Chapter 6

Solving End User Problems with Intel® vPro™ Manageability

The ideal engineer is a composite ... He is not a scientist, he is not a mathematician, he is not a sociologist or a writer; but he may use the knowledge and techniques of any or all of these disciplines in solving engineering problems.

—N. W. Dougherty, 1955

None of the features of Intel® Active Management Technology (Intel AMT) would be of any use if they could not be combined to solve real world problems. In this chapter we will review a set of real world scenarios and how Intel AMT features can be used to solve them. It's also important to note that in most or all of these scenarios, software-only solutions would either not work at all or not solve the problem as effectively or as securely.

Protect from a Worm Outbreak

Virus outbreaks have cost organizations much time and money. As employees come in early in the morning, companies would post announcements telling them not to use their computers until further notice. In these situations each hour a network is down is a huge burden and a fix must be deployed quickly.

When Intel AMT is present and set up on a computer; IT can quickly deploy hardware network filters that stop specific traffic types. If it is determined that a virus attempts to scan a given port on all computers, IT can deploy one or more hardware filters that block inbound and outbound packets that match a given traffic type. Hardware counters can also be used to count how many packets of this type where dropped, making it easy to determine if a computer is infected.

Here is a typical scenario: An employee uses a USB flash stick to transfer files onto a work computer. One of the files is infected with a new and unknown network worm. The worm then proceeds to scan the network for vulnerable computers. The worm spreads quickly throughout the company slowing down the network and making computers unusable. IT determines that the worm is scanning the network for a custom application that is specific to this organization. This application listens to a specific UDP port and determines that the worm must be exploiting vulnerability in the software. Having a fleet of Intel vPro computers, IT pushes a network filter blocking inbound and outbound packets to this port. It also assigns a hardware network packet counter to these filters, as shown in Figure 6.1.

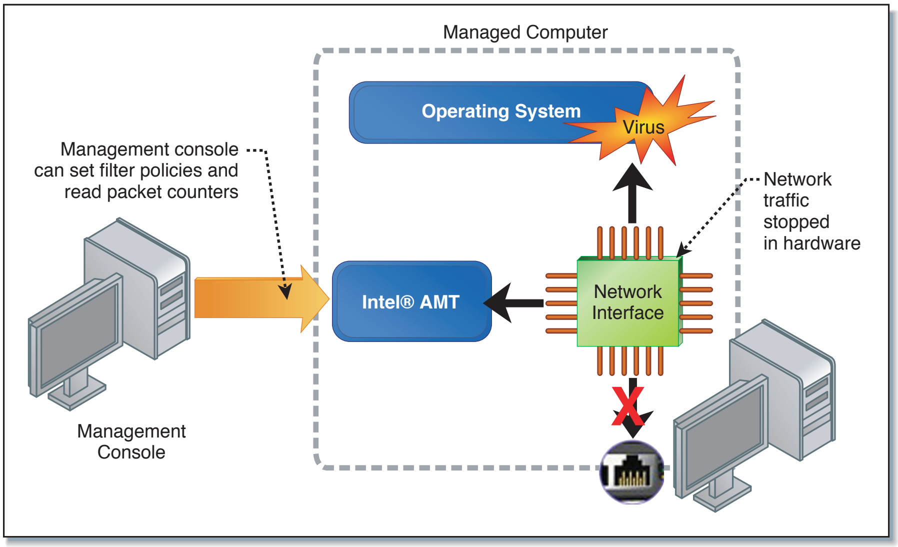

Managed Computer
Operating System
Virus
Management console can set filter policies and read packet counters
Network traffic stopped in hardware
Intel® AMT
Network Interface
Management Console

Figure 6.1 With the Infected Computer's Network Traffic Cut Off, the Administrator Can Still Communicate with Intel® AMT

IT is now in a position to monitor each computer and see which ones are infected with the worm. It can do so without requiring any software to be installed or running on each computer, or without worry that the worm itself would tamper or disable monitoring software running on each computer.

In an extreme case, IT could also disable all network traffic going in and out of a computer, or disable all traffic except for a give type. In our example, the worm attacks some of the computers in the company and these are now isolated and can't attack any other computer. In order to fix computers remotely, IT places a policy that allows traffic to and from the management console to be permitted through. This allows the administrator to contact services running within the operating system and attempt to fix the problem, as shown in Figure 6.2.

