**ELC (Estée Lauder Companies) – Azure Network Security - Proof of Concept (POC)**

**Submitted to**

Text, logo

Description automatically generated

**By**

A logo with colorful dots

Description automatically generated

**Wipro Technologies**

**11-2023**

**Revision History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date of Revision** | **Description of Change** | **Reason for Change** | **Reviewed By** |
| 1.1 | 09-Oct-23 | Initial Draft | NA | Siva |
|  |  |  |  |  |
|  |  |  |  |  |

**Author/Reviewer/Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Designation** | **Responsibility** | **Date** |
| Siva Rami Reddy | Wipro Cloud Security Engineer | Author | 09-Oct-23 |
| Kannan Kuppusamy | Wipro Project Manager | Review and Approval | 00-Oct-23 |
| Felix Jebamani | Wipro Architects | Review and Approval | 00-Oct-23 |
| Jamshid Abedi | ELC ED, Global Head of Security Engineer | Review and Approval | 00-Oct-23 |

Table of Contents

[1.1 Description – 4](#_Toc151397747)

[1.2 Control Domain 4](#_Toc151397748)

[1.3 Non-Compliance Message - 4](#_Toc151397749)

[1.4 Policy Definition- 4](#_Toc151397750)

[1.5 Error Details – 6](#_Toc151397751)

[1.6 Exceptions – 6](#_Toc151397752)

[2 Best 8](#_Toc151397753)

[2.1 Description – Disabling 8](#_Toc151397754)

[2.2 Control Domain - 8](#_Toc151397755)

[2.3 Non-Compliance Message - In 8](#_Toc151397756)

[2.4 Policy Definition - 8](#_Toc151397757)

[2.5 Error Details – 9](#_Toc151397758)

[2.6 Exceptions – 9](#_Toc151397759)

[3 Best 11](#_Toc151397760)

[3.1 Description – Disabling 11](#_Toc151397761)

[3.2 Control Domain - 11](#_Toc151397762)

[3.3 Non-Compliance Message - 11](#_Toc151397763)

[3.4 Policy Definition – 11](#_Toc151397764)

[3.5 Error Details – 12](#_Toc151397765)

[3.6 Exceptions – 12](#_Toc151397766)

[4) 14](#_Toc151397767)

[4.1 Description – Deploy 14](#_Toc151397768)

[4.2 Control Domain - 14](#_Toc151397769)

[4.3 Non-Compliance Message - 14](#_Toc151397770)

[4.4 Policy Definition - 14](#_Toc151397771)

[4.5 Error Details – 16](#_Toc151397772)

[4.6 Exceptions – 16](#_Toc151397773)

**5) Appendix -……………………………………………………………………………………………………………………………… 17**

**5.1 Abbrevations-………………………………………………………………………………………………………………………. 17**

**6) Reference Document Links-……………………………………………………………………………………………………. 17**

**1. Best Practice – Networks/Subnets should be associated with a Network Security Group**

**1.1 Description –** Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs (Network Security Group) (Network Security Group) contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.

**1.2 Control Domain -** Azure Security Benchmark V1.0 - 1.1, CIS Controls v7.1 - 14.1, Azure Security benchmark V 2.0 - NS-1, CIS Controls v7.1 - 14.1, NIST. SP800-53 r4 ID(s) - Sec-7, Azure Security Benchmark V3.0, CIS Controls v7.1 - 14.1, NIST SP800-53 r4 ID(s) - Sec-7, Microsoft Cloud Security Benchmark V1.0 - NS-1, CIS Controls v7.1 ID(s) - 14.1, NIST SP800-53 r4 ID(s) - Sec-7.

**1.3 Non-Compliance Message** -In accordance with ELC IT (Information Technology) Security compliance & Azure Benchmark, it is recommended to be allows the Subnets associated with a Network Security Group. Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **1.4 Policy Definition-**

{ {

    "name": "Deny-Subnet-Without-Nsg",

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

    "apiVersion": "2022-11-22",

    "scope": null,

    "properties": {

      "policyType": "Custom",

      "mode": "All",

      "displayName": "Subnet/Network should have a Network Security Group",

      "description": " policy will deny the creation of a network/subnet without an NSG.",

      "metadata": {

        "version": "1.1.0",

        "category": "Network"

      },

      "parameters": {

        "effect": {

          "type": "String",

          "allowedValues": [

            "Audit",

            "Deny",

            "Disabled"

