



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: | 0.12 |
| Status: | Draft |
| Publish Date: | May 29, 2020 |



Shared Services
Canada Services partagés
Canada

Canada

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

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 | |
| 0.7 | 2020-04-30 | Azure Design Team (CSD) | Peer Review | |
| 0.8 | 2020-04-30 | Azure Design Team (CSD) | Updated section 5 for GR10 | |
| 0.9 | 2020-05-11 | Azure Design Team (CSD) | Included 163dev feedback | |
| 0.10 | 2020-05-22 | Azure Design Team (CSD) | Included additional 163dev feedback | |
| 0.11 | 2020-05-27 | Azure Design Team (CSD) | Included additional ASC and LAW steps | |
| 0.12 | 2020-05-29 | Azure Design Team (CSD) | Included feedback from GAC | |
| | | | | |

TABLE OF CONTENTS

| | | |
|---|---|-----------|
| 1 | Overview..... | 6 |
| 1.1 | <i>Purpose.....</i> | 6 |
| 1.2 | <i>GC Cloud Governance.....</i> | 7 |
| 1.3 | <i>Document Reference.....</i> | 7 |
| 1.4 | <i>Guardrail mappings.....</i> | 8 |
| 2 | Azure Policy Implementation for 30-Day Compliance | 9 |
| 2.1 | <i>Canada Federal PBMM Blueprint.....</i> | 9 |
| 2.1.1 | Implementation Prerequisites | 10 |
| 2.1.2 | PBMM Blueprint Implementation..... | 11 |
| 2.2 | <i>Azure Landing Zone VDC Policy Definition</i> | 16 |
| 2.3 | <i>Azure Security Center</i> | 20 |
| 2.4 | <i>GC Marketplace Whitelist</i> | 20 |
| 3 | Azure AD Tenant Manual Configuration for 30-Day Compliance | 21 |
| 3.1 | <i>Guardrail 1: Protect Root / Global Admins Account.....</i> | 21 |
| 3.2 | <i>Guardrail 2: Management of Administrative Privileges.....</i> | 23 |
| 3.3 | <i>Guardrail 3: Cloud Console Access</i> | 23 |
| 3.4 | <i>Guardrail 4: Enterprise Monitoring Accounts.....</i> | 24 |
| 3.5 | <i>Guardrail 11: Logging and Monitoring.....</i> | 24 |
| 4 | Azure Network Implementation for 30-Day Compliance | 25 |
| 4.1 | <i>SSC Azure Landing Zone Design.....</i> | 25 |
| 5 | Cyber Defense Services | 28 |
| Appendix A – MAPPING ITSG-33 SECURITY CONTROLS TO GUARDRAIL IMPLEMENTATION | | 29 |
| Appendix B – SUGGESTED EVIDENCING OF GUARDRAILS..... | | 30 |
| Evidencing | 30 | |
| 5.1 | <i>Guardrail 1: Protect Root / Global Admins Account.....</i> | 30 |
| 5.2 | <i>Guardrail 2: Management of Administrative Privileges.....</i> | 32 |

| | | |
|------|--|----|
| 5.3 | <i>Guardrail 3: Cloud Console Access</i> | 34 |
| 5.4 | <i>Guardrail 4: Enterprise Monitoring Accounts</i> | 35 |
| 5.5 | <i>Guardrail 5: Data Location</i> | 36 |
| 5.6 | <i>Guardrail 6: Protection of Data-at-Rest</i> | 37 |
| 5.7 | <i>Guardrail 7: Protection of Data-in-Transit</i> | 37 |
| 5.8 | <i>Guardrail 8: Network Segmentation and Separation</i> | 38 |
| 5.9 | <i>Guardrail 9: Network Security Services</i> | 38 |
| 5.10 | <i>Guardrail 10: Cyber Defense Services</i> | 38 |
| 5.11 | <i>Guardrail 11: Logging and Monitoring</i> | 38 |
| 5.12 | <i>Guardrail 12: Configuration of Cloud Marketplaces</i> | 42 |

LIST OF TABLES

| | |
|--|----|
| Table 1: Document Reference List | 7 |
| Table 2: PBMM Policy Assignment/Exception Table | 11 |
| Table 3: Canada Federal PBMM Blueprint Policy Definition | 16 |
| Table 4: Audit Canada Federal PBMM Policy Initiative | 19 |
| Table 5: Cloud Usage Profile | 25 |

LIST OF FIGURES

| | |
|--|----|
| Figure 1: GC PBMM Blueprint Assignment | 9 |
| Figure 2: Create Blueprint | 12 |
| Figure 3: Blueprint Artifact List | 13 |
| Figure 4: Publish Blueprint | 13 |
| Figure 5: Assign Blueprint | 15 |
| Figure 6: SSC Azure Landing Zone Release | 26 |

1 OVERVIEW

This implementation guide provides the 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.*
- **90 day:** *Security controls to validate additional security mechanisms of the tenant environment (people, processes, policies, procedures, operations, ITSM, physical, personnel, etc.) and achieve tenant ATO.*
- **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.

1.1 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 to be compliant for the 30-Day Guardrail verification. Sections 2 – 5 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.

1.2 GC CLOUD GOVERNANCE

A base structure is defined 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.
- **Automation:** In addition to making resources easier for IT to manage, automation is a key component of deploying and securing the environment.
- **Compliance Reporting:** Tenant owner and security personnel need to be aware of cloud resource compliance.

1.3 DOCUMENT REFERENCE

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

<https://gcdocs.gc.ca/ssc-spc/lisapi.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/lisapi.dll/open/44491286 |
| Azure Governance Framework Draft v0.1.docx (work in progress) | |
| SSC Naming and Tagging Standard for Azure | https://gcdocs.gc.ca/ssc-spc/lisapi.dll/open/72288894 |
| Azure Whitelisting | https://gcdocs.gc.ca/ssc-spc/lisapi.dll/open/71440075 |
| Government of Canada Cloud Guardrails | https://gcdocs.gc.ca/ssc-spc/lisapi.dll/open/67925334 |
| Azure Emergency Access Procedure template | https://gcdocs.gc.ca/ssc-spc/lisapi.dll/open/72824320 |
| Cloud usage profiles | https://gcdocs.gc.ca/ssc-spc/lisapi.dll/open/72829765 |
| Office 365 Security Baseline Configuration Controls | https://gcdocs.gc.ca/ssc-spc/lisapi.dll/open/70457657 |
| CBS Overview and Installation Instructions | https://gcdocs.gc.ca/ssc-spc/lisapi.dll/open/73032410 |

Table 1: Document Reference List

Security Classification **Unclassified**

Status: DRFT

Subject: SSC AZURE GUARDRAIL IMPLEMENTATION GUIDE

1.4 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 2.1.1 |
| Guardrail 12: Configuration of Cloud Marketplaces | Enforced thru implementation of the Azure Whitelisting policies. See Section 2.4 |

Table 2: Map of Guardrails

2 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 the identified 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*).

