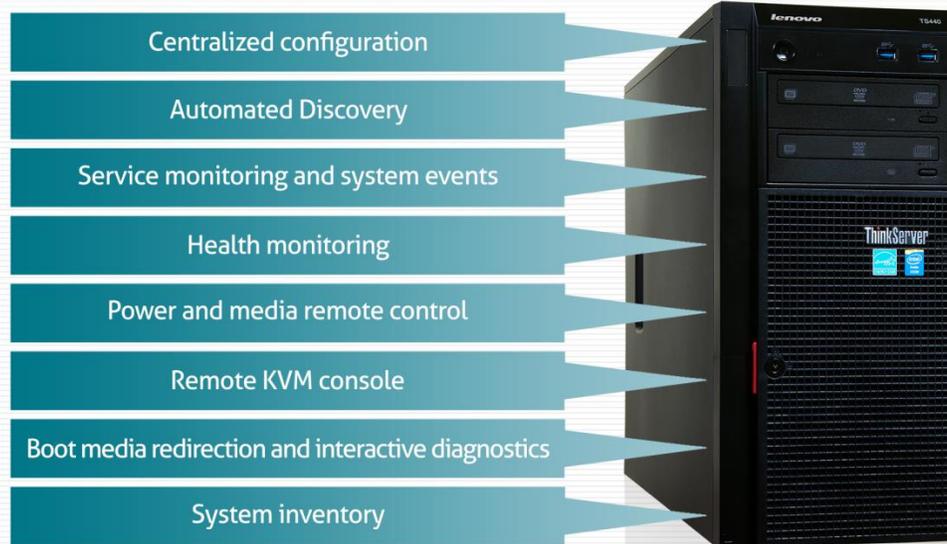


LENOVO THINKSERVER TS440 WITH INTEL AMT 9.0 FOR EASY AND EFFECTIVE SYSTEMS MANAGEMENT



Lenovo® ThinkServer® TS440 - Feature-rich. Highly affordable.

Whether you are looking for your first server, or your business has grown and you need to update your server technology, an essential consideration should be the management capabilities of the platform you select. A key management feature to look for is out-of-band (OOB) management – the ability to manage the server regardless of its state. An effective OOB management platform with features such as remote control and configuration, monitoring and alerting, and remote interactive diagnostics, when combined with a commonly available system management console such as Microsoft® System Center 2012, can save you time and money by reducing the need for on-site support.

The Lenovo® ThinkServer® line, priced to be highly affordable to companies of all sizes, and backed by Intel® Xeon® processors and the latest chipset technology – gives systems administrators a capable, cost-effective, and manageable platform. The newest generation of Lenovo single-CPU towers includes Intel Active Management Technology (AMT) 9.0, which provides OOB management functions built into the system—with no additional costly components required. Intel AMT 9.0 also uses industry-standard management protocols that allow independent software vendors (ISVs) to add support in their management consoles.

In our labs at Principled Technologies, we demonstrated the capabilities of the new Lenovo ThinkServer TS440 with integrated Intel AMT 9.0 in eight common management use cases, running Microsoft System Center 2012 as the centralized



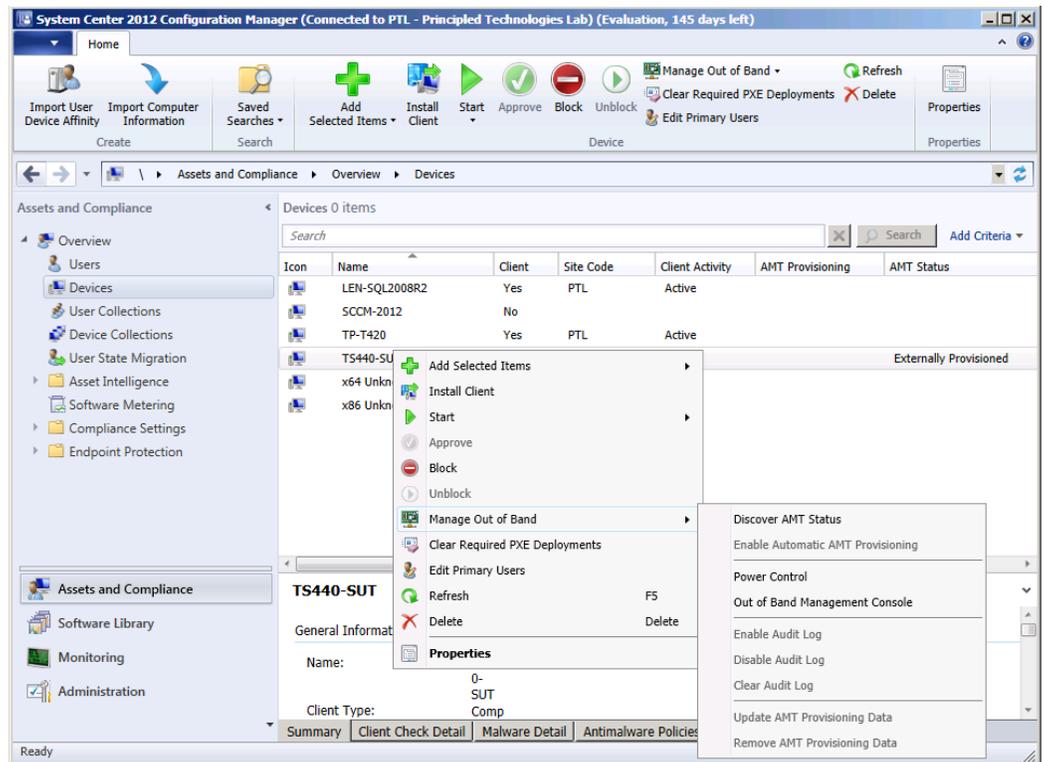
management console. We found the Lenovo ThinkServer TS440 with Intel AMT 9.0 supported each of our eight use cases with ease. Leveraging Intel AMT 9.0, the ThinkServer TS440 proved to be well suited for businesses with constrained budgets that may have little or no IT staff available, businesses that are using managed service providers to manage their overall environment, or businesses that need to manage servers located in remote locations.

A DAY IN THE LIFE OF AN IT ADMINISTRATOR

Whether you are a small business owner managing your own servers or a busy IT administrator, you juggle a wide range of tasks, such as keeping up with system maintenance, handling emergencies, and planning new upgrades. To simplify these common management tasks, administrators use systems management tools and server OOB management capabilities to remotely manage and monitor systems.

OOB management capabilities reduce the need for IT administrators to visit servers on-site, which in turn improves the efficiency and cost-effectiveness of their support. The Microsoft System Center 2012 suite provides support for several OOB management frameworks, including functions for the Intel AMT9.0 technology found in the Lenovo ThinkServer TS440, which enable efficient monitoring and management for local and remote systems. Figure 1 shows an example of the Microsoft System Center Configuration Manager (SCCM) interface used in our testing.

Figure 1: A management console, such as Microsoft SCCM 2012, enabled centralized management of the AMT 9.0-based OOB controllers found in the Lenovo ThinkServer TS440.



For example, the administrator can use AMT 9.0 alerting features and event logging for notification in the event of a server issue. The administrator can determine the status and configuration of the server and return a nonfunctioning server to an operational state using AMT 9.0 remote power controls and remote media. Alternatively, the administrator can verify BIOS settings, analyze underlying hardware issues, and collect the relevant component information needed to order replacement hardware.

In this report, we approached our eight IT management use cases for the Lenovo ThinkServer TS440 from the perspective of an IT administrator. See [Appendix A](#) for detailed information of our test system.

