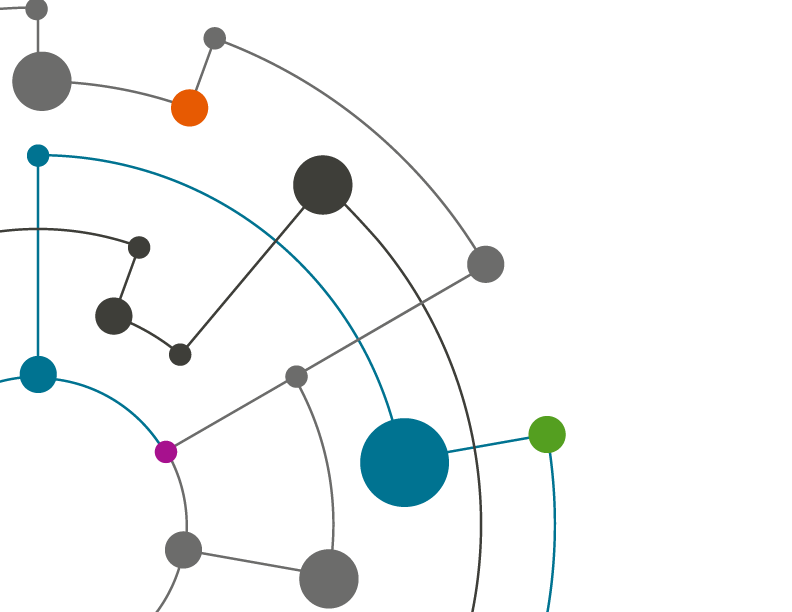
**­­SSC Azure Guardrail Implementation Guide**

Research and Development (R&D)

Cloud Product Management & Services Directorate (CPMS)

Chief Technology Officer Branch (CTO)

Shared Services Canada (SSC)



|  |  |
| --- | --- |
| Document Revision: | 0.6 |
| Status: | Draft |
| Publish Date: | April 29, 2020 |

Document Approvals

The signing authorities below concur with the conditions and responsibilities specified within this document.

|  |  |  |  |
| --- | --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Jacqueline Morcos | Director,  Research and Development  Cloud Product Management & Services Directorate  Chief Technology Officer  Shared Services Canada | Date | Signature |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Philippe Lefebvre | Director,  Digital Transformation Office  Chief Information Office  Shared Services Canada | Date | Signature |
|  |  |  |  |

Document History

**History of Changes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ver. # | Date | Consulted/Reviewers  (name of individual & working group consulted) | Brief description of Change | Author of Change |
| v0.1 | 2020-02-24 | Azure Design Team (CSD) | Initial Release for VDC |  |
| 0.21 | 2020-02-24 | Azure Design Team (CSD) | Updated 3.2 with Whitelisting reference |  |
| 0.22 | 2020-04-14 | Azure Design Team (CSD) | Updated section 4. Added Annex D. |  |
| 0.3 | 2020-04-17 | Azure Design Team (CSD) | Updated section 3- 6 |  |
| 0.4 | 2020-04-27 | Azure Design Team (CSD) | Peer Review |  |
| 0.5 | 2020-04-28 | Azure Design Team (CSD) | Updated Section 3 with controls # |  |
| 0.6 | 2020-04-29 | Azure Design Team (CSD) | Updated GR5 |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

1 Overview 6

1.1 Purpose 6

1.2 GC Cloud Governance 7

1.3 Document Reference 7

1.4 Guardrail mappings 8

2 Azure Policy Implementation for 30-Day Compliance 9

2.1 Canada Federal PBMM Blueprint 9

2.1.1 Implementation Prerequisites 10

2.1.2 PBMM Blueprint Implementation 11

2.2 Azure Landing Zone VDC Policy Definition 13

2.3 Azure Security Center 17

2.4 GC Marketplace Whitelist 17

3 Azure AD Tenant Implementation for 30-Day Compliance 18

3.1 Guardrail 1: Protect Root / Global Admins Account 18

3.2 Guardrail 2: Management of Administrative Privileges 20

3.3 Guardrail 3: Cloud Console Access 20

3.4 Guardrail 4: Enterprise Monitoring Accounts 20

3.5 Guardrail 11: Logging and Monitoring 21

4 Azure Network Implementation for 30-Day Compliance 23

4.1 SSC Azure Landing Zone Design 23

5 Cyber Defense Services 26

Appendix A – MAPPING ITSG-33 SECURITY CONTROLS TO GUARDRAIL IMPLEMENTATION 27

Appendix B – SUGGESTED EVIDENCING OF GUARDRAILS 28

Evidencing 28

5.1 Guardrail 1: Protect Root / Global Admins Account 28

5.2 Guardrail 2: Management of Administrative Privileges 30

5.3 Guardrail 3: Cloud Console Access 32

5.4 Guardrail 4: Enterprise Monitoring Accounts 33

5.5 Guardrail 5: Data Location 34

5.6 Guardrail 6: Protection of Data-at-Rest 34

5.7 Guardrail 7: Protection of Data-in-Transit 35

5.8 Guardrail 8: Network Segmentation and Separation 35

5.9 Guardrail 9: Network Security Services 35

5.10 Guardrail 10: Cyber Defense Services 35

5.11 Guardrail 11: Logging and Monitoring 35

5.12 Guardrail 12: Configuration of Cloud Marketplaces 39

List of Tables

[**Table 1: Document Reference List** 7](#_Toc38982094)

[Table 2: PBMM Policy Assignment/Exception Table 10](#_Toc38982095)

[Table 3: Canada Federal PBMM Blueprint Policy Definition 13](#_Toc38982096)

[Table 4: Audit Canada Federal PBMM Policy Initiative 16](#_Toc38982097)

[Table 5: Cloud Usage Profile 23](#_Toc38982098)

List of Figures

[Figure 1: GC PBMM Blueprint Assignment 9](#_Toc38982099)

[Figure 2: Create Blueprint 11](#_Toc38982100)

[Figure 3: Blueprint Artifact List 12](#_Toc38982101)

[Figure 4: Publish Blueprint 12](#_Toc38982102)

[Figure 5: SSC Azure Landing Zone Release 24](#_Toc38982103)

1. Overview

This Detailed Design Specification (DDS) provides the implementation details of the Azure Cloud Guardrails used to meet PBMM compliance within the Microsoft Landing Zone Virtual Data Center (VDC). It includes prescriptive guidance for establishing a secure baseline configuration within Azure in alignment with TBS mandated 30-day guardrails for PBMM compliance. The Guardrail implementation strategy follows an iterative approach to security and governance through a mix of CSP Policy, Infrastructure as Code (IaC), manual configuration, automation, and people/process. This document will be expanded to include security control definitions and implementation details on the 90, and 180-day guardrails defined to meet GC longer term PBMM compliance.

Departments using the GC PBMM contacts through the SSC Cloud Service Broker must complete a series of onboarding checkpoints to prove cloud security controls are in place. The mandatory security controls are required to maintain an Authority to Operate (ATO) and enforce the security architecture required for PBMM. The timeline uses the concept of security overlays as follows:

* ***30 day:*** *High-priority technical security controls are implemented as part of the GC 30-day guardrails to onboard a secure tenant architecture in the cloud to achieve tenant Interim ATO. Technical controls will be addressed and processes associated with those controls are not addressed and need to be addressed for the ATO within 90-180 days.*
* ***90 day:*** *Security controls to validate additional security mechanisms of the tenant (i.e., Departmental) environment (people, processes, policies, procedures, operations, ITSM, physical, personnel, etc.) and achieve tenant ATO. Note that some of this may already be addressed by existing departmental ATOs, or just require cloud extensions.*
* ***180 day:*** *Security controls to secure onboarding and ATO of application workloads and additional low-priority security controls and security control enhancements identified as part of the GC-approved Azure profile with a total of 134 ITSG-33 security controls. This includes the full set of controls required for DevSecOps onboarding of new applications.*

SSC Cloud Operations are only responsible for the evaluation of the 30-day Guardrails. Detailed scope and procedures for validating the 90-day and 180-day Guardrails are still being evaluated within the Government of Canada.

The SSC Azure Landing Zone (LZ) design artifacts implement a Virtual Data Center with many of these security controls built-in to accelerate the Security Assessment and Authorization (SA&A) process. Following the Azure LZ approach will help to avoid duplication of effort for GC departments to get up and running in Azure. The design does not remove the requirement for departments to follow their own SA&A processes, the goal is to leverage a common architecture where possible to minimize the time and cost to achieve PBMM certification. Application design and data classification is out of scope of the Landing Zone initiative.

* 1. Purpose

This document provides implementation specifics of the SSC Azure 30-Day Guardrail Implementation for the Azure Virtual Data Center (VDC). It is broken down into five sections that must all be implemented to an Azure Tenant in order be compliant for the 30-Day Guardrail verification. Sections 3 – 7 detail how to implement the different components of the 30-Day Guardrails. Appendix A provides a step-by-step, with examples, of the required evidence for the Azure Active Directory component.

* 1. GC Cloud Governance

A base structure is defined for cloud resource naming that allows for governance while supporting flexibility to meet departmental business and technical requirements. The following proposal has been developed in discussion with TBS, SSC, CSE, and Vendors:

* **Application of Governance Frameworks:** The implementation and maintenance of the cloud governance framework is dependent on well documented Cloud Guardrail configuration, compliance monitoring and reporting.
* **Azure Blueprints and Policy:** Provide built-in compliance controls on areas like compute, network and various other Azure services.
* **Resource Management:** Quickly find resources associated with specific workloads, environments, ownership groups, or other important information. Resource identification is critical to assigning organizational roles and access permissions for resource management.
* **ITSG-33 Security Controls:** Naming and tagging plays a key role security monitoring and incident management. A naming and tagging standard is required for ITSG-33 compliance and the implementation of GC Guardrails.
* **Automation:** In addition to making resources easier for IT to manage, a proper organizational naming scheme enables automation as part of resource creation, operational monitoring, and the creation of DevOps processes.
* **Compliance Reporting:** Business owners need to be aware of cloud resource consumption to support chargeback/showback accounting, cloud resources need to be organized to reflect ownership and usage.
  1. Document Reference

GC-Docs Azure Virtual Data Centre project repository (contact CSD Cloud Management Office for read access)

<https://gcdocs.gc.ca/ssc-spc/llisapi.dll/open/61082429>

The following links reference additional support material used in the development of this design.

| Document Title | Description / Link |
| --- | --- |
| Signed CSD-Scope Statement Microsoft Landing Zone Prototype & ConOps.pdf | Microsoft Landing Zone (LZ) Project scope  <https://gcdocs.gc.ca/ssc-spc/llisapi.dll/open/44491286> |
| Azure Governance Framework Draft v0.1.docx (work in progress) | <https://gcdocs.gc.ca/ssc-spc/llisapi.dll/open/59081055> |
| SSC Naming and Tagging Standard for Azure | <https://gcdocs.gc.ca/ssc-spc/llisapi.dll/open/61082429> |
| Azure Whitelisting | Azure Whitelisting Process and instructions  [*https://gcdocs.gc.ca/ssc-spc/llisapi.dll/open/71440075*](https://gcdocs.gc.ca/ssc-spc/llisapi.dll/open/71440075) |
| Government of Canada Cloud Guardrails | <https://gcdocs.gc.ca/ssc-spc/llisapi.dll/open/67925334> |
| Azure Emergency Access Procedure template | <https://gcdocs.gc.ca/ssc-spc/llisapi.dll/open/72824320> |
| Cloud usage profiles | <https://gcdocs.gc.ca/ssc-spc/llisapi.dll/open/72829765> |

**Table 1: Document Reference List**

* 1. Guardrail mappings

|  |  |
| --- | --- |
| Guardrail | Location where implemented |
| Guardrail 1: Protect Root / Global Admins Account | Manual Implementation. See Section 3.1 |
| Guardrail 2: Management of Administrative Privileges | Manual Implementation. See Section 3.2 |
| Guardrail 3: Cloud Console Access | Manual Implementation. See Section 3.3 |
| Guardrail 4: Enterprise Monitoring Accounts | Manual Implementation. See Section 3.4 |
| Guardrail 5: Data Location | Enforced thru implementation of the PBMM policies. See Section 2 |
| Guardrail 6: Protection of Data-at-Rest | Manual Implementation. See Section 2 |
| Guardrail 7: Protection of Data-in-Transit | Manual Implementation. See Section 2 |
| Guardrail 8: Network Segmentation and Separation | As per design in Section 4 |
| Guardrail 9: Network Security Services | As per design in Section 4 |
| Guardrail 10: Cyber Defense Services | Manual Implementation. See Section 5 |
| Guardrail 11: Logging and Monitoring | Manual Implementation. See Section 3.11 |
| Guardrail 12: Configuration of Cloud Marketplaces | Enforced thru implementation of the Azure Whitelisting policies. See Section 2.4 |

**Table 2: Map of Guardrails**

1. Azure Policy Implementation for 30-Day Compliance

Among other things, Azure Policy is a cloud service that enables implementation, enforcement, and auditing of the departmental cloud governance framework. In the context of the 30-Day Guardrails, policies are used to achieve compliance with “*some*” of the PBMM mandatory security controls. This section outlines the policy implementation process within the SSC Azure Landing Zone VDC environment. Three implementation options have been evaluated:

* Manually configuring Azure policy through the portal and code.
* Leveraging the TBS GitHub repository for cloud guardrails @ <https://github.com/canada-ca/cloud-guardrails-azure> .
* Customizing the Canada Federal PBMM Blueprint provided by Microsoft to align with 30-Day guardrail compliance (***recommended***).
  1. Canada Federal PBMM Blueprint

Microsoft, in conjunction with TBS and SSC, have built a baseline blueprint for GC PBMM compliant policy deployment. This blueprint can be applied at either the Management Group or Subscription scopes within the Azure tenant environment. Through the Azure Portal, the Blueprint is created and saved at the appropriate scope. Figure 1 is an example of how SSC has designed their tenant hierarchy.