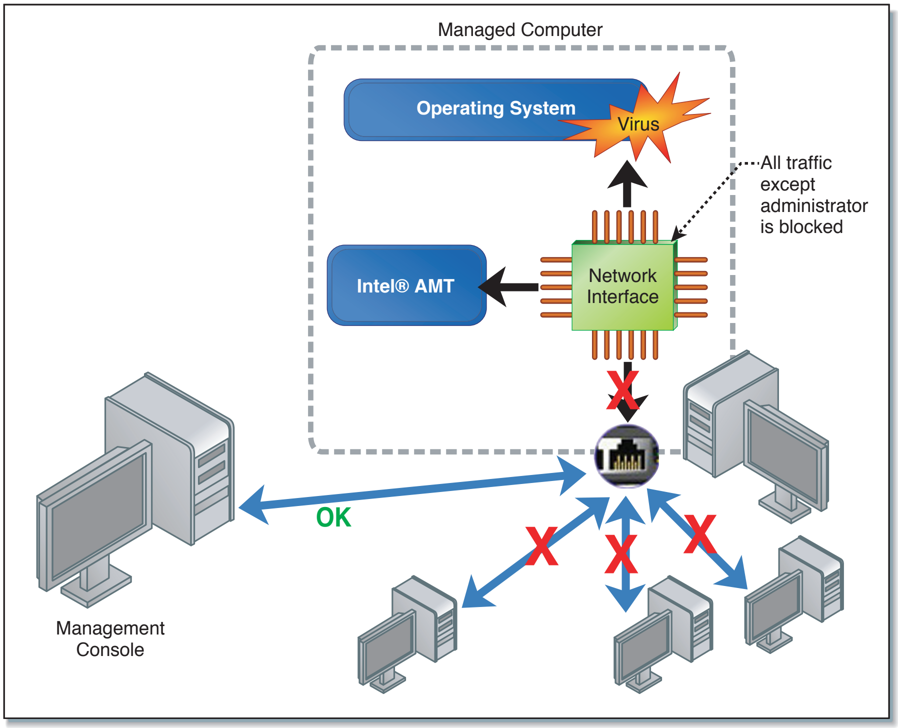


Figure 6.2 All Traffic Cut Off Except for Network Traffic to the Administrative Console. This Allows for Safe Remote Repair.

With Intel AMT 3.0, an additional feature may be useful in this scenario. Heuristic filters can be setup in advance to automatically detect and stop computers that attempt to scan the network. In our scenario, all computers with Intel AMT 3.0 would automatically detect and stop the worm from attempting to find other vulnerable computers.

Tracking Hardware Assets

Hardware theft is a big problem. Universities and corporations operating in poor countries are known to be especially at risk, but no one is immune to hardware theft. Thieves may steal a computer, but can also replace parts. They can replace the computer's CPU with a lower value one or remove some of the RAM, remove one of the PCI cards, and so on.

Let's suppose a scenario where a university campus is the target of occasional RAM theft. Computers still run, but a portion of the RAM is removed.

Using Intel AMT, the university IT department gets the hardware inventory of all of the computers on campus every day. It gets a very accurate picture of the inner components of each computer. Each time the hardware inventory is gathered; it is compared against the previously known inventory for this computer and stored into a database, as illustrated in Figure 6.3.

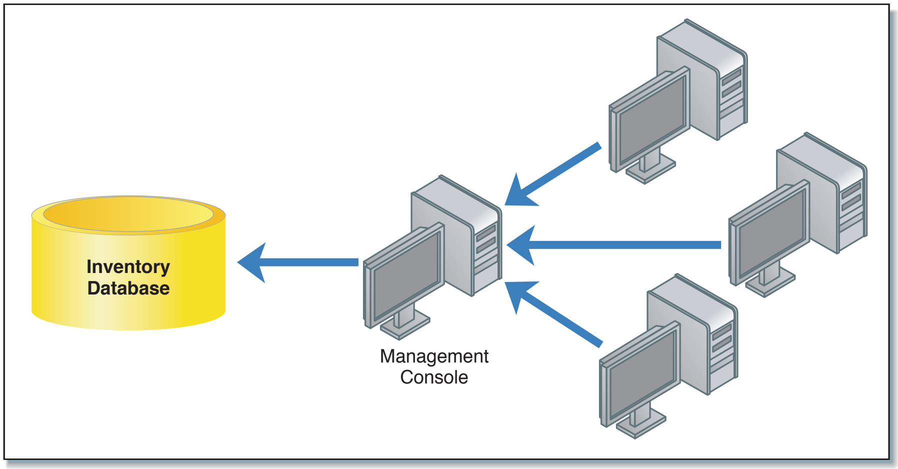


Figure 6.3 Hardware Asset Information Gathered into a Searchable Database

IT has a full inventory of all hardware assets within the university and can print a report showing, among other things, the total amount of RAM for all of the computers in the entire university. When a computer's RAM is decreased, a warning is automatically displayed on the administrator's management console.

