Cloud Guardrails

Oracle Cloud Infrastructure (OCI)

0.04
December 31, 2020

Contents

Introduction

Background

The Government of Canada has a Cloud-first strategy for supporting Departments and Agencies deliver services digitally to Canadians.

Oracle Cloud Infrastructure (OCI) is an approved Cloud Service Provider.

Context

Shared Services Canada is the single-point of entry for Cloud Services. Through the Cloud Brokering Portal, Partners can request Cloud Services including Public, Hybrid and Private, Unclassified and up to Protected B information.

The purpose of the guardrails is to ensure that departments and agencies are implementing a preliminary baseline set of controls within their cloud-based environments.

These minimum guardrails are to be implemented within the GC-specified initial period (e.g. 30 days) upon receipt of an enrollment under the GC Cloud Services Framework Agreement.

This document provides a brief overview of each applicable guardrail and instructions on how to implement them when using OCI.

Access Management

Guardrail 1 - Protect Root / Global Admins Account

Objective

Protect root or master account used to establish the cloud service.

Key Considerations

- ☐ Implement multi-factor authentication (MFA) mechanism for root/master account.
- ☐ Document a break glass emergency account management procedure. Including names of users with root or master account access.
- ☐ Obtain signature from Departmental Chief Information Officer (CIO) and Chief Security Officer (CSO) to confirm acknowledgement and approval of the break glass emergency account management procedures.
- ☐ Implement a mechanism for enforcing access authorizations.
- ☐ Configure appropriate alerts on root/master accounts to detect a potential compromise, in accordance with the GC Event Logging Guidance

Validation

- ☐ Confirm policy for MFA is enabled through screenshots and compliance reports.
- ☐ Confirm that an attestation letter of the emergency break glass procedure has been signed by the Departmental CIO and CSO.

Additional Considerations

- ☐ Leverage enterprise services such as Administrative Access Control System (AACS) for Privileged Access Management (PAM), Attribute-based access control (ABAC).

Applicable Service Models

- IaaS, PaaS, SaaS

How-to protect root and global admins account

1. To enable MTF on the global Oracle cloud admin account, follow the instructions indicated here :

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/usingmfa.htm

How-to confirm policy for MFA

1. To confirm that MFA is enabled for your Cloud admininstrator account, send a screen shot of your Admin user, as shown below. The 'Multi-factor authentication field' must be labeled 'ENABLED'.

Guardrail 2 - Management of Administrative Privileges

Objective

Establish access control policies and procedures for management of administrative privileges.

Key Considerations

- ☐ 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 mechanism for enforcing access authorizations.
- ☐ Implement a mechanism for uniquely identifying and authenticating organizational users, non-organizational users (if applicable), and processes (for example, username and password).
- ☐ Implement a multi-factor authentication mechanism for privileged accounts (for example, username, password and one-time password) and for external facing interfaces.
- ☐ Change default passwords.
- ☐ Ensure that no custom subscription owner roles are created.
- ☐ Configure password policy in accordance with GC Password Guidance.
- ☐ Minimize number of guest users; add only if needed.
- ☐ Determine access restrictions and configuration requirements for GC-issued endpoint devices, including those of non-privileged and privileged users, and configure access restrictions for endpoint devices accordingly. Note: Some service providers may offer configuration options to restrict endpoint device access. Alternatively, organizational policy and procedural instruments can be implemented to restrict access.

Validation

- ☐ Confirm policy for MFA (see Guardrail 1)
- ☐ Confirm that a privileged account management plan and process has been documented.
- ☐ Confirm password policy aligns with GC Password Guidance as appropriate.

Additional Considerations

- ☐ Leverage enterprise services such as Administrative Access Control System (AACS) for Privileged Access Management (PAM), Attribute-based access control (ABAC).

Applicable Service Models

- IaaS, PaaS, SaaS

How-to setup management of administrative privileges

1. To get started with Identity and Access Management and learn about how to control access to your cloud resources, see the document 'Overview of Oracle Cloud Infrastructure Identity and Access Management', located here:

https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm

2. To create users and provide access to cloud resources, see the document 'Managing Users' located here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingusers.htm

3. To create groups to provide access to cloud resources, see the document 'Managing Groups' located here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managinggroups.htm

4. To create policies to provide access to cloud resources, see the document 'How Policies Work' located here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Concepts/policies.htm

5. To organize and isolate your cloud resources, use Compartments, see the document 'Managing Compartments' located here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingcompartments.htm

Guardrail 3 - Cloud Console Access (Developers/Application Owners)

Objective

Limit access to GC managed devices and authorized users.

