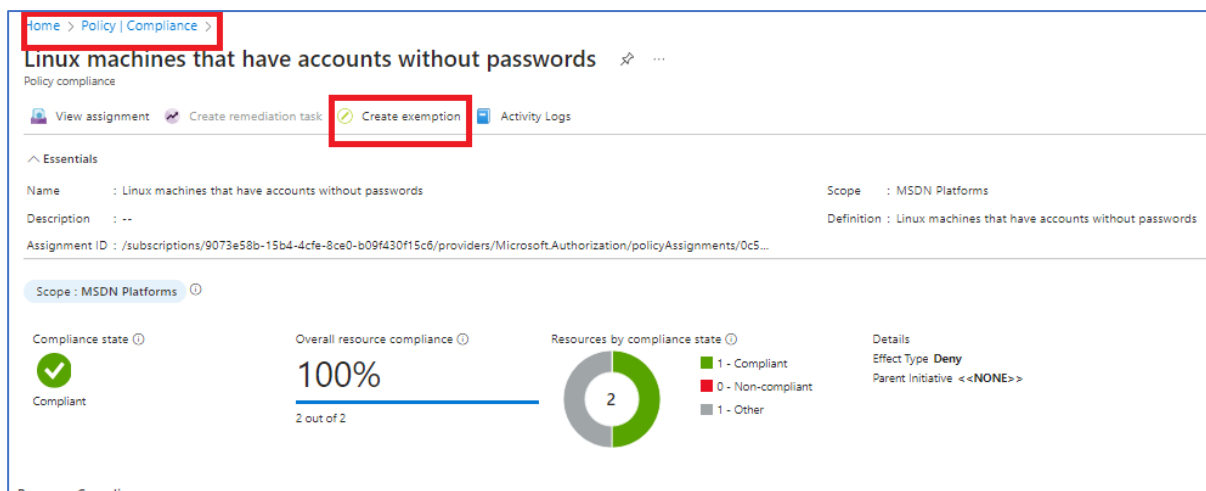


Figure 2 - Select the policy, Click on Create Exemption.

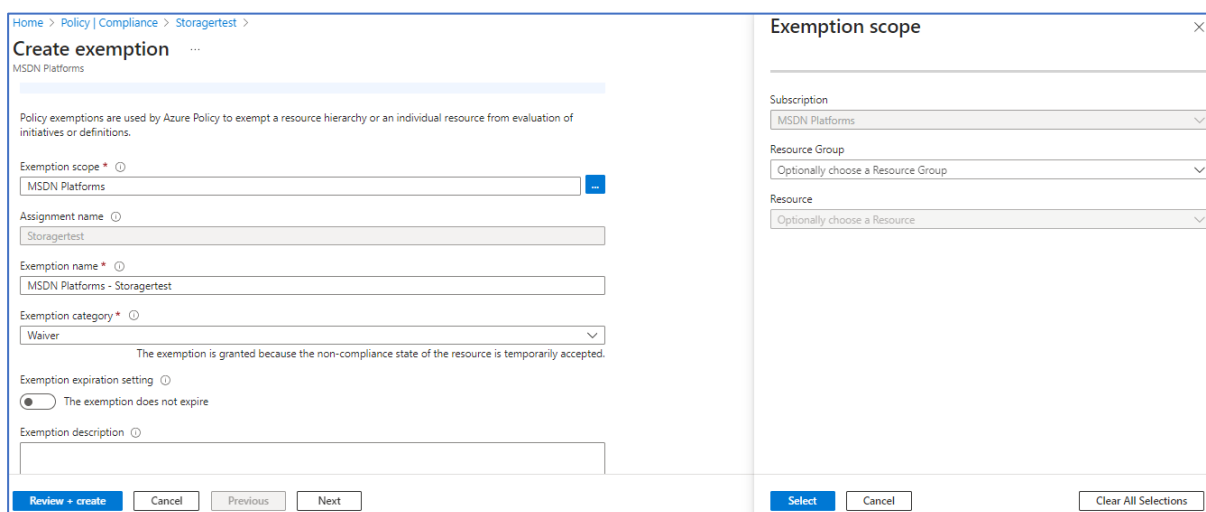


Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

3.0 Best practice 03 - Authentication to Linux machines should require SSH keys.

3.1 Description

Machines are non-compliant if Linux machines that have accounts without SSH keys.