USE CASES WE TESTED

Overview

The following is an overview of the use cases we performed on the Lenovo ThinkServer TS440 in the Microsoft System Center environment:

- **Centralized configuration of AMT 9.0 for the management environment.** [Appendix B](#) provides details on the steps we used to configure the Lenovo ThinkServer TS440 for use with the management console.
- **Automated discovery.** We demonstrated automated discovery of AMT 9.0 in the Lenovo ThinkServer TS440 in SCCM.
- **AMT 9.0 Service monitoring and system events.** We added monitors in Microsoft Systems Center Operations Manager 2012 (SCOM) to notify us when the Lenovo ThinkServer TS440 Intel AMT 9.0 controller interacted with user sessions. We also simulated an unexpected system failure to demonstrate how AMT 9.0 enhances remediation of such problems.
- **Health monitoring.** We viewed health status indicators, including system information for the Lenovo ThinkServer TS440, from within SCOM and SCCM.
- **Power and media remote control.** We performed power-cycling operations, as well as boot device redirection, from SCCM.
- **Remote Keyboard, Video and Mouse (KVM) console.** Using the Intel vPro add-on for SCCM, we initiated remote KVM console sessions.
- **Boot media redirection and interactive diagnostics.** We launched remote media redirection, and performed interactive diagnostics.
- **System inventory.** We retrieved the inventory data reported by Intel AMT 9.0 from within SCCM and describe the information it reported.

Centralized configuration of AMT 9.0 for the management environment

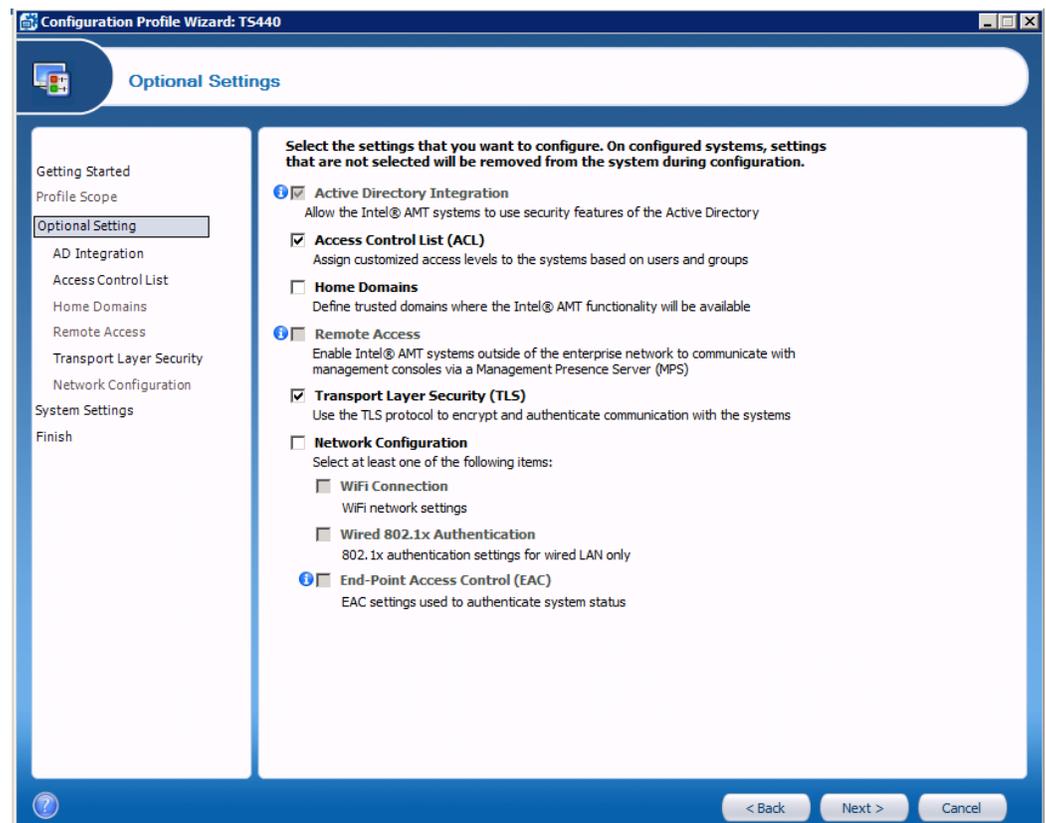
The Lenovo ThinkServer TS440 AMT 9.0 controller needs to be “provisioned” before it can be managed OOB using the Intel AMT 9.0 integrated features. Provisioning provides AMT 9.0 with the information about your network environment, security parameters for the kinds of access allowed on your network, and other relevant information needed for OOB management.

For this use case, we installed the Intel Setup and Configuration Software (SCS) 8.2 on our management server, which includes a configuration console (shown in Figure 2). We used SCS 8.2 to create a configuration profile with the necessary environment configuration settings.

Then, from within Microsoft Windows® on the Lenovo ThinkServer TS440, we executed an SCS Configurator command, which contacted the Remote Configuration Service and deployed our previously configured profile. This approach provided the server with the necessary security parameters and enabled OOB manageability of the Lenovo ThinkServer TS440 by SCCM.

For the step-by-step method, we used to configure the target server for OOB management, see [Appendix B](#).

Figure 2: We built a profile to provision AMT 9.0 on the Lenovo ThinkServer TS440 using Intel SCS 8.2.



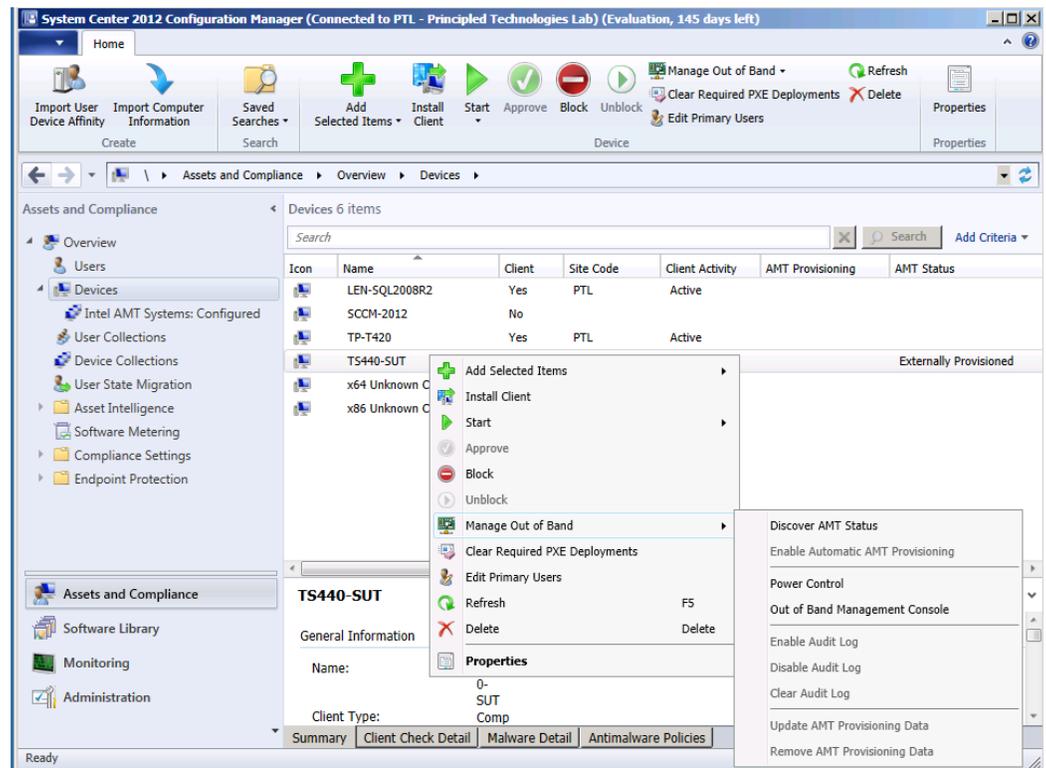
Automated discovery of the TS440 AMT 9.0 controller

After provisioning with the SCS tool, management tools such as SCCM can discover the Lenovo ThinkServer TS440 AMT 9.0 controller. SCCM and SCOM can use agents deployed within the operating system to gather detailed information about a managed system, including information about AMT 9.0, and to provide additional management capabilities.

