Managing Dell Business Client Systems Out of Band using Intel AMT vPro

A Dell™ OpenManage™ Technical White Paper

Systems Management

By

Dell | Product Group

Sandeep Karandikar

Nicholas Grobelny

Sudhakaran Venkatesh

Dell | Tech Center

Warren Byle

Donna Imam

March 2012| Rev 1.0

Contents

Introduction

Remote management of client computers often requires the managed computer to be turned on with an operating system running. When a computer is turned on with a running operating system, the computer is considered in-band.

Out-of-band (OOB) is when a client computer is in one of the following out-of-band states:

- The computer is plugged in but is not actively running (off, standby, hibernating).
- The operating system is not loaded (software or boot failure).
- The software-based management agent is not available.

Out-of-band management is the ability to manage client computers regardless of the state of their power, operating system, or management agents. With Out-of-Band you can remotely change the power state of the computer, collect hardware inventory, and perform other management tasks that would normally require a visit to a client computer. This particular whitepaper will discuss the OOB solutions that are enabled using the networking interface on the system.

Here is a list of prevailing industry OOB solutions:-

- Intel® Active Management Technology (Intel® AMT) 2.0 and later (also known as Intel® vPro and Intel® Centrino® Pro technology)
- Broadcom ASF 2.0 and Intel ASF 2.0
- Broadcom DASH

Overview of Out of Band Management using vPro

Intel Active Management Technology (Intel AMT) is a part of Intel vPro technology, which provides the following technology capabilities:

Remote Manageability:
Remotely inventory, diagnose, and repair computers—even those that are powered off—reducing costly desk-side visits and increasing user uptime.

Security
Third-party security software identifies more threats before they reach the operating system. You can isolate infected systems more quickly and update computers regardless of their power state.

This whitepaper will target the remote manageability aspects of the Intel AMT.

Out of band refers to being able to manage the system in absence of the OS running, meaning the system is reachable and manageable pre-boot, or if the hard drive fails, or if the OS is hung
In Server, OOB functionality is achieved through the iDrac (integrated Dell remote access card) but in client, there are a variety of implementations starting with DASH and ending with vPro that we will cover below

Intel AMT is a solution that is based in hardware and firmware and is connected to the system's auxiliary power plane. Despite the power state or the operating system state of the client computer, Intel AMT provides IT administrators with access to alerts, hardware inventory, power management,

circuit breaker, and agent presence functionality. Intel AMT functionality does not require a software agent to be installed on the client computer.

Industry Competing Technologies

The following breaker section will detail out industry standard technologies, buzz words that are used in conjunction with regards to Out of Band Management.

- DASH(Desktop and mobile Architecture for System Hardware**)**

This is the Industry standard format for remote manageability communication packets. When a system is claimed as DASH Compliance, it implies adherence to a defined mandatory set of supported profiles (a profile represents a set of system attributes used for remotely gathering data or performing a remote system function). These are basically a set of command line used to test the compatibility of the OOB agent on the remote target system. The latest testable compliance version is 1.0 (1.1 compliance tool does not yet exist though specification is ratified).

For additional information on DASH Specifications, please visit -

- TruManage or Broadcom TruManage:

This is the Broadcom Marketing name for a similar set of basic OOB manageability features and the features are DASH 1.0 compliant from a remote manageability viewpoint.

- ISM – Intel Standard Manageability

Intel marketing name for a set of basic OOB manageability features and is somewhat equivalent to the Broadcom TruManage in feature functionality. Like TruManage it provides-

  - Provides DASH 1.0-compliant remote manageability
  - Adds support for remote console (Serial Over LAN) and storage device (IDE-Redirection) redirection, remotely-administered local HW-based firewall (System Defense), and remote detection of local SW agents
  - Feature set is equivalent to Intel AMT 3.x

- AMT – Active Management Technology

Intel marketing name for the complete set of advanced OOB manageability features within the vPro brand.