Key Considerations

- ☐ Implement multi-factor authentication (MFA) mechanism for privileged accounts and remote network (cloud) access.
- ☐ Determine access restrictions and configuration requirements for GC managed devices, including those of non-privileged and privileged users, and configure access restrictions for endpoint devices accordingly.

Note: Some service providers may offer configuration options to restrict endpoint device access. Alternatively, organizational policy and procedural instruments can be implemented to restrict access.

- ☐ Ensure that administrative actions are performed by authorized users using a trusted device that is connected to a trusted network (e.g. GC network).
- ☐ Implement a mechanism for enforcing access authorizations.
- ☐ Implement password protection mechanisms to protect against password brute force attacks.

Validation

- ☐ Confirm policy for MFA (see Guardrail 1)

Additional Considerations

- ☐ Leverage enterprise services such as Administrative Access Control System (AACS) for Privileged Access Management (PAM), Attributed-based access control (ABAC).

Applicable Service Models

- IaaS, PaaS, SaaS

How-to limit access to Cloud Console

1. To get started with Identity and Access Management and learn about how to control access to your cloud resources, see the document 'Getting started with Oracle Cloud Infrastructure Identity and Access Management', located here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm

2. To create users and provide access to cloud resources, see the document 'Managing Users' located here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingusers.htm

3. To create groups to provide access to cloud resources, see the document 'Managing Groups' located here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managinggroups.htm

4. To create policies to provide access to cloud resources, see the document 'How Policies Work' located here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Concepts/policies.htm

5. To organize and isolate your cloud resources, use Compartments, see the document 'Managing Compartments' located here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingcompartments.htm

Guardrail 4 - Enterprise Monitoring Accounts

Objective

Create role-based account to enable enterprise monitoring and visibility.

Key Considerations

- ☐ Assign roles to approved GC stakeholders to enable enterprise visibility. Roles include billing reader, policy contributor/reader, security reader, and global reader.
- ☐ Ensure that multi-factor authentication mechanism for enterprise monitoring accounts is enabled.

Validation

- ☐ Confirm presence of GC enterprise role-based accounts created by Department for GC approved stakeholders.
- ☐ Confirm that accounts have appropriate read access to Departmental tenant environment.

Applicable Service Models

- IaaS, PaaS, SaaS

How-to create enterprise monitoring accounts

1. SSC Cloud Brokering team will be creating a Read only user account in your cloud tenancy which will provide access to billing and auditing data. The user name is labeled 'SSC Admin' and will have the required read privileges.

   No additional action or configuration is required.

Access Management Artifacts

- Emergency Break Glass Procedures Approved by CIO/CSO
- Plan for Managing Privileged Accounts
- Compliance Report

Data Protection

Guardrail 5 - Data location in Canada

Objective

Establish policies to restrict GC sensitive workloads to approved geographic locations.

Key Considerations

- ☐ As per the Direction on Electronic Data Residency (ITPIN 2017-02), "All sensitive electronic data under government control, that has been categorized as Protected B, Protected C or is Classified, will be stored in a GC-approved computing facility located within the geographic boundaries of Canada or within the premises of a GC department located abroad, such as a diplomatic or consular mission."

Validation

- ☐ Confirm policy and tagging for data location.

Applicable Service Models

- IaaS, PaaS, SaaS

How-to enable Data Location in Canada

1. When you sign up for Oracle Cloud Infrastructure, Oracle creates a tenancy for you in one region of your choose, this is your *home region*. You can only provision cloud resources in your home region. Additionally, you can provision resources in other cloud regions, however, before you have that ability, you must first subscribed to the other cloud region. To enable Data Location in Canada, select a Canadian Region as your home region. If you wold like to provision cloud resources in other regions, only subscribe to Canadian Regions. For instructions on how to subscribe to cloud region, see the Oracle document located here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingregions.htm

How-to show that the Data Location is in Canada

1. Sign into your Oracle Cloud Console and select the hamburger menu on the top left corner and choose **Administration** and then **Region Management**.
2. Take a screen shoot of the 'Infrastructure Regions' page.

3. Optionally, you can use the ListRegions API to list the regions that you are subscribed to. The API documentation is located here :

https://docs.cloud.oracle.com/en-us/iaas/api/#/en/identity/20160918/Region/ListRegions

Guardrail 6 - Protection of data-at-rest

Objective

Protect data at rest by default (e.g. storage) for cloud-based workloads.