We imported the target Lenovo ThinkServer TS440 into SCCM 2012 using the system name and mac address, and deployed the Configuration Manager client to the target system. Next, we selected the Lenovo ThinkServer TS440 target server in the SCCM console, right-clicked and selected Manage Out of Band from the menu, and clicked on Discover AMT Status. The Configuration Manager Client detected the controller and reported it to SCCM.

Figure 3 shows the automated discovery in SCCM. See [Appendix B](#) for a step-by-step walkthrough of discovery.

Figure 3: Discovery of the Lenovo ThinkServer TS440 Intel AMT 9.0 in SCCM.



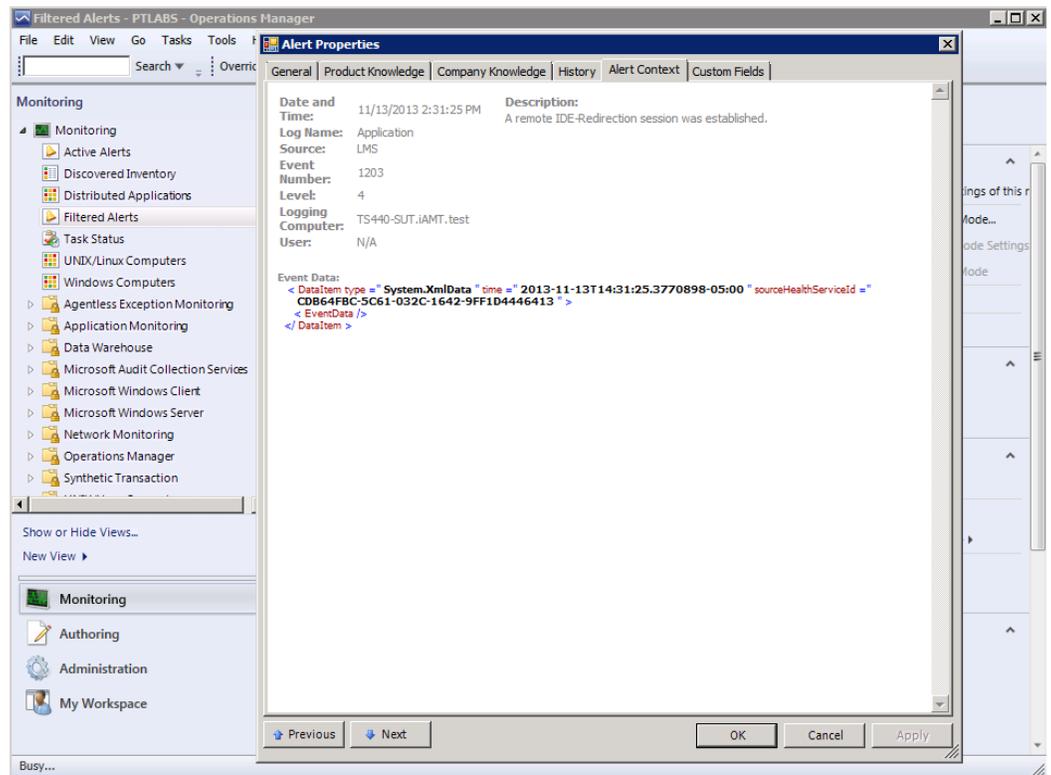
The Lenovo ThinkServer TS440 uses Intel AMT version 9.0, which means a few additional configuration steps are necessary, such as updating the AMT 9.0 status in SCCM and the SCCM database. See [Appendix B](#) for more details. In addition to adding the server to SCCM, we added our Lenovo ThinkServer TS440 to our SCOM console as a monitored server.

OOB service monitoring and system events

Before an administrator can resolve a server issue, they must receive notification of the issue. To simulate this use case, we configured monitoring, alerts, and simulated a system failure.

SCOM provides monitoring and alerting for a variety of events and applications, as well as server health and availability information. We configured an alert to inform us when AMT 9.0 in the Lenovo ThinkServer TS440 interacted with the Windows operating system and wrote an event to the application log via the Local Manageability Service (LMS), as shown in Figure 4. See [Appendix B](#) for details on how we configured monitoring in SCOM.

Figure 4: SCOM provided the framework to monitor events generated by the Intel LMS on the Lenovo ThinkServer TS440 and receive alerts and notifications about those events.



Next, we simulated an event in which the Windows Server operating system became unavailable in order to test the ability of the management and hardware stack – SCCM and SCOM, Intel AMT 9.0, and the Lenovo ThinkServer TS440 – to handle the unforeseen event.

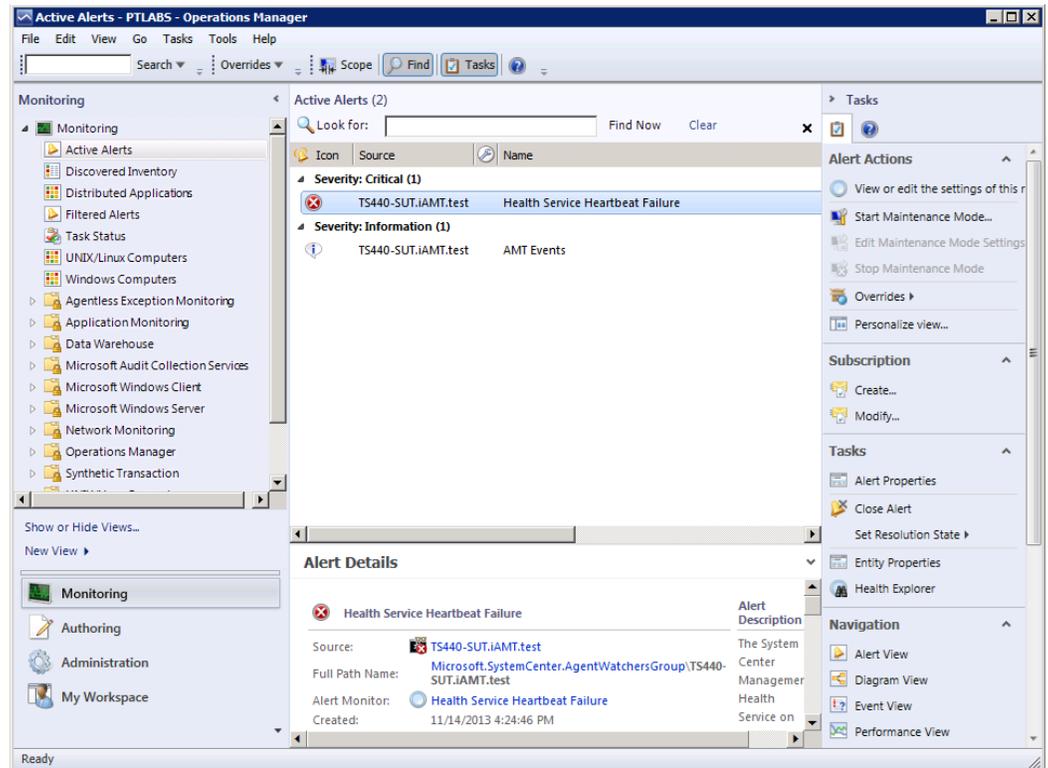
We changed the Startup and Recovery options for the server so that the server would not automatically reboot after a memory dump, ran the PowerShell CLI as Administrator, and executed the command:

```
PS C:\ get-process | stop-process -force
```

which immediately halted running Windows processes, created a memory-dump log, and rendered the operating system unavailable.