          ],

          "defaultValue": "Deny",

          "metadata": {

            "displayName": "Effect",

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

          }

        },

        "excludedSubnets": {

          "type": "Array",

          "metadata": {

            "displayName": "Excluded Subnets",

            "description": "subnets excluded from this policy"

          },

          "defaultValue": [

            "GatewaySubnet",

            "AzureFirewallSubnet",

            "AzureFirewallManagementSubnet"

          ]

        }

      },

      "policyRule": {

        "if": {

          "anyOf": [

            {

              "allOf": [

                {

                  "equals": "Microsoft.Network/virtualNetworks",

                  "field": "type"

                },

                {

                  "exists": "false",

                  "field": "Microsoft.Network/virtualNetworks/subnets [\*]. networkSecurityGroup.id"

                }

              ]

            },

            {

              "allOf": [

                {

                  "equals": "Microsoft.Network/virtualNetworks/subnets",

                  "field": "type"

                },

                {

                  "field": "name",

                  "notIn": "[parameters('excludedSubnets')]"

                },

                {

                  "exists": "false",

                  "field": "Microsoft.Network/virtualNetworks/subnets/networkSecurityGroup.id"

                }

              ]

            }

          ]

        },

        "then": {

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

        }

      }

    }

  }

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

A screenshot of a computer

Description automatically generated

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.

A screenshot of a computer

Description automatically generated

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).

**2 Best Practice – Network interface should not have public Ip Address**

**2.1 Description – Disabling** the public network access property improves security by ensuring your NSG can only be accessed from a private endpoint. This configuration denies all logins that match IP or virtual network-based security system rules.

**2.2 Control Domain -** Azure Security Benchmark V1.0 - 1.1, CIS Controls v7.1 - 12.3, Azure Security benchmark V 2.0 - NS-4, CIS Controls v7.1 - 12.3, NIST. SP800-53 r4 ID(s) - Sec-5, Azure Security Benchmark V3.0 - NS-1, CIS Controls v7.1 - 12.3, NIST. SP800-53 r4 ID(s) - AC-4, Microsoft Cloud Security Benchmark V1.0 - NS-1, CIS Controls v7.1 ID(s) - 12.3, NIST SP800-53 r4 ID(s) - AC-4.

**2.3 Non-Compliance Message - In** accordance with ELC IT Security compliance & Azure Benchmark, it is recommended to "Network interfaces should not have public IPs (Indirect Procurement) (Indirect Procurement)". Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **2.4 Policy Definition -**

{

    "displayName": "Network interfaces should not have public IPs",

    "policyType":"Custom",

    "mode": "Indexed",

    "description":"This policy denies the network interfaces which are configured with any public IP. Public IP addresses allow internet resources to communicate inbound to Azure resources, and Azure resources to communicate outbound to the internet. This should be reviewed by the network security team.",

    "parameters": {},

    "policyRule": {

      "if": {

        "allOf": [

          {

            "field": "type",

            "equals": "Microsoft. Network/network Interfaces"

          },

          {

            "not": {

              "field": "Microsoft. Network/network Interfaces/Ip configurations[\*].publicIpAddress.id",

              "not Like": "\*"

            }

          }

        ]

      },

      "then": {

        "effect": "deny"