2.1 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.

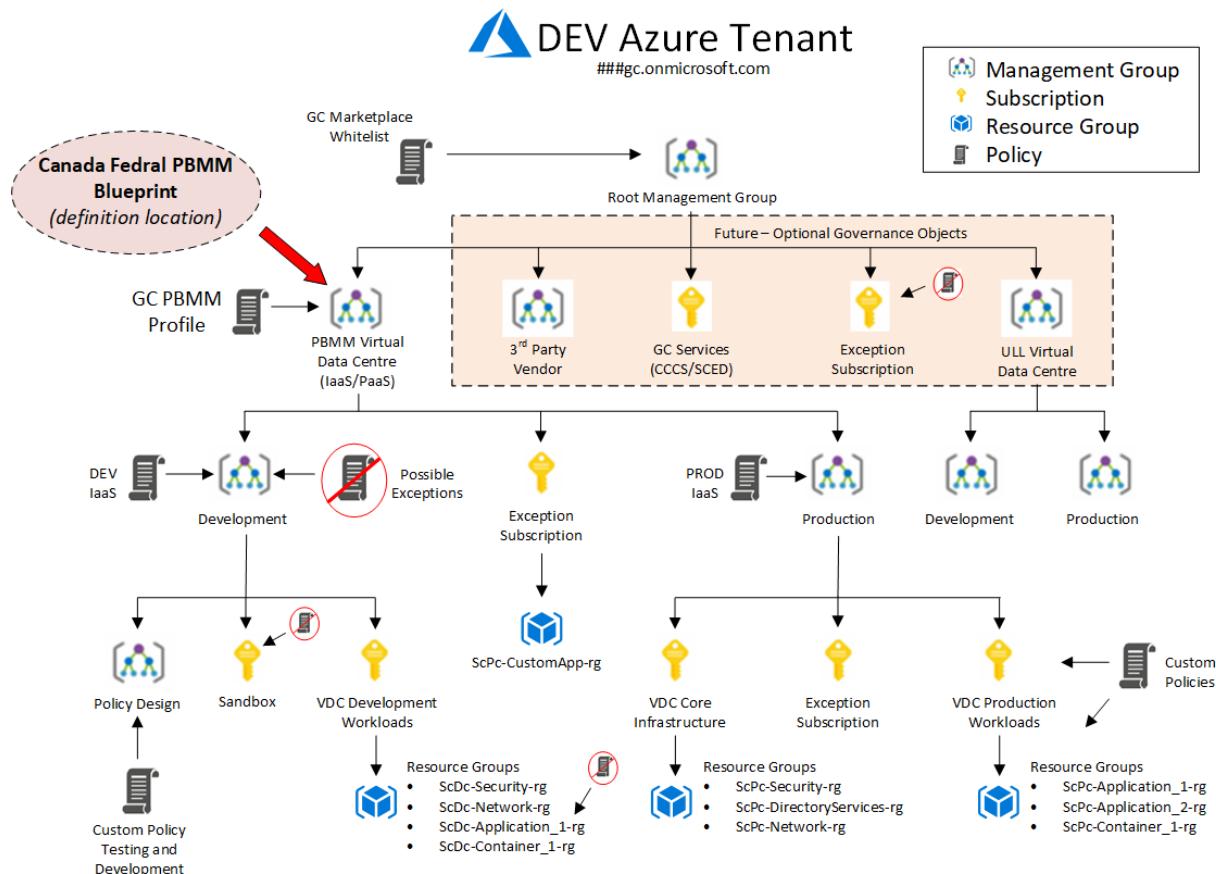


Figure 1: GC PBMM Blueprint Assignment

Security Classification **Unclassified**

Status: DRFT

Subject: SSC AZURE GUARDRAIL IMPLEMENTATION GUIDE

2.1.1 ***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 (LAW) for Security events and Resource Group in accordance with Naming and Tagging convention and the Azure Cloud Governance design.

Security LAW:

- 1) Create a Resource Group for the security monitoring LAW (XXXX-Core_LogAnalytics-rg).
 - 2) Create an automation account (XXXX-CoreSecurity-LogAnalytics-spn). Select “Create Azure Run As account”
 - 3) Create LAW (XXXXCLD-CoreSecurity-law)¹, Retention needs to be 2 years.
 - 1) Workspace summary, add, activity log analytics.
 - 2) Workspace summary, add, antimalware assessment
 - 3) Workspace summary, add, keyvault analytics
 - 4) Usage and estimated costs, Select Pay as you go and extend the retention to 730 days (2 years)
 - 5) Go to RG. Select the automation account, select update management, select the LAW and enable
 - 6) In the Azure AD tenant, select diagnostic setting. Click on Add diagnostic setting. Name is XXXX-Core_LogAnalytics-diags Select send to log analytics and select the LAW. Select audit logs, signint logs
- A Log Analytics Workspace (LAW) for Health events and Resource Group in accordance with Naming and Tagging convention and the Azure Cloud Governance design.

Health LAW:

- 1) Create LAW (XXXXCLD-CoreHealth-law).
 - 1) Workspace summary, add, Azure Log Analytics Agent Health.
 - 2) Usage and estimated costs, Select Pay as you go and extend the retention to 90 days.

¹ Where XXXX refers to the 4 character code identifying the partner and the environment. For example ScPc would refer to SSC, Production environment deployed in Canada Central in accordance with the Naming and Tagging Standard

- 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 |
| | | <i>...complete table to align with departmental requirements</i> | |

Table 2: PBMM Policy Assignment/Exception Table

* Canada Federal PBMM Blueprint with SSC customization

2.1.2 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.

Create blueprint

Basics Artifacts

Blueprint name * ⓘ

GC-PBMM



Blueprint description

Assigns policies to address Canada Federal PBMM controls.