In this scenario, administrators can find the computer with the missing memory and start to investigate. So far, the hardware asset inventory of all computers in the university is only taken every 24 hours and so it may take some time before the stolen RAM is detected. Intel AMT also supports the case intrusion switch and can send an alert to the administrator each time a computer case is open. Even if the computer is not connected at the time of the theft, the next time power and network is connected back, the computer will send the case intrusion alert to the administrator console. The university console can then turn the computer on remotely and automatically verify that the entire hardware inventory is still the same as before. Using the case intrusion switch allows the console to perform asset inventory check more frequently and exactly when needed. The administrator can also detect cases where lower quality RAM is replaced into a computer since Intel AMT reports the speed and serial number of each RAM stick.

Another similar and much more serious scenario has to do with hard disk theft. Intel AMT also reports each hard disk installed on a computer and for each disk, the size and serial number of disk. Administrators can quickly identify and react to a hard disk replacement or theft since Intel AMT does not depend on software or an operating system running on the PC. When a thief steals a hard disk from a computer, the case intrusion switch is triggered and the alert is sent, the administrator can take action.

Lastly, to protect mission critical data and computer assets the university management console can connect to any Intel AMT computer even if it is sleeping. This is useful because the software console can get up to the second report on the connectivity of all university computers. A thief attempting to steal a computer will have to disconnect it from the network causing the console to stop receiving network responses from that computer and the university security can automatically be advised of the problem.

In the past, this type of live monitoring would require the computer to stay on all the time, consuming and wasting energy increasing overall cost of operation. With Intel AMT, computers can be monitored around the clock while staying in full sleep or hibernation mode.

Fixing a "Blue Screen"

One of the most difficult problems to fix remotely is a complete crash of a computer. Luckily the well known "blue screen of death" occurs much less frequently now than it did only a few years ago as operating systems have gotten more reliable. Still, there are cases where such a crash can be costly to repair.

In this scenario, a company operates cash registers for a chain of stores. If one of the cash registers crashes, it may be costly to send someone to go fix it. The preferred solution is to fully diagnose and possibly fix the problem completely remotely. Older crashed cash registers would no longer be reachable through the network, but in our scenario the cash registers are running Intel boards that support Intel AMT. Even when the cash register has crashed, it is still possible to connect to Intel AMT and attempt to diagnose the problem.

Using the IDE redirect (IDE-R) feature, an administrator can remotely boot a recovery operating system (ROS). The administrator uses a CD-ROM disk image (.iso file) containing the recovery operating system and uses the management console software to boot the disk image on the cash register, as shown in Figure 6.4. Once completed, a set of diagnostic tools can be run and actions can be taken to fix the problem.

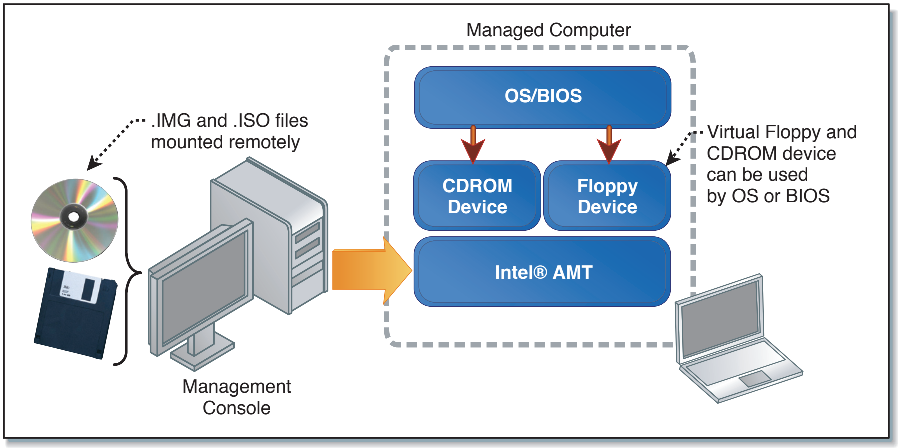

Managed Computer
OS/BIOS
CDROM Device
Floppy Device
Intel® AMT
.IMG and .ISO files mounted remotely
Virtual Floppy and CDROM device can be used by OS or BIOS
Management Console

Figure 6.4 A Console Can Redirect a Floppy and CD-ROM Drive to a Managed Computer and Use Them for Remote Repair

In our case, the administrator realizes that files were accidently corrupted in the operating system and decides to reformat the hard disk with the original factory software. All of the software and tools needed to perform these operations are located on the ROS image file. If the administrator does not have the right tools, a different ROS can be used. The administrator changes the ROS disk image and causes another remote reboot using the new disk image.