  - Provides DASH 1.0-compliance remote manageability
  - Supports all the features of ISM
  - Adds support for graphical remote control (Remote KVM), remotely configured periodic wake and maintenance (PC Alarm Clock / Remote Scheduled Maintenance), logged records of operator actions (Audit Log), HW-based security measurement of AMT FW, and simpler deployment using in-band initiated provisioning (HBP)

  - Also adds support for manageability inside Microsoft NAP-based networks and outside corporate firewalls (CIRA)

- Dell Unique vPro Extensions

Dell Business Client Hardware Systems starting with the Latitude E6x20/Optiplex 990 generation of hardware enable additional manageability extensions via the Intel AMT transport mechanism. These OOB manageability features are exclusive to Dell vPro/AMT products to enable best-in-class feature set that HP and Lenovo can't offer:-

  - Adds support for remote BIOS management to read/write BIOS settings
  - Adds support for remote battery management to read battery status/health
  - Adds support for secure remote HDD data wipe (AMT8 or newer only)

This features are primarily geared towards operations can be performed on 1-to-1 or 1-to-many basis.

OOB Feature Comparison

Out-of-Band Manageability Feature	Feature Description	No OOB	TruManage	ISM	AMT7 2011	AMT8 2012
Asset Management	Method to provide system software and hardware configuration data and inventory to a remote console.	N	Y	Y	Y	Y
HW Alerting	Remote notifications sent to the management console to identify issues such as boot failures, chassis intrusion, failed password entry, and thermal failures. AMT adds support outside the intranet.	N	Y	Y	Y	Y
Remote Power Control	Set of commands to perform power operations (on, off, restart) via a remote console.	N	Y	Y	Y	Y
IPV6 Support	Remote manageability commands and configuration compliant with IPV6-based networks.	N	Y	Y	Y	Y
IDE Redirection (IDEr)	Method of virtualizing a local (to the management console) drive or image to the remote machine to make it appear like a directly connected (to the client) drive.	N	N	Y	Y	Y
Serial Over LAN (SOL)	Method of sending terminal data across the managed ethernet connection for purposes of pre-OS remote booting (aka "text console redirection).	N	N	Y	Y	Y
System Defense	Set of configurable (by the management console) filters, counters, and policies to block network I/O in response to suspicious traffic. Can be used to protect the client from network traffic or to protect the network from malicious client traffic.	N	N	Y	Y	Y
Agent Presence	Ability to detect the presence of a local executable agent. Remote ability to set mitigation policies based on non-presence.	N	N	Y	Y	Y

Remote KVM (Keyboard/Video /Mouse)	Intel technology to enable the remote IT admin to see and control a system even outside the OS or driver environment by directly screen-scraping from the video HW and redirecting keyboard and mouse I/O.	N	N	N	Y	Y
PC Alarm Clock	Periodic wake from sleep states to allow service provider to perform periodic maintenance, such as updating anti-virus patches, etc.	N	N	N	Y	Y
Client Initiated Remote Access (CIRA)	Intel technology which enables the end-user to request an AMT connection via a hotkey to assist in issue resolution from outside the corporate domain or firewall.	N	N	N	Y	Y
Remote Scheduled Maintenance	Remote PCs can be inventoried, updated with required patches, etc. by connecting to their IT console or Service Provider when it's convenient.	N	N	N	Y	Y
Microsoft NAP Support	Support for managing remote OOB connections across networks that are secured with Microsoft NAP.	N	N	N	Y	Y
Audit Log	Log of operator or IT administrator's policy-based actions.	N	N	N	Y	Y
Measured AMT	Security measure to determine whether firmware has been compromised and ensure integrity	N	N/A	N	Y	Y
Host-Based Provisioning	Enables easier system deployment by allowing local client to initiate provisioning with management console on server.	N	N	N	Y	Y
Remote HDD Wipe	Dell Unique feature; enables user to remotely wipe HDD contents	N	N	N	N	Y

Identifying vPro Enabled Systems

Intel vPro Technology has been around for generations. The following are some mechanism