3.2 Control Domain

NIST_SP_800-53_R5, Azure_Security_Benchmark_v3.0, CMMC 2.0 Level 2

3.3 Non-Compliance Message

In accordance with ELC IT-Security & Compliance, it is recommended to create a SSH keys for the virtual machine to access. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

3.4 Policy Definition

```
{
  "mode": "Indexed",
  "policyRule": {
    "if": {
      "anyOf": [
        {
          "allof": [
            {
              "field": "type",
              "equals": "Microsoft.Compute/virtualMachines"
            },
            {
              "anyOf": [
                {
                  "field": "Microsoft.Compute/imagePublisher",
                  "in": [
                    "microsoft-aks",
                    "qubole-inc",
                    "datastax",
                    "couchbase",
                    "scalegrid",
                    "checkpoint",
                    "paloaltonetworks",
                    "debian",
                    "credativ"
                  ]
                },
                {
                  "allof": [
                    {
                      "field": "Microsoft.Compute/imagePublisher",
                      "equals": "OpenLogic"
                    }
                  ]
                }
              ]
            }
          ]
        }
      ]
    }
  }
}
```

```

    {
      "field": "Microsoft.Compute/imageSKU",
      "notLike": "6*"
    }
  ],
  {
    "allof": [
      {
        "field": "Microsoft.Compute/imagePublisher",
        "equals": "Oracle"
      },
      {
        "field": "Microsoft.Compute/imageSKU",
        "notLike": "6*"
      }
    ]
  },
  {
    "allof": [
      {
        "field": "Microsoft.Compute/imagePublisher",
        "equals": "RedHat"
      },
      {
        "field": "Microsoft.Compute/imageSKU",
        "notLike": "6*"
      }
    ]
  },
  {
    "allof": [

```

```

      "field": "Microsoft.Compute/imagePublisher",
      "equals": "center-for-internet-security-inc"
    },
    {
      "field": "Microsoft.Compute/imageOffer",
      "notLike": "cis-windows*"
    }
  ],
  {
    "allof": [
      {
        "field": "Microsoft.Compute/imagePublisher",
        "equals": "Suse"
      },
      {
        "field": "Microsoft.Compute/imageSKU",
        "notLike": "11*"
      }
    ]
  },
  {
    "allof": [
      {
        "field": "Microsoft.Compute/imagePublisher",
        "equals": "Canonical"
      },
      {
        "field": "Microsoft.Compute/imageSKU",
        "notLike": "12*"
      }
    ]
  },

```

```

    ],
    {
      "allof": [
        {
          "field": "Microsoft.Compute/imagePublisher",
          "equals": "microsoft-dsvm"
        },
        {
          "field": "Microsoft.Compute/imageOffer",
          "notLike": "dsvm-win*"
        }
      ]
    },
    {
      "allof": [
        {
          "field": "Microsoft.Compute/imagePublisher",
          "equals": "cloudera"
        },
        {
          "field": "Microsoft.Compute/imageSKU",
          "notLike": "6*"
        }
      ]
    },
    {
      "allof": [
        {
          "field": "Microsoft.Compute/imagePublisher",
          "equals": "microsoft-ads"
        },

```

```

      {
        "field": "Microsoft.Compute/imageOffer",
        "like": "linux*"
      }
    ],
    {
      "allof": [
        {
          "anyOf": [
            {
              "field": "Microsoft.Compute/virtualMachines/osProfile.linuxConfiguration",
              "exists": "true"
            },
            {
              "field": "Microsoft.Compute/virtualMachines/storageProfile.osDisk.osType",
              "like": "Linux*"
            }
          ]
        },
        {
          "anyOf": [
            {
              "field": "Microsoft.Compute/imagePublisher",
              "exists": "false"
            },
            {
              "field": "Microsoft.Compute/imagePublisher",
              "notIn": [
                "OpenLogic",
                "RedHat",
                "credativ",
                "Suse",