Within minutes, our SCOM console reported an alert indicating an issue with the monitored server, as seen in Figure 5. In our role as administrator, we had to investigate and return the server to operational.

Figure 5: SCOM alerted us about an issue with our target server.

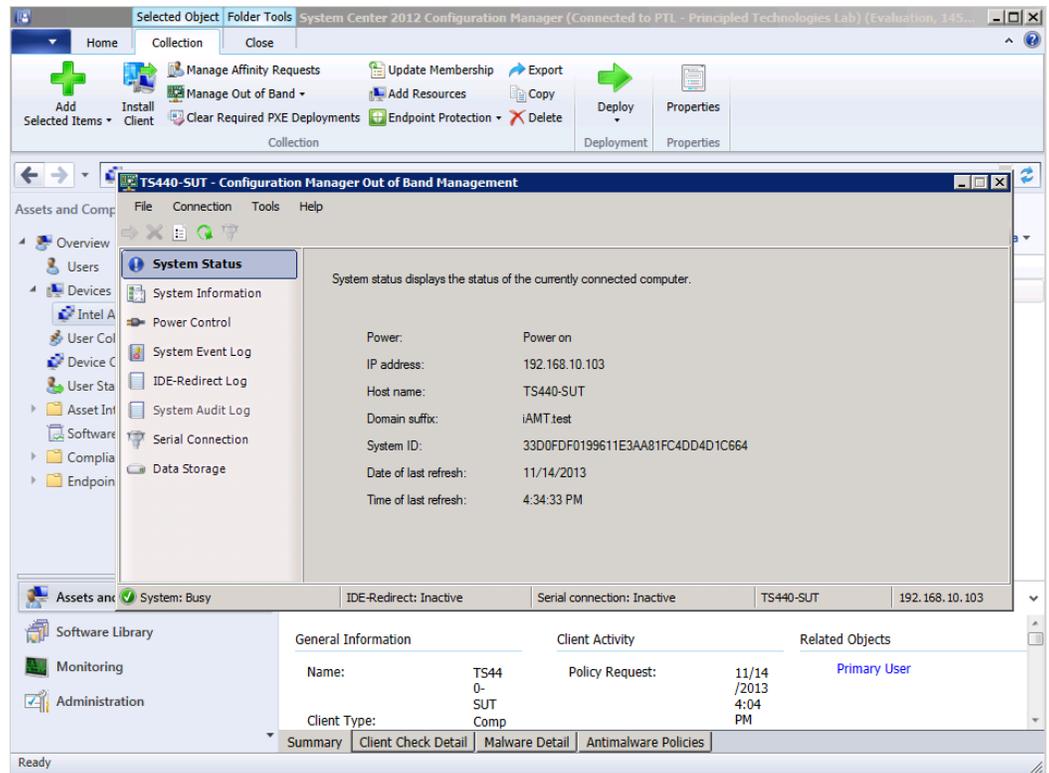


Health monitoring

In the previous use case, SCOM notified the administrator of the server with operating system issues. The next step for the administrator is to assess current system status and check the relevant event logs. When the server is not located on-site, the administrator can use the Lenovo ThinkServer TS440 OOB capabilities provided by Intel AMT 9.0.

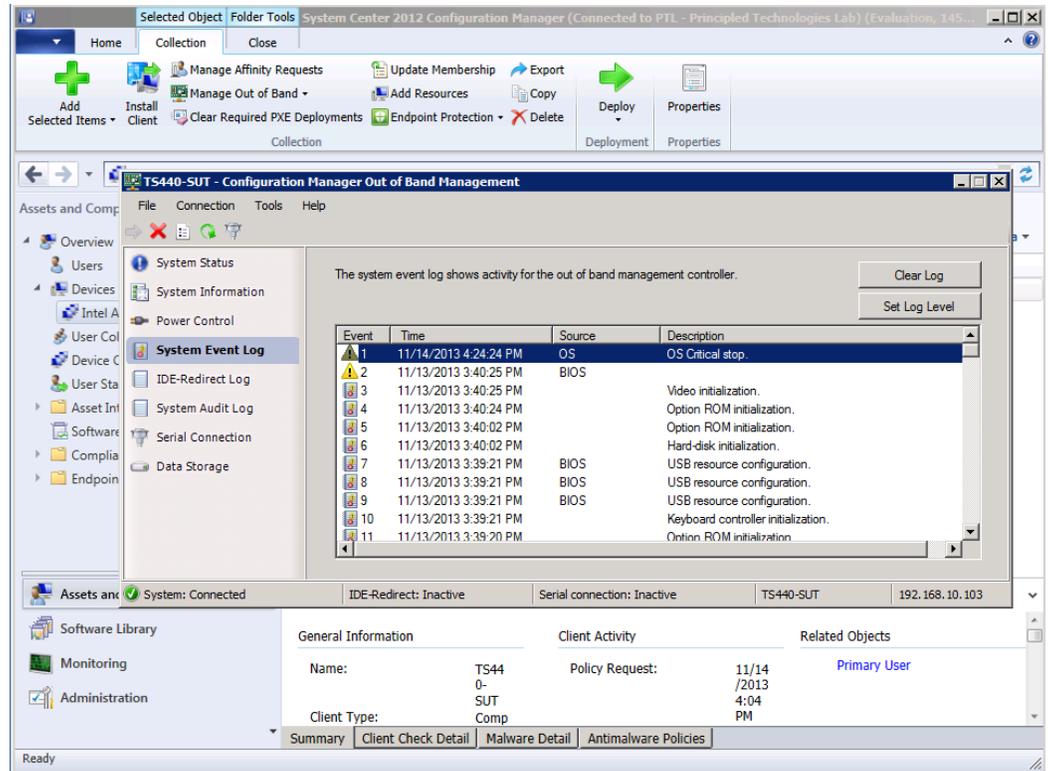
In this use case to assess system status, we launched the SCCM management console, and located the server in question. As the example in Figure 6 shows, we quickly verified the power state and other system information using SCCM to communicate directly with Intel AMT 9.0. We were able to verify that power was still available to the server and that the OOB management features were available. Access to this type of information will accelerate the troubleshooting process for administrators who may have limited site access.

Figure 6: SCCM provided a quick overview of the system status reported by Intel AMT 9.0 on the Lenovo ThinkServer TS440.



To view relevant event log information, we used SCCM to see system events logged by AMT 9.0 in the Lenovo ThinkServer TS440, as shown in Figure 7. These events are typically BIOS and management events that interact with AMT 9.0 and can be useful for troubleshooting system component problems or for viewing OOB management access information. We used the “verbose” log level to view all events.

Figure 7: SCCM provided event-logging details on system events reported by Intel AMT 9.0 on the Lenovo ThinkServer TS440.