- Ivy Bridge CPU supporting Intel VT and TXT

- Panther Point Digital Office PCH (Q77/QM77/QS77)
- TPM 1.2, Revision 103 (or better); possible update to 116 pending
- BIOS that… Enables: Intel VT-x, VT-d, TPM 1.2, AMT; and Supports: TXT
- Intel ME firmware 8.0 (or better)
- Lewisville Gigabit LAN (82579LM)
- Intel WiFi Link (Puma/Jackson/Kilmer/Taylor Peak) – NB only (DT optional)
- Successful pass of Intel's Brand Verification Tool (BVT) or Technology Verification Tool (TVT – fixed workstations only)

Provisioning a System for Out of Band Managements

A system that supports AMT has to be provisioned for a remote server to communicate out of band with the system. The provisioning process includes enabling or disabling the required features of AMT in the system, enabling/disabling TLS and setting up an appropriate Access Control List (Users and access for users) for the system. A system can provisioned using different methods and the mostly the software used to manage the system mandates the provisioning process. The different options on how the system can be provisioned are provided below:

- In-band and Out-of-band provisioning
- USB Provisioning (TLS-PSK vs TLS-PKI)
- Small Business mode provisioning vs Enterprise mode provisioning
- Admin Control mode vs Client Control mode

A provisioning server has a profile with the details of the features that are required to be enabled/disabled along with the ACL details. A system can be provisioned in-band (from within the OS) or out of band (using custom AMT interface). If a user is going to use out of band method of provisioning a DNS A record called provisionserver should be pointing to the provisioning server. For in band provisioning normally an in band agent communicates with the ME via MEI driver and the provisioning server to provision the system. For out of band provisioning, AMT sends a hello packet to the provisioning server and the provisioning is done via the network.

A system can be provisioned securing either using TLS-PSK(pre shared key) or TLS-PKI(public key infrastructure). For TLS-PSK, the provisioning server generates a provisioning id(PID) and provisioning passphrase(PPS) pair. The user can enter this via MEBx or can export the PID/PPS pair to an USB key. When the USB key is inserted and the system is booted, the PID/PPS pair is saved in the MEBx. During the provisioning process, the initial communication between the AMT system and the provisioning server will only contain the PID information and the rest of the communication is secured by encrypting the messages using the TLS-PSK protocol. For TLS-PKI, Dell systems ship with few default certificate hashes that can be purchased and directly used in the infrastructure. For using custom certificate hash information for provisioning, the hash information can be entered in the MEBx directly or via USB.

For quickly reviewing AMT features, a system can be provisioned via MEBx. Enter MEBx, change the default password "admin" to a strong password. Based on the AMT version, either under ME configuration or AMT configuration, "Activate Network" option is available. When selected AMT is provisioned with default options. "Unconfigure network access" option can be selected to unprovision the system.

If a system is provisioned with TLS mode disabled, the system can be accessed via WebUI using the URL http://SUT_HOSTNAME:16992. If a system is provisioned with TLS mode enabled, the system can be accessed using the URL https://SUT_HOSTNAME:16993.

All the above mentioned provisioning methods configures the system in admin control mode, which means except for KVM feature, the remote console has complete access to the system. A system can be put in client control mode using a tool called HostBasedSetup from Intel SDK. When the system is in client control mode, the remote console has limited control to the system and requires user consent from the AMT system to complete the remote operation.

The following are the different types of provisioning methods:

1) Small Business/Normal Business mode
2) Host Based Provisioning

Following section will detail the basic mechanism of provisioning the system and the verification steps to ensure the provisioning is successful.

Small Business/Normal Business mode

Provisioning Process

Depending on the version of AMT, this provisioning mode is either referred to small business or

Normal business mode.

For AMT 6 and later platforms:

1) Enter MEBx (Ctrl-P during boot or F12 and chose Intel MEBx)
2) Change the default MEBx password
3) Either under ME Settings/AMT Settings (depending on AMT version), under Network
    a. Name settings; change the hostname of SUT and domain name of SUT.
4) Either under ME Settings/AMT Settings (depending on AMT version), select Activate
    a. Network Access.