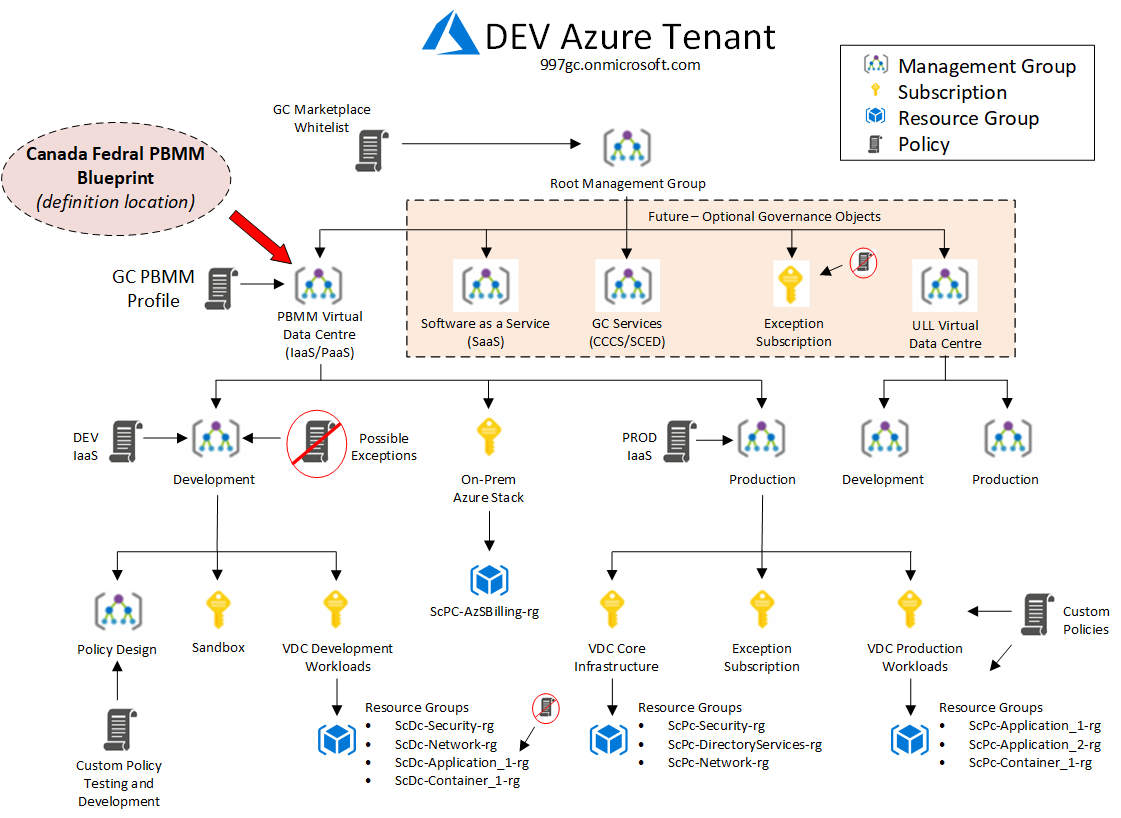


Figure 1: GC PBMM Blueprint Assignment

* + 1. Implementation Prerequisites

The implementation process specified in this document leverage the Microsoft managed Canada Federal PBMM Blueprint. The Azure governance strategy and Cloud Adoption Framework is an evolving architecture that undergoes iterative reviews to ensure business requirements and security compliance concerns are addressed. This Azure Policy implementation guide is aligned with the Azure Governance Framework Technical Architecture Document (TAD) that has been developed as part of the Azure Landing Zone Base Cloud Architecture project, refer to the document references in section 1.3 for required artifacts.

Prior to deploying the PBMM Blueprint the following prerequisites are required:

* Azure Naming and Tagging standard for the Tenant.
* Azure Governance Hierarchy design for Management Groups, Subscriptions, and Resource Groups. Create the required governance objects.
* Determine the Blueprint *Definition Location* within the Azure hierarchy. As illustrated in the diagram above, the Blueprint is defined at the Azure Virtual Data Center management group level.
* Review Blueprint artifacts and add/remove polices as required (detailed below).
* Owner level access to the top level VDC Management Group, Global Admin on the Azure Tenant. If implementing the GC Whitelist policy, access is required to the root Management Group.
* A Log Analytics Workspace for Security events and Resource Group in accordance with Naming and Tagging convention and the Azure Cloud Governance design.
* Create a Policy Assignment/Exclusion table that defines the scope for the Blueprint policies based on the target cloud profile and the governance hierarchy.

| Scope | Name | Blueprint/Policy | Type |
| --- | --- | --- | --- |
| Subscription | ScPc-PBMM VDC Core | Canada Federal PBMM Blueprint\*  Azure Security Center (ASC) Policy Initiative | Assignment |
| Subscription | ScPc-PBMM VDC Production | Canada Federal PBMM Blueprint\*  Azure Security Center (ASC) Policy Initiative | Assignment |
| Subscription | ScDc-PBMM VDC DevTest | Canada Federal PBMM Blueprint\*  Azure Security Center (ASC) Policy Initiative | Assignment |
| Subscription | ScSc-PBMM VDC Sandbox | Azure Security Center (ASC) Policy Initiative | Assignment |
| Resource Group | ScPc-VDC\_Security\_Core\_  External-rg | Networks interfaces should not have Assign public IPs | Exception |
|  |  | ***…complete table to align with departmental requirements*** |  |

Table 2: PBMM Policy Assignment/Exception Table

\* Canada Federal PBMM Blueprint with SSC customization

* + 1. PBMM Blueprint Implementation

The PBMM Blueprint is deployed following the implementation steps defined by Microsoft at <https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/canada-federal-pbmm/deploy>. The current blueprint consists of 14 policy definitions and the *[Preview]: Audit Canada Federal PBMM controls and deploy specific VM Extensions to support audit requirements* policy initiative. The policy initiative includes 68 policy definitions which are fixed but the single entry definitions can be edited. Review the list and customize the blueprint to meet the specific cloud profile as required. The PBMM Blueprint is implemented as defined below.

Follow the Microsoft deployment instructions at the link above with the following parameters:

* Create the blueprint and assign the location based on your VDC architecture.

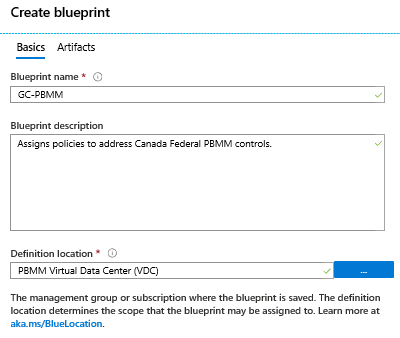


Figure 2: Create Blueprint

* Add or remove artifacts based on the 30-Day policy design. The VDC uses the default blueprint with two policy assignments added as illustrated below. Note that the “Audit Canada Federal…” policy assignment is the Microsoft configured ***initiative*** that cannot be edited. It can be removed and specific policy definitions can be cherry picked based on the cloud usage profile.

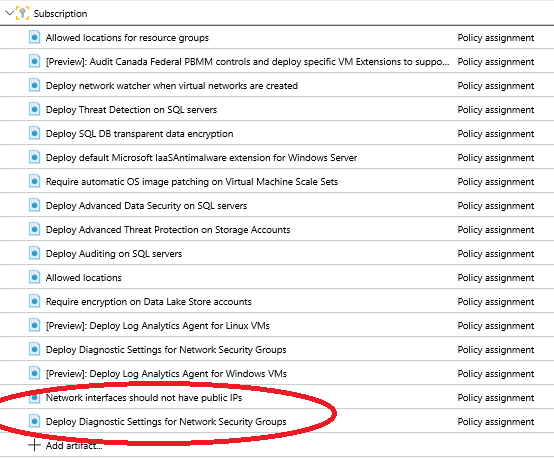


Figure 3: Blueprint Artifact List

* Publish the Blueprint

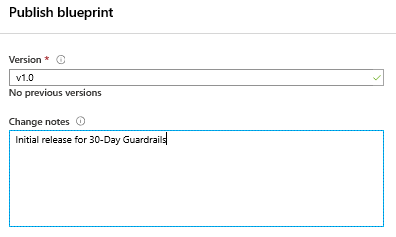


Figure 4: Publish Blueprint

* Assign the Blueprint based on Policy Assignment/Exclusion table created for the Virtual Data Center. Follow steps provided by Microsoft.
  1. Azure Landing Zone VDC Policy Definition

The Canada Federal PBMM Blueprint provides the following Azure Policy to ITSG-33 Control mapping. See <https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/canada-federal-pbmm/control-mapping> for the latest version of this mapping. The blueprint is created to align with GC Cloud profiles 3, 5, and 6 using the following policy definitions:

| GR # | Policy Definition | Effect | ITSG-33 | 30-Day |
| --- | --- | --- | --- | --- |
| 9,10 | Deploy network watcher when virtual networks are created | DeployIfNotExists | SI-4 | Yes |
| 1,2,3,4,9,10 | Deploy Advanced Data Security on SQL servers | DeployIfNotExists | AC-7  AU-12  RA-5  SC-28(1)  SI-4 | Yes |
| 5 | Allowed locations for resource groups | Deny |  | Yes |
| 9,10 | Deploy Threat Detection on SQL servers | DeployIfNotExists | SI-4 | Yes |
| 10 | Require automatic OS image patching on Virtual Machine Scale Sets |  | SI-2 | Yes |
| 9,10,11 | [Preview]: Deploy Log Analytics Agent for Windows VMs | DeployIfNotExists | AU-3(2)  AU-6(4)  AU-12  SI-4 | Yes |
|  | Deploy default Microsoft IaaSAntimalware extension for Windows Server | DeployIfNotExists | SI-3 | No |
| 11 | Deploy Diagnostic Settings for Network Security Groups | DeployIfNotExists | AU-12 | Yes |
| 6 | Deploy SQL DB transparent data encryption | DeployIfNotExists | SC-28(1) | Yes |
| 5 | Allowed locations | Deny |  |  |
| 9,10 | Deploy Advanced Threat Protection on Storage Accounts | DeployIfNotExists | SI-4 | Yes |
| 1,2,3,4,9,10 | Deploy Auditing on SQL servers | DeployIfNotExists | AU-12  SI-4 | Yes |
| 6 | Require encryption on Data Lake Store accounts | Deny | SC-28(1) | Yes |
| 1,2,3,4,9,10 | [Preview]: Deploy Log Analytics Agent for Linux VMs | DeployIfNotExists | AU-3(2)  AU-6(4)  AU-12  SI-4 | Yes |
| 11 | Activity log should be retained for at least one year | AuditIfNotExists | AU-9  AU-11 | Yes |
| 9 | Network interfaces should not have public IPs | Deny |  | Yes |
| 11 | Deploy Diagnostic Settings for Network Security Groups | DeployIfNotExists | AU-12 | Yes |
|  | [Preview]: Audit Canada Federal PBMM controls and deploy specific VM Extensions to support audit requirements | See Table Below (68 policy definitions) |  |  |

Table 3: Canada Federal PBMM Blueprint Policy Definition

| GaurdRail # | Policy Definition | Effect | ITSG-33 | 30-Day |
| --- | --- | --- | --- | --- |
| 1,2,3,4 | MFA should be enabled on accounts with owner permissions on your subscription | AuditIfNotExists | IA-2(1)  IA-8 | Yes |
| 1,2,3,4 | MFA should be enabled accounts with write permissions on your subscription | AuditIfNotExists | IA-2(1)  IA-8 | Yes |
| 10 | System updates on virtual machine scale sets should be installed | AuditIfNotExists | SI-2 | Yes |
| 8,9 | CORS should not allow every resource to access your Web Applications | AuditIfNotExists | AC-4 | Yes |
| 1,2,3,4 | Deprecated accounts should be removed from your subscription | AuditIfNotExists | AC-2 | Yes |
| 1,2,3,4 | Deprecated accounts with owner permissions should be removed from your subscription | AuditIfNotExists | AC-2 | Yes |
| 1,2,3,4 | External accounts with owner permissions should be removed from your subscription | AuditIfNotExists | AC-2 | Yes |
| 1,2,3,4 | External accounts with read permissions should be removed from your subscription | AuditIfNotExists | AC-2 | Yes |
| 8,9 | Access through Internet facing endpoint should be restricted | AuditIfNotExists | SC-7 | Yes |
| 1,2,3,4 | External accounts with write permissions should be removed from your subscription | AuditIfNotExists | AC-2 | Yes |
| 7 | Function App should only be accessible over HTTPS | Audit | SC-8(1) | Yes |
| 7 | Web Application should only be accessible over HTTPS | Audit | SC-8(1) | Yes |
| 7 | API App should only be accessible over HTTPS | Audit | SC-8(1) | Yes |
| 9,10,11 | [Preview]: Audit Log Analytics Agent Deployment - VM Image (OS) unlisted | AuditIfNotExists | AU-3(2)  AU-6(4)  AU-12  SI-4 | Yes |
| 9,10,11 | [Preview]: Audit Log Analytics Agent Deployment in VMSS - VM Image (OS) unlisted | AuditIfNotExists | AU-3(2)  AU-6(4)  AU-12  SI-4 | Yes |
| 9,10,11 | [Preview]: Audit Log Analytics Workspace for VM - Report Mismatch | Audit | AU-3(2)  AU-6(4)  AU-12  SI-4 | Yes |
| 1,2,3,4 | A maximum of 3 owners should be designated for your subscription | AuditIfNotExists | AC-5  AC-6 | Yes |
| 1,2,3,4 | There should be more than one owner assigned to your subscription | AuditIfNotExists | AC-5  AC-6 | Yes |
| 10 | Vulnerabilities in security configuration on your virtual machine scale sets should be remediated | AuditIfNotExists | RA-5  SI-2 | Yes |
|  | Remote debugging should be turned off for Function Apps | AuditIfNotExists | AC-17(1) | No |
|  | Remote debugging should be turned off for Web Applications | AuditIfNotExists | AC-17(1) | No |
|  | Remote debugging should be turned off for API Apps | AuditIfNotExists | AC-17(1) | No |
| 9 | DDoS Protection Standard should be enabled | AuditIfNotExists | SC-5 | Yes |
| 1,2,3,4 | [Preview]: Show audit results from Linux VMs that allow remote connections from accounts without passwords | AuditIfNotExists | IA-5(1) | Yes |
| 1,2,3,4 | [Preview]: Show audit results from Linux VMs that have accounts without passwords | AuditIfNotExists | IA-5(1) | Yes |
| 1,2,3,4 | [Preview]: Show audit results from Linux VMs that do not have the passwd file permissions set to 0644 | AuditIfNotExists | IA-5(1) | Yes |
| 1,2,3,4 | [Preview]: Show audit results from Windows VMs that allow re-use of the previous 24 passwords | AuditIfNotExists | IA-5(1) | Yes |
| 1,2,3,4 | [Preview]: Show audit results from Windows VMs that do not have a maximum password age of 70 days | AuditIfNotExists | IA-5(1) | Yes |
| 1,2,3,4 | [Preview]: Show audit results from Windows VMs that do not have a minimum password age of 1 day | AuditIfNotExists | IA-5(1) | Yes |
| 1,2,3,4 | [Preview]: Show audit results from Windows VMs that do not have the password complexity setting enabled | AuditIfNotExists | IA-5(1) | Yes |
| 1,2,3,4 | [Preview]: Show audit results from Windows VMs that do not restrict the minimum password length to 14 characters | AuditIfNotExists | IA-5(1) | Yes |
|  | Endpoint protection solution should be installed on virtual machine scale sets | AuditIfNotExists | SI-3  SI-3(1) | No |
|  | [Preview]: Deploy prerequisites to audit Linux VMs that allow remote connections from accounts without passwords | DeployIfNotExists | IA-5(1) | No |
| 1,2,3,4 | [Preview]: Deploy prerequisites to audit Linux VMs that have accounts without passwords | DeployIfNotExists | IA-5(1) | Yes |
| 1,2,3,4 | [Preview]: Deploy prerequisites to audit Linux VMs that do not have the passwd file permissions set to 0644 | DeployIfNotExists | IA-5(1) | Yes |
| 1,2,3,4 | [Preview]: Deploy prerequisites to audit Windows VMs that allow re-use of the previous 24 passwords | DeployIfNotExists | IA-5(1) | Yes |
| 1,2,3,4 | [Preview]: Deploy prerequisites to audit Windows VMs that do not have a maximum password age of 70 days | DeployIfNotExists | IA-5(1) | Yes |
| 1,2,3,4 | [Preview]: Deploy prerequisites to audit Windows VMs that do not have a minimum password age of 1 day | DeployIfNotExists | IA-5(1) | Yes |
| 1,2,3,4 | [Preview]: Deploy prerequisites to audit Windows VMs that do not have the password complexity setting enabled | DeployIfNotExists | IA-5(1) | Yes |
| 1,2,3,4 | [Preview]: Deploy prerequisites to audit Windows VMs that do not restrict the minimum password length to 14 characters | DeployIfNotExists | IA-5(1) | Yes |
| 9,12 | Adaptive Network Hardening recommendations should be applied on internet facing virtual machines | AuditIfNotExists | CM-2  SI-4 | Yes |
| 9 | Monitor missing Endpoint Protection in Azure Security Center | AuditIfNotExists | SI-3  SI-3(1) | Yes |
| 10 | System updates should be installed on your machines | AuditIfNotExists | SI-2 | Yes |
| 10 | Vulnerabilities in security configuration on your machines should be remediated | AuditIfNotExists | RA-5  SI-2 | Yes |
|  | Adaptive Application Controls should be enabled on virtual machines | AuditIfNotExists | CM-7(5)  CM-11 | No |
| 8 | Just-In-Time network access control should be applied on virtual machines | AuditIfNotExists | SC-7(3)  SC-7(4) | Yes |
| 10 | Vulnerabilities on your SQL databases should be remediated | AuditIfNotExists | RA-5  SI-2 | Yes |
| 6 | Disk encryption should be applied on virtual machines | AuditIfNotExists | SC-28(1) | Yes |
| 10 | Vulnerabilities should be remediated by a Vulnerability Assessment solution | AuditIfNotExists | RA-5  SI-2 | Yes |
| 11 | Audit diagnostic setting | AuditIfNotExists | AU-5  AU-12 | Yes |
| 7 | Only secure connections to your Redis Cache should be enabled | Audit | SC-8(1) | Yes |
| 1,2,3,4 | An Azure Active Directory administrator should be provisioned for SQL servers | AuditIfNotExists | AC-2(7) | Yes |
| 7 | Secure transfer to storage accounts should be enabled | Audit | SC-8(1) | Yes |
| 1,2,3,4,9,10 | Advanced data security should be enabled on your SQL managed instances | AuditIfNotExists | AC-7  AU-5  AU-12  RA-5  SC-28(1)  SI-4 | Yes |
|  | Auditing on SQL server should be enabled | AuditIfNotExists |  | No |
| 1,2,3,4,9,10 | Advanced data security should be enabled on your SQL servers | AuditIfNotExists | AC-7  AU-5  AU-12  RA-5  SC-28(1)  SI-4 | Yes |
| 1,2,3,4 | Show audit results from Windows VMs in which the Administrators group contains any of the specified members | AuditIfNotExists | AC-5  AC-6 | Yes |
| 1,2,3,4 | Show audit results from Windows VMs in which the Administrators group does not contain all of the specified members | AuditIfNotExists | AC-5  AC-6 | Yes |
| 1,2,3,4 | Show audit results from Windows web servers that are not using secure communication protocols | AuditIfNotExists | AC-5  AC-6 | Yes |
| 6 | Transparent Data Encryption on SQL databases should be enabled | AuditIfNotExists | SC-28(1) | Yes |
| 8 | Audit unrestricted network access to storage accounts | Audit | AC-17(1)  SC-7 | Yes |
| 1,2,3,4 | Service Fabric clusters should only use Azure Active Directory for client authentication | Audit | AC-2(7) | Yes |
|  | Audit virtual machines without disaster recovery configured | AuditIfNotExists | CP-7 | No |
| 1,2,3,4 | Deploy prerequisites to audit Windows VMs in which the Administrators group contains any of the specified members | DeployIfNotExists | AC-5  AC-6 | Yes |
| 1,2,3,4 | Deploy prerequisites to audit Windows VMs in which the Administrators group does not contain all of the specified members | DeployIfNotExists | AC-5  AC-6 | Yes |
| 1,2,3,4 | Deploy prerequisites to audit Windows web servers that are not using secure communication protocols | DeployIfNotExists | AC-5  AC-6 | Yes |
|  | Web ports should be restricted on Network Security Groups associated to your VM | AuditIfNotExists |  | No |
| 7 | Secure transfer to storage accounts should be enabled | Audit | SC-8(1) | Yes |