This scenario equally applies to remote kiosks, corporate computers, ATM machines, and much more. IDE redirect is a powerful tool for fixing many types of problems remotely.

Compliance Network Alert

A healthy network starts with healthy computers that run up to date anti-virus, firewall, and repair agent software. A computer is said to be compliant with IT policies if it is running all of the correct IT software. Keeping track of computers that are not in compliance can be a problem.

Thanks to the agent presence feature of Intel AMT, it's possible to monitor what applications are running within the operating system. To do this, applications must periodically send a heartbeat to announce their presence to Intel AMT. Serving as a trusted entity on behalf of the network administrator, Intel AMT can report back on any changes in the running state of an application, as shown in Figure 6.5. In this way, many applications can be tracked and compliance maintained.

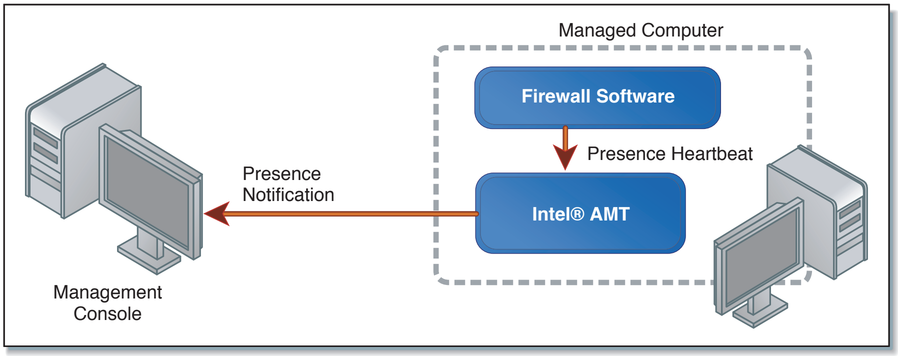


Figure 6.5 Intel® AMT Agent Presence Feature Monitors the Running of Firewall Software and Can Notify the Console of the Running State

When an application starts or stops reporting its presence, Intel AMT can send a network alert to the management console and/or log this as an event on the platform's event log. Since the event log is kept on the motherboard flash memory, it can be retrieved later, as shown in Figure 6.6. Keeping presence information in the event log can be very useful.

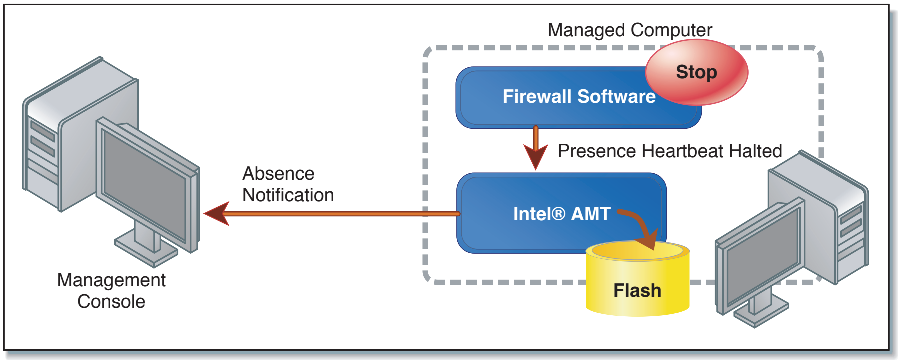


Figure 6.6 If the Firewall Software Is Stopped, the Console Can Be Notified with a Network Alert and an Event Can Be Stored in the Intel® AMT Event Log

For mobile platforms, the administrator can monitor compliance even when the computer is not connected to the managed network. When connected again, the event log can be examined to see if compliance was maintained.

Tracking Power Usage

For the first time, with Intel vPro technology, a network administrator can query over the network the power state of a computer without waking it up. This means that administrators can tell the difference between a computer that is powered on, a sleeping computer, and one that is disconnected from the network altogether. This feature in Intel AMT makes it easier to know if operating system configured power saving policies are working correctly. It also makes it possible for administrators to see in near real time how many computers are in which power state and which ones are currently disconnected from the network, as shown in Figure 6.7.