      }

    }

}

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

A screenshot of a computer

Description automatically generated

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

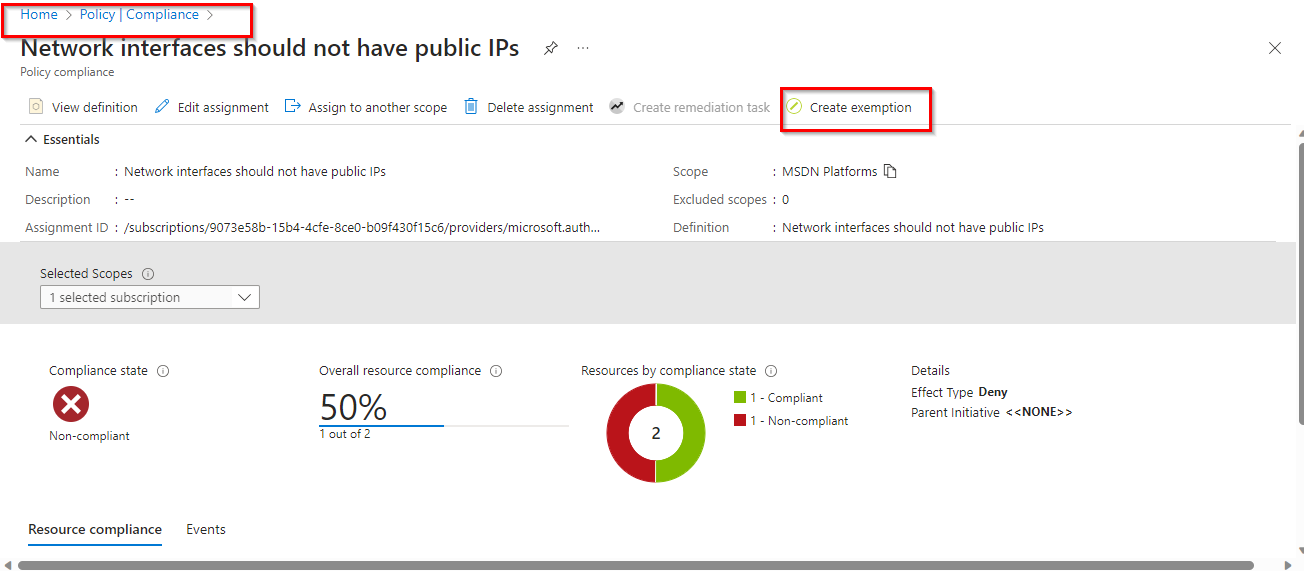


Figure 4 - Select the policy, Click on Create Exemption.

A screenshot of a computer

Description automatically generated

Figure 5 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

**3 Best Practice – Public Network Access Should be Disabled on Azure SQL Database**

**3.1 Description –** Disabling the public network access property improves security by ensuring your Azure SQL Database can only be accessed from a private endpoint. This configuration denies all logins that match IP (Indirect Procurement) or virtual network-based security system rules.

**3.2 Control Domain -** Azure Security Benchmark V1.0 - 1.1, CIS Controls v7.1 - 12.3, Azure Security benchmark V 2.0 - NS-4, CIS Controls v7.1 - 12.3, NIST. SP800-53 r4 ID(s) - Sec-5, Azure Security Benchmark V3.0 - NS-1, CIS Controls v7.1 - 12.3, NIST. SP800-53 r4 ID(s) - AC-4, Microsoft Cloud Security Benchmark V1.0 - NS-1, CIS Controls v7.1 ID(s) - 12.3, NIST SP800-53 r4 ID(s) - AC-4.

**3.3 Non-Compliance Message -** in accordance with ELC IT Security compliance & Azure Benchmark, it is recommended to "Public Network Access Should be Disabled on Azure SQL Database". Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **3.4 Policy Definition –**

{

    "properties": {

      "displayName": "Public network access on Azure SQL Database should be disabled",

      "policyType": "Custom",

      "mode": "Indexed"

      }

      "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. SQL/servers"

            },

            {

              "field": "Microsoft. SQL/servers/publicNetworkAccess",

              "not Equals": "Disabled"

            }

          ]

        },

        "then": {

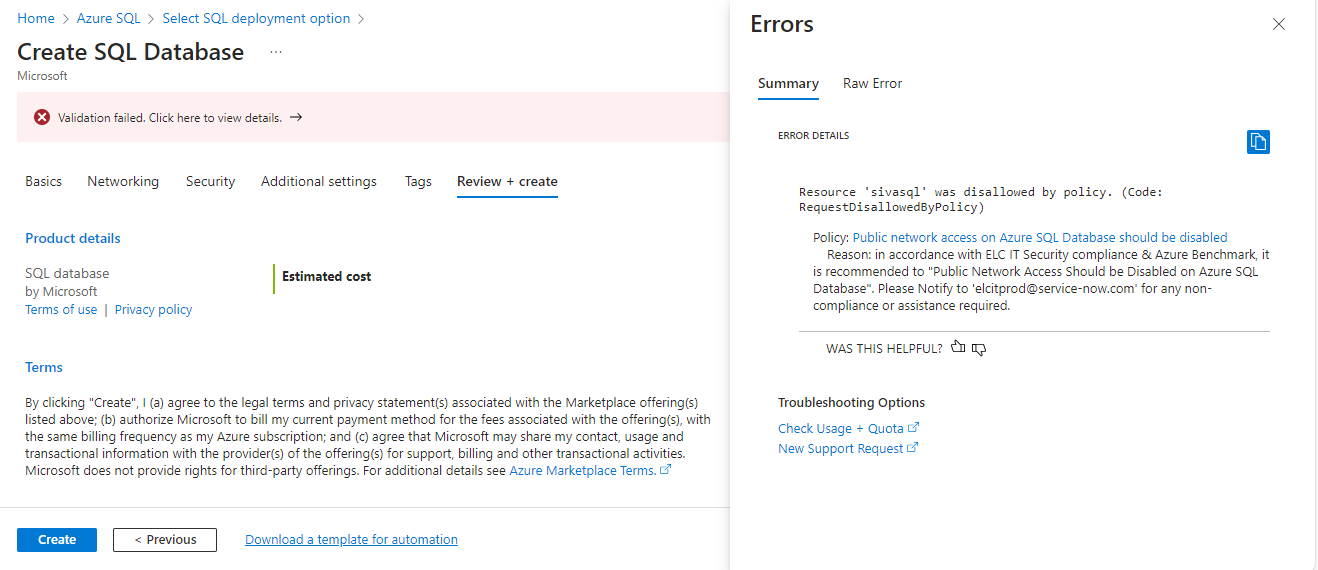
          "effect": "[parameters('effect')]"