How to verify provisioning is successful:

1) Access WebUI of the AMT system (Example: <IP_AMT_SYSTEM>:16992) from a Management console and login with the MEBx credentials.
2) Intel's privacy icon in OS or IMSS (Intel Manageability and Security Status) icon(Under

Advanced tab -> Intel ME status will show as configured).

3) Run MEInfo. Configuration state should refer and completed and Provisioning mode should refer as Small business.

Host Based Provisioning

Host based provisioning is the ability to be able to provision the AMT from within an operating systems environment.

1. Download the appropriate AMT SDK and unzip it.
    a. Under the SDK>\Windows\Intel_Manageability_Configuration\Bin\HostBasedSetup\HostBasedSetupTyped, run: HostBasedsetup –setup –newpass PASSWORD
2. For WMI based provisioning, under the
3. <SDK>\Windows\Intel_Manageability_Configuration\Bin\HostBasedSetup\HostBasedSetupTyped, run: HostBasedsetup –setup –newpass PASSWORD -wmi
4. To verify if the provisioning is successful - Access WebUI of the AMT system (Example: <IP_AMT_SYSTEM>:16992) from amanagement console and login with the MEBx credentials.
5. Intel's privacy icon in OS or IMSS (Intel Manageability and Security Status) icon(Under Advanced tab -> Intel ME status will show as configured).
6. Run MEInfo. Configuration state should refer and completed and Provisioning mode should refer as Client Control Mode
7. For WMI based provisioning, under the <SDK>\Windows\Intel_Manageability_Configuration\Bin\HostBasedSetup\HostBasedSetupTyped, run: HostBasedsetup –discovery, it should refer system is provisioned

