ORACLE
Cloud Infrastructure

OCI Marketplace Stacks

Partner Standards and Controls

ORACLE WHITEPAPER | JULY 2019

F17685-02

Contents

Overview

Oracle Cloud Infrastructure allows Oracle partners to distribute their solutions to OCI customers via the OCI Marketplace. Oracle customers trust that these solutions are built and maintained in a way that ensures that their security and privacy is priority one. Customers also expect solutions to deliver as promised, include excellent documentation, and that the support experience is effective and low friction. This document describes the minimum bar required of Oracle partners for inclusion in the OCI Marketplace. Partners are encouraged to exceed these specifications.

This document is updated regularly. Check for the newest version at:
https://docs.cloud.oracle.com/iaas/Content/General/Reference/aqswhitepapers.htm

Solutions that include exceptions to these standards must be reviewed and approved by OCI.

Key Words

This document uses key words as defined by IETF RFC 2119.

- **MUST**
  - This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
- **MUST NOT**
  - This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
- **SHOULD**
  - This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- **SHOULD NOT**
  - This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- **MAY**
  - This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

Vulnerability Severity Levels

Where this document discusses security vulnerability severity levels it uses the Common Vulnerability Scoring System (CVSS) v3.0 ratings system.

A Security Focused Culture

Partners MUST read and understand the entire OCI Security Overview.

> *We [Oracle] believe that a dynamic security-first culture is vital to building a successful security-minded organization. We have cultivated a holistic approach to security culture in which all our team members internalize the role that security plays in our business and are actively engaged in managing and improving our products' security posture. We have also implemented mechanisms that assist us in creating and maintaining a security-aware culture.*

Partners MUST maintain a Security First Culture that understands and values the trust of our mutual customers.

Controls

Partners MUST maintain awareness of security alerts and advisories that impact their solution. Some common sources:

a. SecurityFocus maintains recent advisories for many open source and commercial products.

b. The National Vulnerability Database.

c. US-CERT and the Industrial Control Systems CERT (ICS-CERT) publish regularly updated summaries of the most frequent, high-impact security incidents.

d. Full Disclosure at SecLists.org, is a high volume, public, vendor-neutral forum for detailed discussion of vulnerabilities and exploitation techniques.

e. The Computer Emergency Readiness Team Coordination Center (CERT/CC) has up-to-date vulnerability information for the most popular products.

2. Partners SHOULD watch for OCI platform updates that may impact images they have published.

    a. What's New - https://docs.cloud.oracle.com/iaas/Content/home.htm

    b. Release Notes – https://docs.cloud.oracle.com/iaas/releasenotes/

    c. Known Issues - https://docs.cloud.oracle.com/iaas/Content/knownissues.htm

3. Partners MUST notify OCI within 3 business days of any newly discovered vulnerabilities that impact their solution with a CVSS rating of 9.0 or higher.

4. Partners MUST notify OCI within 5 business days of any newly discovered vulnerabilities that impact their solution with a CVSS rating between 7.0 and 8.9.

5. Partners MUST notify OCI within 20 business days of any newly discovered vulnerabilities that impact their solution with a CVSS rating between 4.0 and 6.9.

6. Partners MUST publish updated solutions that mitigate newly discovered vulnerabilities in a timely fashion.

7. Partners MUST allow customers to keep their solution updated to protect against newly discovered vulnerabilities. Some common patterns are:

    a. Automatically applying security updates.

    b. Allowing a customer to run a command to apply security updates.

    c. Providing a process that allows a customer to replace any current deployments with an updated version.

i. This process should be sufficiently low friction so that a customer is not discouraged from performing the work required.

8. Partners SHOULD publish updated solutions with general security updates on a quarterly basis.
9. If the partner may require the execution of a non-disclosure agreement before disclosing a vulnerability to Oracle the partner MUST have executed an Oracle Confidentiality Agreement (CDA) prior to publication of their first image. Your Oracle Partner team will assist with this process.

Marketplace Artifacts

Oracle Cloud Infrastructure Marketplace is an online store that offers applications specifically for customers of Oracle Cloud Infrastructure. In the Oracle Cloud Infrastructure Marketplace catalog, customers can find and launch images and stacks from Oracle or trusted partners that will provision the required OCI resources, including the Compute instance and application.

Images are templates of virtual hard drives that determine the operating system and software to run on an instance. With an image from a partner, you have a more streamlined way of getting started with their software.