Definition location * ⓘ

PBMM Virtual Data Center (VDC)



...

The management group or subscription where the blueprint is saved. The definition location determines the scope that the blueprint may be assigned to. Learn more at aka.ms/BlueLocation.

Figure 2: Create Blueprint

- Add or remove artifacts based on the 30-Day policy design. The VDC uses the default blueprint with one additional 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.

Home > Blueprints | Blueprint definitions > Create blueprint

Create blueprint

Basics Artifacts

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

| Name | Artifact type | Parameters |
|---|-------------------|---------------------------------|
| Subscription | | |
| Allowed locations for resource groups | Policy assignment | 1 out of 1 parameters populated |
| [Preview]: Audit Canada Federal PBMM controls and deploy specific VM Ext... | Policy assignment | 0 out of 4 parameters populated |
| Deploy network watcher when virtual networks are created | Policy assignment | None |
| Deploy Threat Detection on SQL servers | Policy assignment | None |
| Deploy SQL DB transparent data encryption | Policy assignment | None |
| Deploy default Microsoft IaaSAntimalware extension for Windows Server | Policy assignment | None |
| Require automatic OS image patching on Virtual Machine Scale Sets | Policy assignment | None |
| Deploy Advanced Data Security on SQL servers | Policy assignment | None |
| Deploy Advanced Threat Protection on Storage Accounts | Policy assignment | 0 out of 1 parameters populated |
| Deploy Auditing on SQL servers | Policy assignment | 0 out of 2 parameters populated |
| Allowed locations | Policy assignment | 1 out of 1 parameters populated |
| Require encryption on Data Lake Store accounts | Policy assignment | None |
| [Preview]: Deploy Log Analytics Agent for Linux VMs | Policy assignment | 0 out of 2 parameters populated |
| Deploy Diagnostic Settings for Network Security Groups | Policy assignment | 0 out of 2 parameters populated |
| [Preview]: Deploy Log Analytics Agent for Windows VMs | Policy assignment | 0 out of 2 parameters populated |
| Network interfaces should not have public IPs | Policy assignment | None |
| + Add artifact... | | |

Figure 3: Blueprint Artifact List

- Publish the Blueprint

Publish blueprint

Version * ⓘ

No previous versions

Change notes ⓘ

Initial release for 30-Day Guardrails

Figure 4: Publish Blueprint

- Assign the Blueprint based on Policy Assignment/Exclusion table created for the Virtual Data Center. Follow steps provided by Microsoft.

Assign blueprint

Basics

Subscription(s) * ⓘ

[Create new](#)

Name of the subscription being assigned

Assignment name * ⓘ

Location * ⓘ

Blueprint definition version * ⓘ

Lock Assignment

Don't Lock Do Not Delete Read Only

The assignment is not locked. Users, groups, and service principals with permissions can modify and delete deployed resources.
[Learn more](#)

Managed Identity ⓘ
 System assigned
 User assigned

By clicking "Assign" with a system assigned identity, you agree to grant the Azure Blueprints service temporary Owner access to this subscription so that we can properly deploy all Artifacts. We will automatically remove this access when the blueprint assignment process is finished.

Assign blueprint

Subscription

- [Preview]: Audit Canada Federal PBMM controls and deploy specif...**

| | | |
|--|--------------------------------------|---|
| Log Analytics Workspace Id that VMs should be configured for | 9f088a37-ea3b-4779-9e70-77b4e4aecdc3 | ✓ |
| Resource Types | 46 selected | ▼ |
| List of users that should be excluded from Windows VM Administrators group | Guest | ✓ |
| List of users that should be included in Windows VM Administrators group | Administrator | ✓ |
- [Preview]: Deploy Log Analytics Agent for Linux VMs**

| | | |
|--|--------------------------------------|---|
| Log Analytics workspace for Linux VMs | 9f088a37-ea3b-4779-9e70-77b4e4aecdc3 | ✓ |
| Optional: List of VM images that have supported Linux OS to add to scope | □ | |
- [Preview]: Deploy Log Analytics Agent for Windows VMs**

| | | |
|--|--------------------------------------|---|
| Log Analytics workspace for Windows VMs | 9f088a37-ea3b-4779-9e70-77b4e4aecdc3 | ✓ |
| Optional: List of VM images that have supported Windows OS to add to scope | □ | |

Allowed locations

| | |
|------------------------|---------------------------------|
| listOfAllowedLocations | ["canadacentral", "canadaeast"] |
|------------------------|---------------------------------|

Allowed locations for resource groups

| | |
|------------------------|---------------------------------|
| listOfAllowedLocations | ["canadacentral", "canadaeast"] |
|------------------------|---------------------------------|

Deploy Advanced Data Security on SQL servers

Deploy Advanced Threat Protection on Storage Accounts

| | |
|--------|----------|
| Effect | Disabled |
|--------|----------|

Deploy Auditing on SQL servers

| | | |
|--|---------------------------|---|
| Retention days (optional, 180 days if unspecified) | 180 | |
| Resource group name for storage accounts | ScPc-Core_LogAnalytics-rg | ✓ |

Deploy default Microsoft IaaSAntimalware extension for Windows Server

Deploy Diagnostic Settings for Network Security Groups

| | | |
|--|---------------------------|---|
| Storage Account Prefix for Regional Storage Account | scpc | ✓ |
| Resource Group Name for Storage Account (must exist) | ScPc-Core_LogAnalytics-rg | ✓ |

Deploy Diagnostic Settings for Network Security Groups

| | | |
|---|---------------------------|---|
| Storage Account Prefix for Regional Storage Account (Policy: Deploy Diagnostic Settings for Network Security Groups) | scpc | ✓ |
| Resource Group Name for Storage Account (must exist) (Policy: Deploy Diagnostic Settings for Network Security Groups) | ScPc-Core_LogAnalytics-rg | ✓ |

Deploy network watcher when virtual networks are created

Deploy SQL DB transparent data encryption

Deploy Threat Detection on SQL servers

Network interfaces should not have public IPs

Require automatic OS image patching on Virtual Machine Scale Sets

Require encryption on Data Lake Store accounts

Figure 5: Assign Blueprint

Security Classification **Unclassified**

Status: DRFT

Subject: SSC AZURE GUARDRAIL IMPLEMENTATION GUIDE

2.2 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 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 | | Yes |
| 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 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

| GR # | 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 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 AU-6(4) AU-12 SI-4 | Yes |
| 9,10,11 | [Preview]: Audit Log Analytics Workspace for VM - Report Mismatch | Audit | AU-3 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 reuse of the previous 24 passwords | AuditIfNotExists | IA-5(1) | Yes |

Security Classification **Unclassified**

Status: DRFT

Subject: SSC AZURE GUARDRAIL IMPLEMENTATION GUIDE

| | | | | |
|---------|--|-------------------|--------------------|-----|
| 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 | 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

2.3 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>

2.4 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/lisapi.dll/open/71440075>]. This is required for Guardrail 12 compliance.