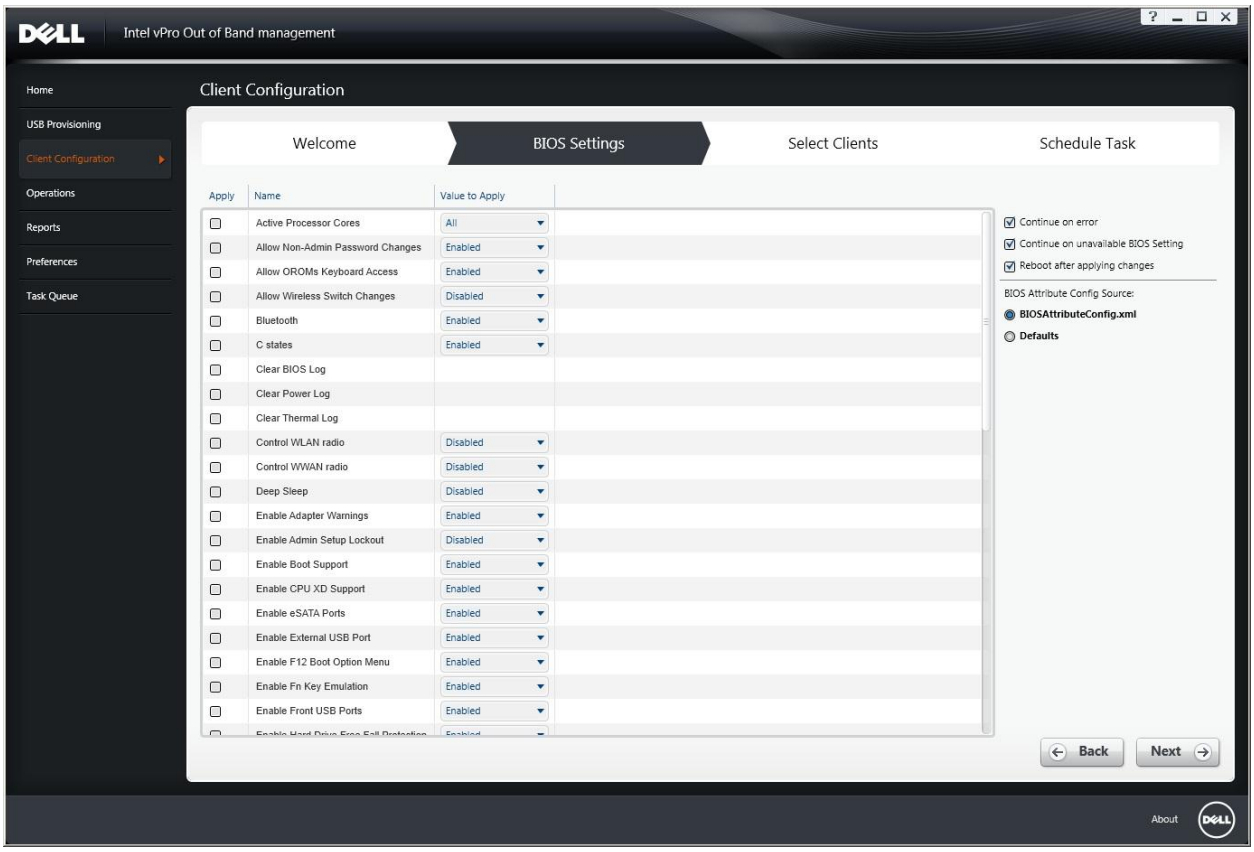
Dell Unique vPro Extension

The following section details the unique features that are enabled via extensions to Intel AMT Out of Band interface.

BIOS Management

BIOS management capability in an out of band context refers to be the ability to configure the BIOS when the system is practically un-reachable. Some of the user actions in such a situation may include recovering the system password (resetting it a new default), changing the boot order to deploy a new operating systems or configurable certain bios options for optimum performance.

Additional use cases may include a scenario where the administrator wants to deploy the same bios changes on multiple systems. This is especially useful in cases where the host OS on the system may be a hypervisor running in which case the host OS and thereby the in-band tools may not have complete access to the BIOS. The following screenshot shows an example of the BIOS options that can be configured via the Out of Band Management interface.



Battery Management

Battery management feature provides the ability to query additional properties of the batteries included on the system. The following table shows an example of the properties that can be queried from a target system using the out of band management interface.

The Battery Health Report provides information (obtained from the CIM_Battery class) pertaining to the characteristics and health state of each battery installed on an Intel AMT enabled system.

The battery management feature allows for querying the battery state regardless of the power state of the system.

Item	Value
Service Tag	1QJB1P1
Asset Tag	9876543210
Host Name	SB-JDD1
Domain Name	dcm.local
Firmware Version	7.0.0.0053
Last Updated	03/29/2011 6:30 PM

Item	Battery 1	Battery 2
Device ID	DELL DTG0V0C	DELL DTG0V0C
Element Name	DELL DTG0V0C	DELL DTG0V0C
Chemistry	Li-Ion	Li-Ion
Design Capacity (mW-h)	9990	9990
Full Charge Capacity (mW-h)	9907	9950
Operational Status	OK	OK
Health State	OK	OK
Enabled State	Enabled	Enabled
Requested State	Enabled	Enabled
Battery Status	Fully Charged	Fully Charged
Charging Status	Idle	Idle
Charge Remaining	100%	100%

Power Management

Power Off shuts down a system regardless of the state of the operating system. (This can result in loss of data especially if the OS is currently running. Dell developed plug-ins provide for a way to cause a graceful shutdown if the OS is reachable prior to attempting a shutdown operation. The feature is currently only supported on Windows Oses. The following table shows the individual capabilities and the differences between AMT enabled power management operation and the Dell value-add.

The Power On command brings the system to full ON from any state (sleep, hibernate, or off).

Command	UI Label	Description
Power On	AMT Power On (out-of-band)	Brings system to full ON from any power state.
Power Off	AMT Power Off (out-of-band)	Ungraceful shutdown.
Shutdown	Graceful OS shutdown, then ungraceful if failed	Attempt graceful shutdown of the OS. If failed, do AMT Power Off.

Restart	Graceful OS restart, then ungraceful if failed	Attempt graceful shutdown of the OS. If failed, do AMT Power Off; then do AMT Power On.

