



Using Openstack* UEFI Boot Support to Enhance Security in Multi-Tenant Cloud Applications

Abstract

GRUB¹ boot has been around for years, but it is being deprecated in favor of the Unified Extensible Firmware Interface (UEFI).² Windows* systems are well on their way to discontinuing support for GRUB in the future. OpenStack³, one of the leading open-source cloud operating systems, will start to support UEFI boot in its Mitaka release, scheduled for release April 2016. In so doing, it will support the launch of newer OS images that have eschewed GRUB boot support altogether, such as the Clear Linux* OS for Intel® architecture.

This white paper explains the motivation for supporting UEFI boot and details the changes that were necessary in OpenStack Nova, Libvirt, and Glance to provide this support. We conclude with the benefits that the Clear Linux OS has unlocked within the OpenStack platform.

Why UEFI boot support?

The Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and the platform firmware. It replaces the Basic Input / Output System (BIOS) firmware interface and provides the following advantages:

- Hard drive partitions can be larger than two terabytes
- Supports more than four hard drive partitions
- Faster operating system boot
- More efficient power and system management
- Supports remote diagnostics and repair
- More robust, with better fault management

Support for UEFI boot only is quickly becoming the norm. The Windows OS is well on the way to deprecating traditional GRUB boot support in favor of UEFI, and Clear Linux OS for Intel architecture only supports UEFI boot.

Bringing UEFI Boot Support to OpenStack

OpenStack, one of the leading open-source, hypervisor-agnostic, cloud operating systems, utilizes [libvirt](#) to launch virtual machines (VMs). Although libvirt has supported UEFI boot since version 1.2.8, the libvirt version bundled with the OpenStack Nova project did not carry UEFI boot support. To resolve this gap, Intel proposed a blueprint⁴ and delivered an implementation.⁵

OpenStack* Virtual Machine Launch Flow

Let's take a look at the steps involved in launching a virtual machine (VM) in OpenStack.

1. The Glance service is used to upload any VM image and its associated metadata. Metadata can span whether the VM is to be public or protected (meaning the VM cannot be modified), in addition to possibly containing launch time suggestions for placement constraints to get optimal performance.
2. A VM launch request begins with the OpenStack Nova service retrieving the image requested from Glance along with its metadata. The two are combined to generate an XML file that specifies the launch parameters.
3. The Nova libvirt driver then boots the VM using the generated XML file as input.

To support UEFI boot in OpenStack in the most straightforward manner, Intel first introduced a new property called "hw_firmware_type". When uploading an image using the Glance service, the property is specified as shown below.

```
property="hw_firmware_type=uefi"
```

When the Glance service perceives the property, it attaches property to the Glance image metadata. The Glance image create command with the UEFI property specified is shown below:

```
glance image-create --file cloud-2730.qcow --disk-format qcow2 \
  --container-format bare --property="hw_firmware_type=uefi" \
  --name clear-linux-image
```

In the Glance database, the metadata is visible as shown:

| Property | Value |
|------------------|--------------------------------------|
| checksum | None |
| container_format | bare |
| created_at | 2016-01-27T10:13:16Z |
| disk_format | qcow2 |
| hw_firmware_type | uefi |
| id | acf0e994-c110-4657-9c31-ad61b1437aa1 |
| min_disk | 0 |
| min_ram | 0 |
| name | clear-linux-image |
| owner | 6b2797e0bf794383b3055331a6fc8c74 |
| protected | False |
| size | None |
| status | queued |
| tags | [] |
| updated_at | 2016-01-27T10:13:17Z |
| virtual_size | None |
| visibility | private |

Next, Intel introduced a new global variable named DEFAULT_UEFI_LOADER_PATH for use by the Nova libvirt driver. This variable captures the absolute file path to the UEFI firmware that exists on the Nova compute node. The path will be added into the generated VM XML launch file.

```
DEFAULT_UEFI_LOADER_PATH={
  "x86_64": "/usr/share/OVMF/OVMF_CODE.fd"}

```

With these two new attributes in place, when a VM boot request is initiated, the image metadata is transferred from the Glance service to the Nova service. During the VM preparation stage, the libvirt driver in the Nova service checks to determine if the image metadata carries the special property hw_firmware_type, and upon finding it, constructs the launch XML file to include the path to the UEFI firmware. This provides the support necessary to boot using UEFI.