3 AZURE AD TENANT MANUAL CONFIGURATION FOR 30-DAY COMPLIANCE

This section addresses the manual procedures required for the implementation of the 30-day guardrails to the Azure Active Directory Tenant in order to support IaaS/PaaS.

3.1 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_PrivRoles², 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) (AZ-L2-001)

- 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

² First three characters should describe the Department. Change XXX to Department Identification in accordance with Naming and Tagging Standard

- 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

4- Other settings

- 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`

3.2 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

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

3.3 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-CloudAccess³, select All Admin roles, exclude break glass account, all cloud apps, condition-select all trusted locations, grant MFA, enable policy, create

3.4 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.

3.5 GUARDRAIL 11: LOGGING AND MONITORING

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

- Select Pricing & settings
 - For each subscription, repeat the following steps
 - 1) Pricing tier - Select standard
 - 1) Data collection - Set auto provisioning to ON
Select another workspace and Select the XXXXCLD-CoreSecurity-law
Select All events
 - 2) Email notification - enter email and phone number (select send email for high severity alerts)
 - 3) Threat detection – enable both options

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

- Select hunting to see what's going on
- 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

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.

³ First three characters should describe the Department. Change XXX to Department Identification in accordance with Naming and Tagging Standard

4 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>

4.1 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 | <ul style="list-style-type: none">Cloud-based services hosting sensitive (up to Protected B) informationNo 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 | <ul style="list-style-type: none">Cloud-based services hosting sensitive (up to Protected B) informationGC cloud-based systems required to interact with systems in GC data centersEnvironment accessible for both GC users and External users and servicesSolution implemented, managed and operated by a GC department/agency | IaaS, PaaS | Type 3 - CXP (SCED) |

Table 5: Cloud Usage Profile

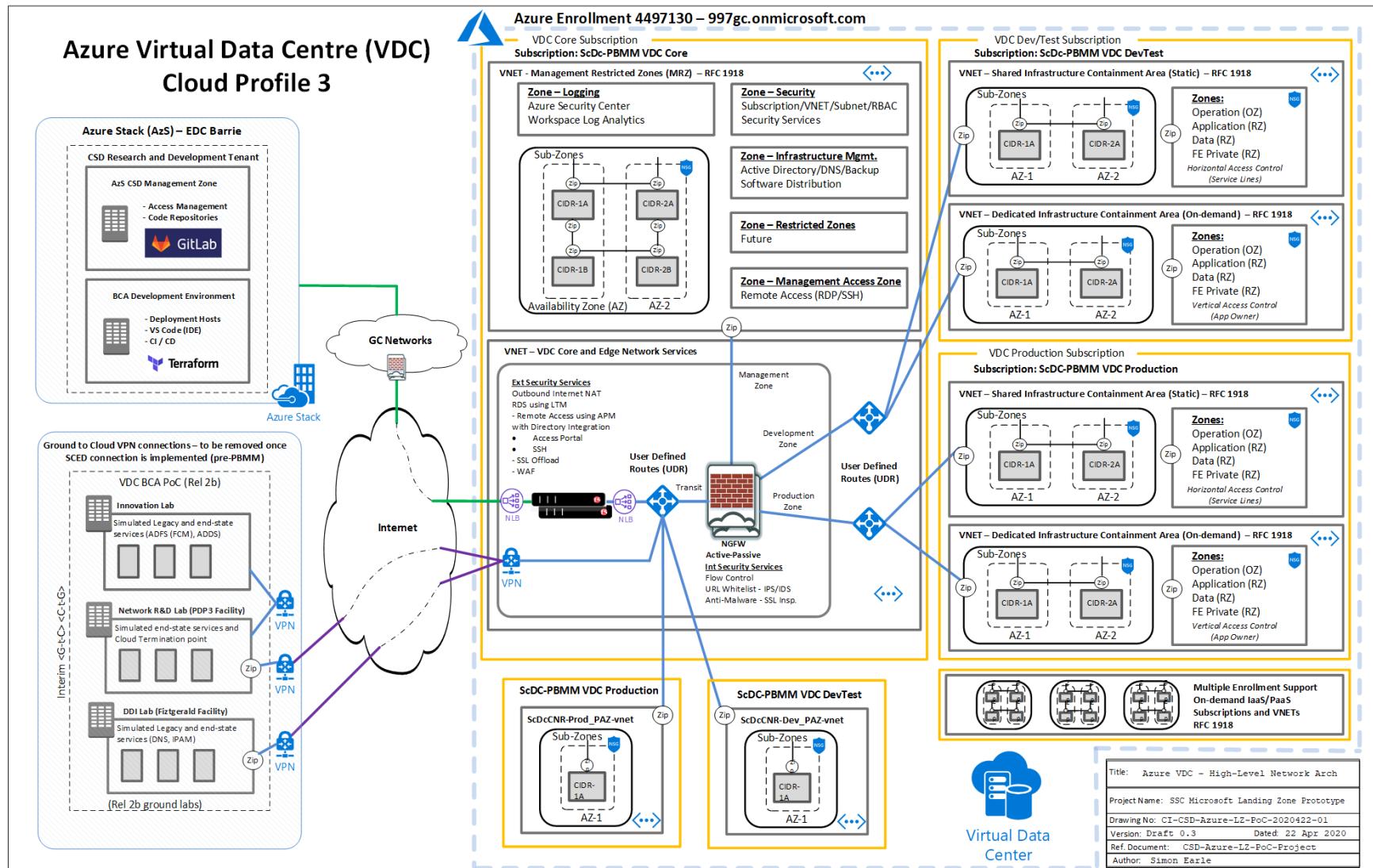


Figure 6: SSC Azure Landing Zone Release

Security Classification **Unclassified**

Status: DRFT

Subject: SSC AZURE GUARDRAIL IMPLEMENTATION GUIDE

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;

5 CYBER DEFENSE SERVICES

Partners must establish and sign an MOU with CSE (Cyber Centre Security) CCCS 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.