        }

      }

}

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



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

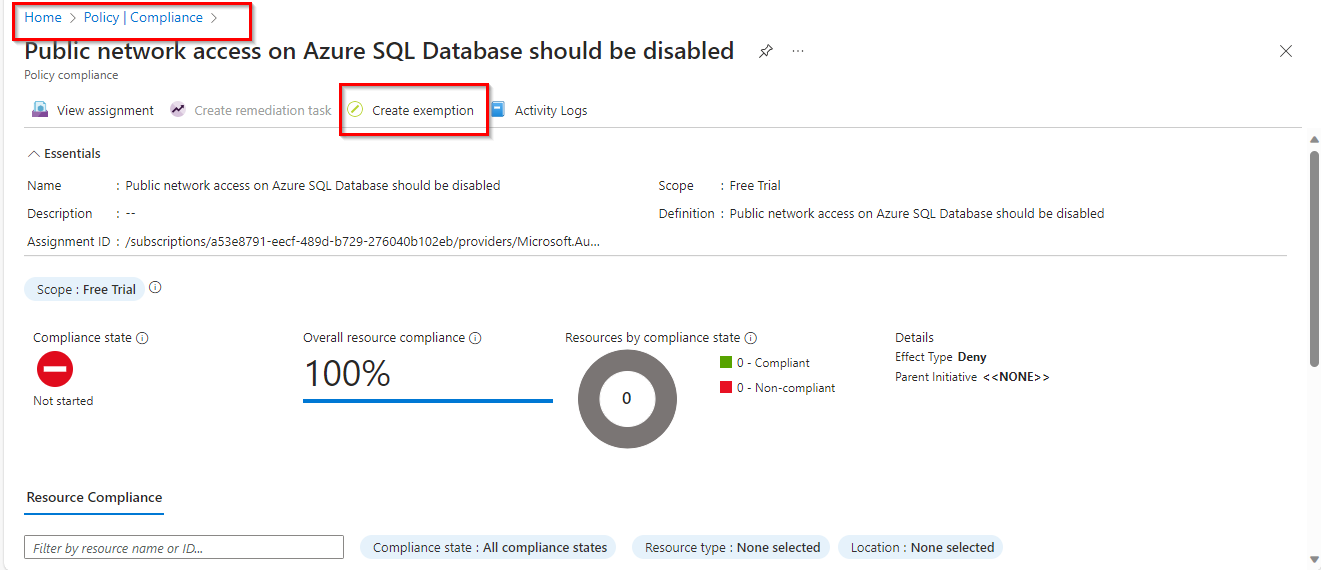


Figure 6 - Select the policy, Click on Create Exemption.

