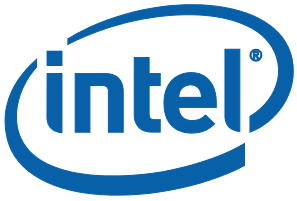

Intel® vPro™ Technology Use Case Reference Design

Desktop Virtualization: Updating the BIOS on a Type 1 Hypervisor

Revision 1.0

December, 2010

Document ID: 1098

Revision History

Revision	Revision History	Date
1.0	Initial release.	December, 2010

Contents

1 Preface

Many current OEM BIOS update utilities rely on a Microsoft* Windows* based operating system (OS) being available in order to perform updates to the BIOS software. Mostly this is a convenience for both end users (so that they do not have to figure out how to boot to a DOS environment and then manually run the flash utility) and for IT departments (so they can use in-band Windows based patching utilities).

This becomes a problem, however, when your Windows based operating system is running on top of a hypervisor and does not have direct access to the hardware. The flash application and the Windows operating system itself do not have the ability to reboot the hypervisor and have it boot the flash utility to update the BIOS. In order to accomplish a BIOS update on a system running a type 1 hypervisor, you need a way to force the hypervisor to reboot the system and boot into an environment that can run the BIOS update utility. If you are running local to the system, forcing a reboot and booting up to a USB flash drive is fairly simple. However, if you are remote to the system, such as an IT administrator pushing updates to a group of clients, you need a different solution. Here is where Intel® Active Management Technology (Intel® AMT) on Intel® vPro™ technology based platforms can help.

1.1 Document Scope

This document discusses how to remotely update the BIOS flash on Intel vPro technology based platforms running a type 1 hypervisor. The capabilities that enable this use case are available on systems that have Intel AMT 1.0 and newer. However, the management software used in the examples relies on features (WS-Man support) that are only found in Intel AMT 3.0 and newer.

1.2 Intended Audience

This document is intended for IT professionals who are deploying or are thinking about deploying a desktop virtualization solution.

1.3 Related Documentation

For more information about Intel® Virtualization Technology, visit the Intel Virtualization Technology web site:
http://www.intel.com/technology/virtualization/technology.htm?iid=tech_vt+tech

For more information about Intel Active Management Technology, visit the Intel Active Management Technology web site:

http://www.intel.com/technology/platform-technology/intel-amt/

2 Introduction

Patch management in a corporate infrastructure is a constant battle, whether you are validating that the patches being deployed do not break other software running in the client OS or dealing with installation failures during the deployment of patches out to the thousands of clients in the environment. Good client management practices coupled with desktop virtualization help solve many of the patch management headaches that IT departments face by reducing the number of unique OS images that need to be managed and providing centralized management of those images.

However, what happens when the underlying BIOS software needs to be updated? Virtualized environments do not generally have access directly to the BIOS, so Windows based installers will not work. If the clients you have in your environment are Intel vPro technology based platforms with Intel AMT, then this issue becomes trivial.

The next few sections will be discussing some of the different technologies that will be used in this use case. Section 3 of this document provides the details on how to implement this use case with examples from some of the many available client management software packages that make use of Intel AMT.

2.1 Client Virtualization

There are six general models of desktop delivery in use today: Terminal Service, Virtual Hosted Desktop, OS Streaming, Application Virtualization, Client Side Virtual Container, and Traditional Local Install. This document addresses the Client Side Virtual Container model, specifically type 1 hypervisors.

2.1.1 Hypervisors

The term *hypervisor* describes a software layer that runs between the hardware and virtualized operating systems, and manages the virtual OS access to the hardware. For additional information regarding virtualization and hypervisors go to http://www.intel.com/technology/itj/2006/v10i3/2-io/3-vmm-software-architecture.htm

A type 1 hypervisor is a small purpose built OS that runs directly on the hardware and manages the hardware access of general purpose operating systems that run on top of the hypervisor.