Table 4: Audit Canada Federal PBMM Policy Initiative

* 1. Azure Security Center

Configure for all subscriptions hosting PBMM workloads – possibly exclude sandbox resource groups and resources based on cost and requirement. The standard pricing tier enables threat detection for networks and virtual machines, provides threat intelligence, anomaly detection, and behavior analytics in Azure Security Center.

*“Security Centre covers security recommendations to follow when setting various security policies on an Azure Subscription. A security policy defines the set of controls, which are recommended for resources within the specified Azure subscription. Please note that the majority of the recommendations mentioned only produce an alert if a security violation is found. They do not actually enforce security settings by themselves. Alerts should be acted upon and remedied in a timely fashion.”*

Ref: <https://docs.microsoft.com/en-us/azure/security-center/security-center-intro>

* 1. GC Marketplace Whitelist

The SSC Cloud Broker team (CBS) maintains a whitelist of Azure marketplace templates that have been approved for GC consumption. These products have been evaluated through supply chain integrity checks by SSC and CSE. The GC Marketplace Whitelist policy is implemented at the Tenant Root Management Group and must be updated by the tenant owner as new products are approved by CSE. Follow the SSC Cloud Broker instructions to implement the Whitelist policy. [ [*https://gcdocs.gc.ca/ssc-spc/llisapi.dll/open/71440075*](https://gcdocs.gc.ca/ssc-spc/llisapi.dll/open/71440075)]. This is required for Guardrail 12 compliance.

1. Azure AD Tenant Implementation for 30-Day Compliance

This section addresses the manual procedures required for the implementation of some of the 30-day guardrails to the Azure Active Directory Tenant within the Azure Landing Zone Virtual Data Center.

* 1. Guardrail 1: Protect Root / Global Admins Account

1- Break Glass account: Need a break glass account and procedure. Refer to the template for a break glass emergency account management procedure. Create accounts and amend the proposed procedure in accordance with the guidance from the departmental CIO and CSO

Requirements

* Must have two break glass accounts using non conspicuous identities
* Must have a written break glass account procedure
* Account must be created in the tenant Azure Active Directory
* Must have P2 or equivalent licensing
* No MFA, controls or conditional access policies applied to these account(s) – can’t restrict access in anyway
* Responsibility of break glass accounts must be with someone not-technical, director level or above
* Associate account(s) with a non-technical individual, Director or above and include their phone number and email contact information.
* Change authentication method – same as the non-technical individual as above. The proper account must use a strong password
* Verify that both break glass account are licensed for identity protection. Go to Azure Active Directory, Users and find the break glass accounts. For each of them, click on Licenses and make sure they are licensed for Identity protection (Microsoft 365 E5)

2- Azure AD, Security, conditional access policies

* New policy, XXX-AAD\_PrivRoles[[1]](#footnote-1), select Global Admin roles, exclude break glass account, all cloud apps, grant MFA, enable policy, create (AZ-L1-001)
* New policy, XXX-AzureMFAPolicy, all users, exclude break glass account, cloud apps - Microsoft azure management, grant MFA, enable policy, create (AZ-L2-001)

3- Identity Protection is licensed as part of the Azure AD Premium P2 license. (https://docs.microsoft.com/en-us/azure/active-directory/active-directory-identityprotection ). (AZ-L1-001) (AZ-L1-076)

* Browse to Azure Active Directory > Security > Identity Protection > MFA registration policy.
  + Under Assignments i.Users - Choose All users but exclude the break glass account
  + Under Controls i.Ensure the checkbox Require Azure MFA registration is checked and choose Select.
  + Enforce Policy - On
  + Save
* Browse to Azure Active Directory > Security > Identity Protection > Overview.
* Select Configure user risk policy.
  + Under Assignments i.Users - Choose All users but exclude the break glass account
    - Conditions - User risk Microsoft's recommendation is to set this option to High.
  + Under Controls i.Access - Microsoft's recommendation is to Allow access and Require password change.
  + Enforce Policy - On
  + Save - This action will return you to the Overview page.
* Select Configure sign-in risk policy.
  + Under Assignments i.Users - Choose All users but exclude the break glass account
    - Conditions - Sign-in risk Microsoft's recommendation is to set this option to Medium and above.
  + Under Controls i.Access - Microsoft's recommendation is to Allow access and Require multi-factor authentication.
  + Enforce Policy - On
  + Save
* Password reset notification (AZ-L1-005) (AZ-L2-003)
  + Go to `Azure Active Directory`
  + Go to `Password reset`
  + Go to `Notification`
  + Set `Notify users on password resets?` to `Yes`
  + Set `Notify all admins when other admins reset their passwords?` to `Yes`
* MFA required to join devices (AZ-L1-008)
  + Go to `Azure Active Directory`
    - Go to `Devices`
    - Go to `Device settings`
    - Set `Require Multi-Factor Auth to join devices` to `Yes`
  + Go to `Azure Active Directory` (AZ-L2-002)
    - Go to `Users and group`
    - Go to `All Users`
    - Click on `Multi-Factor Authentication` button on the top bar
    - Click on `service settings`
    - Disable `Allow users to remember multi-factor authentication on devices they trust`
* Enable multi-factor authentication for remote network (cloud) access (AZ-L1-006)
  + Go to `Azure Active Directory`
    - Go to `Users and group`
    - Go to `User settings`
    - Set `Restrict access to Azure AD administration portal` to `Yes`
  + Go to `Azure Active Directory` (AZ-L2-011) (AZ-L2-012)
    - Go to `Users and group`
    - Go to `Group settings`
    - Set `Users can create security groups` to `No`
    - Set `Users who can manage security groups` to `None`
  1. Guardrail 2: Management of Administrative Privileges

Document a process for managing accounts, access privileges, and access credentials for organizational users, non-organizational users (if required), and processes based on the principles of separation of duties and least privilege (for example, operational procedures and active directory)

Implement a multi-factor authentication mechanism for privileged accounts (for example, username, password and one-time password) and for external facing interfaces. Consult <https://intranet.canada.ca/wg-tg/rtua-rafu-eng.asp>. It is important to note that SMS is not an acceptable PB 2FA mechanism.

Navigate to Security Center, then under Resource Security Hygiene, click on Identity & Access. Select each policy identified below and make sure that no subscription is identified as unhealthy.

* Remove deprecated accounts
  + Deprecated accounts should be removed from your subscription
  + Deprecated accounts with owner permissions should be removed from your subscription
* Remove External accounts
  + External accounts with owner permissions should be removed from your subscription
  + External accounts with write permissions should be removed from your subscription
  + External accounts with read permissions should be removed from your subscription
* Remove Guest users (AZ-L1-002)
* Navigate to Azure AD, Users
* Select “User Type:Guest” as a Filter and delete any account unless it is absolutely required
  1. Guardrail 3: Cloud Console Access
* Limit access to GC IP addresses only(via DCAM access rules)
  + ADFS configuration to restrict access based on source IP
  + Source IP based restrictions at cloud firewall (in front of the RDS farm) for OS console access
* Azure AD, Security,
  + Named location. Create new location(s) that includes the IP addresses ranges of all people that will require Cloud console access
  + conditional access policies
    - New policy, XXX-CloudAccess[[2]](#footnote-2), select All Admin roles, exclude break glass account, all cloud apps, condition-select all trusted locations, grant MFA, enable policy, create

* 1. Guardrail 4: Enterprise Monitoring Accounts
* Confirm that an Azure AD native account named SSC-CBS-Reporting@###gc.onmicrosoft.com (where ### is your tenant number) has been created as part of the implementation of the Azure Whitelisting . Make the account a member of the CSD-Reader group.

* 1. Guardrail 11: Logging and Monitoring

**Create Log Analytic Workspaces for Enterprise monitoring**

• WORKSPACES - need 2 only ( 1 for security and 1 for performance and health)

Security: create a RG for security monitoring. Create LAW, Retention needs to be 2 years.

1) Workspace summary, add the log types: activity log analytics. Ensure to add all subscriptions except sandbox

2) Workspace summary, add, antimalware assessment

3) Workspace summary, add, keyvault analytics

4) Create a resource, automation account

5) Go to RG. Select the account, update management, select the LAW and enable

6) In the tenant, select diagnostic setting. Select the LAW and select audit logs, sigint logs

7) Need to redirect blueprint to this LAW

8) Go to Azure sentinel and select the LAW and add it to sentinel. Go to data connectors. Add azure activity, office 365 and anything we use

Health: create a RG for performance and health monitoring. Create LAW, Retention needs to be 90 days.

1) Workspace summary, add the log types. Add all subscriptions except environments, i.e. sandbox or IaaS Development.

2) Workspace summary, add, Azure Log Analytics Agent Health

4) Create a resource, automation account

5) Go to RG. Select the account, update management, select the LAW and enable

6) In the tenant, select diagnostic setting. Select the LAW and select …..

7) Need to redirect blueprint to this LAW

**Azure security center. Select standard tier (AZ-L2-016)**

- Send all logs to the security LAW

1) Data collection - Send all events

2) Email notification - enter email and phone number (select send email for high severity alerts)

3) Threat detection - enable

**Sentinel - Connect Azure security center to sentinel. Enable create incidents**

- Select hunting to see what’s going on

**Advanced Threat Protection – Deploy on Storage Accounts**

- For some partners, this could be unaffordable to enable across all storage accounts. May need to be considered on a case by case.

**Azure AD Privileged identity management (AZ-L2-019)**

Select Manage - Settings,

Select the Global administrators role, click edit

- lower activation to 1 hr and require approval from director or security director. They both need security identifiers.

- Remove "allow permanent active assignment".

- 1 year for renewal of role

Repeat for the following roles: Security admins, conditional access admins, privileged role admin, authentication admin, password administrator, privileged authentication admin

Verify that both break glass account are licensed for identity protection. Go to Azure Active Directory, Users and find the break glass accounts. For each of them, click on Licenses and make sure they are licensed for Identity protection (Microsoft 365 E5)

1. Azure Network Implementation for 30-Day Compliance

Hosting PBMM IaaS/PaaS workloads in the public cloud requires the creation of a Virtual Datacenter (VDC) or Landing Zone (LZ). The Virtual Datacenter provides the network, security management, and other core infrastructure services such as DNS, AD, Remote Access, etc. Compliance with TBS 30-day guardrails 8 and 9 require the deployment of ITSG 22/38 compliant network zoning architecture (VDC).

Microsoft provides different VDC operating models and designs as part of their cloud adoption framework. Working with the cloud network and security teams, design the virtual datacenter to meet departmental business and technical requirements. Partners must develop a target network security design that considers segmentation via network security zones, in alignment with ITSG 22 and ITSG 38.