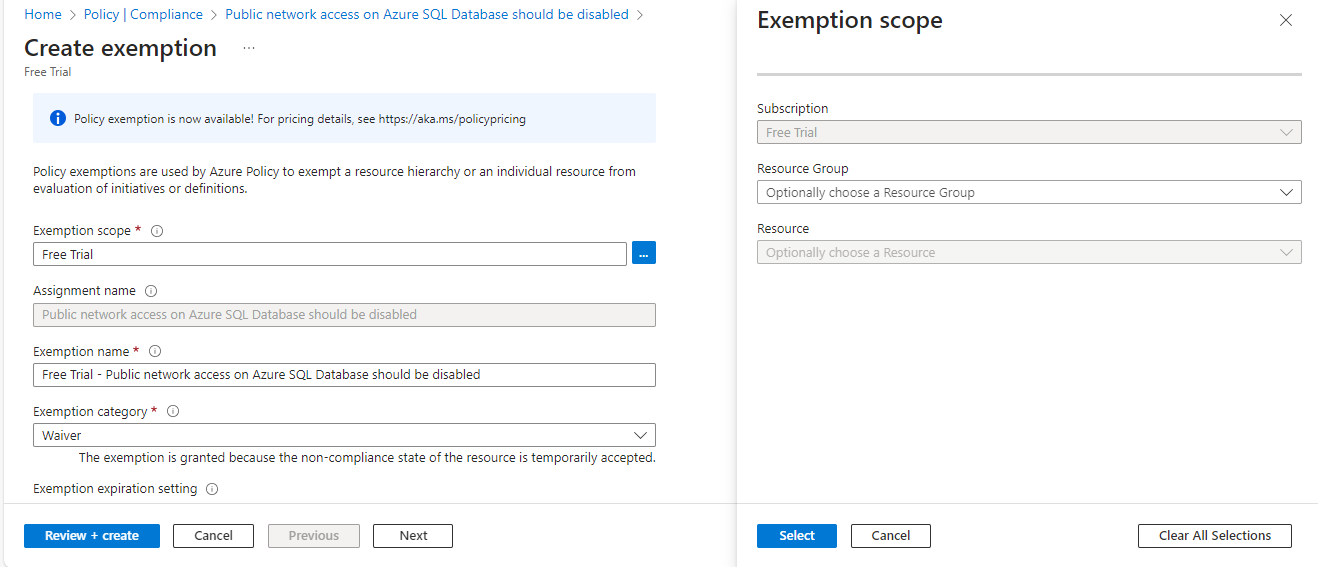


Figure 7 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

**4) Best Practice – Web Application Firewall (WAF) should be enabled for Application Gateway**

**4.1 Description – Deploy** Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.

**4.2 Control Domain -** Azure Security Benchmark V1.0 - 1.7, CIS Controls v7.1 - 12.9, Azure Security benchmark V 2.0 - NS-4, CIS Controls v7.1 - 12.9, NIST. SP800-53 r4 ID(s) - Sec-7, Azure Security benchmark V 3.0 - NS-6, CIS Controls v7.1 - 12.9, NIST. SP800-53 r4 ID(s) - Sec-7, Microsoft Cloud Security Benchmark V1.0 - NS-6, CIS Controls v7.1 ID(s) - 12.9, NIST SP800-53 r4 ID(s) - Sec-7.

**4.3 Non-Compliance Message -** in accordance with ELC IT Security compliance & Azure Benchmark, it is recommended to "Web Application Firewall (WAF) should be enabled for Application Gateway". Please Notify to 'elcitprod@service-now.com' for any non-compliance or assistance required.

# **4.4 Policy Definition -**

{

    "properties": {

      "displayName": "Web Application Firewall (WAF) should be enabled for Application Gateway",

      "policyType": "Custom",

      "mode": "Indexed",

      "metadata": {

        "version": "2.0.0",

        "created By": "bc8ede02-acb0-4a23-baf8-2c43ac0c2acf",

        "createdOn": "2023-11-01T03:46:01.9402353Z",

        "updated By": 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.Network/applicationGateways"

            },

            {

              "field": "Microsoft.Network/applicationGateways/webApplicationFirewallConfiguration",

              "exists": "false"

            },

            {

              "field": "Microsoft.Network/applicationGateways/firewallPolicy",

              "exists": "false"

            }

          ]

        },

        "then": {

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

        }

      }

    },

    "id": "/subscriptions/a53e8791-eecf-489d-b729-276040b102eb/providers/Microsoft.Authorization/policyDefinitions/bd3992e4-693e-46ee-8e7c-f547dfdf2bd6",