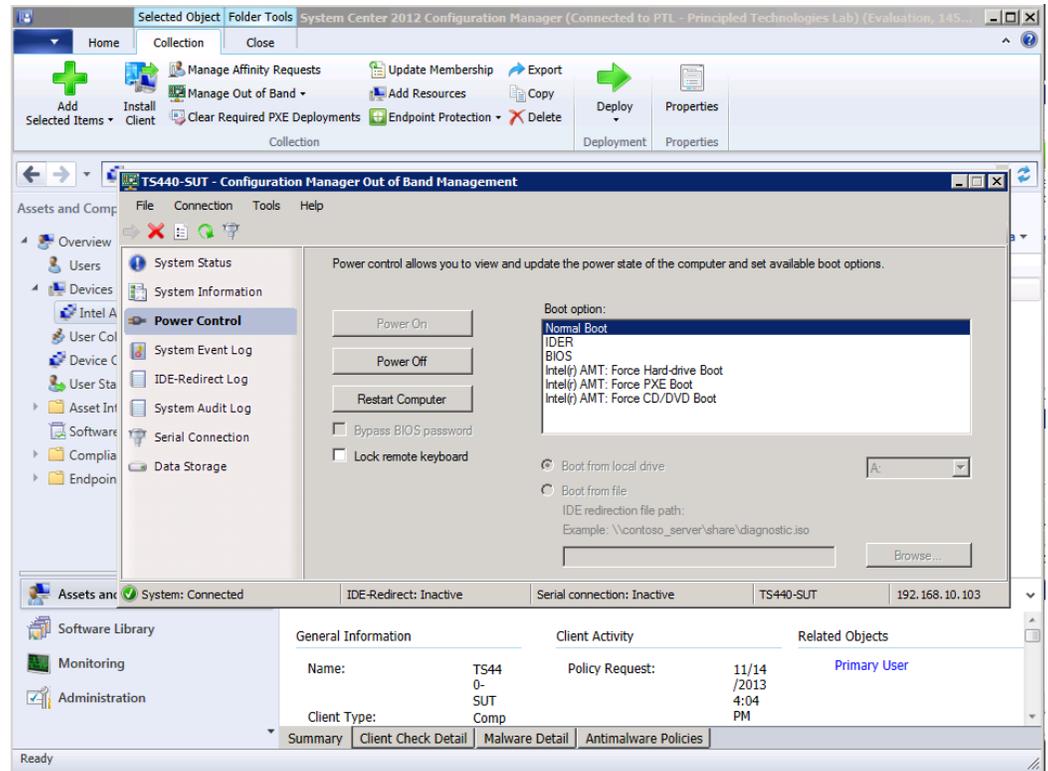


Power and media remote control functions

The ability to power on and off machines remotely is a critical feature of latest-generation servers and provides improved support efficiency and cost reductions since on-site visits are less necessary. In this use case, Intel AMT 9.0 and the Lenovo ThinkServer TS440 enabled us to execute remote control power functions from SCCM. In addition to being able to perform system resets via SCCM, in AMT 9.0 Intel added the “Graceful Shutdown” feature to their web client.

If a system reset does not correct the issue, the administrator can perform additional corrective actions using SCCM and AMT 9.0 in the Lenovo ThinkServer TS440, such as forcing the server to boot to a redirected media. An administrator can use this option to reimage a damaged operating system and prepare it for recovery from backup. OOB power controls are useful when a server is not responsive but it is not a replacement for a graceful OS-generated reboot or shutdown. Figure 8 shows an example of the available options.

Figure 8: The SCCM OOB management console provided a quick, menu-driven approach to performing remote power-cycle operations to the Lenovo ThinkServer TS440.

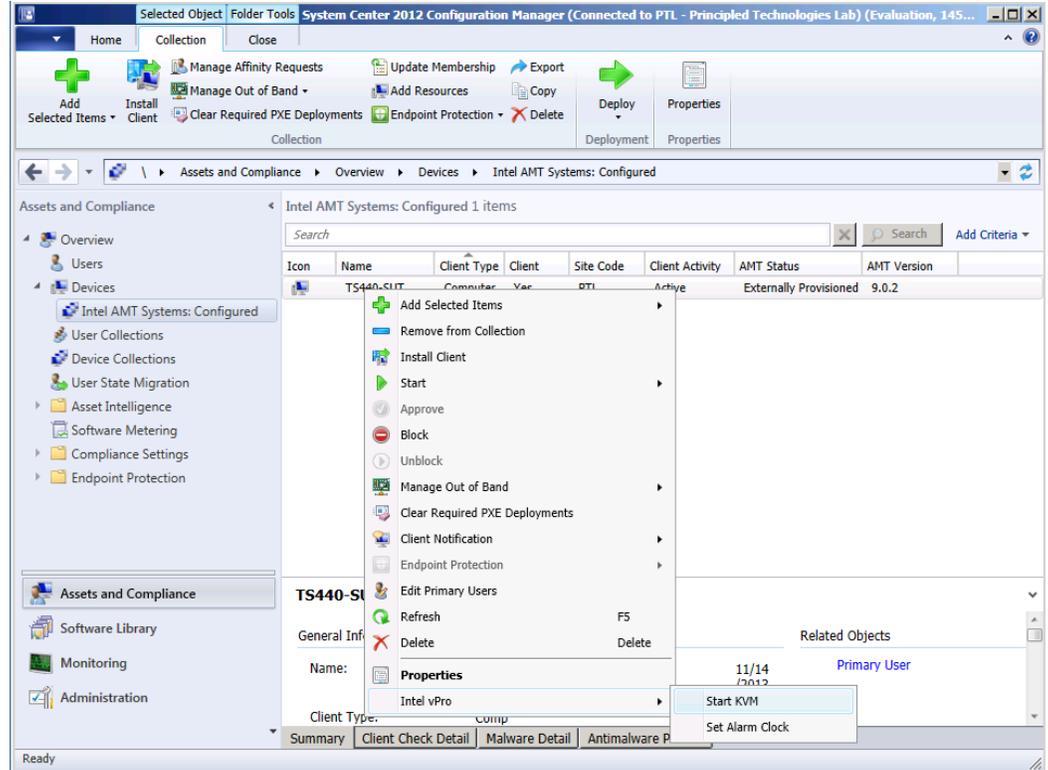


Remote KVM console

KVM sessions provide remote keyboard, monitor, and mouse functions even when the operating system is off. KVM sessions are critical to remote management because they allow the administrator to perform system configuration changes, such as altering hard-disk configurations, making BIOS changes, or performing hardware diagnostics without setting foot on-premises.

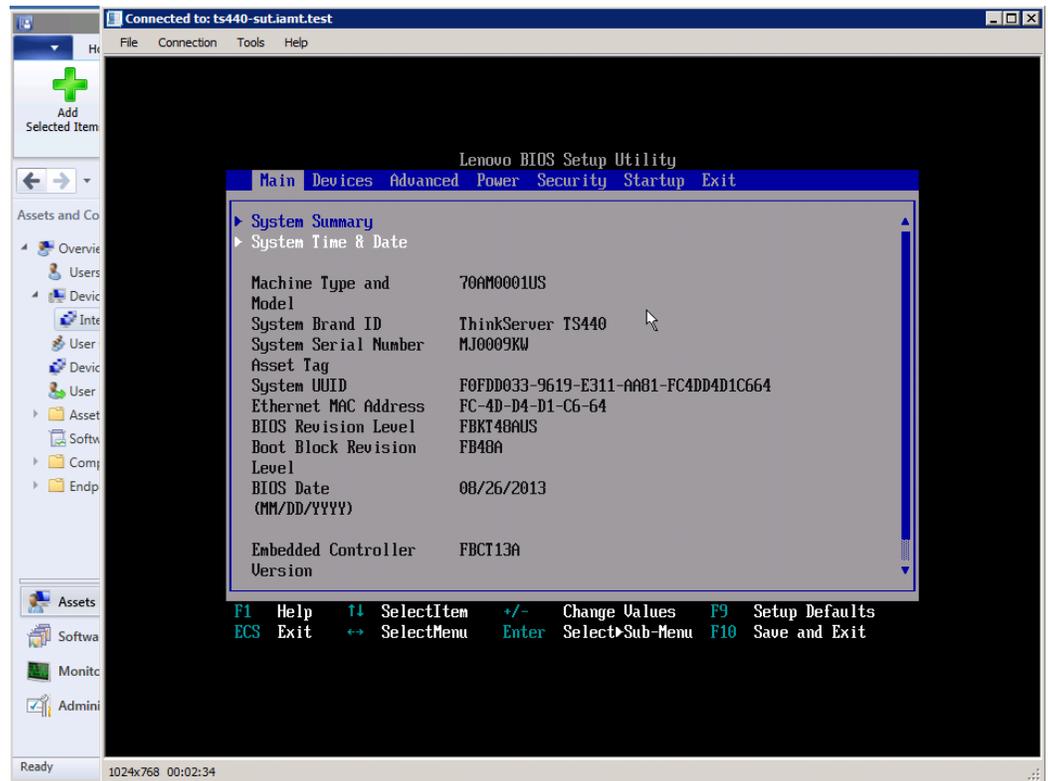
To test this use case, we used the Intel vPro add-on for SCCM, which adds a KVM client to the SCCM framework, providing an OOB console for the Lenovo ThinkServer TS440. We restarted the Lenovo ThinkServer TS440 again and then started a KVM session by right clicking the affected server and selecting Intel vPro→Start KVM, as seen in Figure 9. For details on installing the vPro add-on for SCCM, see [Appendix B](#).