Unlocking the Benefits of Clear Linux OS for Intel® Architecture and Intel® Clear Containers through UEFI Boot Support in OpenStack

The Clear Linux Project for Intel Architecture is focused on delivering lightweight Linux OS distributions for cloud use cases. It showcases the best of Intel architecture technology, from low-level kernel features to more complex features in the OS. Further, the distribution includes multiple OpenStack software components and features such as Autoproxy, Function Multiversioning (FMV), Telemetry, AutoFDO, and others, making it a drop-in, ready-to-use distribution on an OpenStack compute node.

Clear Linux OS for Intel architecture⁶ also supports Intel Clear Containers.⁷ Traditional containers, popular for their small memory footprint and fast launch, do not provide the security of address space isolation that VMs provide. Intel® Clear Containers do provide this security. They are essentially double-bagged containers; that is, they are containers in a lightweight VM that take advantage of Intel® Virtualization Technology (Intel® VT). The memory footprint of Clear Linux OS for Intel architecture and Intel Clear Containers allows densely packed VMs on a compute node. The distribution's low launch latency stems from its UEFI firmware boot. All these benefits are unlocked through building UEFI launch support into OpenStack. The security of Intel Clear Containers addresses the number one concern for broader container adoption in multi-tenant cloud scenarios.

Summary

Intel developed UEFI boot support in OpenStack to provide boot support for non-legacy boot images. In doing so, Intel also facilitated the use of Clear Linux OS for Intel architecture and Intel Clear Containers in OpenStack.

These technologies bring features designed for the cloud to OpenStack, including small footprint, fast launch, and security features that enable multi-tenant cloud applications with greater security in OpenStack.

Authors:

Xiaohui Xin
Malini Bhandaru

Advancing the World's Leading Cloud OS

Together with the OpenStack* community, Intel is actively working to enhance enterprise-class features within OpenStack and make it easier to deploy across compute, networking, and storage. In addition, Intel collaborates with leading cloud innovators to test, tune, and optimize OpenStack-based solutions. As a result, businesses can easily harness this exceptional cloud OS and take best advantage of the benefits of OpenStack on Intel® architecture.

Learn more at intel.com/openstack

Additional Resources

OpenStack website. <https://wiki.openstack.org/>

Open Virtual Machine Firmware (OVMF) Status Report.

<http://www.linux-kvm.org/downloads/larsek/ovmf-whitepaper-c770f8c.txt>

Optimizing solutions with Clear Linux Project.

<https://01.org/blogs/2015/optimizing-solutions-intel-clear-linux>



¹ GNU GRUB: <https://www.gnu.org/software/grub/>

² Unified Extensible Firmware Interface Specification: http://www.uefi.org/sites/default/files/resources/UEFI%20_5.pdf

³ Unified Extensible Firmware Interface, Wikipedia definition: https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface

⁴ OpenStack UEFI support specification: <https://review.openstack.org/#/c/235983/>

⁵ OpenStack UEFI support implementation: <https://review.openstack.org/#/c/262930/>

⁶ Clear Linux Project Wraps Containers in Speedy VMs. <https://blogs.intel.com/evangelists/2015/05/19/clear-linux/>

⁷ Contain(er-ize) yourself, it's Intel Clear Linux, ComputerWeekly.com. 2015. <http://www.computerweekly.com/blogs/open-source-insider/2015/05/contain-yourself-its-the-intel-clear-linux-project.html>

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL' PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at www.intel.com.

Copyright © 2014 Intel Corporation. All rights reserved. Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

* Other names and brands may be claimed as the property of others.

Printed in USA

0316/NRK/PDF

Please Recycle

334088-001US