ORACLE
Cloud Infrastructure

OCI Marketplace

Partner Standards and Controls

ORACLE WHITE PAPER | APRIL 2019

F18125-01

FIND THE MOST RECENT VERSIONS OF OCI WHITEPAPERS HERE

HTTPS://DOCS.US-PHOENIX-1.ORACLECLOUD.COM/CONTENT/GENERAL/REFERENCE/AQSWHITEPAPERS.HTM

Table of 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.

Listings

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

- MUST include prominent, detailed instructions for connecting to an instance.
    - This MUST include a list of TCP ports that customers need to open in their OCI Security List rules.
- 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.

Custom Images

Custom images are the most common format partners use to distribute their solutions via the Marketplace. OCI offers both Bare Metal and Virtual Machine shapes with and without locally attached NVMe storage. For VM shapes we offer three different modes, NATIVE, PARAVIRTUALIZED, and EMULATED.

- Partners MAY distribute images that run on Bare Metal shapes.
- Instances running in native mode are Hardware Virtual Machines (HVM). Partners MAY distribute images that run in native mode.
- Instances running in paravirtualized mode leverage virtio for near-bare metal performance. Partners SHOULD distribute images that run in paravirtualized mode.
- Instances running in emulated mode are fully emulated. Emulated mode VMs are more compatible with older operating systems while being slower than native VMs. Partners SHOULD NOT distribute images that run in emulated mode.

Specific Image Security Standards

Many of these security standards do not apply to appliance images where the customer cannot, in any way, access an operating system shell; i.e Cisco IOS, Junos. Where this is the case the partner MUST identify it as such during the onboarding process.

- Images MUST have the root user disabled.
- The root user's login shell MUST be set to `/sbin/nologin`.
- Any `authorized_keys` files in the image MUST NOT contain any keys.
- The SSH service MUST be configured to prevent root user logins –

```
PermitRootLogin no
```

- The SSH service MUST be configured to prevent password based logins -

```
ChallengeResponseAuthentication no
PasswordAuthentication no
UsePAM no
```

- The `root/.ssh/authorized_keys` file MUST contain the following stanzas –

```
no-port-forwarding
no-agent-forwarding
no-X11-forwarding
```

- Other than the `/root/.ssh/authorized_keys` file the root user's home directory MUST be empty.
- There MUST NOT be any SSH fingerprints in the image.

```
rm ./etc/ssh/ssh_host*
```

- SELinux SHOULD be enabled and in enforcing/targeted mode.
- The OS firewall MUST be enabled and configured to block any ports not specifically required.
- Images SHOULD NOT have any operating system level users configured with a password.
- SELinux SHOULD be enabled and in enforcing/targeted mode.
    - Verify that the SELinux context for `/etc/crontab` is set to `system_cron_spool_t`
- A Mandatory Access Control scheme SHOULD be enabled.
- There MUST NOT be evidence of the image build process.

    - Partners MUST ensure that all logs in an image are empty. This includes `.bash_history`, `/var/logs/*` and similar files.
        - For images based on Oracle Linux the `oci-instance-cleanup` tool available in the `oci-utils` package will do this.
    - Where applicable remove non-compiled code.
    - Remove comments from non-compiled code where they are not relevant to the customer's use case.
- Linux images that allow customers to SSH into them MUST ingest a public SSH key provided by a customer as part of the instance launch process and allow the customer to login as a non-root user with that key.
    - This user SHOULD use be ‘opc’.
    - The OCI instance meta-data service is compatible with cloud-init. OCI recommends using the cloud-init packages to manage customer supplied keys.
- There SHOULD NOT be any hard-coded application level passwords.
    - Generate all application passwords the first time the instance launches.

General Image Standards

- The image MUST be tested and working on all shapes listed in the documentation.
- DHCP MUST be enabled on the primary interface.
- There MUST NOT be a hardcoded MAC address.
- Any network managers MUST be stopped.
    - i.e CentOS Network-Manager

Shape specific options -

- VM.DenseIO.* -
    - Images MUST have the kernel NVMe driver enabled.
    - Images SHOULD have `nvme_core.shutdown_timeout=5` set in `/proc/cmdline`.
- VM.*1.* –
    - Images MUST have the PF and VF drivers for the Intel 82599 network card (ixgbe.ko/ixgbevf.ko) installed and enabled at startup.
- VM.*2.* –

- Images MUST have the driver for the Broadcom NetXtreme-E network card (bnxt_en.ko) installed and enabled at startup.

Mode specific options -

NATIVE

Partners building for native mode MUST base their image on an OCI distributed image. Partners SHOULD NOT change any of the following parameters –

- Boot related options.
- iSCSI replacement timeout.
- Network device naming options.

PARAVIRTUALIZED

Partners building for native mode SHOULD base their image on an OCI distributed image. Paravirtualized images.

Images MAY include all these drivers and MUST include drivers for the shapes the image is designed to support.

Appendix A

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

April 2019