```

```
        "microsoft-dsvm",
        "cloudera",
        "microsoft-ads",
        "center-for-internet-security-inc",
        "Oracle",
        "AzureDatabricks",
        "azureopenshift"
    ]
}
]
},
{
    "allOf": [
        {
            "value": "[parameters('IncludeArcMachines')]",
            "equals": "true"
        },
        {
            "anyOf": [
                {
                    "allOf": [
                        {
                            "field": "type",
                            "equals": "Microsoft.HybridCompute/machines"
                        },
                        {
                            "field": "Microsoft.HybridCompute/imageOffer",
```



```

        "like": "linux*"
    }
}
],
},
{
    "allof": [
        {
            "field": "type",
            "equals": "Microsoft.ConnectedVMwarevSphere/virtualMachines"
        },
        {
            "field": "Microsoft.ConnectedVMwarevSphere/virtualMachines/osProfile.osType",
            "like": "linux*"
        }
    ]
}
]
}
]
},
"then": {
    "effect": "[parameters('effect')]",
    "details": {
        "type": "Microsoft.GuestConfiguration/guestConfigurationAssignments",
        "name": "LinuxNoPasswordForSSH",
        "existenceCondition": {
            "field": "Microsoft.GuestConfiguration/guestConfigurationAssignments/complianceStatus",
            "equals": "Compliant"
        }
    }
}
}
}

```

```

    },
    "parameters": {
        "IncludeArcMachines": {
            "type": "String",
            "metadata": {
                "displayName": "Include Arc connected servers",
                "description": "By selecting this option, you agree to be charged monthly per Arc connected machine.",
                "portalReview": "true"
            },
            "allowedValues": [
                "true",
                "false"
            ],
            "defaultValue": "false"
        },
        "effect": {
            "type": "String",
            "metadata": {
                "displayName": "Effect",
                "description": "Enable or disable the execution of this policy"
            },
            "allowedValues": [
                "AuditIfNotExists",
                "deny",
                "Disabled"
            ],
            "defaultValue": "deny"
        }
    }
}
}

```

3.5 Error Details

The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.



Figure 5 - Validation Failed error summary details.

3.6 Exceptions

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

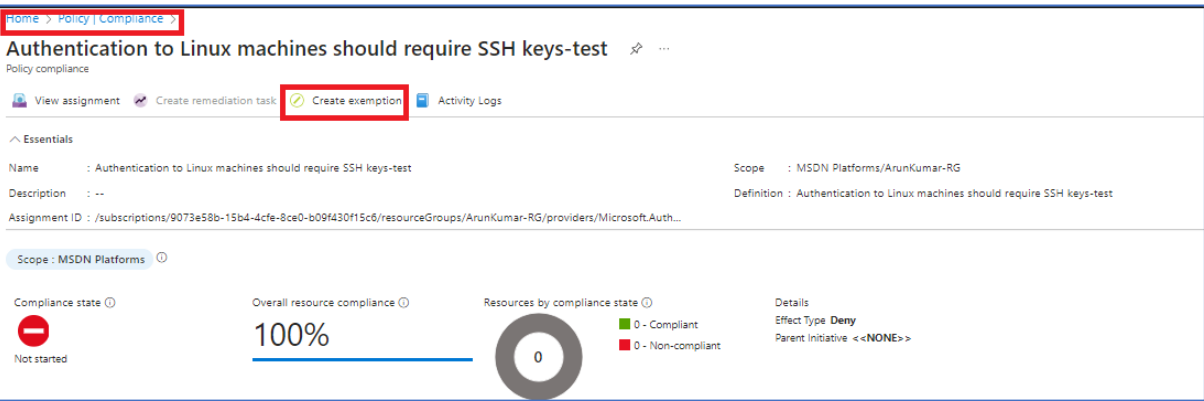


Figure 2 - Select the policy, Click on Create Exemption.