Ref: <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/reference/networking-vdc>

* 1. SSC Azure Landing Zone Design

The SSC Cloud Research and Development team has developed an Azure Landing Zone automated deployment through Infrastructure as Code (IaC) using Terraform (formally called GC Accelerators). The current release deploys the core network and security components for TBS Cloud Profile 3 compliance. Future release will include IaC deployments to support Cloud Usage Profile 6 once SCED is available.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ref.  # | Profile | Characteristics | Cloud Service Model | Connection Type |
| **3** | Sensitive (up to PB) cloud-based services | * Cloud-based services hosting sensitive (up to Protected B) information * No direct system to system network interconnections required with GC data centers | IaaS, PaaS, SaaS | Type 1 - EIS/IIS  (no SCED) |
| **6** | Cloud-based services with External user access and interconnection to GC data centers | * Cloud-based services hosting sensitive (up to Protected B) information * GC cloud-based systems required to interact with systems in GC data centers * Environment accessible for both GC users and External users and services * Solution implemented, managed and operated by a GC department/agency | IaaS, PaaS | Type 3 - CXP  (SCED) |

Table 5: Cloud Usage Profile

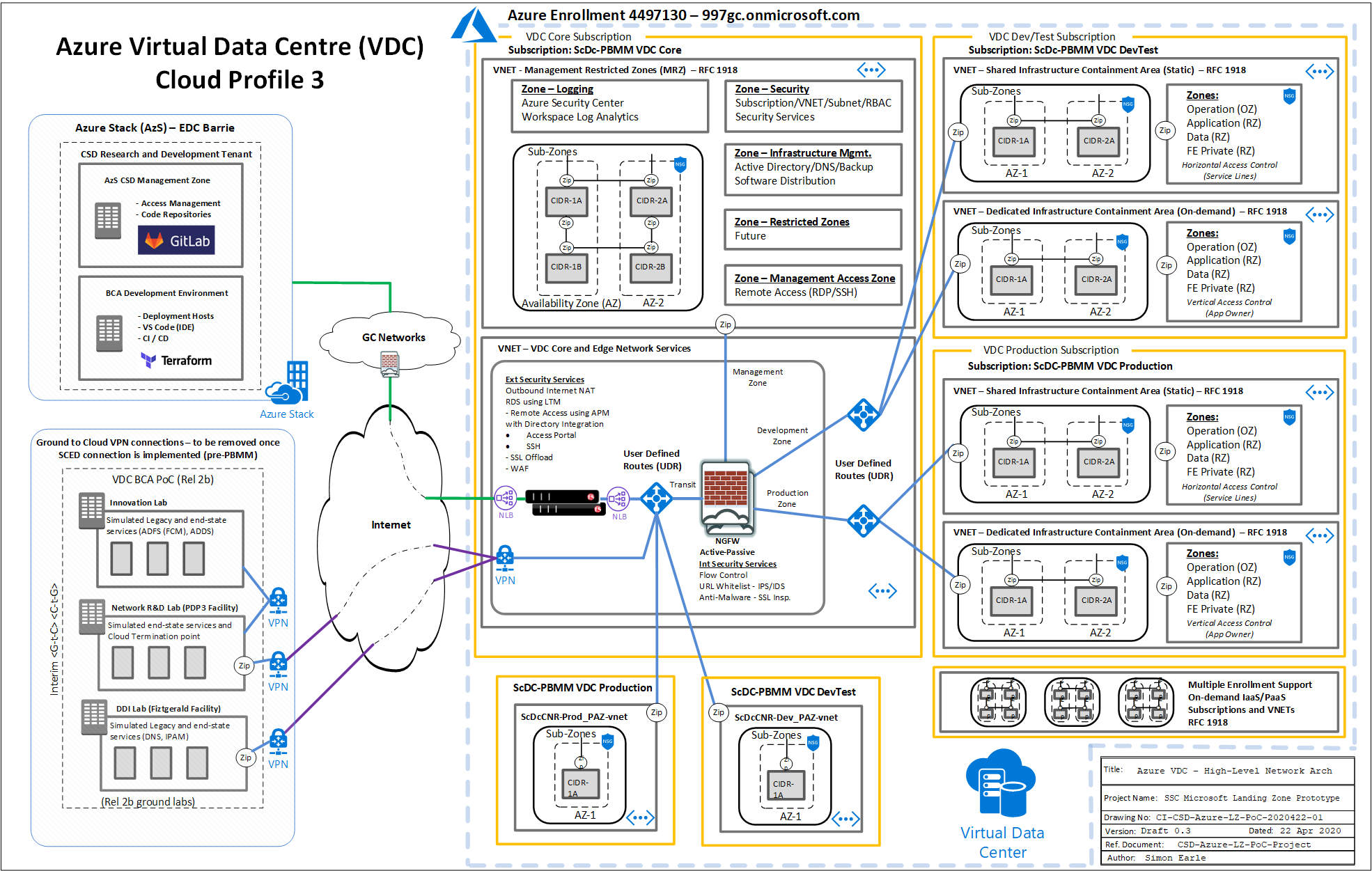


Figure 5: SSC Azure Landing Zone Release

DDOS Protection basic should be enabled on VNets with Public IPs. In addition, partners may implement an alternative solution on the perimeter firewall and load balancer virtual firewalls providing some additional level of protection. Note that enabling DDoS protection on VNets can be expensive based on traffic;

1. Cyber Defense Services

Partners must establish and sign an MOU with CSE (Cyber Centre Security) CCCS an MOU for defensive services and threat monitoring protection services. Partners must also implement defensive services including HBS, CBS, and NBS in accordance with CCCS onboarding guidance. Contact CCCS ( CDOServiceDeployments@cyber.gc.ca ) to initiate engagement.

Appendix A – MAPPING ITSG-33 SECURITY CONTROLS TO GUARDRAIL IMPLEMENTATION

Appendix B – SUGGESTED EVIDENCING OF GUARDRAILS

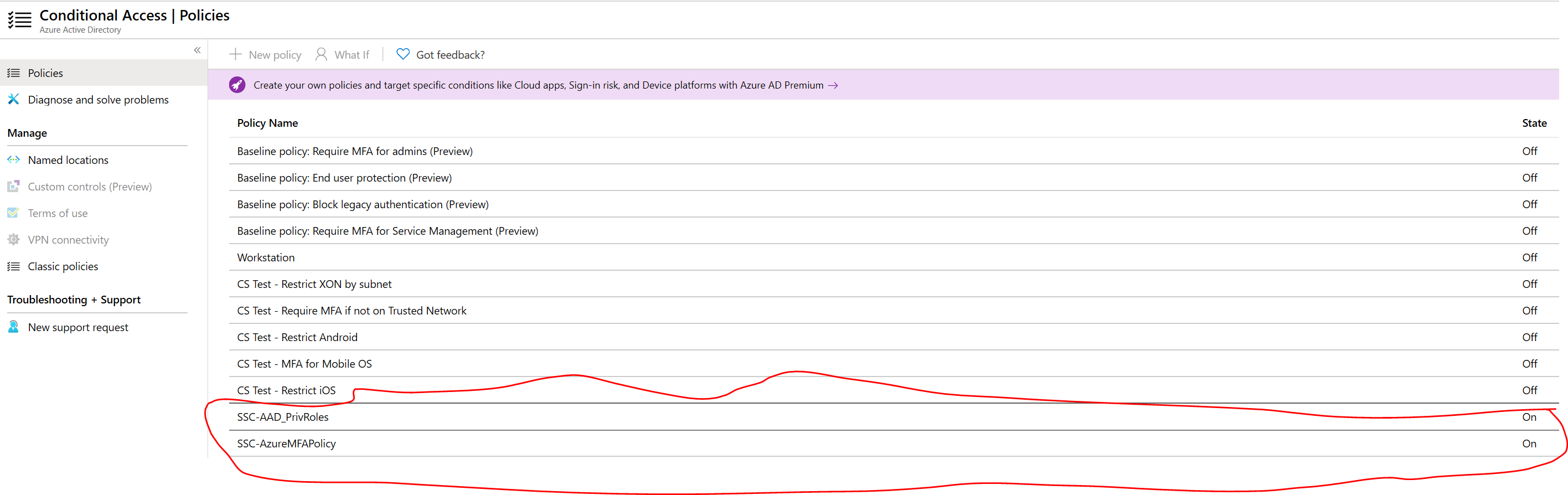
## Evidencing

This section describes a set of suggested minimum guardrails evidence required.

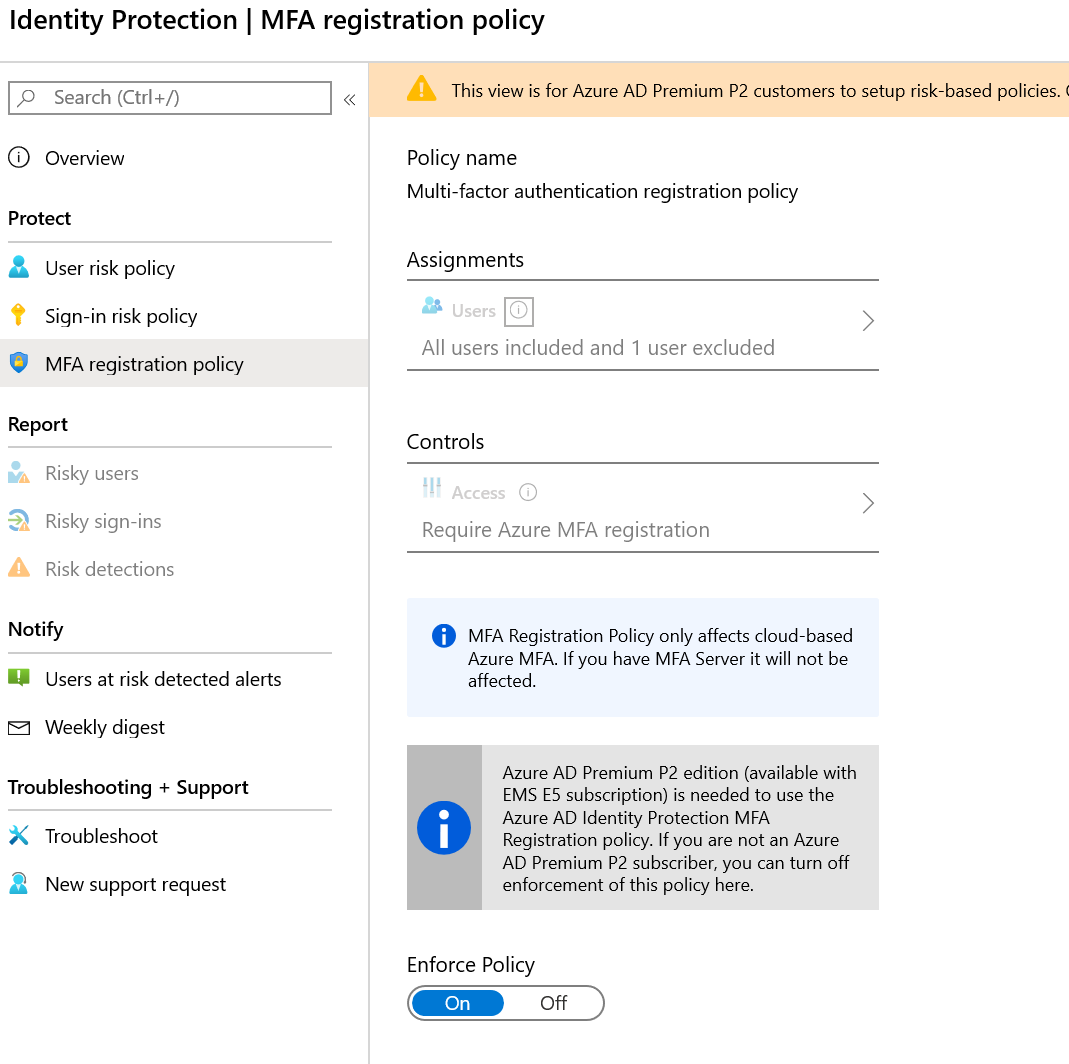
* 1. Guardrail 1: Protect Root / Global Admins Account

1 - Break Glass account: Provide a signed copy of the break glass emergency account management procedure (See [template](https://gcdocs.gc.ca/ssc-spc/llisapi.dll/open/72824320) ).

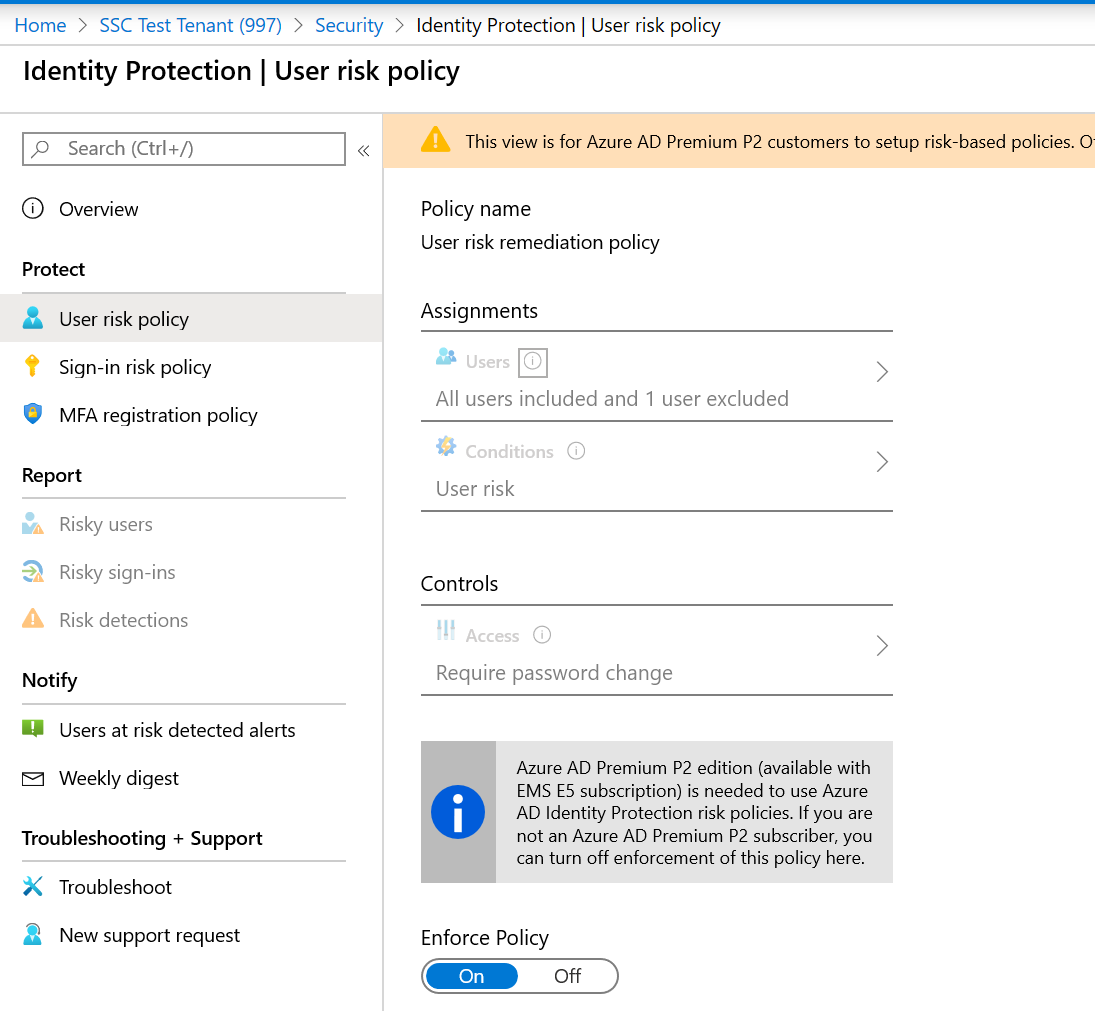
2- Azure AD, Security, conditional access policies