Stacks are Terraform configuration files (templates) and a input variable schema file packaged in a zip file that are responsible to build the described infrastructure which includes low-level components such as compute instances, storage and networking, as well as high-level components such as DNS entries, application configuration scripts, license keys, etc. Stacks launched by customers runs on top of Oracle Resource Manager.

Marketplace publishers, when creating their listings, MUST include Artifacts like Terraform Templates or OCI Compute Image. These Artifacts are attached to an Install Package associated with the Marketplace listing.

Marketplace Listings

Each published solution includes a set of customer facing documentation. This documentation:

- MUST include prominent, detailed instructions for connecting to an instance.
- MUST include usage documentation or a link to the documentation.
- MUST include support details or a link to those details.
- MUST list compatible shapes.
- MUST document all network ports open by default on the instance.

Marketplace Stack Standards

Oracle recommends publishers to adopt general Terraform best practices for building their Terraform template code. However, there are specific Marketplace Stack standards to follow in order to publish a Stack:

- MUST use Marketplace Package schema
  - MUST package the configuration file(s) and input variables schema (.yaml) in a zip file.
  - MUST include at least 1 configuration file (.tf) in the root folder.
  - MUST include Input Variables schema file (.yaml) in the root folder.
  - Zip file MUST NOT have a Terraform State file as state files are managed by Oracle Resource Manage. Once customers launch a Stack, ORM creates and manage the resources, and state file become available for download only.
  - Zip file MUST NOT include Terraform runtime configuration folder (.terraform)

- SHOULD enable customers to either create all the infrastructure resources or point to existing ones (network, storage, etc). Publishers SHOULD leverage Terraform Modules to create re-usable building blocks.
- SHOULD follow Naming Conventions & Formatting
  - Casing - Use *lower_snake_case* for all naming. This applies to variable names, resource names, module names, file names, display names, etc.
  - Specifying Resource Type - Do not include the resource or data source type in the name. In Terraform, resources and data sources are always referenced by "<type>.<name>". As such, there is no need to include the type in the nameitself.
  - ID vs OCID - In OCI, "id" generally refers to a field that takes an OCID. As such, variables should use "id" when referring to OCID values (instead of using "ocid").
  - Variable Names - Variable names for OCI resources should typically use the same name as used for the Terraformresource.
  - Display Names - Display names for OCI resources should typically use the same name as used for the Terraformresource.
  - Naming module variables and outputs - When using a module, the naming of the input (variables) and the outputs are exposed to the caller.
  - Apply "terraform fmt" to all Terraform before checking in.

- MUST only point to an application published as a Marketplace Image. Marketplace Stacks must point to already published Marketplace Images, with a hard-coded reference to the image. Every time a new Image version is published, Stacks SHOULD be updated

  Sample code:

```
# Referencing Oracle Secure Global Desktop image
locals {
  mp_listing_id               =
"ocid1.appcataloglisting.oc1..aaaaaaaal2iorlvahwdqqy37fmsu6vmfyneswgatqlq6sz6agk6nd7pm
frza"
  mp_listing_resource_id      =
"ocid1.image.oc1..aaaaaaaaizdss5humeepnr5syhsz3bj62auihs4kr5h73adks2t7o7os7ozq"
  mp_listing_resource_version = "5.4-020820191726"
}


resource "oci_core_instance" "TFInstance1" {
   ...

  source_details {
    source_type = "image"
    source_id   = "${local.mp_listing_resource_id}"
  }
```

- MUST NOT download binaries from external repositories. All binaries and dependencies MUST be baked into the published Marketplace Image.
- MUST only use Remote Exec provisioner within OCI domain. Marketplace Stacks should not use Terraform remote exec provisioner to download files on a remote server.
- MUST NOT download code using cloud-init.
  - Cloud-init is a commonly-used startup configuration utility for cloud compute instances. It accepts configuration via user-data mechanisms specified as part of the metadata definition on oci_core_instance resource.
  - There are multiple user-data formats supported by cloud-init: https://cloudinit.readthedocs.io/en/latest/topics/format.html
  - Regardless of the user-data format, cloud-init must not be used for downloading any 3rd party code/binary. All binaries required during the instance launch process (bootstrap), if not available within the image, should be downloaded by a process (script) baked as part of the image distribution, not injected via cloud-init (e.g. leveraging wget).

- However, partners may have cloud-init template setup for customers to use in some particular scenarios, e.g. import a license key file, import a configuration file. In that case, they should provide a variable in their Terraform template code to enable customers to enter some data into the cloud-init building block, e.g., leveraging Terraform template file data source.