Figure 9: The Intel vPro add-on for SCCM provided a remote KVM console connection for performing operations outside the operating system on the Lenovo ThinkServer TS440.



As shown in Figure 10, we used the remote KVM functionality to enter the BIOS Setup Utility, checked the system summary, verified devices, checked other settings, and continued with the reboot process.

Figure 10: The remote KVM session accessed the Intel AMT 9.0 features and interacted with the Lenovo ThinkServer TS440, even when the OS was not responding.



Boot media redirection and interactive diagnostics

In some cases, the administrator may need to use boot media redirection to perform diagnostics on the system. This is helpful in cases where manufacturers, in this case Lenovo, include diagnostics tools via ISO image or physical media and the maintenance must be performed off site.

To test this use case, we downloaded the latest diagnostics disc for the Lenovo ThinkServer TS440 from the Lenovo website, and saved the ISO file in a location accessible from our SCCM server. Using the Power Control feature of the SCCM OOB management console, we selected IDE Redirection (IDER) as the boot option, and clicked Restart Computer. Figure 11 shows SCCM using the IDER feature.

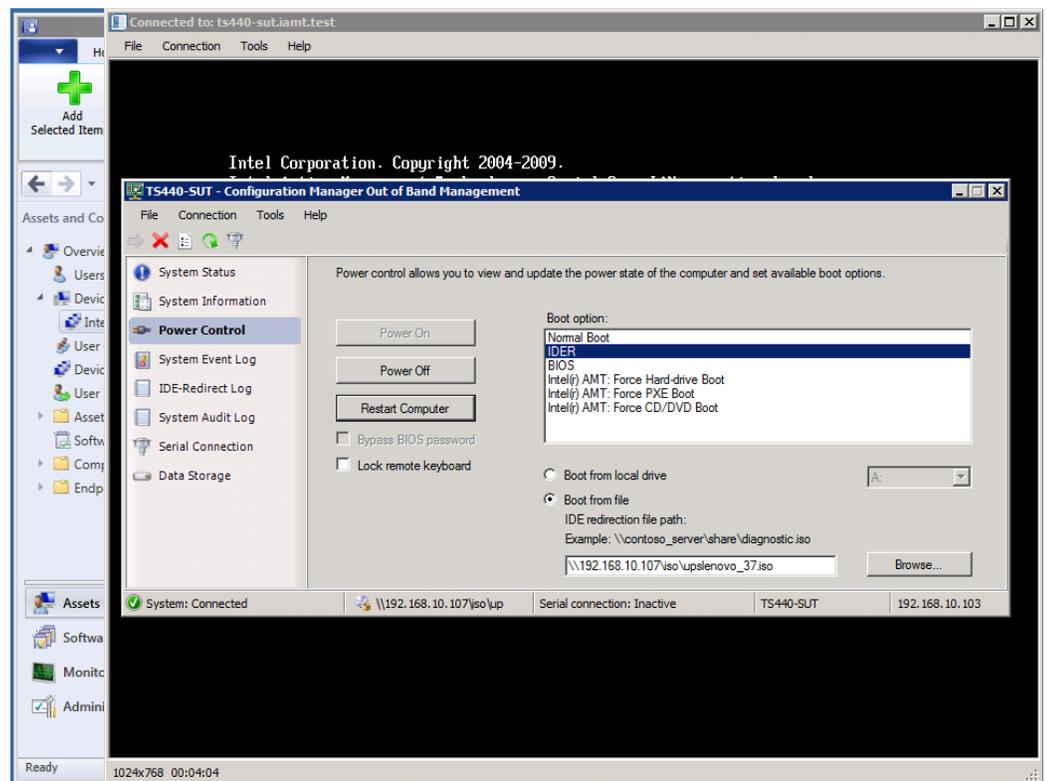
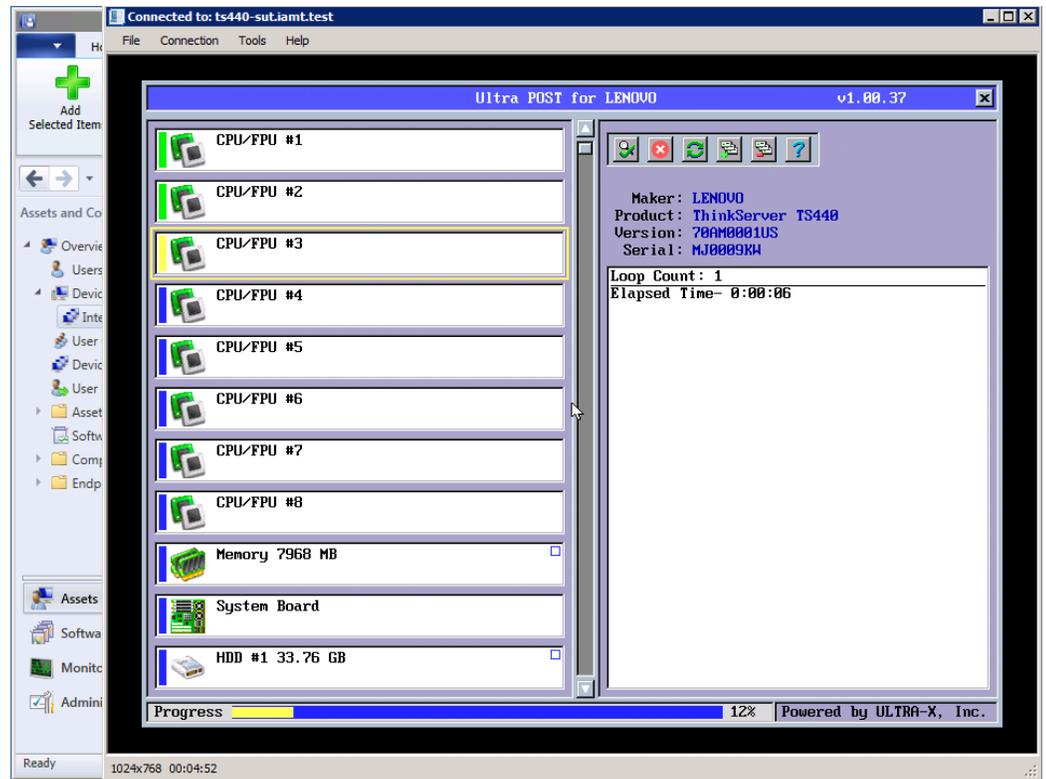


Figure 11: The IDER features of the Intel AMT 9.0 technology built into the Lenovo ThinkServer TS440 enabled many off-site investigative and corrective actions.

