ORACLE

OCI Compute Self Health Checks

Ensure you are using the best practices and all related OCI compute services so that you can improve your performances, security and costs.

December 2022, Version 1.1

Florian Bonneville
EMEA Master Principal Cloud Specialist Engineer

Table of contents

Best practices framework **3**
Security checklist **3**
Securing compute **3**
Hardening an Oracle Linux Server **3**
CIS Benchmarks **3**
Infrastructure Services **4**
Compute Shapes 4
Flexible Shapes 4
ARM Shapes 4
Availability & Fault Domains 4
Burstable Instances 4
Shielded Instances 4
Storage Services **5**
Backup Instances 5
Volume Groups 5
Volume Groups Replication 5
Dynamic Performance Scaling 5
Monitoring Services **6**
Compute Metrics 6
Compute Events 6
Compute Notifications 6
Compute Monitoring 6
Notification Service 6
Endpoint Health Checks 6
Management Services **7**
Compute Agent 7
OS Management 7
Cloud Advisor 7
Cloud Guard 7
Vulnerability Scanning 8
OCI Tagging 8
Network Services **9**
Service Gateway 9
OCI Bastion 9
Network Path Analyzer 9

Best practices framework

Ensure you implemented best practices in Security & Compliance, Reliability & Resilience, Performance & Cost Optimization and Operational efficiency.

- https://tiny.one/oci-best-practices

Security checklist

Use these controls to manage access to your services and segregate operational responsibilities to reduce the risk associated with potentially malicious and accidental user actions.

The remainder of this document presents all the security controls available in Oracle Cloud Infrastructure, as checklists that you can use when designing, deploying, and managing your workloads in Oracle Cloud.

- https://tiny.one/Instance-Security

Securing compute

To use Compute securely, learn about your security and compliance responsibilities.

Oracle provides security of cloud infrastructure and operations, such as cloud operator access controls and infrastructure security patching. You are responsible for securely configuring your cloud resources. Security in the cloud is a shared responsibility between you and Oracle.

Use these checklists to identify the tasks you perform to secure Compute in your Oracle Cloud Infrastructure tenancy

- https://tiny.one/securing-compute

Hardening an Oracle Linux Server

Oracle Linux provides a complete security stack, from network firewall control to access control security policies. While Oracle Linux is designed "secure by default," this article explores a variety of those defaults and administrative approaches that help to minimize vulnerabilities.

- https://tiny.one/harden-oracle-linux

CIS Benchmarks

An objective, consensus-driven security guideline for the Oracle Cloud Infrastructure Cloud Providers and the Oracle Linux Operating Systems.

- https://tiny.one/cis-oci
- https://tiny.one/cis-oracle-linux
- https://tiny.one/cis-oci-benchmark

Infrastructure Services

CONTROL	DESCRIPTION	DOCUMENTATION	TECHNICAL EXAMPLE
Ensure you are using last instance generation	**Compute Shapes** • Gain more performances at the same price.	• https://tiny.one/computeshapes	Get Started with Oracle Cloud Infrastructure Core Services: • https://tiny.one/core-labs
Ensure you are using Flexible shapes	**Flexible Shapes** • Take advantage of CPU/MEMORY right sizing.	• https://tiny.one/flexible-shapes	Get Started with Oracle Cloud Infrastructure Core Services: • https://tiny.one/core-labs
Think about using Arm-Based Compute	**ARM Shapes** • Ampere A1 Compute instances are suitable for a wide range of applications and use cases with the best price-performance in the market.	• https://tiny.one/ampere	
Ensure your instances are distributed across different Availability Domains & Fault Domains	**Availability & Fault Domains** • Protect your instances against unexpected facility, network, hardware failures or hardware maintenance.	• https://tiny.one/regions • https://tiny.one/fault-domains	**Build a Disaster Recovery (DR) topology**: • https://tiny.one/dr-labs **Deploy a highly available web application:** • https://tiny.one/ha-labs
Think about using burstable instances	**Burstable Instances** • Gain the ability to burst to a higher CPU level for free.	• https://tiny.one/burstable	
Think about using shielded instances	**Shielded Instances** • Harden the firmware security on instances to defend against malicious boot level software	• https://tiny.one/shielded	

Storage Services

CONTROL	DESCRIPTION	DOCUMENTATION	TECHNICAL EXAMPLE
Ensure your instances are backed up properly	**Backup Instances** • Automate point-in-time snapshots of your data on a boot/block volume.	• https://tiny.one/bv-backup • https://tiny.one/dv-backup	Block Volumes Backup and Restoration: • https://tiny.one/watch-backup
Think about using Volume Groups	**Volume Groups** • Simplify the process to create time-consistent backups managing multiple storage volumes across multiple instances.	• https://tiny.one/volume-groups	
Think about using Volume Groups Cross Region Replication	**Volume Groups Replication** • Replicate your volumes and/or backups to another OCI region.	• https://tiny.one/vg-replication	
Think about using Dynamic Performance Scaling	**Dynamic Performance Scaling** • configure your volumes so that the service adjusts the performance level automatically to optimize performance.	• https://tiny.one/dynamic-scaling	