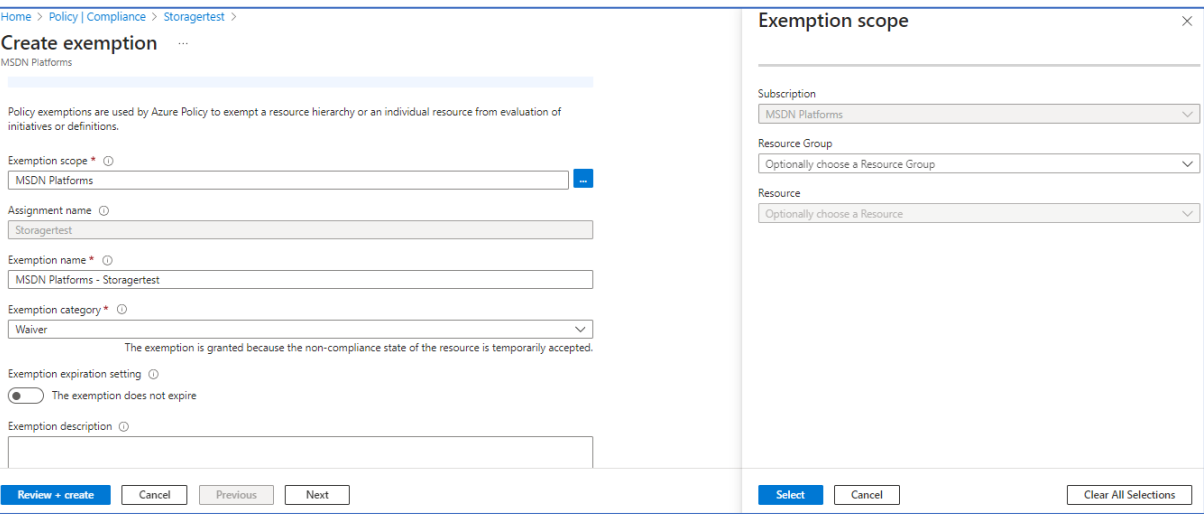


Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

4.0 Best practice 04 - Boot Diagnostics should be enabled on Linux virtual machines.

4.1 Description

Machines are non-compliant if Boot Diagnostics on disable in Linux virtual machines.

4.2 Control Domain

Azure_Security_Benchmark_v3.0.

4.3 Non-Compliance Message

In accordance with ELC IT-Security & Compliance, it is recommended to enable the Boot Diagnostics on virtual machines. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

4.4 Policy Definition

```
{
  "properties": {
    "displayName": "Boot Diagnostics should be enabled on Linux virtual machines",
    "policyType": "Custom",
    "mode": "Indexed",
    "description": "Azure virtual machines should have boot diagnostics enabled.",
    "metadata": {
      "version": "1.0.0-preview",
      "preview": true,
      "createdBy": "829e58c3-742e-4964-aba4-58334c64fa42",
      "createdOn": "2023-11-01T07:28:16.7152932Z",
      "updatedBy": null,
      "updatedOn": null
    }
  },
  "parameters": {
    "effect": {
      "type": "String",
      "metadata": {
        "displayName": "Effect",
        "description": "Enable or disable the execution of the policy"
      },
      "allowedValues": [
        "Audit",
        "deny",
        "Disabled"
      ],
      "defaultValue": "deny"
    }
  },
  "policyRule": {
    "if": {
```