The Lenovo ThinkServer TS440 rebooted and loaded the diagnostics CD image as if it was physically present in the optical drive. We were able to then execute the necessary diagnostics tests, and gather information about each component, as seen in Figure 12.

Figure 12: Our administrator performed hardware diagnostics remotely using the Remote KVM and IDER Intel AMT 9.0 features built into the Lenovo ThinkServer TS440 OOB controller.

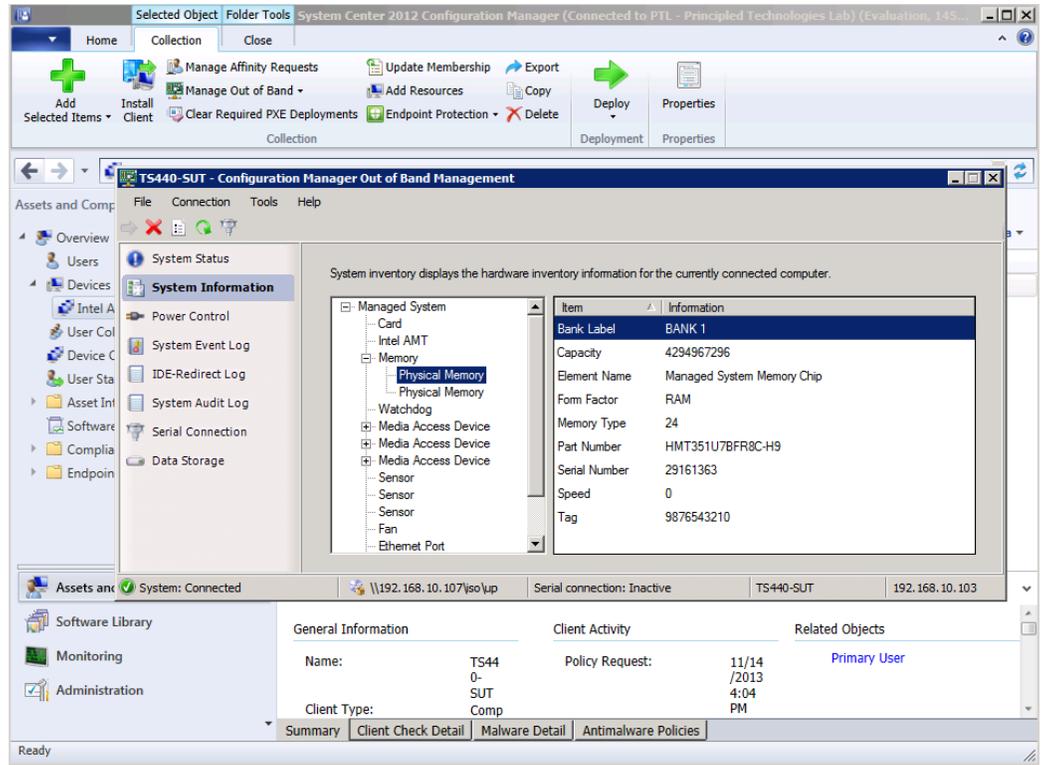


System inventory

Without the ability to assess component inventory on a system, an administrator may have to plan a site visit, and remove the server from operation in order to open it and then remove the part for identification. The SCCM OOB management console provides a view of system component information reported by the AMT 9.0 controller, preventing such maintenance hassle. We were able to pull the information directly from the affected system, expediting the simulated replacement process.

As seen in Figure 13, selecting an item such as a memory DIMM revealed detailed information including the specific part number, manufacturer, size and other relevant information.

Figure 13: The OOB management console in SCCM displayed a quick inventory of the Lenovo ThinkServer TS440 hardware components, as reported by the on-board AMT 9.0 OOB controller.



WHAT WE FOUND

The Lenovo ThinkServer TS440 leveraged the Intel AMT 9.0 integrated OOB technology with a third-party management console to successfully execute the selected eight management use cases, typical of those a systems administrator may perform for managed servers. The use cases and supporting components are shown in Figure 14.

Use Case	Available on the Lenovo ThinkServer TS440 with Intel AMT 9.0
OOB automated discovery	✓
Customized environment configurations	✓
Health and status monitoring	✓
System inventory	✓
System events tracking	✓
Remote power control	✓
Remote KVM access	✓
Remote diagnostics	✓

Figure 14: The Intel AMT 9.0 on the Lenovo ThinkServer TS440 provided OOB manageability in eight common use cases.

WHAT WE TESTED

About Lenovo ThinkServer TS440

With the Intel Xeon processor E3-1200 v3 product family, Lenovo designed the ThinkServer TS440 to be affordable, easy to expand, and easy to manage. The ThinkServer TS440 is ENERGY STAR-certified and offers scalability and remote manageability in a cost-effective, enterprise-class server solution for MSPs, branch offices, and small businesses. Memory features include ECC memory for reliability with capacities of up to 32GB. Storage features include an onboard storage controller with RAID capabilities and hot-swappable enterprise SAS or SATA drive options, with capacities of up to 32TB. Other expandability and redundancy features include up to nine 1Gb Ethernet ports, redundant power supplies, and four PCI/PCIe slots. According to Lenovo, the Lenovo ThinkServer TS440 is designed to run 24x7 and is certified for MSP support with many ecosystem vendors. Lenovo designed the chassis to reduce noise, and claims that the TS440's 33 decibels are 40 percent quieter than its predecessor.

For management, Lenovo offers tools for deployment, monitoring, and ongoing management. Using the latest Intel AMT 9.0, the TS440 provides out-of-band, remote management — regardless of the server's status. The TS440's Web console works directly out of the box, providing point-and-click management tools designed for branch offices or remote deployments with limited IT resources.

For more information, visit shop.lenovo.com/us/en/servers/thinkserver/ts-series/ts440/.

About Intel AMT 9.0

Intel AMT 9.0 for servers is a feature of selected Intel Xeon and Core i3 processors. Intel AMT 9.0 uses integrated platform capabilities and popular third-party management and security applications to allow for discovery, repair, and protection of networked computing assets, including PCs, workstations and servers, and features remote diagnosis and repair of these assets. It utilizes the same infrastructure and tools across platforms for management consistency.

About Microsoft System Center Configuration Manager 2012

Microsoft System Center 2012 is a management solution that allows you to manage your IT environment, including servers and client devices, from a unified platform. With System Center 2012, you can manage applications, multiple hypervisors, hardware, and resources from the same familiar management console.

Microsoft System Center Configuration Manager 2012 provides IT administrators with a solution that helps them maintain compliance with corporate

policy directives while providing employees with the capability to use their notebooks or tablets as they need to get work done. SCCM provides important management capabilities around:

- **Application delivery.** With a new user-centric approach to application delivery in SCCM 2012, Configuration Manager evaluates user identity, application dependencies, and device type to deliver the best experience for each user, no matter what device they use.
- **Device management.** Use the same unified management infrastructure to organize inventory, wipe devices remotely, or enforce pin codes for physical and virtual clients.
- **Security.** Configuration Manager manages System Center 2012 Endpoint Protection to ensure your infrastructure remains secure, Client compliance and remediation capabilities and antimalware features let you secure your client infrastructure from the same unified platform.

To learn more about Microsoft System Center Configuration Manager 2012, visit www.microsoft.com/en-us/server-cloud/system-center/configuration-manager-2012-overview.aspx.

