CITRIX

XenServer 7.5 Measured Boot Supplemental Pack Guide

May 2018

Measured Boot Supplemental Pack Guide for XenServer 7.5

Summary

The XenServer Measured Boot Supplemental Pack enables customers to measure key components of their XenServer hosts at boot time, and provides APIs that enable remote attestation solutions to securely collect these measurements. This supplemental pack works with Intel computer systems that support *Trusted Execution Technology* (TXT).

This supplemental pack is available to download from the XenServer 7.5 Enterprise Edition page.

Note: Measured Boot Supplemental Pack is available for XenServer Enterprise edition customers, or those who have access to XenServer through their XenApp/XenDesktop entitlement.

Background

After installation of this Supplemental Pack, when a XenServer host next boots, Intel's TXT takes measurements of low level system components (such as firmware, BIOS, Xen hypervisor, dom0 kernel and the dom0 initrd) and stores them in a secure location on the host known as the *Trusted Platform Module* (TPM). A new interface is provided for clients, such as a remote attestation solution, to securely collect these measurements.

Remote Attestation

Remote Attestation solutions work by connecting to a XenServer host that is in a 'known good' clean state. It can remotely and securely query the XenServer host's TPM for a list of low level key system measurements and stores them in a 'white-list' or 'known good' measurements list.

At this point the remote attestation software periodically collects key system measurements and compares them to its 'known good' list.

If the remote attestation software is unable to collect these measurements, or if the measurements change, or if the cryptographic keys are not valid, then the host is considered 'un-trusted'. In this event, the customer is notified and higher-level orchestration software, such as CloudStack, OpenStack, or workload balancing software can perform intelligent security operations on the affected hosts.

Preparing the XenServer Host

In order for this Supplemental Pack to function correctly, before attempting to gather data, customers should edit the following settings in their host's BIOS:

1. Set up the XenServer host to boot in legacy mode.
   Note: UEFI boot mode is not supported with measured boot.
2. Enable **Intel AES-NI**.
3. Switch on **TPM Security** or **on with pre-boot measurements**.
4. Clear the TPM.
   This erases any previous settings and passwords associated with the TPM to allow the XenServer Measured Boot Supplemental Pack to take control of the TPM.
   Note: A reboot is usually required after this step.
5. Enable **TPM**.
   Note A reboot is usually required after this step.
6. Enable **Intel TXT**.
   Note: A reboot is usually required after this step.

Note: BIOS settings vary according to hardware manufacturer. Customers should consult their hardware documentation to see how to fully enable the TPM and TXT for their specific environment.

Installing the Supplemental Pack

Customers should use the XenServer CLI to install this Supplemental Pack. As with any software update, Citrix advises customers to back up their data before applying this supplemental pack.

Please note that Supplemental Packs can be transmitted within a *zip* file. If the Supplemental Pack ISO is contained within a zip file, the zip file should be unzipped (to produce the disk ISO image), before carrying out the steps below.

Installing onto a Running XenServer System

1. Download the Supplemental Pack directly to the XenServer host to be updated (Citrix recommends storing it in the /tmp/ directory), alternatively you may wish to download the file to an Internet-connected computer, and burn the ISO image to a CD.
2. Use XenCenter to access the XenServer host's console, or use secure shell (SSH) to log on directly.
3. The simplest method is to install directly from the ISO file. To do this, enter the following:

   ```
   xe-install-supplemental-pack /tmp/XenServer-7.5-measured-boot.iso
   ```

   Alternatively, if you chose to burn the ISO to a CD, you must mount the disk. For example, for a CD-ROM, enter the following:

   ```
   mkdir -p /mnt/tmp
   mount /dev/<path to cd-rom> /mnt/tmp
   ```

```
cd /mnt/tmp/
./install.sh
cd /
umount /mnt/tmp
```

4. In order for the changes to take effect, reboot your host.

Re-installation

Customers who may be installing this Supplemental Pack on top of a previous version, should confirm overwriting the previous installation; enter **Y** when prompted during xe-install-supplemental-pack installation.

Updating default password

In previous versions of the supplemental pack, the default password was set to 'xenroot' with a trailing newline. This trailing newline has been removed for the default password in this version of the supplemental pack with the new default password being 'xenroot'.

A custom password can be set in `/opt/xensource/tpm/config` and must be a sha1 hash of a plain text password, which can be generated with "`echo -n <password> | sha1sum`". If the `-n` is omitted from this command line, a trailing newline is included in the password.

Setting Asset Tags

Asset tags can be set using the `/opt/xensource/tpm/xentpm` binary with `the --tpm_set_asset_tag` and `--tpm_clear_asset_tag` methods, or can also be set using the XenAPI "`tpm`" plugin with the `tpm_set_asset_tag` (taking a 'tag' argument) and `tpm_clear_asset_tag` functions:

```
/opt/xensource/tpm/xentpm --tpm_set_asset_tag <tag_sha1>
/opt/xensource/tpm/xentpm --tpm_clear_asset_tag
xe host-call-plugin uuid=<host_uuid> plugin=tpm fn=tpm_set_asset_tag
args:tag=<tag_sha1>
xe host-call-plugin uuid=<host_uuid> plugin=tpm fn=tpm_clear_asset_tag
```

Note: A reboot is usually required after this step.

More Information

To download the Measured Boot Supplemental Pack, see the XenServer 7.5 Enterprise Edition page.

If you experience any difficulties with installing this Supplemental Pack, contact Citrix Technical Support.

For XenServer 7.5 documentation, visit the Citrix Product Documentation website.

About Citrix

Citrix (NASDAQ:CTXS) aims to power a world where people, organizations and things are securely connected and accessible to make the extraordinary possible. Its technology makes the world's apps and data secure and easy to access, empowering people to work anywhere and at any time. Citrix provides a complete and integrated portfolio of Workspace-as-a-Service, application delivery, virtualization, mobility, network delivery and file sharing solutions that enables IT to ensure critical systems are securely available to users via the cloud or on-premise and across any device or platform. With annual revenue in 2015 of $3.28 billion, Citrix solutions are in use at more than 400,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.

851 West Cypress Creek Road
Fort Lauderdale, FL 33099
954-267-3000
www.citrix.com