- MUST use OCI ORM Approved Terraform providers. Other cloud providers/3rd party application providers are not supported.
- MUST use local-path based modules only. In case Terraform Modules are used on Stacks, partners must use only local-path modules as Stacks MUST not point to external resources.
- SHOULD NOT specify OCI Provider in the configuration file. If specified, MUST use Instance Principal Authorization. User based authentication is not supported and only region property should be declared in the provider resource, and optionally, provider version.

  Sample code:

```
provider "oci" {
  version          = ">= 3.0.0"

  auth = "InstancePrincipal"
  region = "${var.region}"
}
```

Marketplace Stacks Input Variables Schema

When launching Marketplace Stacks, customers will be prompted to fill in a form containing the list of variables that are part of the Stack definition. In order to provide a better user experience to customers, OCI designed a schema file that enables publishers to specify how these variables can be displayed and used by customers during the Launch Stack process.

Background

Terraform allows developers to define input variables in their code to create a truly configurable, parameterizable template, which enables customers to modify specific settings according to their needs. In Terraform configuration language (HCL), variables support a default value, a description, and three types of values: string, list, and maps. This makes it difficult for users of Stacks to understand what values are permitted for each variable.

To enable customers to easily navigate through the list of input variables, OCI Marketplace Stack defined a schema document, included as part of the Stack package, described as a JSON or YAML format. The schema contains a list of input variables, static or dynamic, and their validations

and constraints. It also includes a description of the ordering and grouping of input variables that will be displayed in the Launch Stack page.

Appendix A

Sample Schema File

To download a sample schema file containing the usage of static and dynamic variables, click here.

Meta-Schema File

The meta-schema should be used for syntax-level validation of the schema file. To download a meta-schema file, click here.

Suggested iptables Rules for Instance Metadata

```
<?xml version="1.0" encoding="utf-8"?>
<direct>
  <passthrough ipv="ipv4">-A OUTPUT -m state --state RELATED,ESTABLISHED -m -j ACCEPT</passthrough>
  <passthrough ipv="ipv4">-A OUTPUT -d 169.254.0.2/32 -p tcp -m owner --uid-owner root -m tcp --dport 3260 -m -j ACCEPT</passthrough>
  <passthrough ipv="ipv4">-A OUTPUT -d 169.254.2.0/24 -p tcp -m owner --uid-owner root -m tcp --dport 3260 -m -j ACCEPT</passthrough>
  <passthrough ipv="ipv4">-A OUTPUT -d 169.254.0.2/32 -p tcp -m tcp --dport 80 -m -j ACCEPT</passthrough>
  <passthrough ipv="ipv4">-A OUTPUT -d 169.254.169.254/32 -p udp -m udp --dport 53 -m -j ACCEPT</passthrough>
  <passthrough ipv="ipv4">-A OUTPUT -d 169.254.169.254/32 -p tcp -m tcp --dport 53 -m -j ACCEPT</passthrough>
  <passthrough ipv="ipv4">-A OUTPUT -d 169.254.0.3/32 -p tcp -m owner --uid-owner root -m tcp --dport 80 -m -j ACCEPT</passthrough>
  <passthrough ipv="ipv4">-A OUTPUT -d 169.254.0.4/32 -p tcp -m tcp --dport 80 -m -j ACCEPT</passthrough>
  <passthrough ipv="ipv4">-A OUTPUT -d 169.254.169.254/32 -p tcp -m tcp --dport 80 -m -j ACCEPT</passthrough>
  <passthrough ipv="ipv4">-A OUTPUT -d 169.254.169.254/32 -p udp -m udp --dport 67 -m -j ACCEPT</passthrough>
  <passthrough ipv="ipv4">-A OUTPUT -d 169.254.169.254/32 -p udp -m udp --dport 69 -m -j ACCEPT</passthrough>
  <passthrough ipv="ipv4">-A OUTPUT -d 169.254.0.0/16 -p tcp -m tcp -m -j REJECT --reject-with tcp-reset</passthrough>
  <passthrough ipv="ipv4">-A OUTPUT -d 169.254.0.0/16 -p udp -m udp -m -j REJECT --reject-with icmp-port-unreachable</passthrough>
  <passthrough ipv="ipv4">-A OUTPUT -d <NETRANGE> -p tcp -m tcp --dport 80 -m -j ACCEPT</passthrough>
</direct
```

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

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

Integrated Cloud Applications & Platform Services

July 2019