Key Considerations

- ☐ Seek guidance from privacy and access to information officials within institutions before storing personal information in cloud-based environments.
- ☐ Implement an encryption mechanism to protect the confidentiality and integrity of data when data are at rest in your solution's storage.
- ☐ Use CSE-approved cryptographic algorithms and protocols, in accordance with 40.111 and 40.062.
- ☐ Implement key management procedures.

Validation

- ☐ Confirm policy for encryption (e.g. storage and/or VM based on risk-based assessment).

Applicable Service Models

- IaaS, PaaS, SaaS

How-to enable protection of data-at-rest

1. Oracle's Cloud security posture is to automatically encrypt all data at rest, therefore no further action is required to enable protection of data-at-rest. Additional information regarding this security control can be found here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Concepts/security_guide.htm

2. Database Services are also encrypted by default using transparent data encryption (TDE), therefore no further action is required. The master key is stored Oracle Wallet. You can choose to set a Password on the Oracle Wallet. Consult the following document for additional information:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Security/Reference/dbaas_security.htm

Guardrail 7 - Protection of data-in-transit

Objective

Protect data transiting networks through the use of appropriate encryption and network safeguards.

Key Considerations

- ☐ Implement an encryption mechanism to protect the confidentiality and integrity of data when data are in transit to and from your solution.
- ☐ Use CSE-approved cryptographic algorithms and protocols.
- ☐ Encryption of data in transit by default (e.g. TLS v1.2, etc.) for all publicly accessible sites and external communications as per the direction on Implementing HTTPS for Secure Web Connections (ITPIN 2018-01).
- ☐ Encryption for all access to cloud services (e.g. Cloud storage, Key Management systems, etc.).
- ☐ Consider encryption for internal zone communication in the cloud based on risk profile and as per the direction in CCCS network security zoning guidance in ITSG-22 and ITSG-38.
- ☐ Implement key management procedures.

Validation

- ☐ Confirm policy for secure network transmission.

Applicable Service Models

- IaaS, PaaS, SaaS

How-to protect data-in-transit

1. VPN connect provides site-to-site IPSec VPN between your on-premises network and Oracle Cloud. The IPSec protcol encypts all network packets that are in transit between on-premises and the Oracle Cloud. Further information regarding VPN Connect can be found here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Tasks/overviewIPsec.htm

2. To configure VPN Connect, follow the instructions located here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Tasks/quickstartIPsec.htm

3. If you are using FastConnect to connect your on-premises to Oracle OCI, please follow the instructions in the document to enable encryption using FastConnect:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Resources/Assets/whitepapers/encrypted-fastconnect-public-peering.pdf

Data Protection Artifacts

- Compliance Report

Network Security

Guardrail 8 – Segment and Separate

Objective

Segment and separate information based on sensitivity of information.

Key Considerations

- ☐ Develop a target network security design that considers segmentation via network security zones, in alignment with ITSG-22 and ITSG-38.
- ☐ Implement increased levels of protection for management interfaces.

Validation

- ☐ Confirm that department has a target network architecture diagram with appropriate segmentation between network zones.

Applicable Service Models

- ☐ IaaS, PaaS

How-to isolate cloud resources

1. To organize and isolate your cloud resources, use Compartments, see the document 'Managing Compartments' located here:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Identity/Tasks/managingcompartments.htm

Guardrail 9 - Perimeter Security Services

Objective

Establish external and internal network perimeters and monitor network traffic.

Key Considerations

- ☐ Ensure that egress/ingress points to and from GC cloud-based environments are managed and monitored. Use centrally provisioned network security services where available.
- ☐ Implement network boundary protection mechanisms for all external facing interfaces that enforce a deny-all or allow-by-exception policy.
- ☐ Perimeter security services such as boundary protection, intrusion prevention services, proxy services, TLS traffic inspection, etc. must be enabled based on risk profile, in alignment with GC Secure Connectivity Requirements and ITSG-22 and ITSG-38..
- ☐ Access to Cloud storage shall be limited to authorized source IP addresses only (generally GC only).

Validation

- ☐ Confirm policy for network boundary protection.
- ☐ Confirm policy for limiting number of public IPs.
- ☐ Confirm policy for limiting to authorized source IP addresses (e.g. GC IP addresses).