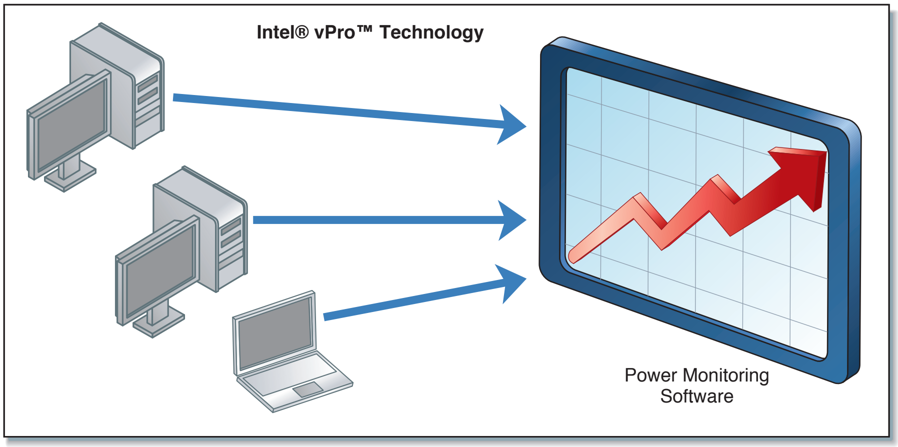


Figure 6.7 Power Monitoring Software Can Collect Power State for Many Computers and Show an Overview Graph of the Organization's Power Use

For Experts

There are a few tricks for using Intel AMT for power monitoring. On its own, Intel AMT will not send a network alert to a monitoring application when a computer changes power state. Events generally occur when a computer first boots up, but this will not help the monitoring software know when a computer goes to sleep and back, sometimes many times within a day.

The usual way to gather this data is to poll all computers with Intel AMT for their power state every few minutes. This works well, but may not be optimal. One clever trick is to use the Intel AMT agent presence feature and setup a new dummy watchdog that no application will ever use. Within Intel AMT, an agent presence watchdog will change to the "Suspended" state when the computer is in any sleep state, and back to "Expired" when it wakes up again. By causing this watchdog to send alerts, the monitoring software can be notified when a computer changes power state. When going to sleep, the monitoring software can then query the computer for its exact power state: S1 to S5.

This trick can help monitoring software get more accurate power data without continually polling all of the computers for their power state. Still, continual polling does have one important benefit. There is no way a computer can send a network alert notifying the monitoring software that it has been disconnected from the network. This information may be important and so, routinely performing a PING on each computer in addition to getting power notifications can insure both good power data in addition to knowing if the computer is still connected on the network.

Changing BIOS Settings Remotely

Probably one of the easiest and most immediately compelling demonstrations of Intel AMT is remote BIOS changes. Suppose a BIOS setting is incorrect such as the booting order of disk drives is not set correctly. The administrator can use Intel vPro–enabled administrative console software to remotely reboot the computer into BIOS and redirect the text mode display to the Intel AMT virtual serial port. The administrator can then send keystrokes back to the

BIOS that will be acted upon just as if the user was typing that key, as shown in Figure 6.8.

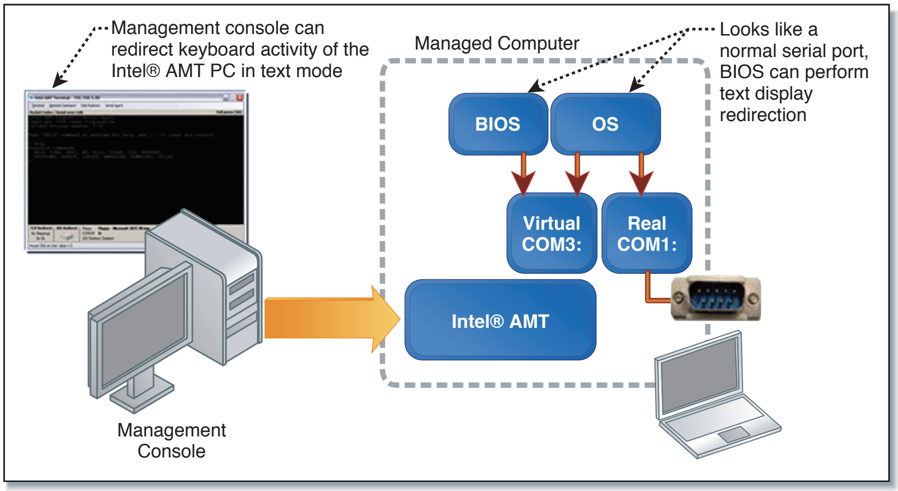

Management console can redirect keyboard activity of the Intel® AMT PC in text mode
Managed Computer
Looks like a normal serial port, BIOS can perform text display redirection
BIOS
OS
Virtual COM3:
Real COM1:
Intel® AMT
Management Console

Figure 6.8 A Virtual Serial Port Is Redirected to the Management Console Allowing Remote Control When the Managed Computer Is in Text Mode Display

The administration console gets a complete remote view of the BIOS and, on some platforms, can even block local keyboard input from the local user. This is a very powerful feature but it can be augmented even further with terminal scripting on the administrator console. Because the terminal is text mode, it can easily be scripted, and manual changes in the BIOS can thus be automated.