2.2 Intel® Active Management Technology (Intel® AMT)

Intel AMT is a feature on Intel vPro technology based platforms that enables remote platform level management of clients regardless of the current power state. For more about Intel AMT go to http://www.intel.com/technology/platform-technology/intel-amt/

2.2.1 Remote Boot Redirection

One of the features of Intel AMT is remote boot redirection. This allows an IT administrator to connect to an Intel AMT configured machine and remotely instruct the machine to either boot or reboot and specify either a local or remote boot device to use as the operating system.

For example, an IT administrator could connect to a client, tell it to boot and use an ISO image located on a network drive. This is a key feature needed for updating software located at or below the hypervisor level.

3 Detailed Procedures

In order to get to the point where a remote update of the BIOS on a system running a type 1 hypervisor is possible, the following is needed:

1. The system must be an Intel vPro technology based platform with Intel AMT configured.
2. A DOS bootable .iso image with the DOS version of the flash program and .BIO file version that will be used to update the system.
3. Optionally, a KVM utility that is able to make use of the Intel AMT KVM Remote Control capability such as Radmin* Viewer (for Intel AMT basic mode) or RealVNC's VNC* Viewer Plus (for Intel AMT standard and advanced mode).

See http://www.radmin.com/ for more information about Radmin Viewer.

See http://www.realvnc.com/products/viewerplus/index.html for more information about RealVNC's VNC Viewer Plus.

3.1 Intel AMT Configuration

Before you can use Intel AMT's remote boot and redirection capabilities, Intel AMT must first be configured. To support this reference design, Intel AMT can be set up in any of the configuration modes (basic, standard, advanced). The key point is that Intel AMT must be configured before the client system can be remotely accessed at the hardware level.

To learn more about how to configure and activate Intel AMT go to the Intel® vPro™ Expert Center web site under Activations: (http://communities.intel.com/community/openportit/vproexpert/activation).

The following is a link to a white paper that goes in depth regarding the configuration process:

http://communities.intel.com/docs/DOC-1323

3.2 ISO Preparation

Included with this reference design is a utility called DOS ISO Builder that will create a DOS bootable .iso image. In addition, files can be specified by the user to be included in the .iso image. For example, to create an .iso image to update the BIOS on a Dell 4310 laptop, do the following:

1. Download the DOS version of the BIOS update utility.
2. Double-click **dos_iso_builder.hta** in the program folder.
3. If ImDisk is not installed on the system, the first screen will prompt you to install ImDisk. Click the **Install ImDisk** button to install ImDisk.
4. If ImDisk is installed, the main screen is displayed.
5. Enter a name for the .ISO file in the space provided.

6. Click **Browse...** and select each file you want included in the .ISO file. Manual entry of file names is not supported.
   - If you want to delete a selected file, click the **Delete** button to remove the file from the list of selected files to be added to the .ISO file.
7. Click the **Build ISO** button to execute the script and build the .ISO file using the name supplied.
8. Click the **Open File Location** button to open a Windows Explorer window to the location of the .ISO file.
9. The .ISO file can be used to boot a system locally or remotely using the Intel AMT IDE Redirection (IDE-R) feature.

3.3 Remote Boot with Redirection

IDE-R allows a user to remotely reboot an Intel AMT enabled system and direct that system to boot to an alternative boot device that is not local to the system (remote CD-ROM, .iso files located on the network, etc). Usually with feature is combined with either the Serial Over LAN (SOL) or KVM Remote Control in order to allow the user to remotely use the system once it has completed boot.

3.3.1 Client Update

Once the system has been booted to the .iso file, updating the system BIOS can be accomplished the same as if the user was sitting in front of the system. Using either SOL or KVM Remote Control, the user can navigate the DOS file structure and run the BIOS update utilities that were included with the .iso file was created. Once the update is complete, the user can use Intel AMT power control to force the system to reboot and return to the original boot order.

Since the .iso that is created uses DOS, automating some of the processes can be as easy as creating **config.sys** and **autoexec.bat** files to automatically launch other applications or scripts.