Power management commands

Dell Developed Plug-ins

Dell Client Integration Pack (DCIP) for Systems Center 2007/2012

Dell Client Integration Pack is a plug-in developed by Dell for Enterprise Customers that use Microsoft Systems Center Configuration Manager products to manage their environment.

The Dell Client Integration pack allows customers to utilize in-band and out-band capabilities to manage their Optiplex, Latitude and Precision systems.

Create Dell Windows PE Boot Images:

This feature enables Configuration Manager to configure and push your customized operating system image on your client system using the features available on DCIP.

Creating and Importing Dell Driver Packages

This feature enables Configuration Manager to configure and push your customized driver packages onto your client system.

OMCI Integration

This feature enables Configuration Manager to use the features available on Dell OpenManage Client Instrumentation (OMCI) such as remote management applications, accessing managed node information, manage client state, receiving alerts for client events.

Pre/Post OS BIOS Configuration

Dell Client Configuration Toolkit (CCTK) is packaged software offering that provides BIOS configuration capability to Dell client systems such as OptiPlex, Latitude, and Precision in an operating system present environment. The feature helps configuring the BIOS for Dell client systems using the CCTK Self Contained Executable (SCE) package. CCTK does require and OS present (Host or WinPE) to be enabled to configure the BIOS and has more extensive BIOS configuration options than those enabled via Intel AMT interface.

Intel AMT vPro OOB Management

This is an Out-of-band (OOB) management feature using Intel AMT. It is supported through a standalone application running on the Configuration Manager server. This feature provides the core functionality to manage client systems remotely and automatically regardless of the state of the operating system.

Windows 2011 Small Business Server Essentials Plugin

Small Business Server (SBS) Environment provides a semi-unmanaged environment in the sense of there is no central console administrator administering those end user systems. An SBS environment caters to anywhere from 25-75 clients.

Intel AMT out-of-band management features include client provisioning, BIOS/MEBx configuration, various OOB management operations, and OOB configuration reporting; all of which can be done irrespective of the state of the client's operating system.

Dell provided plug-in will be installed on the Server and be used to manage the console via the Out of Band Web services interface provided by the Intel vPro enabled clients on the end points. This plug-in will co-exist alongside the Intel SBA plug-in and will provide additional Dell unique capabilities to customers.

Intel provides a Host based provisioning capability which will put the Clients in Client Controlled Mode (CCM) or basic mode. Dell provided vPro extensions are only available in Admin Controlled mode (ACM) or advance mode. The following lists out the various features that will be available based on the End node client system state.

Dell plug-in will be able to co-exist alongside the Intel plug-in and installation of one will not require removal of the other. The following table lists out the 2 operational modes for the SBS plug-in.

	Basic Mode	Advanced Mode
Battery Reports	✓	✓
Power Profile Setting	✓	✓
Boot Order	✓	✓
BIOS Settings		✓
BIOS Passwords		✓
Remote Hard Drive Wipe		✓

Summary

Dell Business Client platforms that are AMT enabled provided unique out of band serviceability options along with the Dell developed plug-ins in most commonly used industry consoles.

References

1. Dell Systems Management Landing Page: http://support.dell.com/support/systemsinfo/documentation.aspx?c=us&l=en&s=gen&~subcat=108&~cat=6
2. Dell Client Integration Pack

   http://support.dell.com/support/edocs/SOFTWARE/smdcip/
3. Intel AMT vPro Plug-in

   http://support.dell.com/support/edocs/SOFTWARE/smAMT/
4. Desktop and Mobile Architecture for System Hardware

http://dmtf.org/standards/dash

5. Windows Small Business Server Plug-in

   http://en.community.dell.com/techcenter/b/techcenter/archive/2012/07/31/dell-intel-vpro-out-of-band-management-plug-in-for-windows-small-business-server-2011-essentials.aspx

6. Dell TechCenter Enterprise Client Page (Best Practices, Whitepapers, How-to Videos)

   http://delltechcenter.com/enterpriseclient