Terminal scripting is especially valuable when a single BIOS change must be done on many computers, or when BIOS settings on many computers have to be audited. A script can read existing settings or perform the correct operations to make changes. Of course, because BIOS takes different forms the script may have to adapt to the specific BIOS that is present on the target computer.

Once the BIOS changes are completed, it's then possible to save the changes and reboot the computer normally. This is usually done in the same way that it's done when sitting in front of the managed computer. If needed, Intel AMT can be used to power cycle the computer.

Remote Platform Diagnostics

The Intel AMT event log records events from various sources and can be helpful in remotely diagnosing platform level problems. If an application fails, the operating system logs are a good source of information on what caused the problem. If the platform fails to boot, the Intel AMT event log plays the same role at the platform level, as shown in Figure 6.9.

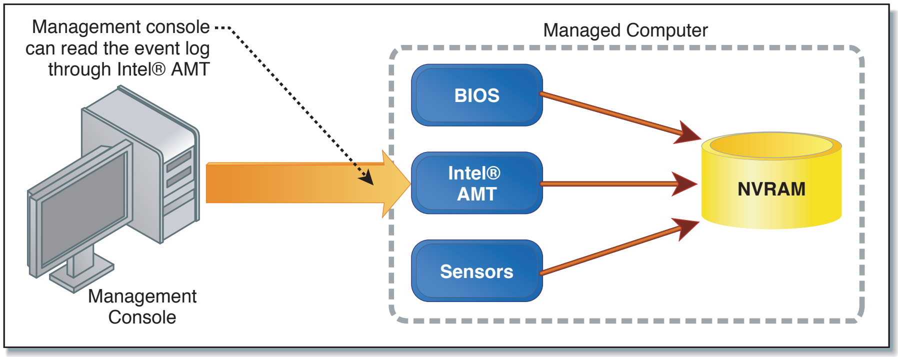
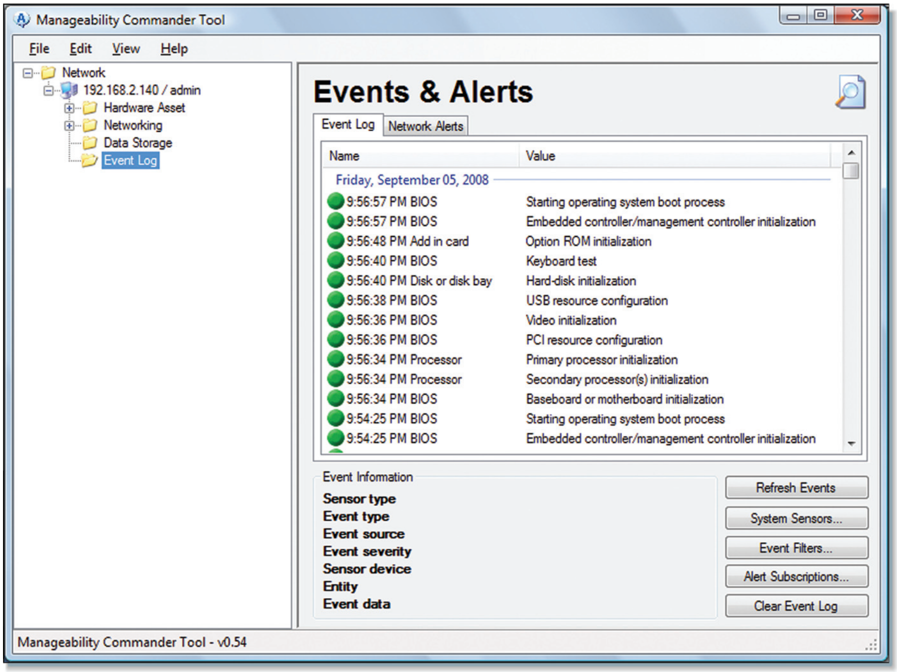

Management console can read the event log through Intel® AMT
Management Console
Managed Computer
BIOS
Intel® AMT
Sensors
NVRAM

Figure 6.9 The Management Console Can Access Events Sent by Various Sources through Intel® AMT's Event Log Stores in Platform Flash Memory

The event log is stored in the platform's flash memory and so, is kept regardless of the health of disk storage. It gets events from three main sources: BIOS, platform sensors, and Intel AMT itself. BIOS events generally include boot up events and system failures. Platform sensors include the case intrusion switch, processor, add-in cards, and sometimes temperature warning sensors. Lastly, Intel AMT will record many events such as system defense and agent presence state changes, and so on.