Monitoring Services

CONTROL	DESCRIPTION	DOCUMENTATION	TECHNICAL EXAMPLE
Enable Compute Metrics and Monitoring	**Compute Metrics** • Monitor the health, capacity, and performance of resources by using metrics, alarms, and notifications.	• https://tiny.one/compute-metrics	
Use automation to track infrastructure maintenance events	**Compute Events** • Monitor the health, capacity, and performance of resources by using metrics, alarms, and notifications.	• https://tiny.one/oci-events • https://tiny.one/compute-events	**Event Type | Compute Instance** - Failed Instance - Live Migration Begin - Live Migration End - Schedule Maintenance - Update - Terminate Begin - Terminate End **Event Type | Block Volume** - Create Boot Volume Backup Begin - Create Boot Volume Backup End - Create Volume Backup Begin - Create Volume Group Backup Begin - Create Volume Group Backup End
Enable Contextual Notifications for your Instances	**Compute Notifications** • Get messages when something happens with a compute instance.	• https://tiny.one/compute-notifications	
Enable OCI Monitoring for Compute Instances	**Compute Monitoring** • Get data about the activity level and throughput of your instances.	• https://tiny.one/compute-monitoring	
Enable OCI Notifications service	**Notification Service** • Use Notifications to get messages whenever alarms, service connectors, and event rules are triggered.	• https://tiny.one/notification-service	
Enable OCI Health Checks for your Instances	**Endpoint Health Checks** • Provide external monitoring to help you determine the availability and performance of any public-facing instances.	• https://tiny.one/HealthChecks	

Management Services

CONTROL	DESCRIPTION	DOCUMENTATION	TECHNICAL EXAMPLE
Review used/unused Oracle Cloud Agent Plugins	**Compute Agent** • Plugins collect performance metrics, install OS updates, and perform other instance management tasks.	• https://tiny.one/compute-agent	
Think about using OCI OS Management	**OS Management** • Manage & monitor updates & patches for Linux & Windows and discover & monitor resources on your instances.	• https://tiny.one/os-management	OS Management on OCI : https://tiny.one/watch-os-management
Ensure you are using OCI Cloud Advisor	**Cloud Advisor** • Analyze your OCI cloud resources and get recommendations to maximize cost savings and optimize your tenancy's performance, security and availability.	• https://tiny.one/CloudAdvisor	Enable Cloud Advisor • https://tiny.one/watch-CloudAdvisor • https://tiny.one/watch-CloudAdvisor-b
Ensure you are using OCI Cloud Guard	**Cloud Guard** • Maintain a strong security posture analyzing your resources for security weakness related to configuration, and your OCI operators for risky activities.	• https://tiny.one/Cloud-Guard	Enable Cloud Guard • https://tiny.one/watch-CloudGuard • https://tiny.one/cloud-guard-labs

CONTROL	DESCRIPTION	DOCUMENTATION	TECHNICAL EXAMPLE
Ensure you are using OCI Vulnerability Scanning	**Vulnerability Scanning** • Improve your security posture by routinely checking hosts and container images for potential vulnerabilities.	• https://tiny.one/scanning	Enable Vulnerability Scanning • https://tiny.one/vulnerability-labs • https://tiny.one/watch-vulnerability
Ensure you are using OCI Tagging	**OCI Tagging** • Add metadata to your resources, which enable you to define keys and values and associate them with resources. Use the tags to organize and list resources based on your business needs.	• https://tiny.one/oci-tagging	OCI Tagging • https://tiny.one/watch-tagging

Network Services

CONTROL	DESCRIPTION	DOCUMENTATION	TECHNICAL EXAMPLE
Ensure you are using OCI Service Gateway	**Service Gateway** • Enable access to OCI cloud resources to privately & directly access Oracle services without going through internet.	• https://tiny.one/ServiceGateway	
Think about using OCI Bastion service	**OCI Bastion** • Provide restricted and time-limited access to target resources that don't have public endpoints.	• https://tiny.one/bastion	Managed SSH Session • https://tiny.one/bastion-labs
Think about using OCI Network Path Analyzer	**Network Path Analyzer** • NPA Helps you identify virtual network configuration issues (up to layer 4) by analyzing the configured connectivity.	• https://tiny.one/path-analyzer	

Connect with us

Visit **oracle.com**. find your local office at: **oracle.com/contact**.

 blogs.oracle.com  facebook.com/oracle  twitter.com/oracle