Applicable Service Models

- ☐ IaaS, PaaS, SaaS

How-to setup external and internal network perimeters

1. There are several ways you can control security for your cloud network, for general information regarding network security and understanding the concepts, consult this Oracle document: https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Concepts/waystosecure.htm

2. The networking services offers two virtual firewalls features to control traffic at the packet level, know as Security Lists and Network security Groups both of which use security lists. To create and manage security lists, use the following Oracle document:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Concepts/securitylists.htm

3. To send traffic outside of your Oracle Cloud network, route tables are used, the following Oracle document provides additional information:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Network/Tasks/managingroutetables.htm

How-to monitor network traffic

1. You can use VCN Flow Logs to monitor and view network traffic withing your Oracle Virtual Cloud Network (VNC). To use Flow Logs, follow the instructions located in this document:

   https://blogs.oracle.com/cloud-infrastructure/announcing-vcn-flow-logs-for-oracle-cloud-infrastructure

2. Additionally, you can use OCI network inspector. To use OCI network inspector, follow the instructions located in this document:

   https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/References/oci-network-inspector.htm

Network Security Artifacts

- Target Network Architecture Diagram

Operations

Guardrail 10 – Cyber Defense Services

Objective

Establish MOU for defensive services and threat monitoring protection services.

Key Considerations

- ☐ Sign an MOU with CCCS.
- ☐ Follow onboarding guidance.

Validation

- ☐ Confirmation from CCCS that the MOU has been signed by the Department.

Applicable Service Models

- ☐ IaaS, PaaS, SaaS

How-to implement cyber defense services

1. Contact the CCCS to obtain guidance on implementation of cyber defense services for the Oracle Cloud Infrastructure.

Guardrail 11 – Logging and monitoring

Objective

Enable logging for the cloud environment and for cloud-based workloads.

Key Considerations

- ☐ Implement adequate level of logging and reporting, including a security audit log function in all information systems.
- ☐ Identify the events within the solution that must be audited in accordance with GC Event Logging.

Note: You may need to configure your solution to send the audit log records to a centralized logging facility, if one is available, where existing auditing mechanisms will be applied.

- ☐ Configure alerts and notifications to be sent to the appropriate contact/team in the organization.
- ☐ Configure or use an authoritative time source for the time-stamp of the audit records generated by your solution components.
- ☐ Continuously monitor system events and performance.

Validation

- ☐ Confirm policy for event logging is implemented.
- ☐ Confirm event logs are being generated.
- ☐ Confirm that security contact information has been configured to receive alerts and notifications.

Applicable Service Models

2. IaaS, PaaS, SaaS

How-to setup logging

1. The Oracle Infrastructure Audit service automatically records calls to all supported Oracle Cloud Infrastructure public application programming interface (API) endpoints as log events.

   No additional configuration is required.

   For an overview of the Audit capabilities, consult this Oracle document :

   https://docs.cloud.oracle.com/en-us/iaas/Content/Audit/Concepts/auditoverview.htm

2. To view to Audit Logs, consult the following document :

   https://docs.cloud.oracle.com/en-us/iaas/Content/Audit/Tasks/viewinglogevents.htm

Guardrail 12 – Configuration of Cloud Marketplaces

Objective

Restrict Third-Party CSP Marketplace software to GC-approved products.

Key Considerations

- ☐ Only GC approved cloud marketplace products are to be consumed. Turning on the commercial marketplace is prohibited.
- ☐ Submit requests to add third-party products to marketplace to SSC Cloud Broker.

Validation

- ☐ Confirm that third-party marketplace restrictions have been implemented.

Applicable Service Models

- IaaS, PaaS, SaaS

How-to Configure Cloud Marketplace

SSC Cloud Brokering team will be whitelisting which Oracle Cloud Marketplace images are approved for consumption.

Whitelisted images can be provisioned within your cloud tenancy.

No additional action or configuration is required.

Operations Artifacts

- MOU Signed with CCCS
- Compliance Report

References

Cloud Guardrails

ID.	Guardrail
01	Protect root / global admins account
02	Management of administrative privileges
03	Cloud console access
04	Enterprise monitoring accounts
05	Data location
06	Protection of data-at-rest
07	Protection of data-in-transit
08	Segment and separate*
09	Network security services
10	Cyber defense services*
11	Logging and monitoring
12	Configuration of cloud marketplaces

* Not part of this document

- Cloud Guardrails on Git

Compliance Audit Process (SSC)

When a Departments procures from the Protected B contract, they have up to 30 days to implement the Cloud guardrails, become compliant and show how they are compliant.

TBS has published a standard operating procedure (SOP) for validating Cloud guardrails. The following section provides an overview of the SSC auditing process.

1. Department procures Protected B
2. SSC's Cloud Provider Operations team sends a Welcome Email to the Department
3. Within the 30 days from procurement:
    a. Departments create a document with sections for each guardrail
    b. Departments email SSC (cloud inbox) with complete package
    c. Receive a pass or fail on compliance
4. SSC sends a monthly compliance report to TBS