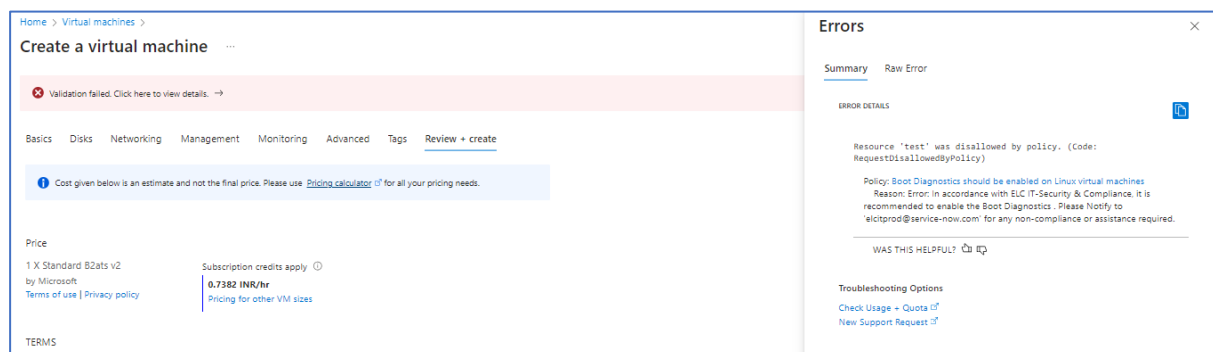
```

    "allof": [
      {
        "field": "type",
        "equals": "Microsoft.Compute/virtualMachines"
      },
      {
        "field": "Microsoft.Compute/virtualMachines/diagnosticsProfile.bootDiagnostics.enabled",
        "notEquals": "true"
      }
    ],
    "then": {
      "effect": "[parameters('effect')]"
    }
  },
  "id": "/subscriptions/9073e58b-15b4-4cfe-8ce0-b09f430f15c6/providers/Microsoft.Authorization/policyDefinitions",
  "type": "Microsoft.Authorization/policyDefinitions",
  "name": "2dd5225f-1230-497e-ad04-bd8166b0c7de",
  "systemData": {
    "createdBy": "arunkumar@virtualkannan.com",
    "createdByType": "User",
    "createdAt": "2023-11-01T07:28:16.4690394Z",
    "lastModifiedBy": "arunkumar@virtualkannan.com",
    "lastModifiedByType": "User",
    "lastModifiedAt": "2023-11-01T07:28:16.4690394Z"
  }
}

```

4.5 Error Details

The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.



Home > Virtual machines > Create a virtual machine

Validation failed. Click here to view details. →

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Cost given below is an estimate and not the final price. Please use [Pricing calculator](#) for all your pricing needs.

Price

1 X Standard B2ats v2 by Microsoft

Subscription credits apply ⓘ

0.7382 INR/hr

[Pricing for other VM sizes](#)

TERMS

Errors

Summary Raw Error

ERROR DETAILS

Resource 'test' was disallowed by policy. (Code: RequestDisallowedByPolicy)

Policy: Boot Diagnostics should be enabled on Linux virtual machines

Reason: Error: In accordance with ELC IT-Security & Compliance, it is recommended to enable the Boot Diagnostics. Please Notify to 'elcprod@service-now.com' for any non-compliance or assistance required.

WAS THIS HELPFUL? ⓘ ⓘ

Troubleshooting Options

[Check Usage + Quota](#) ⓘ

[New Support Request](#) ⓘ

Figure 6 - Validation Failed error summary details.

4.6 Exceptions

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

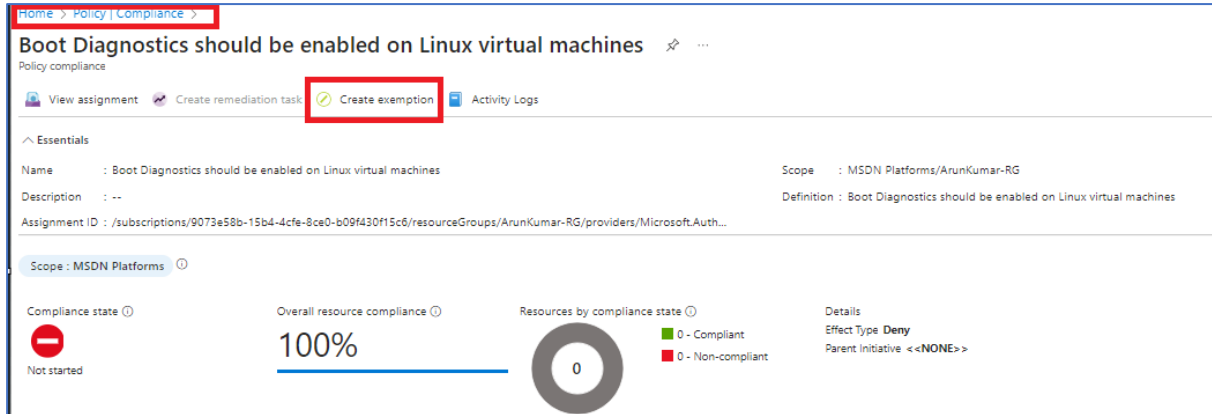


Figure 2 - Select the policy, Click on Create Exemption.