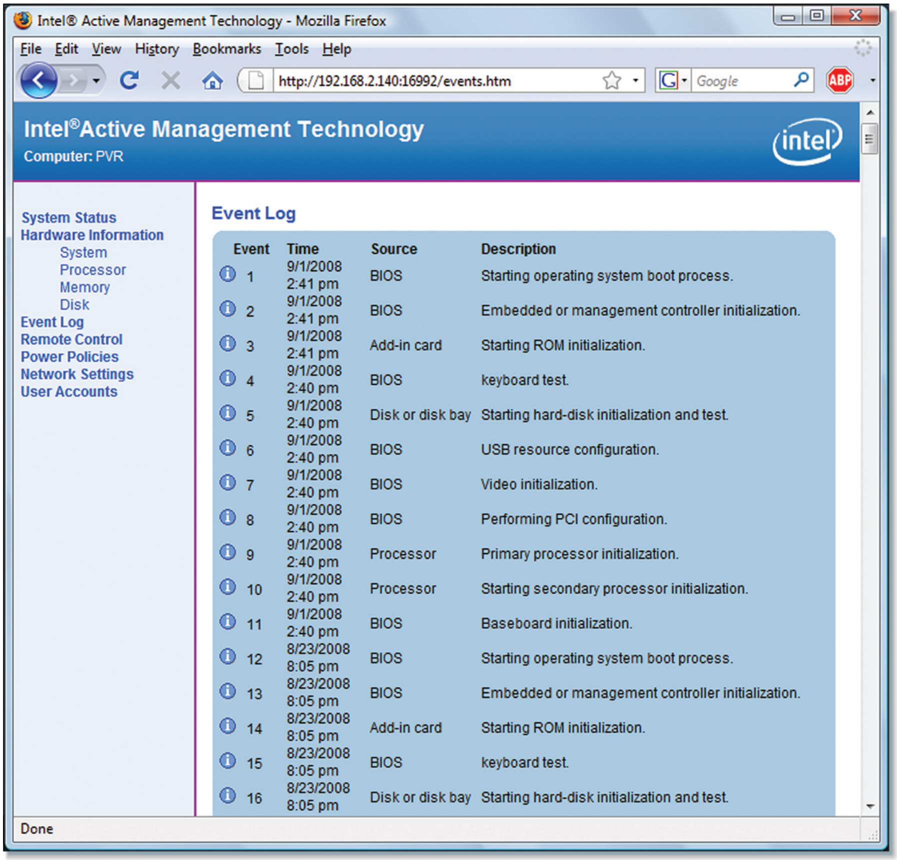
The combination of all these events recorded into flash makes the Intel AMT event log an interesting place to start when trying to remotely diagnose platform level issues.

The event log can be accessed using most Intel vPro–enabled console software as shown in Figure 6.10 and also using the built-in Intel AMT Web server shown in Figure 6.11.



Name	Value
Friday, September 05, 2008	
● 9:56:57 PM BIOS	Starting operating system boot process
● 9:56:57 PM BIOS	Embedded controller/management controller initialization
● 9:56:48 PM Add in card	Option ROM initialization
● 9:56:40 PM BIOS	Keyboard test
● 9:56:40 PM Disk or disk bay	Hard-disk initialization
● 9:56:38 PM BIOS	USB resource configuration
● 9:56:36 PM BIOS	Video initialization
● 9:56:36 PM BIOS	PCI resource configuration
● 9:56:34 PM Processor	Primary processor initialization
● 9:56:34 PM Processor	Secondary processor(s) initialization
● 9:56:34 PM BIOS	Baseboard or motherboard initialization
● 9:54:25 PM BIOS	Starting operating system boot process
● 9:54:25 PM BIOS	Embedded controller/management controller initialization