The CBS onboarding instructions can be found at <https://gcdocs.gc.ca/ssc-spc/lisapi.dll/open/73032410>

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.

5.1 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](#)).

2- Azure AD, Security, conditional access policies

The screenshot shows the 'Conditional Access | Policies' section in the Azure Active Directory portal. On the left, there's a sidebar with links like 'Policies', 'Diagnose and solve problems', 'Manage', 'Named locations', 'Custom controls (Preview)', 'Terms of use', 'VPN connectivity', 'Classic policies', and 'Troubleshooting + Support'. The main area shows a list of policies under 'Workstation' and 'CS Test' categories. A red circle highlights the 'SSC-AzureMFAPolicy' entry in the 'CS Test' list, which has 'On' listed under 'State'. Other policies shown include 'Baseline policy: Require MFA for admins (Preview)', 'Baseline policy: End user protection (Preview)', 'Baseline policy: Block legacy authentication (Preview)', 'Baseline policy: Require MFA for Service Management (Preview)', 'CS Test - Restrict XON by subnet', 'CS Test - Require MFA if not on Trusted Network', 'CS Test - Restrict Android', 'CS Test - MFA for Mobile OS', and 'CS Test - Restrict iOS'. There are also entries for 'SSC-AAD_PrivRoles' and 'SSC-AzureMFAPolicy'.

3- Identity Protection.

Identity Protection | MFA registration policy

Search (Ctrl+ /) <>

⚠ This view is for Azure AD Premium P2 customers to setup risk-based policies.

① Overview

Protect

- User risk policy
- Sign-in risk policy
- MFA registration policy**

Report

- Risky users
- Risky sign-ins
- Risk detections

Notify

- Users at risk detected alerts
- Weekly digest

Troubleshooting + Support

- Troubleshoot
- New support request

Policy name
Multi-factor authentication registration policy

Assignments
Users >
All users included and 1 user excluded

Controls
Access >
Require Azure MFA registration

Info MFA Registration Policy only affects cloud-based Azure MFA. If you have MFA Server it will not be affected.

Info Azure AD Premium P2 edition (available with EMS E5 subscription) is needed to use the Azure AD Identity Protection MFA Registration policy. If you are not an Azure AD Premium P2 subscriber, you can turn off enforcement of this policy here.

Enforce Policy
On Off

4- Configure user risk policy.

Home > SSC Test Tenant (997) > Security > Identity Protection | User risk policy

Identity Protection | User risk policy

Search (Ctrl+ /) <>

⚠ This view is for Azure AD Premium P2 customers to setup risk-based policies.

① Overview

Protect

- User risk policy**
- Sign-in risk policy
- MFA registration policy

Report

- Risky users
- Risky sign-ins
- Risk detections

Notify

- Users at risk detected alerts
- Weekly digest

Troubleshooting + Support

- Troubleshoot
- New support request

Policy name
User risk remediation policy

Assignments
Users >
All users included and 1 user excluded

Conditions >
User risk

Controls
Access >
Require password change

Info Azure AD Premium P2 edition (available with EMS E5 subscription) is needed to use Azure AD Identity Protection risk policies. If you are not an Azure AD Premium P2 subscriber, you can turn off enforcement of this policy here.

Enforce Policy
On Off

5- Configure sign-in risk policy.

Security Classification **Unclassified**

Status: DRFT

Subject: SSC AZURE GUARDRAIL IMPLEMENTATION GUIDE

Identity Protection | Sign-in risk policy

This screenshot shows the configuration of a 'Sign-in risk remediation policy' in the Azure AD Identity Protection section. The left sidebar includes categories like Overview, Protect (User risk policy, Sign-in risk policy, MFA registration policy), Report (Risky users, Risky sign-ins, Risk detections), Notify (Users at risk detected alerts, Weekly digest), and Troubleshooting + Support (Troubleshoot, New support request). The main pane displays policy details, assignments (Users, Conditions), controls (Access), and a note about Azure AD Premium P2 edition requirements. An 'Enforce Policy' switch is set to 'On'.

5.2 GUARDRAIL 2: MANAGEMENT OF ADMINISTRATIVE PRIVILEGES

External and deprecated accounts

This screenshot shows the 'Identity & access' recommendations section in the Azure Security Center. It highlights several recommendations related to account management, such as 'A maximum of 3 owners should be designated for your subscription' and 'Deprecated accounts should be removed from your subscription'. A red box surrounds these specific recommendations. The interface includes a search bar, navigation tabs for Overview, Subscriptions, and Key vaults, and a detailed table of findings with columns for Recommendation, Failed Resources, and Severity.

| Recommendation | Failed Resources | Severity |
|---|------------------|----------|
| A maximum of 3 owners should be designated for your subscription | None | Low |
| Deprecated accounts should be removed from your subscription | None | Low |
| Deprecated accounts with owner permissions should be removed from your subscription | None | Low |
| External accounts with owner permissions should be removed from your subscription | None | Low |
| External accounts with read permissions should be removed from your subscription | None | Low |
| External accounts with write permissions should be removed from your subscription | None | Low |
| MFA should be enabled on accounts with owner permissions on your subscription | None | Low |
| MFA should be enabled on accounts with read permissions on your subscription | None | Low |
| MFA should be enabled on accounts with write permissions on your subscription | None | Low |
| There should be more than one owner assigned to your subscription | None | Low |

Password reset notification

Security Classification **Unclassified**

Status: DRFT

Subject: SSC AZURE GUARDRAIL IMPLEMENTATION GUIDE

Home > SSC Test Tenant (997) > Password reset | Notifications

Password reset | Notifications

SSC Test Tenant (997) - Azure Active Directory

Notify users on password resets? ⓘ

Yes No

Notify all admins when other admins reset their password? ⓘ

Yes No

Diagnose and solve problems

Manage

-
-
-
-

MFA required to join devices

Home > SSC Test Tenant (997) > Devices | Device settings

Devices | Device settings

SSC Test Tenant (997) - Azure Active Directory

Users may join devices to Azure AD ⓘ

All Selected None

Selected

No member selected

Users may register their devices with Azure AD ⓘ

All None

[Learn more on how this setting works](#)