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

    "name": "bd3992e4-693e-46ee-8e7c-f547dfdf2bd6",

    "systemData": {

      "createdBy": "siva@arunkumarv12outlook.onmicrosoft.com",

      "createdByType": "User",

      "createdAt": "2023-11-01T03:46:01.9057596Z",

      "lastModifiedBy": "siva@arunkumarv12outlook.onmicrosoft.com",

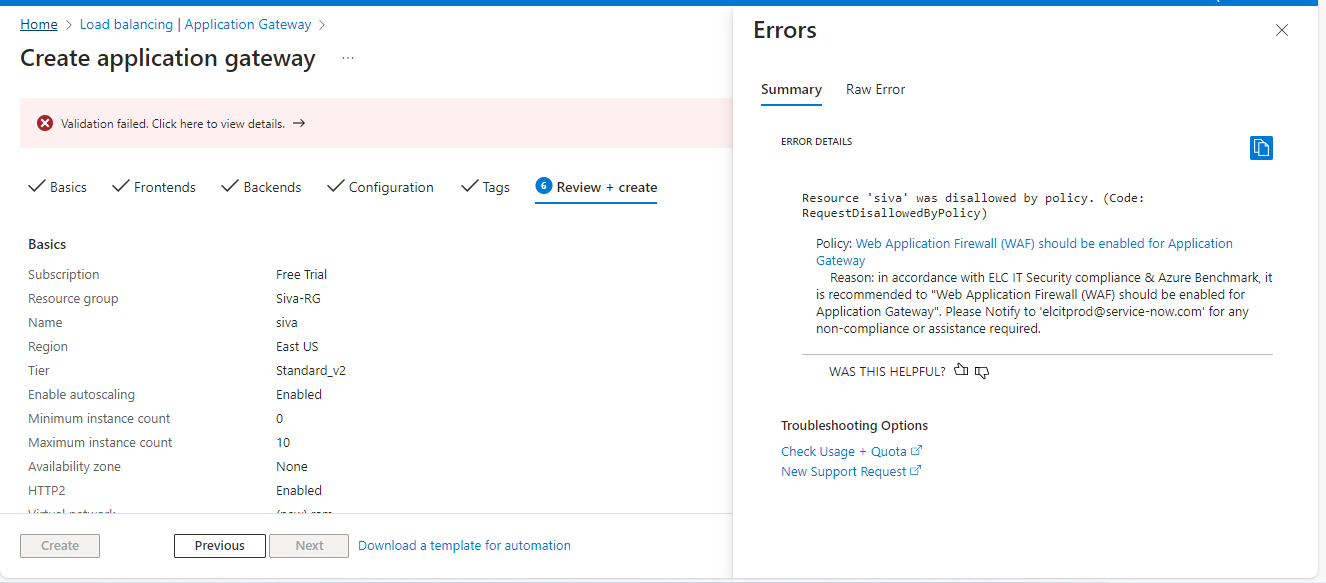
      "lastModifiedByType": "User",

      "lastModifiedAt": "2023-11-01T03:46:01.9057596Z"