Figure 6.10 Event Log as Displayed within Intel Manageability Commander



Intel® Active Management Technology

Computer: PVR

Event Log

Event	Time	Source	Description
1	9/1/2008 2:41 pm	BIOS	Starting operating system boot process.
2	9/1/2008 2:41 pm	BIOS	Embedded or management controller initialization.
3	9/1/2008 2:41 pm	Add-in card	Starting ROM initialization.
4	9/1/2008 2:40 pm	BIOS	keyboard test.
5	9/1/2008 2:40 pm	Disk or disk bay	Starting hard-disk initialization and test.
6	9/1/2008 2:40 pm	BIOS	USB resource configuration.
7	9/1/2008 2:40 pm	BIOS	Video initialization.
8	9/1/2008 2:40 pm	BIOS	Performing PCI configuration.
9	9/1/2008 2:40 pm	Processor	Primary processor initialization.
10	9/1/2008 2:40 pm	Processor	Starting secondary processor initialization.
11	9/1/2008 2:40 pm	BIOS	Baseboard initialization.
12	8/23/2008 8:05 pm	BIOS	Starting operating system boot process.
13	8/23/2008 8:05 pm	BIOS	Embedded or management controller initialization.
14	8/23/2008 8:05 pm	Add-in card	Starting ROM initialization.
15	8/23/2008 8:05 pm	BIOS	keyboard test.
16	8/23/2008 8:05 pm	Disk or disk bay	Starting hard-disk initialization and test.

Figure 6.11 Event Log as Displayed in the Intel® AMT Web Page

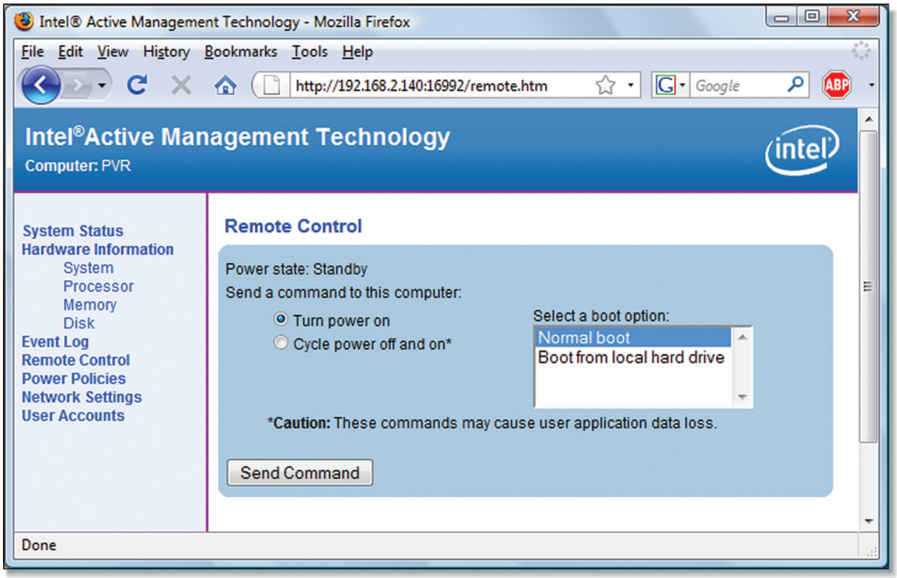
Lockup Detection and Power Control

Another powerful feature of Intel AMT allows the administrator to remotely control the power state of the computer: power up, power down, power cycle, and detect an operating system hang. As an example, a remote tourist kiosk is locked up and has become unusable. In the past, the kiosk would no longer be reachable through the network and any remote operation was impossible.

Such a kiosk would stay locked up for hours or days until someone manually performed a power cycle.

With Intel vPro, the Intel Manageability Engine Interface (Intel MEI) driver (called the HECI driver in the past) periodically notifies Intel AMT that it is running correctly. Since it's a driver and runs at a higher privilege level, a stop in these notifications indicates that something quite serious has happened to the operating system. A management console can read the operating system lock-up flag when reading the power state of the computer; it's the same call that reports both.

In our example, a tourist kiosk can lock up and the administrative console can notice this using the agent presence feature indicating the tourist application is no longer running and/or reading the lock-up flag. Once the determination is made of an operating system lockup, the administrator can power cycle the system remotely, as shown in Figure 6.12.



Intel® Active Management Technology - Mozilla Firefox

http://192.168.2.140:16992/remote.htm

Intel® Active Management Technology

Computer: PVR

Remote Control

Power state: Standby

Send a command to this computer:

● Turn power on

○ Cycle power off and on*

Select a boot option:

Normal boot

Boot from local hard drive

*Caution: These commands may cause user application data loss.

Done

Figure 6.12 Remote Control Feature in the Intel® AMT Web Page

Obtaining the current power state and performing remote power operations is also available within the Intel AMT built-in Web page. For our tourist kiosk example, one of the tourist guides with minimal knowledge of Intel AMT can log into the Web page of the locked-up computer and reset it. No additional software is needed.

Summary

We have reviewed some of the most typical discover, heal, and secure scenarios that can be solved using Intel AMT. In the next few chapters we will take a look at the details of these scenarios and how a developer can add these and other Intel AMT features into their own management software. A good understanding of the features available with Intel AMT means that developers and users can make the most of them.