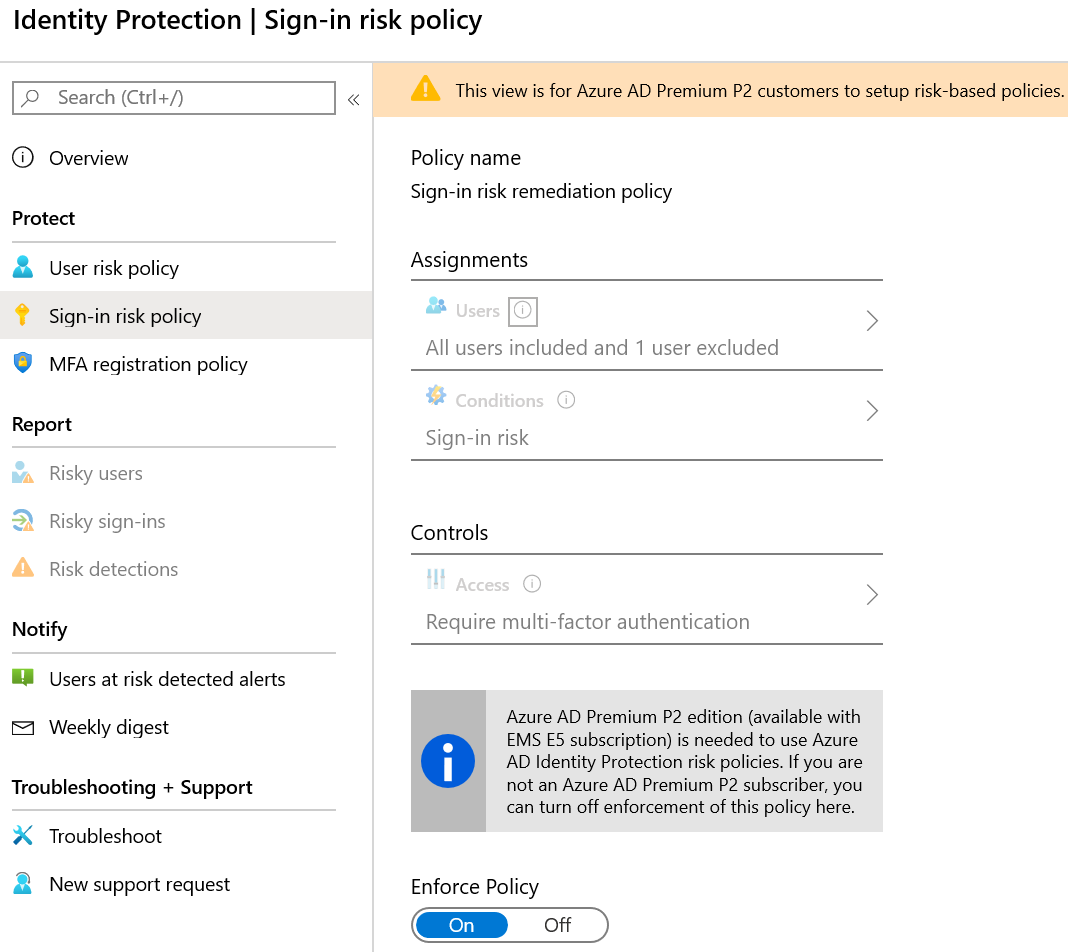
3- Identity Protection.



4- Configure user risk policy.

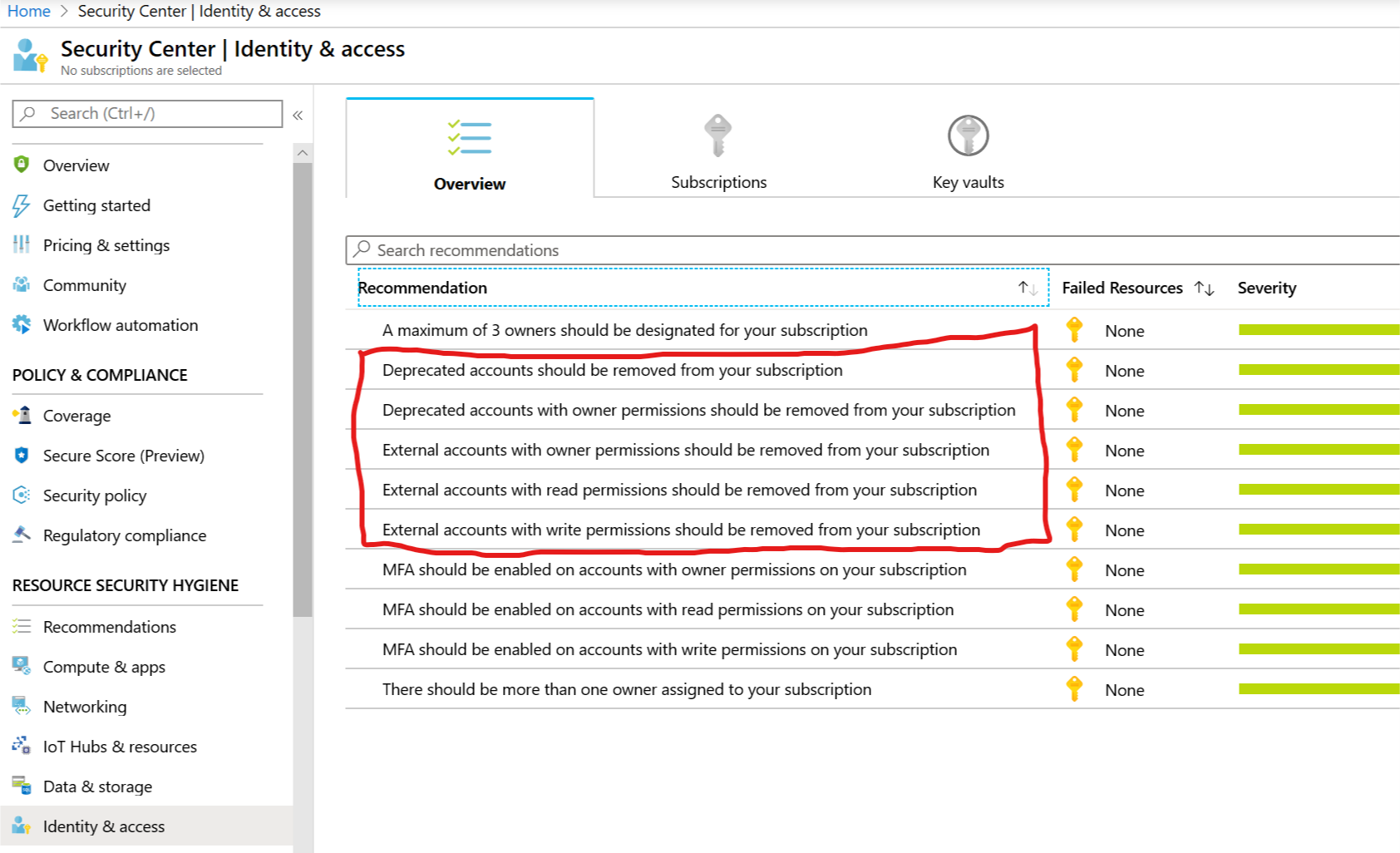


5- Configure sign-in risk policy.