Require Multi-Factor Auth to join devices ⓘ

Yes No

Maximum number of devices per user ⓘ

50

All devices

Device settings

Diagnose and solve problems

Activity

Troubleshooting + Support

MFA settings

multi-factor authentication

users service settings

app passwords [\(learn more\)](#)

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(learn more\)](#)

- Skip multi-factor authentication for requests from federated users on my intranet
- Skip multi-factor authentication for requests from following range of IP address subnets

| |
|------------------|
| 198.103.167.0/24 |
| 172.16.212.0/24 |
| 104.251.107.0/24 |
| 205.193.212.0/24 |

verification options [\(learn more\)](#)

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

remember multi-factor authentication [\(learn more\)](#)

- Allow users to remember multi-factor authentication on devices they trust
- Days before a device must re-authenticate (1-60):

Security Classification **Unclassified**

Status: DRFT

Subject: SSC AZURE GUARDRAIL IMPLEMENTATION GUIDE

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

Home > SSC Test Tenant (997) > Users | User settings

Users | User settings
SSC Test Tenant (997) - Azure Active Directory

All users
Deleted users
Password reset
User settings
Diagnose and solve problems

Activity
Sign-ins
Audit logs
Bulk operation results (Preview)

Troubleshooting + Support
New support request

Save Discard

Enterprise applications
Manage how end users launch and view their applications

App registrations
Users can register applications
Yes No

Administration portal
Restrict access to Azure AD administration portal
Yes No

LinkedIn account connections
Allow users to connect their work or school account with LinkedIn.
Data sharing between Microsoft and LinkedIn is not enabled until us
Learn more about LinkedIn account connections
Yes Selected group No

Azure Active Directory Group settings

Home > SSC Test Tenant (997) > Groups | General

Groups | General
SSC Test Tenant (997) - Azure Active Directory

All groups
Deleted groups
Diagnose and solve problems

Settings
General
Expiration
Naming policy

Activity
Access reviews
Audit logs
Bulk operation results (Preview)

Save Discard

Self Service Group Management
Owners can manage group membership requests in the Access Panel
Yes No

Restrict access to Groups in the Access Panel
Yes No

Security Groups
Users can create security groups in Azure portals
Yes No

Owners who can assign members as group owners in Azure portals
All Selected None

Office 365 Groups
Users can create Office 365 groups in Azure portals
Yes No

Owners who can assign members as group owners in Azure portals
All Selected None

5.3 GUARDRAIL 3: CLOUD CONSOLE ACCESS

- Azure AD, Security, Named location.

Security Classification **Unclassified**

Status: DRFT

Subject: SSC AZURE GUARDRAIL IMPLEMENTATION GUIDE

- conditional access policies

| Policy Name | Status |
|---|-------------|
| Baseline policy: Require MFA for admins (Preview) | Off |
| Baseline policy: End user protection (Preview) | Off |
| Baseline policy: Block legacy authentication (Preview) | Off |
| Baseline policy: Require MFA for Service Management (Preview) | Off |
| Workstation | |
| CS Test - Restrict XON by subnet | Off |
| CS Test - Require MFA if not on Trusted Network | Off |
| CS Test - Restrict Android | Off |
| CS Test - MFA for Mobile OS | Off |
| CS Test - Restrict iOS | Off |
| SSC-AAD_PriRoles | On |
| SSC-AzureMFAPolicy | On |
| SSC-CloudAccess | Report-only |

5.4 GUARDRAIL 4: ENTERPRISE MONITORING ACCOUNTS

- Confirm an Azure AD native account named SSC-CBS-Reporting@###gc.onmicrosoft.com



SSC-CBS-Reporting



Sign in allowed

Account Devices Licenses and Apps Mail OneDrive

Username

SSC-CBS-Reporting@997gc.onmicrosoft.com

All Users

[Manage username](#)

[Manage groups](#)

Roles

Billing admin

Service support admin

Reports reader

[Manage roles](#)

Contact information

Display Name

First Name

SSC-CBS-Reporting

Phone number

Last Name

[Manage contact information](#)

Office activations ⓘ

Multifactor authentication

[View Office activations](#)

[Manage multifactor authentication](#)

5.5 GUARDRAIL 5: DATA LOCATION

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

Home > Policy | Compliance

Policy | Compliance

Search (Ctrl+ /) Assign policy Assign initiative Refresh

| Scope | Type | Compliance state | Search |
|---|-----------------------------|---|---|
| 8 selected | All definition types | All compliance states | location |
| Overall resource compliance 89% 1567 out of 1759 | | Non-compliant initiatives 9 out of 15 | Non-compliant policies 148 out of 1132 |
| | | Non-compliant resources 192 out of 1759 | |
| Name | Scope | Compliance state | Resource complia... Non-Compliant Resources |
| Allowed locations for resource groups | ScSc-PBMM VDC Sandbox | Compliant | 100% (9 out of 9) 0 |
| Allowed locations | ScSc-PBMM VDC Sandbox | Compliant | 100% (11 out of 11) 0 |
| Allowed locations | ScPc-PBMM VDC Prod | Compliant | 100% (116 out of 116) 0 |
| Allowed locations for resource groups | ScPc-PBMM VDC Prod | Compliant | 100% (6 out of 6) 0 |
| Allowed locations | ScDc-PBMM VDC PolicyDesi... | Compliant | 100% (47 out of 47) 0 |
| Allowed locations for resource groups | ScDc-PBMM VDC PolicyDesi... | Compliant | 100% (5 out of 5) 0 |
| Allowed locations | ScDc-PBMM VDC PolicyDesi... | Compliant | 100% (5 out of 5) 0 |
| Allowed locations | ScDc-PBMM VDC DevTest | Compliant | 100% (3 out of 3) 0 |
| Allowed locations for resource groups | ScDc-PBMM VDC DevTest | Compliant | 100% (5 out of 5) 0 |
| Allowed locations for resource groups | ScPc-PBMM VDC Core | Compliant | 100% (11 out of 11) 0 |
| Allowed locations | ScPc-PBMM VDC Core | Compliant | 100% (134 out of 134) 0 |

5.6 GUARDRAIL 6: PROTECTION OF DATA-AT-REST

Home > Security Center | Compute & apps

Security Center | Compute & apps

No subscriptions are selected

Search (Ctrl+/) Add Servers

Overview VMs and Servers VM scale sets Cloud services App ser...