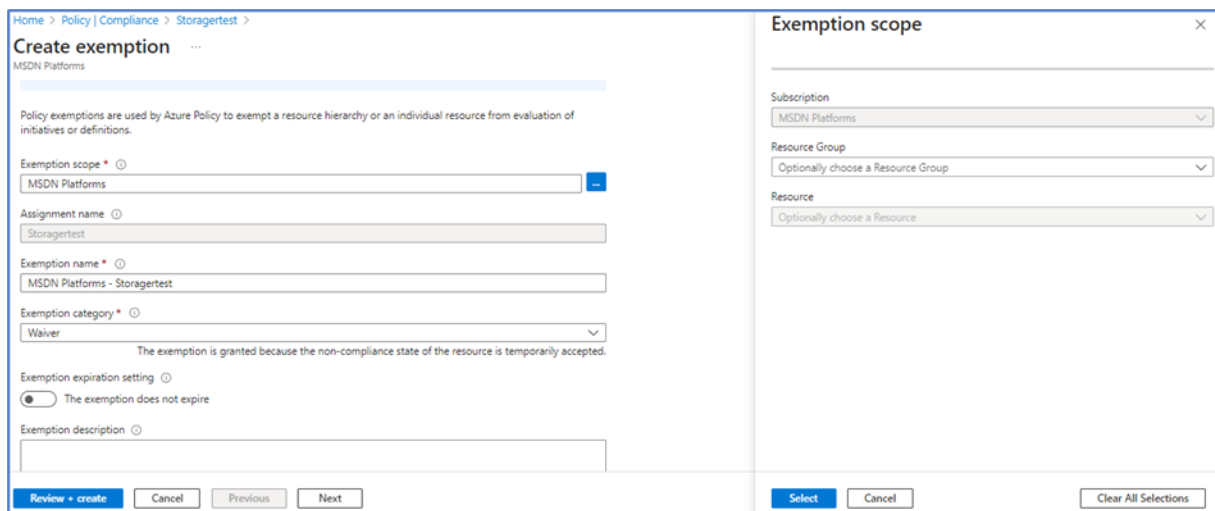


Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

5.0 Best practice 05 - A managed identity should be enabled on your machine.

5.1 Description

Machines are non-compliant Resources managed by Auto manage should have a managed identity.

5.2 Control Domain

NIST_SP_800-53_R5, Azure_Security_Benchmark_v3.0.

5.3 Non-Compliance Message

In accordance with ELC IT-Security & Compliance, it is recommended to managed identity should be enabled on your machine. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

5.4 Policy Definition

```
{
  "properties": {
    "displayName": "A managed identity should be enabled on your machine",
    "policyType": "Custom",
    "mode": "Indexed",
    "description": "Resources managed by Automanage should have a managed identity.",
    "metadata": {
      "version": "1.0.0-preview",
      "preview": true,
      "createdBy": "829e58c3-742e-4964-aba4-58334c64fa42",
      "createdOn": "2023-11-01T10:42:11.2130576Z",
      "updatedBy": null,
      "updatedOn": null
    },
    "parameters": {
      "effect": {
        "type": "String",
        "metadata": {
          "displayName": "Effect",
          "description": "Enable or disable the execution of the policy"
        },
        "allowedValues": [
          "Audit",
          "deny",
          "Disabled"
        ],
        "defaultValue": "deny"
      }
    },
    "policyRule": {
      "if": {
        "allOf": [
```