    }

  }

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



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

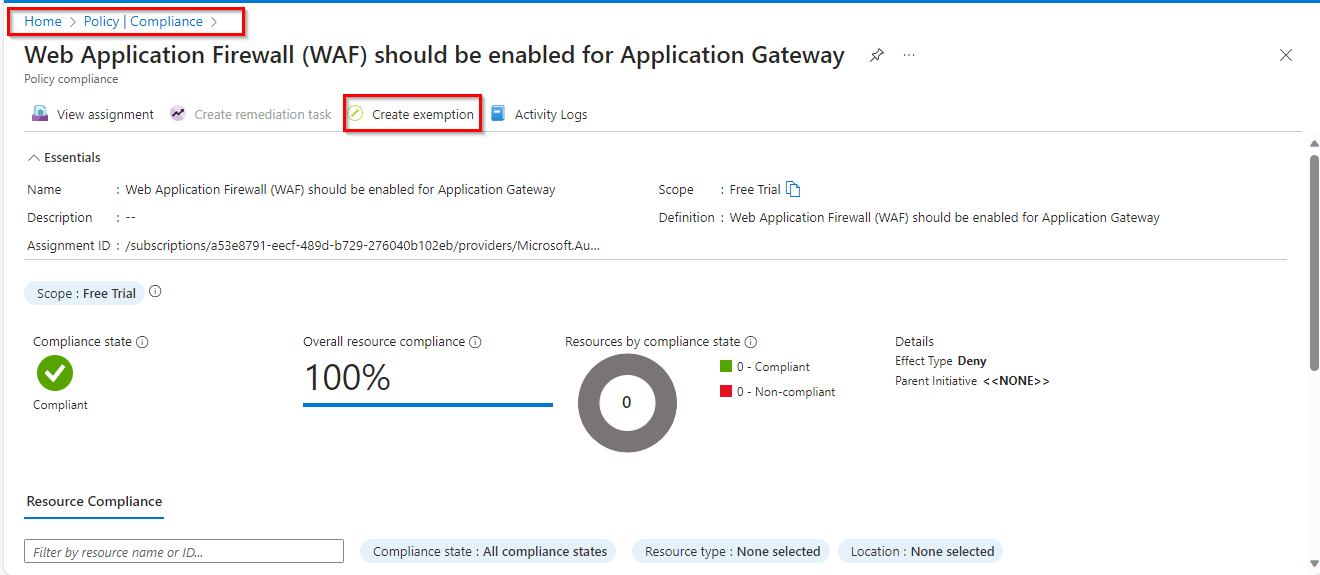


Figure 8 - Select the policy, Click on Create Exemption.

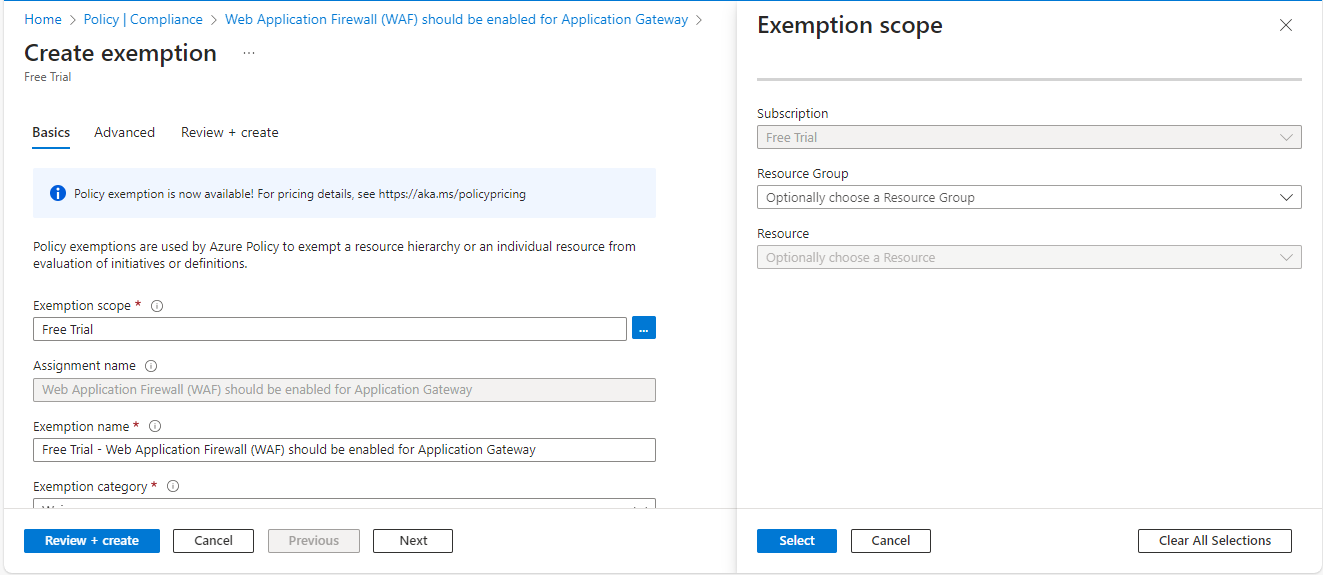


Figure 9 - Select the Exemption Scope (Subscription/ Resource Group / Resource).

**5.** **Appendix**

**5.1** **Abbreviations**

|  |  |
| --- | --- |
| **Abbreviations** | **Descriptions** |
| **CIS** | Center for Internet Security |
| **CMMC** | Cybersecurity Maturity Model Certification |
| **NSG** | Network Security Group |
| **IoT** | Internet of Things |
| **NIST** | National Institute of Standards and Technology |
| **NA** | Not Applicable |
| **WAF** | Web Application Firewall |
| **ACL** | Access Control List |

**6. 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)

<https://elcompanies.sharepoint.com/:f:/s/CloudSecurity/EijeYgvn7QJMroSKfXcXaSUBX8h5fditQG2ZMtJHPpNSzQ?e=wwhdsH>

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)