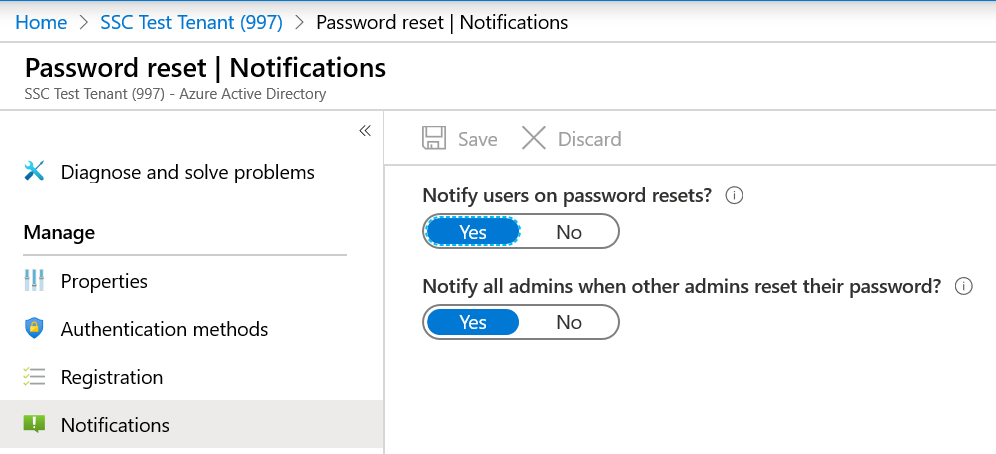


* 1. Guardrail 2: Management of Administrative Privileges

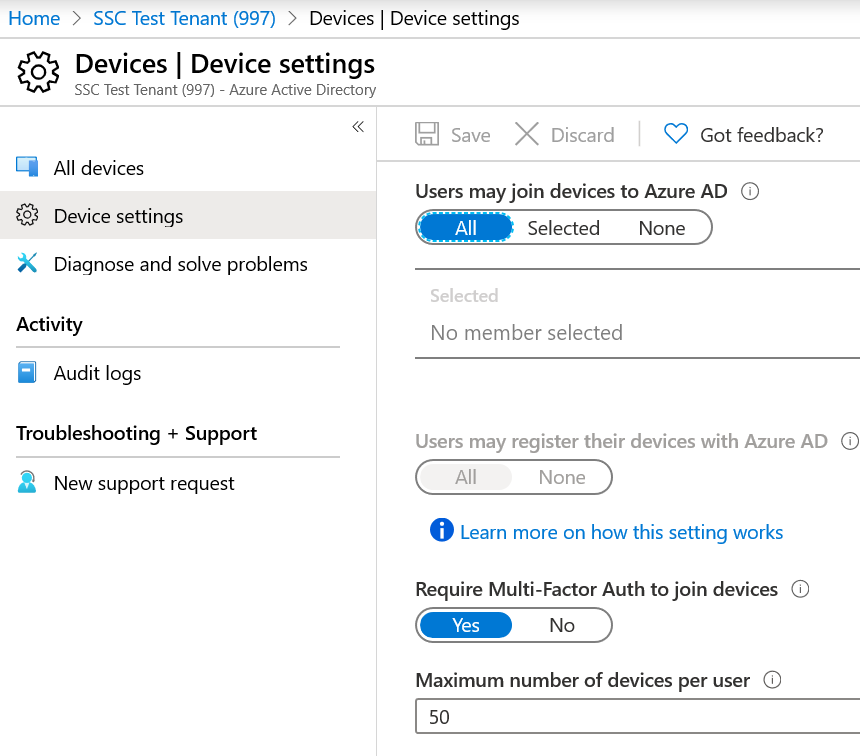
External and deprecated accounts



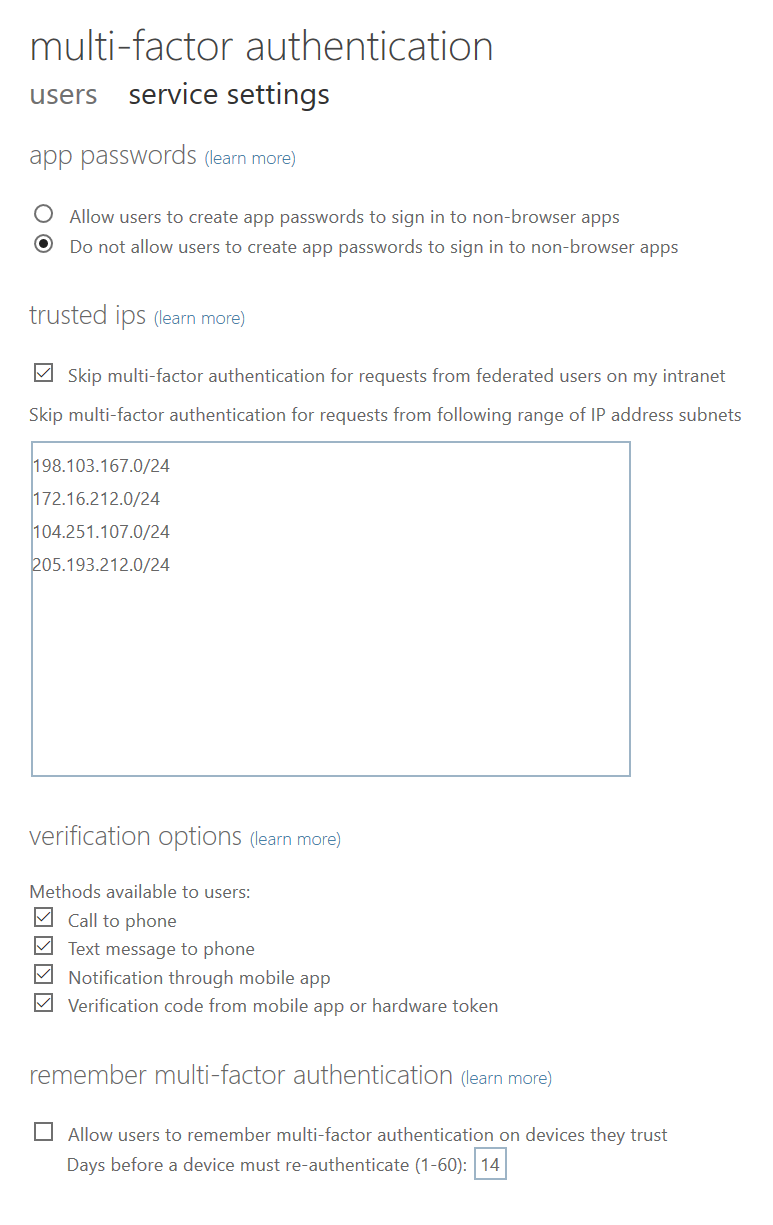
Password reset notification



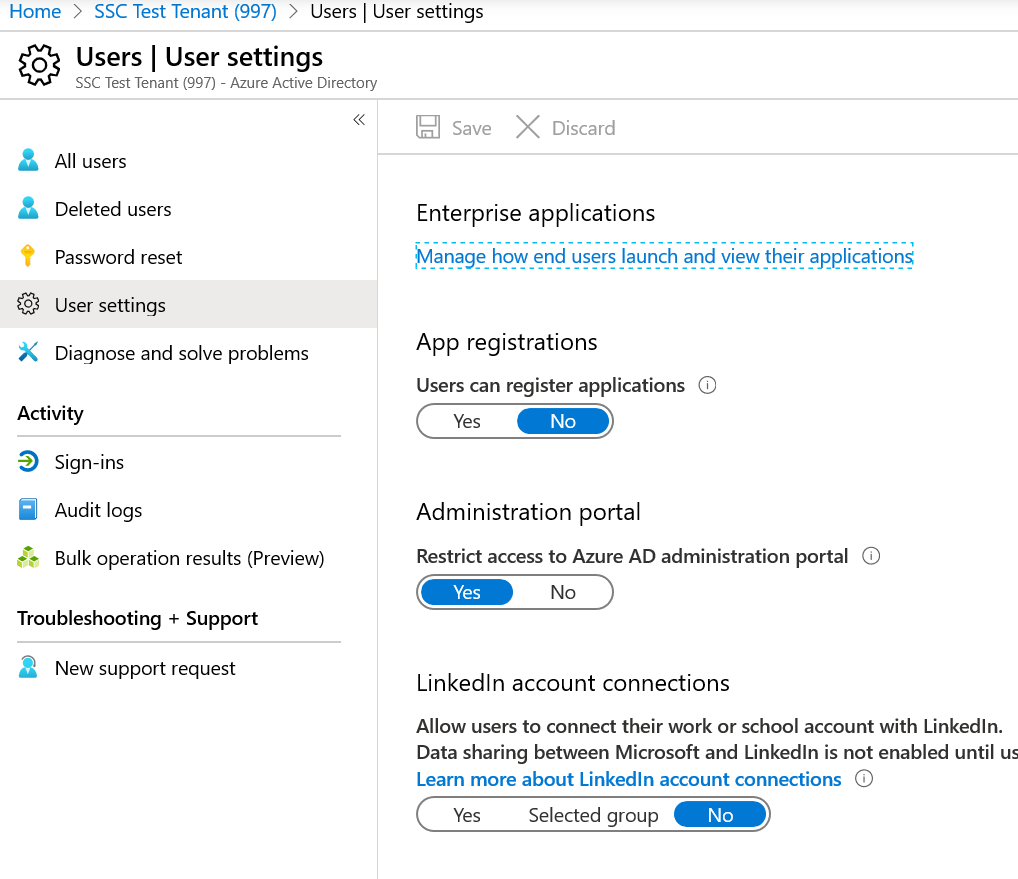
MFA required to join devices



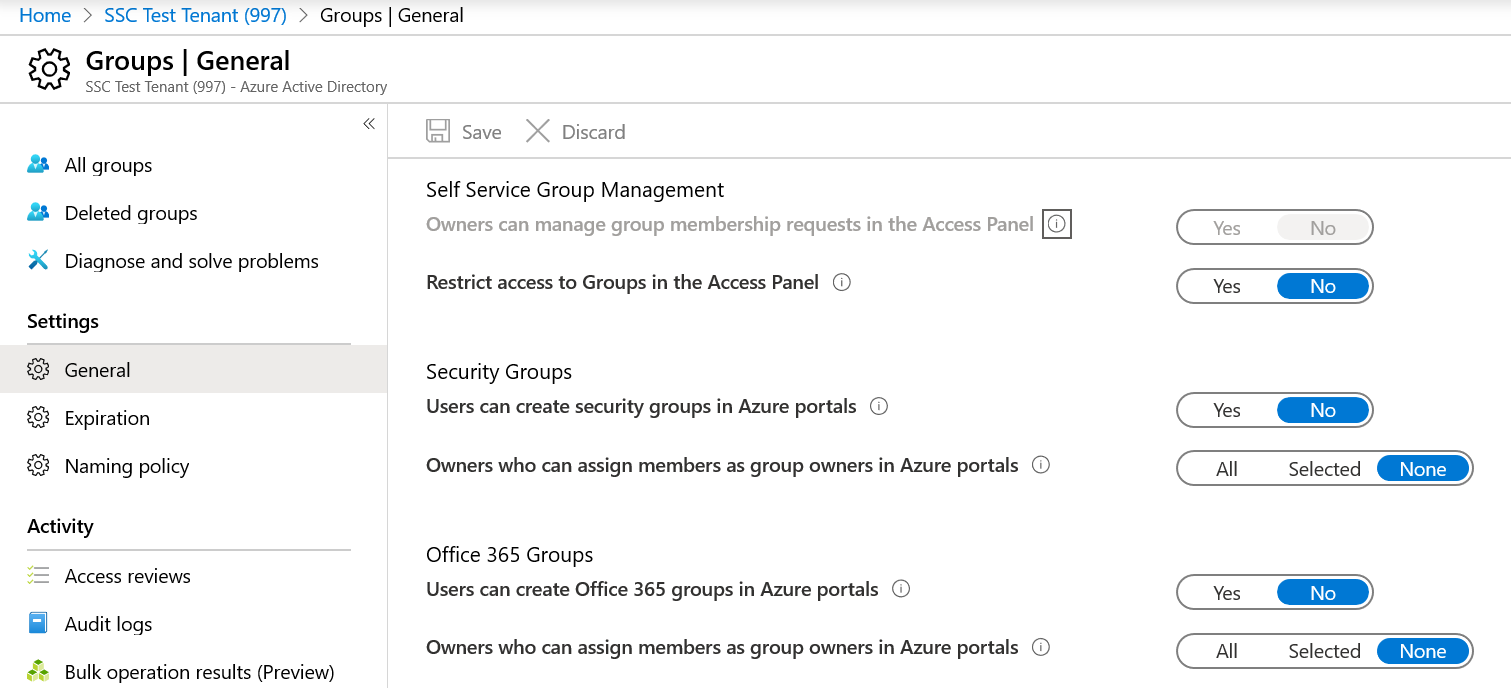
MFA settings



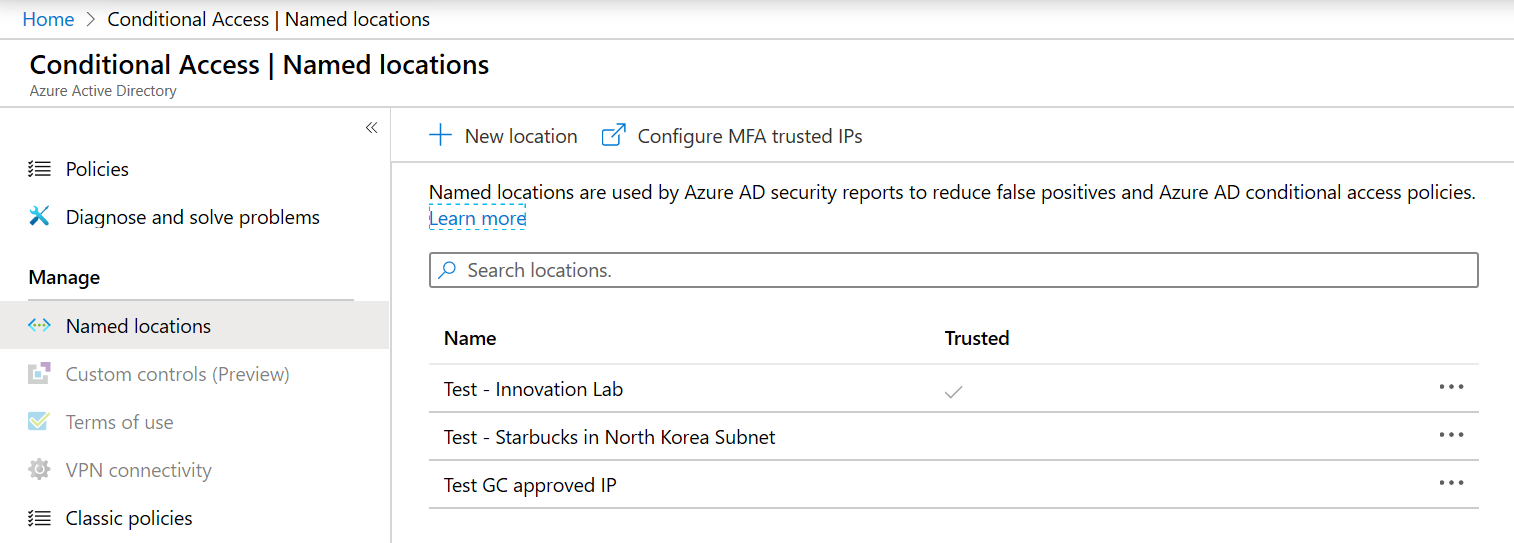
Enable multi-factor authentication for remote network (cloud) access



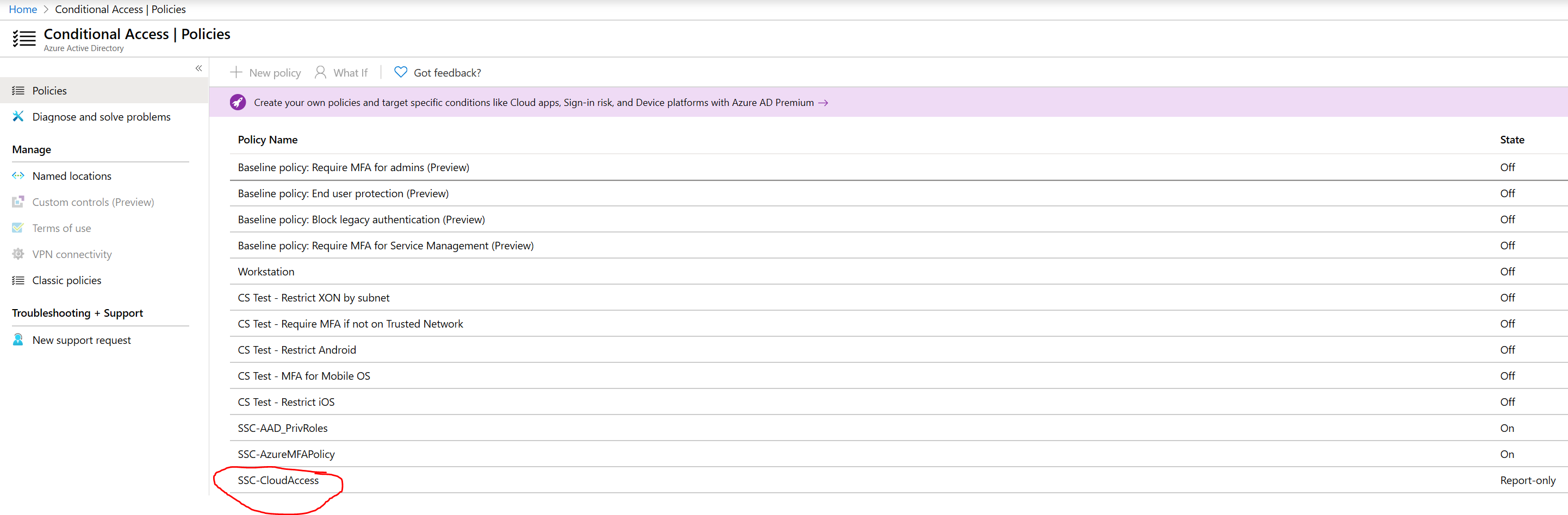
Azure Active Directory Group settings



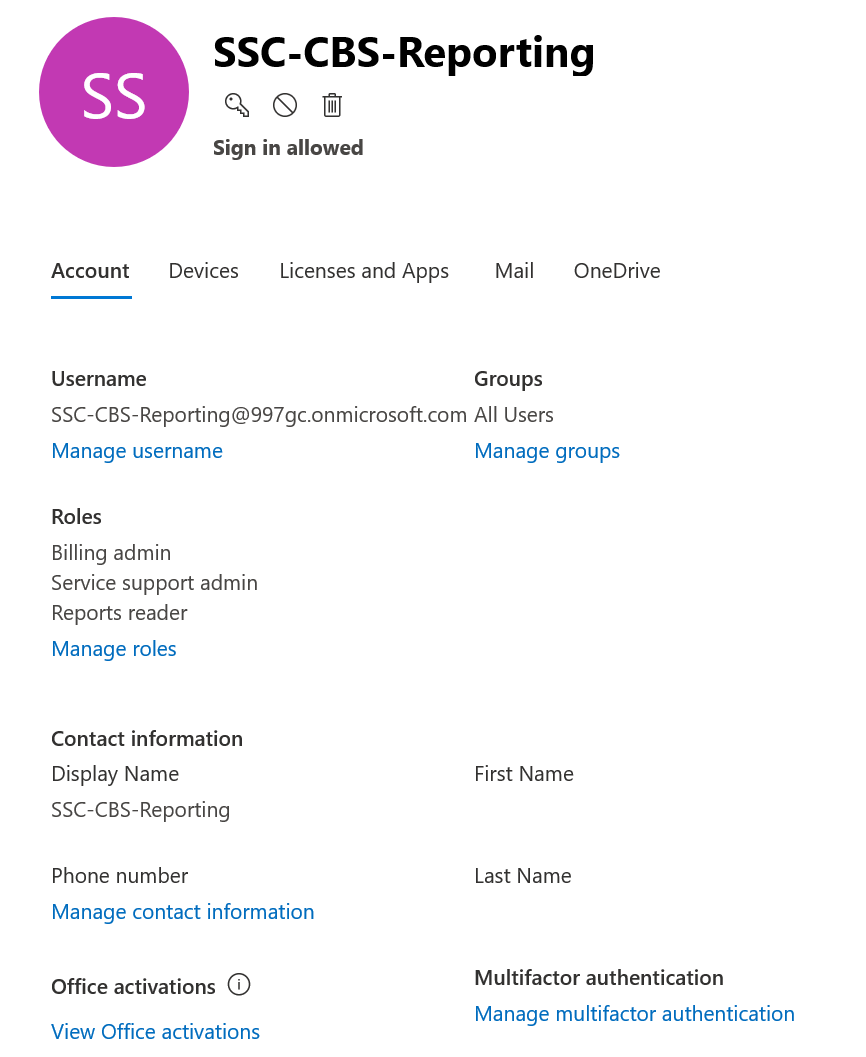
* 1. Guardrail 3: Cloud Console Access
* Azure AD, Security, Named location.



* conditional access policies

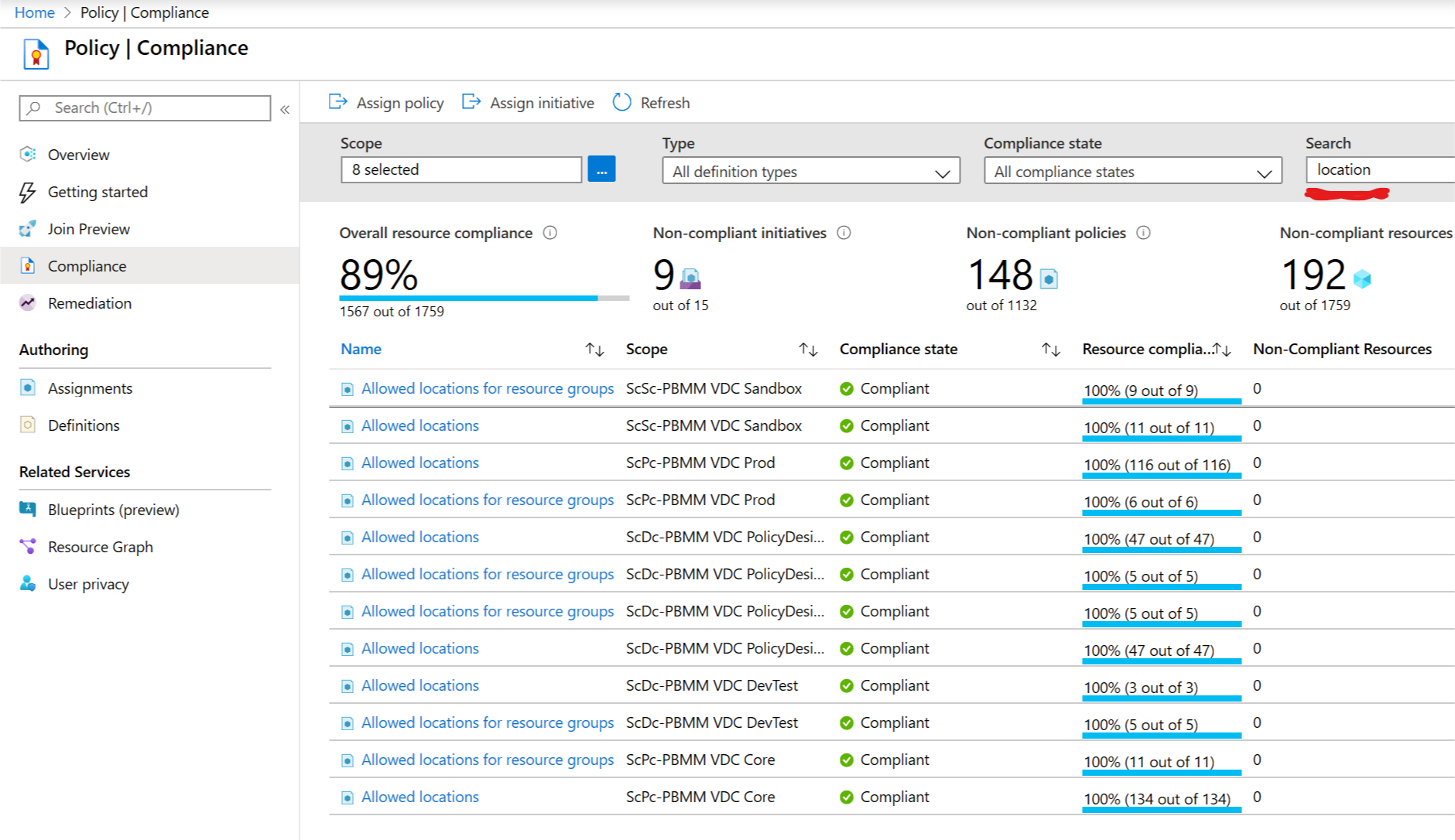


* 1. *Guardrail 4: Enterprise Monitoring Accounts*
* Confirm an Azure AD native account named SSC-CBS-Reporting@###gc.onmicrosoft.com