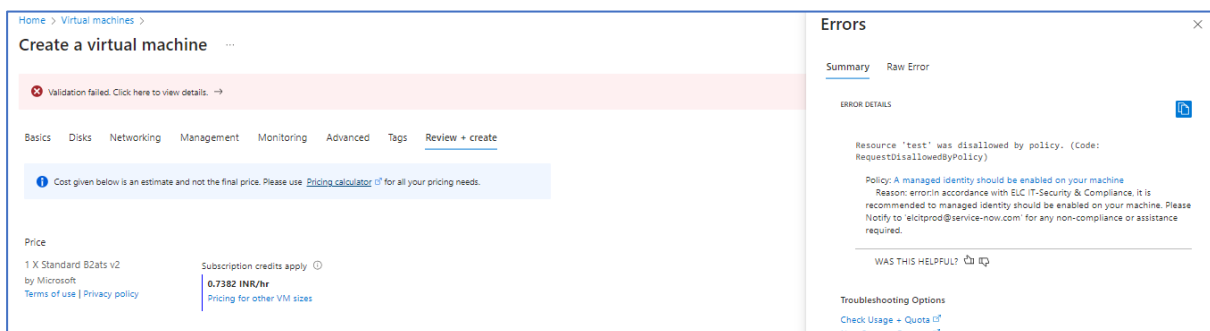
```

{
  "field": "type",
  "in": [
    "Microsoft.Compute/virtualMachines",
    "Microsoft.HybridCompute/machines"
  ],
},
{
  "field": "identity.type",
  "notContains": "SystemAssigned"
},
{
  "field": "identity.type",
  "notContains": "UserAssigned"
}
],
"then": {
  "effect": "[parameters('effect')]"
}
},
},
"id": "/subscriptions/9073e58b-15b4-4cfe-8ce0-b09f430f15c6/providers/Microsoft.Authorization/policyDefinitions",
"type": "Microsoft.Authorization/policyDefinitions",
"name": "1323f081-d378-47bd-bc33-bc0e786a37de",
"systemData": {
  "createdBy": "arunkumar@virtualkannan.com",
  "createdByType": "User",
  "createdAt": "2023-11-01T10:42:11.1519229Z",
  "lastModifiedBy": "arunkumar@virtualkannan.com",
  "lastModifiedByType": "User",
  "lastModifiedAt": "2023-11-01T10:42:11.1519229Z"
}
}

```

5.5 Error Details

The location of the error details depends on what aspect of Azure Policy you're working with & error summary details.



Home > Virtual machines > Create a virtual machine

Validation failed. Click here to view details. →

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Cost given below is an estimate and not the final price. Please use [Pricing calculator](#) for all your pricing needs.

Price

1 X Standard B2ats v2 by Microsoft

Subscription credits apply ⓘ

0.7382 INR/hr

[Pricing for other VM sizes](#)

[Terms of use](#) | [Privacy policy](#)

Errors

Summary Raw Error

ERROR DETAILS

Resource 'test' was disallowed by policy. (Code: RequestDisallowedByPolicy)

Policy: A managed identity should be enabled on your machine
Reason: error in accordance with ELC IT-Security & Compliance, it is recommended to managed identity should be enabled on your machine. Please Notify to 'elcprod@service-now.com' for any non-compliance or assistance required.

WAS THIS HELPFUL? 👍 👎

Troubleshooting Options

[Check Usage + Quota](#) ⓘ

[New Support Request](#) ⓘ

Figure 7 - Validation Failed error summary details.