Search recommendations

| Recommendation | Failed Resources | Severity |
|--|--------------------------|----------|
| Adaptive Network Hardening recommendations should be applied on internet facing virtual machines | 1 of 33 virtual machi... | High |
| Disk encryption should be applied on virtual machines | 29 of 33 virtual mac... | High |
| Install monitoring agent on your virtual machines | None | Medium |
| IP forwarding on your virtual machine should be disabled (Preview) | None | Medium |
| Your machines should be restarted to apply system updates | 2 of 33 virtual machi... | Medium |
| Management ports should be closed on your virtual machines | None | Medium |
| Monitoring agent health issues should be resolved on your machines | 20 of 33 virtual mac... | Medium |
| Network traffic data collection agent should be installed on Linux virtual machines (Preview) | 2 of 3 virtual machin... | Medium |
| Install endpoint protection solution on virtual machines | 11 of 33 virtual mac... | High |

5.7 GUARDRAIL 7: PROTECTION OF DATA-IN-TRANSIT

Security Classification Unclassified

Status: DRFT

Subject: SSC AZURE GUARDRAIL IMPLEMENTATION GUIDE

Home > Security Center | Data & storage

Security Center | Data & storage

No subscriptions are selected

Search (Ctrl+ /) Overview Getting started Pricing & settings Community Workflow automation

POLICY & COMPLIANCE

- Coverage
- Secure Score (Preview)
- Security policy
- Regulatory compliance

SQL Information Protection

Overview SQL Storage accounts Redis

Search recommendations

| Recommendation | Failed Resources | Severity |
|---|----------------------|----------|
| Storage accounts should be migrated to new Azure Resource Manager resources | None | High |
| Secure transfer to storage accounts should be enabled | 1 of 14 storage a... | Medium |

Quick Fix!

5.8 GUARDRAIL 8: NETWORK SEGMENTATION AND SEPARATION

As per network design

5.9 GUARDRAIL 9: NETWORK SECURITY SERVICES

Network watcher

Home > Network Watcher

Network Watcher

Subscriptions: All 8 selected – Don't see a subscription? Open Directory + Subscription settings

| Name | Region | Status |
|---------------------------------|--------------|-------------------|
| ScDc-CSD-Sandbox-24049 | 33 regions | Partially enabled |
| ScDc-CSD-VDC_Core-24049 | > 33 regions | Partially enabled |
| ScDc-CSD-VDC_DevTest-24049 | > 33 regions | Partially enabled |
| ScDc-CSD-VDC_PolicyDesign-24049 | > 33 regions | Partially enabled |
| ScDc-CSD-VDC_Prod-24049 | > 33 regions | Partially enabled |
| ScSc-CSD-VDC_Core-24049 | > 33 regions | Partially enabled |
| ScSc-CSD-VDC_DevTest-24049 | > 33 regions | Partially enabled |
| ScSc-CSD-VDC_Prod-24049 | > 33 regions | Partially enabled |

5.10 GUARDRAIL 10: CYBER DEFENSE SERVICES

Evidence of MOU with CCCS

5.11 GUARDRAIL 11: LOGGING AND MONITORING

Log Analytic Workspaces

Security Classification **Unclassified**

Status: DRFT

Subject: SSC AZURE GUARDRAIL IMPLEMENTATION GUIDE

| Microsoft Azure | | Search resources, services, and docs (G+) | | |
|--|---|---|---------------------------------|-------------|
| Log Analytics workspaces | | | | |
| SSC Test Tenant (997) | | | | |
| + Add | Manage view | Refresh | Export to CSV | Assign tags |
| Filter by name... | Subscription == all | Resource group == all | Location == all | Add filter |
| Showing 1 to 8 of 8 records. | | | | |
| <input type="checkbox"/> Name ↑ | Resource group ↑↓ | Location ↑↓ | Subscription ↑↓ | |
| <input type="checkbox"/> GC-Guardrails-Workspace | GC-Guardrails | Canada Central | ScDc-CSD-Sandbox-24049 | |
| <input type="checkbox"/> ScDc-CSD-Embotics | ScDc-CSD-VDC_R2a_Network_Core-rg | Canada Central | ScDc-CSD_VDC_Core-24049 | |
| <input type="checkbox"/> ScDc-CSD-sharedsvcs-log | scd-csd-sharedsvcs-rg | Canada Central | ScDc-CSD-Sandbox-24049 | |
| <input type="checkbox"/> ScDc-CSD-VDCR2aCoreLogAnalytics-law | ScDc-CSD-VDC_R2a_Core_LogAnalytics-rg | Canada Central | ScDc-CSD_VDC_Core-24049 | |
| <input type="checkbox"/> ScDc-CSD-VDCR2aMonitorPolicyDesign-law | ScDc-CSD-VDC_R2a_Monitor_PolicyDesign-rg | Canada Central | ScDc-CSD_VDC_PolicyDesign-24049 | |
| <input type="checkbox"/> ScDc-CSD-VDCR2aPolicyDesignLogAnalytics-law | ScDc-CSD-VDC_R2a_PolicyDesign_LogAnalytics-rg | Canada Central | ScDc-CSD_VDC_PolicyDesign-24049 | |
| <input type="checkbox"/> ScDcSEC-VDCCore-law | ScDc-CSD-VDC_SetLog-rg | Canada Central | ScDc-CSD_VDC_Core-24049 | |
| <input type="checkbox"/> ScSc-CSD-VDCR2aNetworkCoreEA-law | ScSc-CSD-VDC_R2a_Network_Core_EA-rg | Canada Central | ScSc-CSD_VDC_Core-24049 | |

AZURE SECURITY CENTER.

Security Center | Pricing & settings
Showing 8 subscriptions

Search (Ctrl+)

- Overview
- Getting started
- Pricing & settings **(selected)**
- Community
- Workflow automation

POLICY & COMPLIANCE

- Coverage
- Secure Score (Preview)
- Security policy
- Regulatory compliance

RESOURCE SECURITY HYGIENE

- Recommendations
- Compute & apps
- Networking
- IoT Hubs & resources
- Data & storage
- Identity & access
- Security solutions

ADVANCED CLOUD DEFENSE

- Adaptive application controls
- Just in time VM access
- Adaptive network hardening
- File Integrity Monitoring

THREAT PROTECTION

- Security alerts
- Security alerts map (Preview)

Pricing & Settings

Configure pricing, data collection and additional settings of your Azure subscriptions and workspaces.