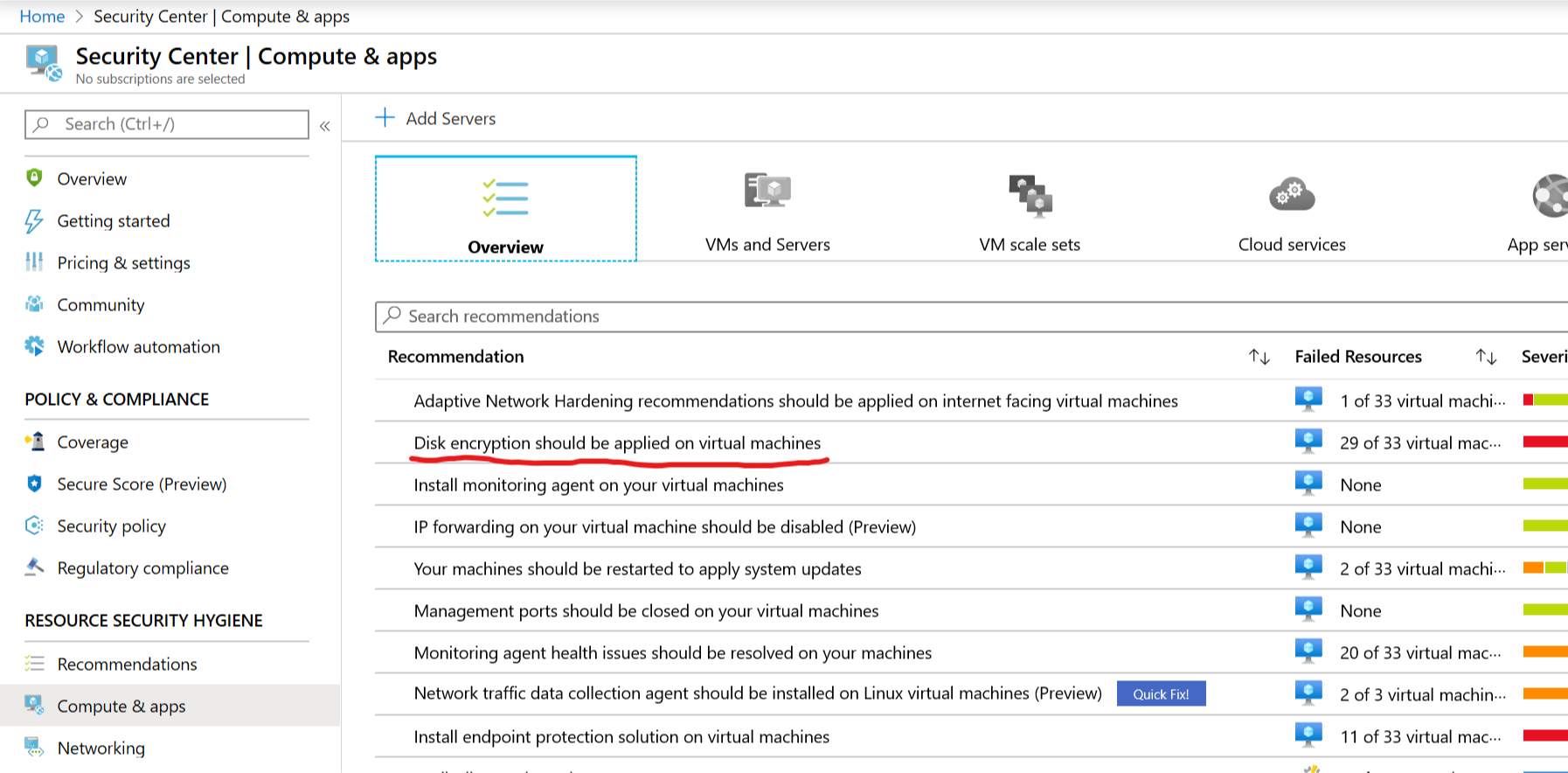


* 1. Guardrail 5: Data Location

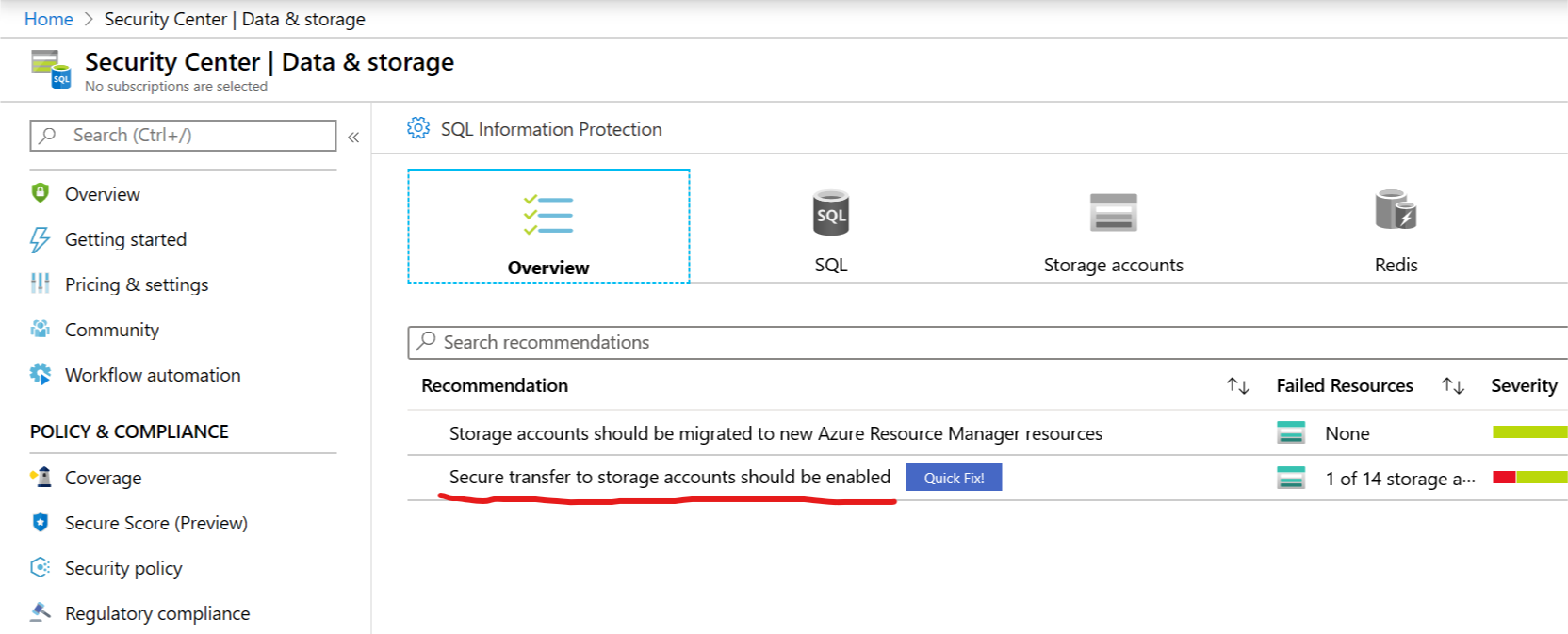
Evidence that PBMM policy has been implemented. In particular the “Allowed locations” and “allowed resource group locations” policies