5.6 Exceptions

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

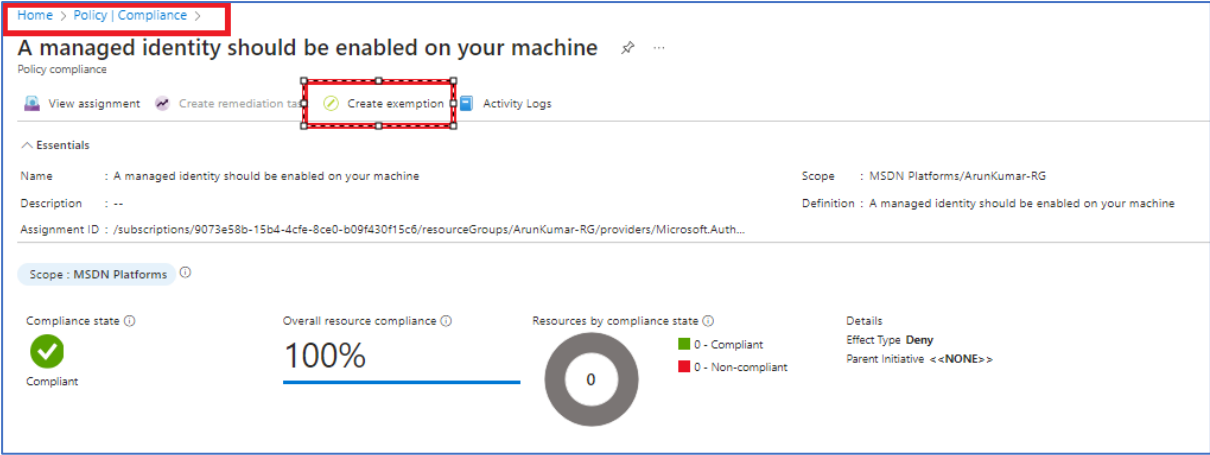


Figure 2 - Select the policy, Click on Create Exemption.

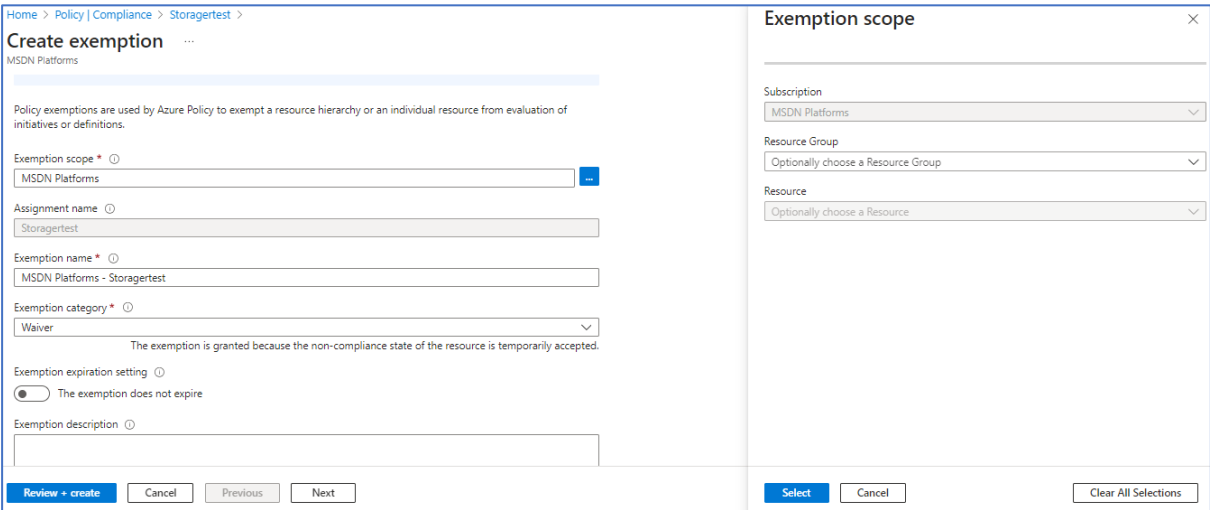


Figure 3 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

6.0 Appendix

6.1 Abbreviations

Abbreviations	Descriptions
CIS	Center for Internet Security
CMMC	Cybersecurity Maturity Model Certification
VM	Virtual Machine
IoT	Internet of Things
NIST	National Institute of Standards and Technology
NA	Not Applicable

7.0 Reference Document links

- Azure Security Benchmark 3.0
[Overview of the Azure Security Benchmark v3 | Microsoft Learn](#)
- <https://elcompanies.sharepoint.com/:f:/s/CloudSecurity/EijeYgvn7QJMroSKfXcXaSUBX8h5fditQG2ZMtJHPpNSzQ?e=wwhdsH>
- Regulatory Compliance
[Regulatory Compliance details for ISO 27001:2013 - Azure Policy | Microsoft Learn](#)