5 MANAGEMENT GROUPS 8 SUBSCRIPTIONS 8 WORKSPACES

| Name | Pricing tier |
|---|--------------------|
| Tenant Root Group (8 of 8 subscriptions) | |
| ScDc-CSD-AzureVDC-mg (8 of 8 subscriptions) | |
| ScDc-CSD-Development-mg (4 of 4 subscriptions) | |
| ScDc-CSD-PolicyDesign-mg (2 of 2 subscriptions) | |
| ScDc-CSD-Sandbox-24049 | Standard |
| ScDc-CSD-VDC_PolicyDesign-24049 | Standard |
| ScDc-CSD-VDC_DevTest-24049 | Standard |
| ScDc-CSD-VDC_DevTest-24049 | Standard (partial) |
| ScDc-CSD-Production-mg (4 of 4 subscriptions) | |
| ScDc-CSD-VDC_Core-24049 | Standard |
| ScDc-CSD-VDC_Prod-24049 | Standard |
| ScDc-CSD-VDC_Core-24049 | Standard (partial) |
| ScDc-CSD-VDC_Prod-24049 | Standard (partial) |
| GC-Guardrails-Workspace | N/A |
| ScDc-CSD-sharedsvcs-log | N/A |
| ScDc-CSD-VDCR2aCoreLogAnalytics-law | Free |
| ScDc-CSD-Embotics | N/A |
| ScDcSEC-VDCCore-law | Standard (partial) |
| ScDc-CSD-VDCR2aMonitorPolicyDesign-law | N/A |
| ScDc-CSD-VDCR2aPolicyDesignLogAnalytics-law | N/A |
| ScSc-CSD-VDCR2aNetworkCoreEA-law | Free |

Security Classification **Unclassified**

Status: DRFT

Subject: SSC AZURE GUARDRAIL IMPLEMENTATION GUIDE

Home > Security Center | Pricing & settings > Settings | Data Collection

Settings | Data Collection

ScDc-CSD-VDC_Core-24049

Search (Ctrl+ /) Save

Settings

- Pricing tier
- Data Collection**
- Email notifications
- Threat detection
- Workflow automation
- Continuous export

Security Center collects security data and events from your resources across your organization.

Auto Provisioning

This enables the automatic installation of the Microsoft Monitoring Agent component on Azure VMs. If the Microsoft Monitoring agent (MMA) extension is installed, it will have it provisioned. [Learn more](#)

On Off

i If a VM already has either SCOM or OMS agent installed locally, the Microsoft Monitoring agent (MMA) extension will be provisioned in the workspace.

Workspace configuration

Data collected by Security Center is stored in Log Analytics workspace(s). You can choose to store data in a workspace created by Security Center or in an existing workspace you created. [Learn more](#)

Use workspace(s) created by Security Center (default)
Connect Azure VMs to report to workspaces created by Security Center

Use another workspace
Connect Azure VMs to report to selected user workspace

ScDcSEC-VDCCore-law

Home > Security Center | Pricing & settings > Settings | Email notifications

Settings | Email notifications

ScDc-CSD-VDC_Core-24049

Search (Ctrl+ /) Save

Settings

- Pricing tier
- Email notifications**
- Threat detection
- Workflow automation
- Continuous export

i Enter contact information for the administrator who should be notified when a security event occurs.

Email address

Phone number

Email notification settings

Send email notification for high severity alerts On Off

Also send email notification to subscription owners On Off

Settings | Threat detection
ScDc-CSD-VDC_Core-24049

Search (Ctrl+/
Save

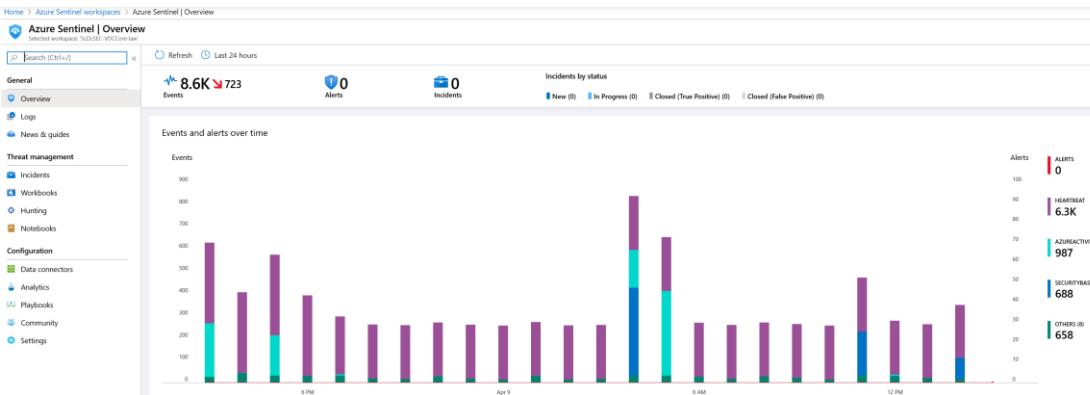
Enable integrations

To enable Security Center to integrate with other Microsoft security services, allow those services to access your data.

- Allow Microsoft Cloud App Security to access my data. [Learn more >](#)
- Allow Windows Defender ATP to access my data. [Learn more >](#)

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

- Select hunting to see what's going on



Azure AD Privileged identity management

Home > Privileged Identity Management > Quick start

Quick start
Privileged Identity Management - Azure AD roles

Quick start

Tasks

- My roles
- Pending requests
- Approve requests
- Review access

Manage

- Roles
- Members
- Alerts
- Access reviews
- Settings

Activity

- Resource audit
- My audit

Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. [Learn more](#)

Assign

Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary

Activate

Activate your eligible admin roles so that you can get limit standing access to the privileged identity

Approve

View and approve all activation requests for specific Azure AD roles that are configured to approve

Audit

View and export privileged identity activation requests and stay

Buttons

- Assign Eligibility
- Activate your role
- Approve requests
- View your history

Security Classification **Unclassified**

Status: DRFT

Subject: SSC AZURE GUARDRAIL IMPLEMENTATION GUIDE

5.12 GUARDRAIL 12: CONFIGURATION OF CLOUD MARKETPLACES

Evidence of the implementation of the Azure Whitelisting policies