* 1. Guardrail 6: Protection of Data-at-Rest



* 1. Guardrail 7: Protection of Data-in-Transit

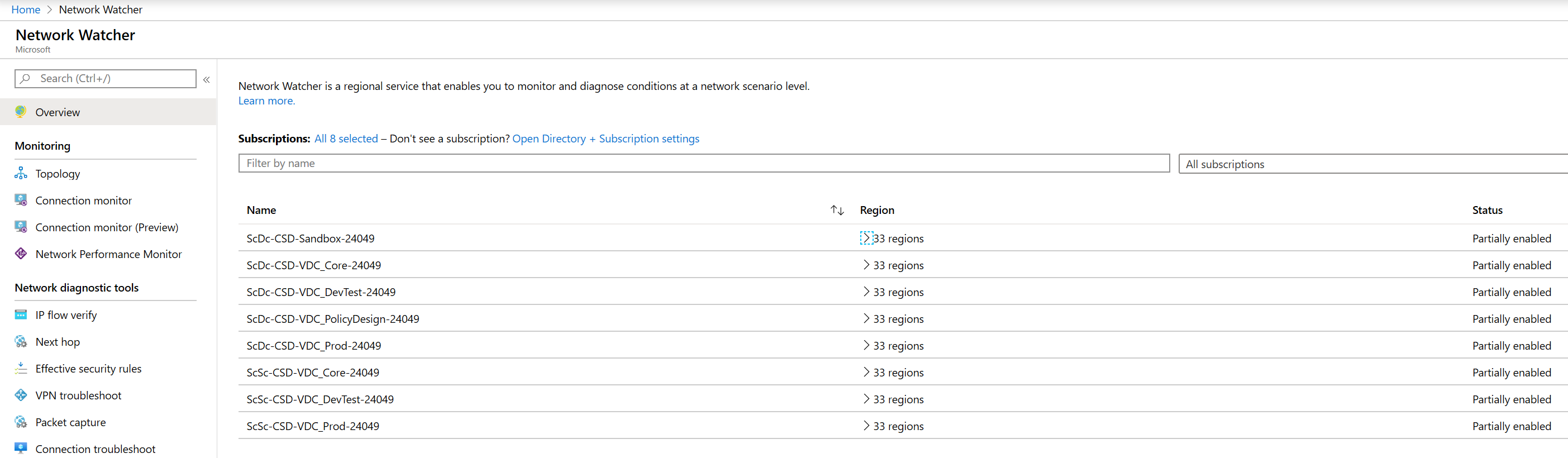


* 1. Guardrail 8: Network Segmentation and Separation

**As per network design**

* 1. Guardrail 9: Network Security Services

Network watcher

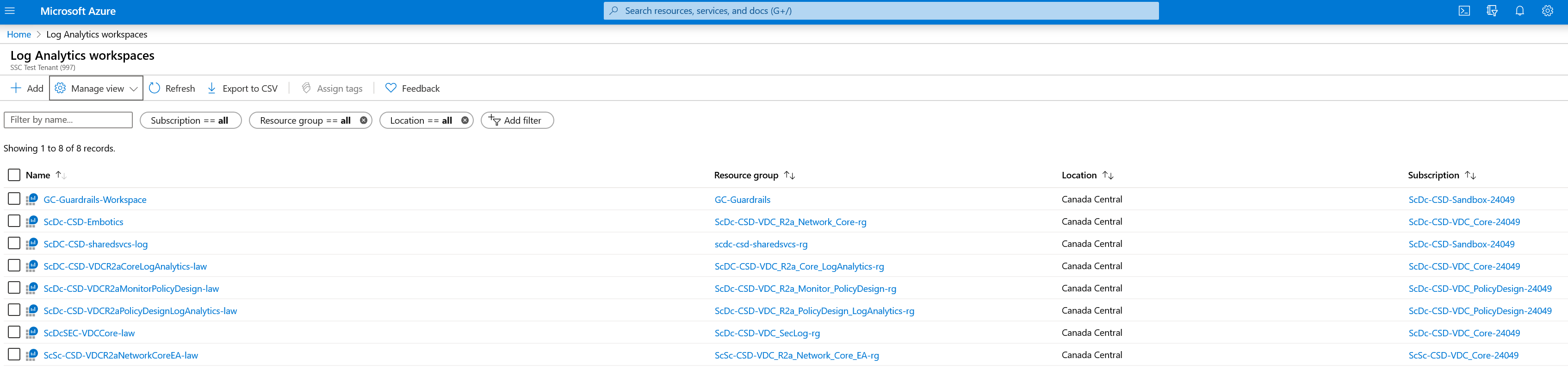


* 1. Guardrail 10: Cyber Defense Services

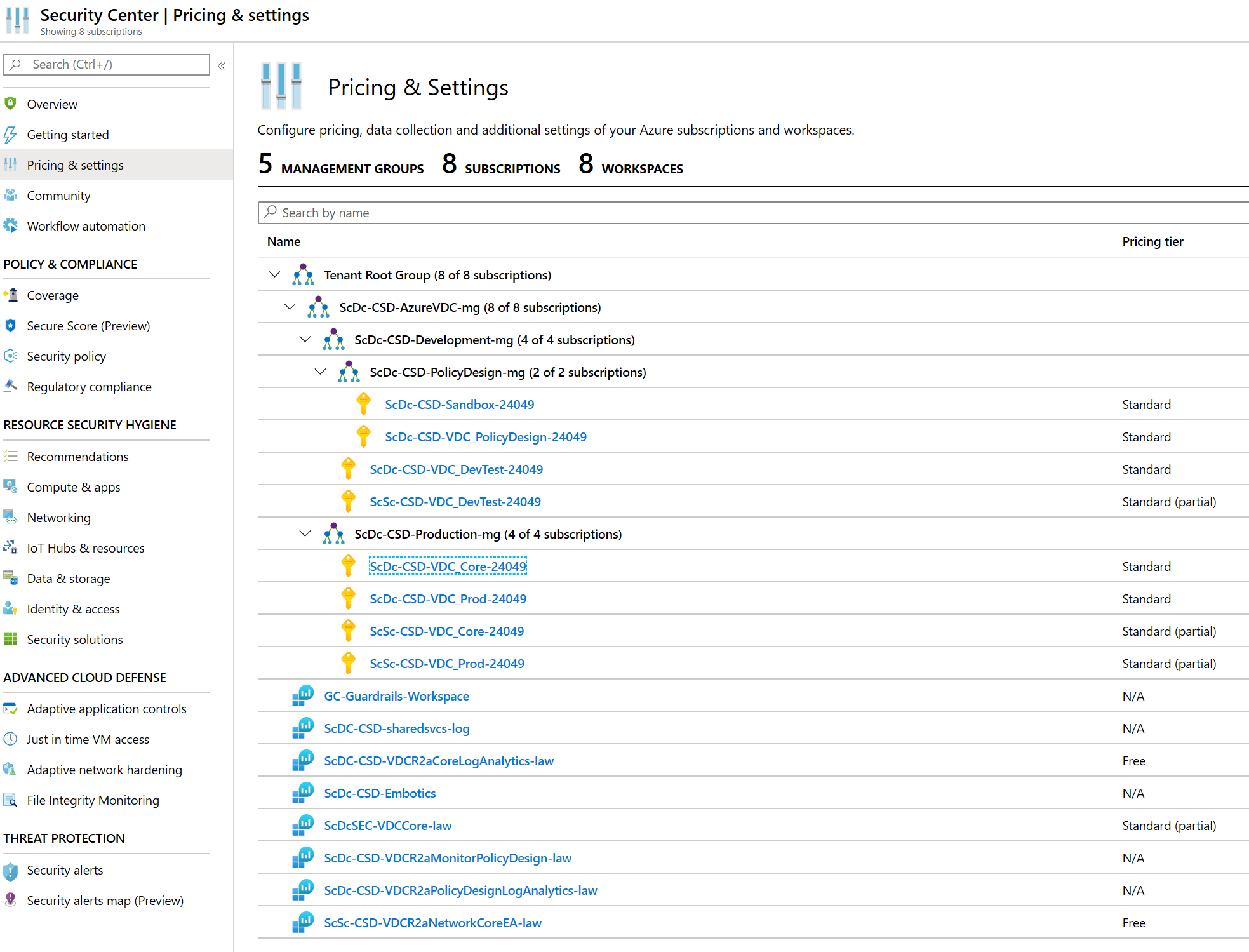
**Evidence of MOU with CCCS**

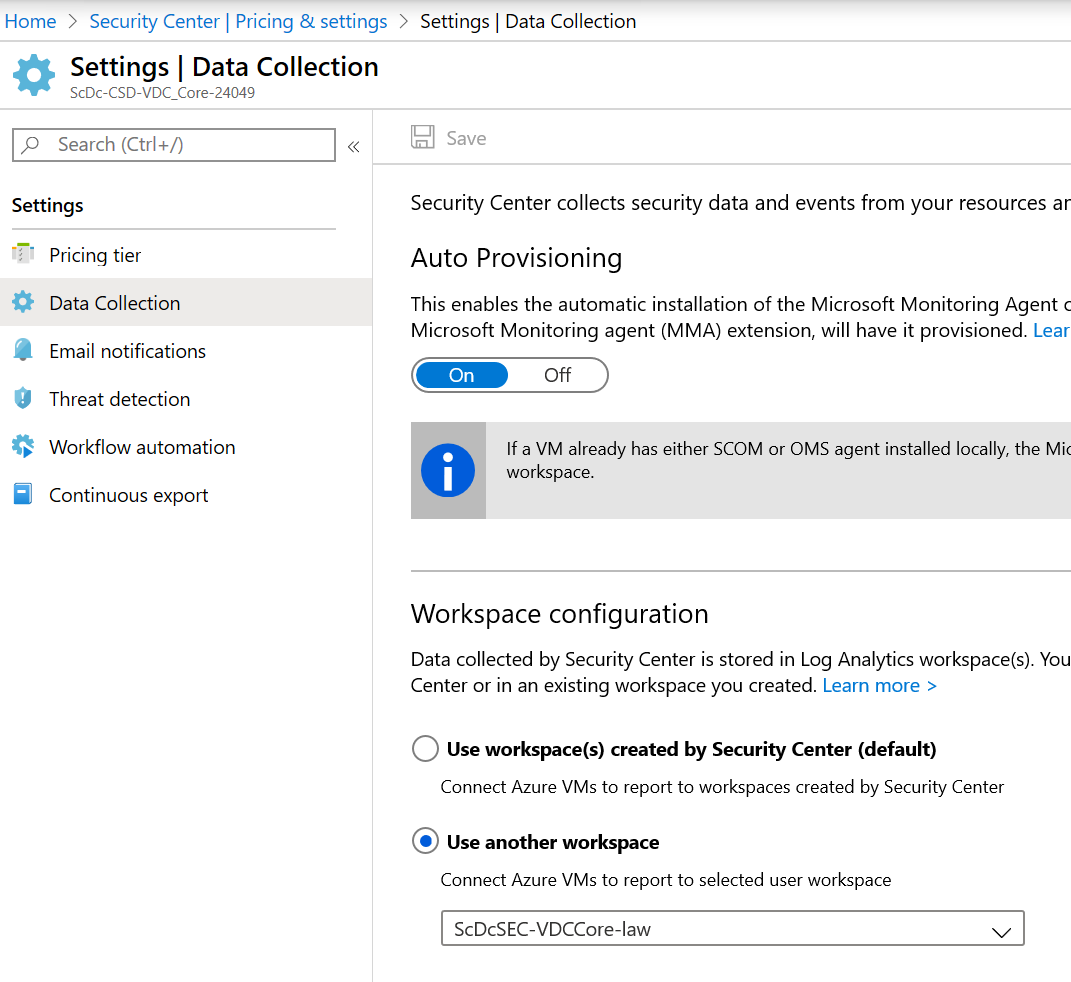
* 1. Guardrail 11: Logging and Monitoring

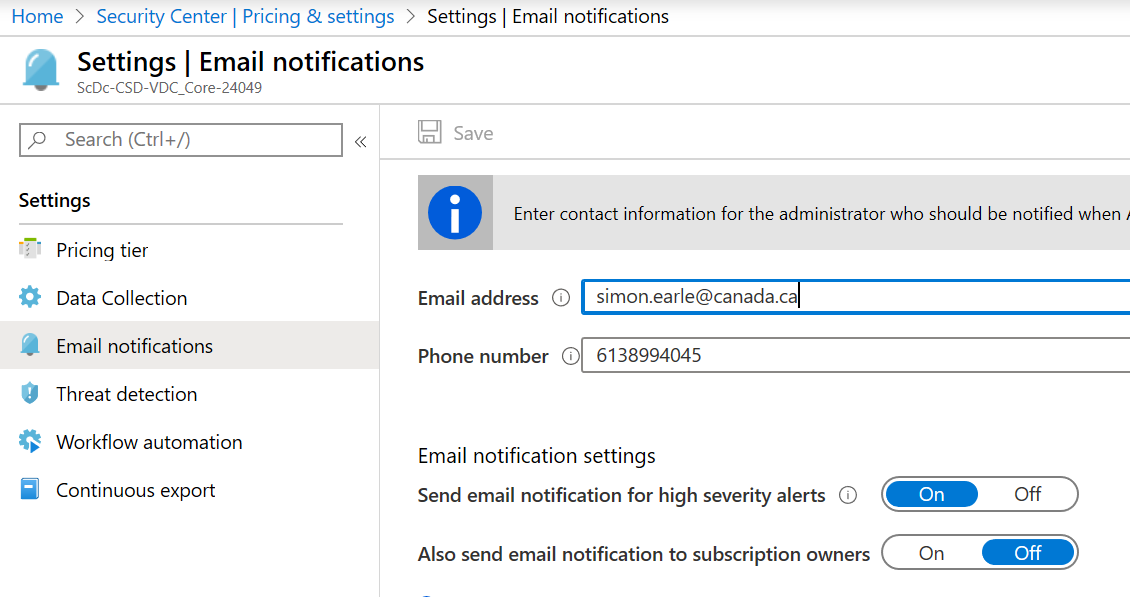
Log Analytic Workspaces

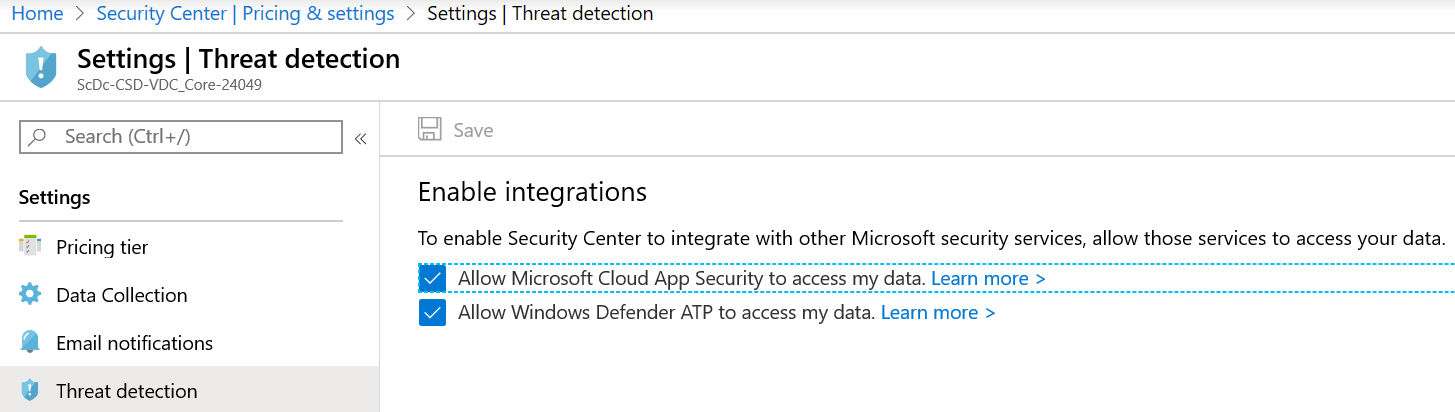


AZURE SECURITY CENTER.



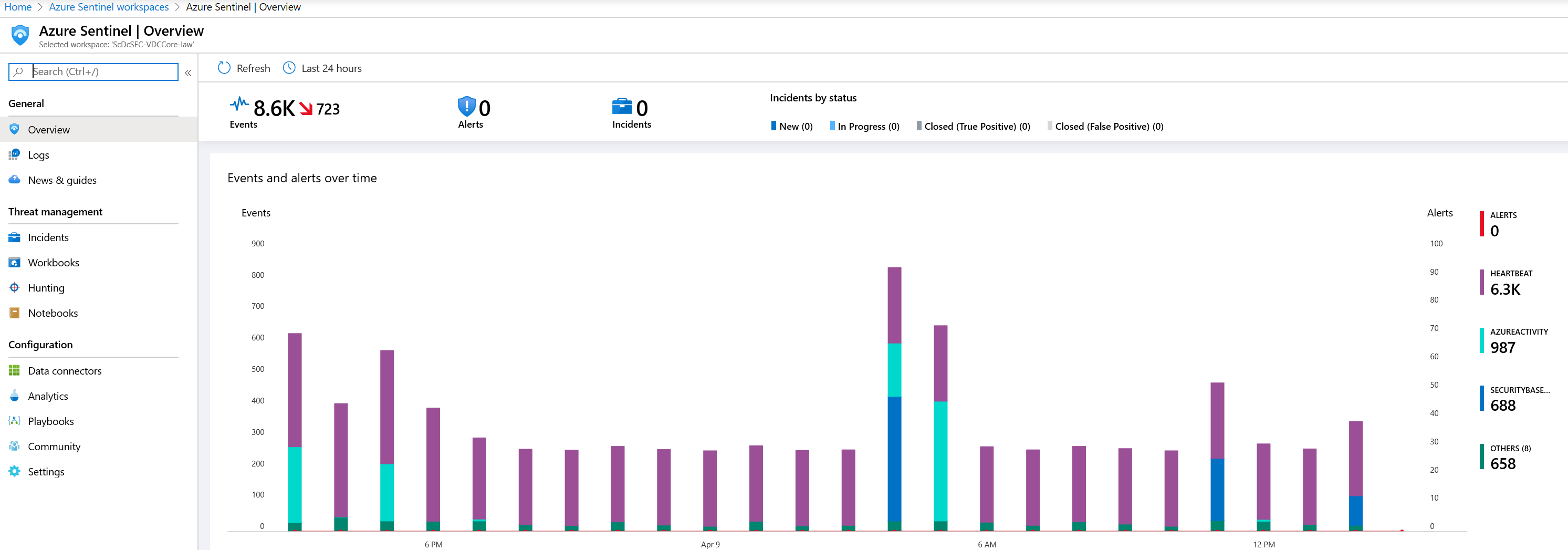




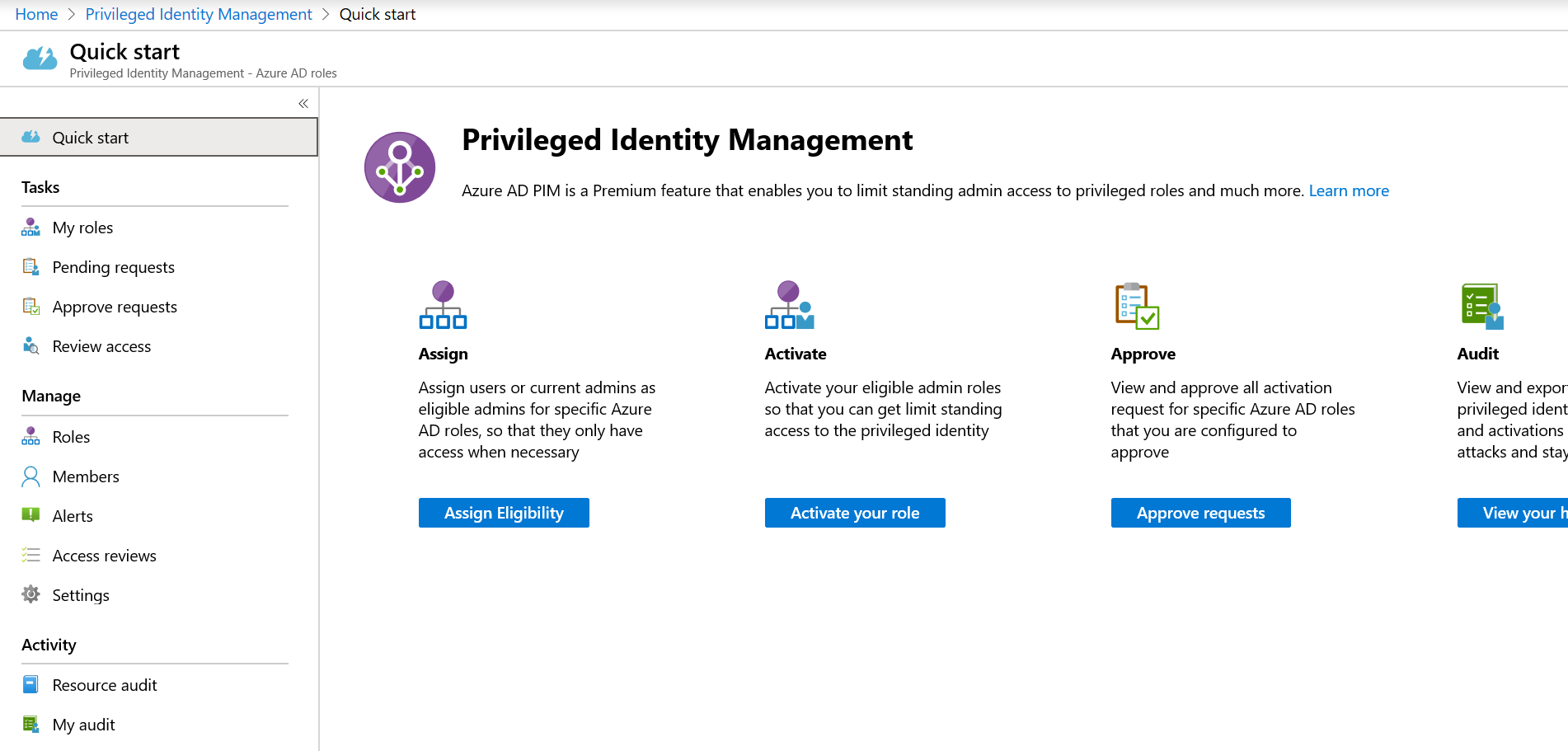


Sentinel - Connect Azure security center to sentinel. Enable create incidents

- Select hunting to see what’s going on



Azure AD Priviledge identity management



* 1. Guardrail 12: Configuration of Cloud Marketplaces

Evidence of the implementation of the Azure Whitelisting policies

1. First three characters should describe the Department. Change XXX to Department Identification in accordance with Naming and Tagging Standard [↑](#footnote-ref-1)
2. First three characters should describe the Department. Change XXX to Department Identification in accordance with Naming and Tagging Standard [↑](#footnote-ref-2)