About Microsoft System Operations Manager 2012

A component of Microsoft Systems Center 2012, System Center 2012 Operations Manager (SCOM 2012) enables IT administrators to monitor the health status, hardware, and performance information for many servers from a single management application. Additionally, SCOM 2012 features alerting capabilities for the tasks it monitors, including health status, performance, and hardware state information.

IN CONCLUSION

The Lenovo ThinkServer TS440 provides customers with a solid and cost-effective solution for server OOB management by utilizing the Intel AMT 9.0 technology built into the processors and chipsets. By combining this technology with a third-party system management console, businesses can significantly reduce the costs associated with server management add-ons without sacrificing the management features they need.

APPENDIX A – SYSTEM CONFIGURATION INFORMATION

Our test bed consisted of virtualized infrastructure servers hosted on a Lenovo ThinkServer RD530, and a single Lenovo ThinkServer TS440. The Lenovo ThinkServer TS440 had Windows Server 2012 Standard as its operating system. All virtual servers in our test bed ran Windows Server 2008 R2 Standard, except for the Enterprise Certificate Authority server, which required Windows Server 2008 R2 Enterprise. We patched all servers with the latest available updates. Figure 15 provides detailed configuration information for the test system.

System	Lenovo ThinkServer TS440
Power supplies	
Total number	1
Vendor and model number	Lenovo
Wattage of each (W)	405 W
Cooling fans	
Total number	2
Vendor and model number	AVC DS09225R12HP235
Dimensions (h x w) of each	92mm x 92mm
Volts	12V
Amps	.41 A
General	
Number of processor packages	1
Number of cores per processor	4
Number of hardware threads per core	2
System power management policy	N/A
CPU	
Vendor	Intel
Name	Xeon
Model number	E3-1275 v3
Stepping	C0
Socket type	LGA1150
Core frequency (GHz)	3.5
Bus frequency	5GT/s DMI
L1 cache	128k+128k
L2 cache	1 MB
L3 cache	8 MB
Platform	
Vendor and model number	Lenovo ThinkServer TS440
Motherboard model number	70AM0001US
BIOS name and version	Lenovo BIOS FBKT48A 0.0
BIOS settings	Default

System	Lenovo ThinkServer TS440
Memory module(s)	
Total RAM in system (GB)	8
Vendor and model number	Hynix HMT351U7BFR8C-H9
Type	DDR3
Speed (MHz)	1333
Speed running in the system (MHz)	1333
Timing/Latency (tCL-tRCD-tRP-tRASmin)	9-9-9-36
Size (GB)	4
Number of RAM module(s)	2
Chip organization	512Mx72
Rank	2
Operating system	
Name	Windows Server 2012
Build number	6.2.9200
File system	NTFS
Language	English
Graphics	
Vendor and model number	Intel HD Graphics P4600
Graphics memory (MB)	128 MB
Driver	9.18.10.3165
RAID controller	
Vendor and model number	LSI MegaRAID SAS 9240-8i
Firmware version	2.130.384-2291
Driver version	5.2.122.0
Hard drives	
Vendor and model number	Seagate® ST2000NM0033
Number of drives	2
Size (GB)	2 TB
RPM	7200
Type	SATA
Ethernet adapter	
Vendor and model number	Intel I217-LM
Type	Integrated 1Gbps
Driver	12.6.47.0
Optical drive(s)	
Vendor and model number	PLDS DH16ACSH
Type	DVD-RW
USB ports	
Number	6 / 2
Type	USB 3.0 / USB 2.0

Figure 15: Detailed information about our test system.

APPENDIX B –METHODOLOGY

We used the following steps to create our test environment. Our environment included one Windows 2008 R2 standard server for Active Directory, one for SQL 2008 R2, one for System Center 2012 SP1, and one Windows 2008 R2 Enterprise server used as an Enterprise Certification Authority. Additionally, we installed Windows Server 2012 on the Lenovo ThinkServer TS440.

Setting up the management server

Installing required Windows features and roles for System Center Configuration Manager

1. Log in to the System Center site server with domain\administrator.
2. Launch the Server Manager from the taskbar.
3. Click Add Features or Roles.
4. Click Next.
5. Click Next.
6. Select Web Server IIS.
7. Click Add Required Role Services.
8. Add Windows Software Update Services.
9. Run Windows Update, and install updates.
10. Register ASP.NET with IIS:
C:\Windows\Microsoft.NET\Framework64\v4.0.30319>aspnet_regiis.exe –r

Installing the Windows Assessment and Deployment Kit for Windows 8 Release Preview

1. Download the Windows Assessment and Deployment Kit for Windows 8 Release Preview from <http://www.microsoft.com/en-us/download/details.aspx?id=29929>
2. Run adksetup.exe.
3. Select Install the Assessment and Deployment Kit to this computer, and choose an installation path. Click Next.
4. Select No when prompted to join the Customer Experience Improvement Program (CEIP).
5. Accept the license agreement.
6. Select Deployment tools and Windows Preinstallation Environment features, and User State Migration. Click Install.
7. Click Close when the install finishes.

Extending the Active Directory schema

1. Log onto the Domain controller with an account that is a member of the Schema Admins security group.
2. Run \SMSSETUP\BIN\x64\extadsch.exe from the installation source to extend the AD schema.
3. Review extadsch.log in the root of the system drive to confirm the operation was successful.

Creating Active Directory accounts for System Center Configuration Manager

1. Log in to the Domain Controller using the domain\administrator account.
2. Create the following accounts and objects in Active Directory:
3. Create a global security group `Kerberos Admins`
4. Add Domain Admins group to the Kerberos Admins global security group.
5. Add the computer account of the SCCM server to the Kerberos Admins security group

6. Create an Organizational Unit for AMT managed systems `AMT`
7. Create a security group `AMT`
8. Add the Kerberos Admins group to the AMT security group.

Creating system management container and permissions

1. On the Active Directory server, run `adsiedit.msc`, and connect to the domain for the site server.
2. Expand the Domain `<computer FQDN>`, `<DN>`, right-click `CN=System`, click `New`, and click `Object`.
3. Select `Container`, and click `Next`.
4. In the `Value` field, type `System Management`. Click `Next`.
5. Click `Finish`.
6. Expand the site server's domain in the console pane.
7. Expand `DC=<server DN>`, and then expand `CN=System`.
8. Right-click `CN=System Management`, and then click `Properties`.
9. Click the `Security` tab, and click `Add` to the site server computer account.
10. Grant `Full Control` permissions.
11. Click `Advanced`, select the site server's computer account, and click `Edit`.
12. In the `Apply Onto` list, choose this object and all descendant objects.
13. Click `OK` to close `ADSI Edit`.

Configuring an enterprise certificate authority

1. Login to the Windows 2008 R2 Enterprise server designated for Certificate Authority as `domain\administrator`.
2. Launch `Server Manager`.
3. Select the menu item for `Roles`. Click `Add Roles`. Click `Next`.
4. Choose the option `Active Directory Certificate Services`. Click `Next`.
5. Click `Next`. Choose the option `Certification Authority`, and click `Next`.
6. Select `Enterprise` for the setup type, and click `Next`.
7. Choose `Root CA` for the CA type, and click `Next`.
8. Select `Create a New Private Key`, and click `Next`.
9. Accept all remaining defaults, and click `Next` through the remaining screens.
10. When prompted to begin installation, click `Install`.
11. To exit the wizard, click `Close`. Restart the server before continuing to the next steps.

Creating certificate templates for OOB management

1. Log in to the Windows 2008 R2 Enterprise server designated for Certificate Authority as `domain\administrator`.
2. Click `Start->Administrative Tools->Certification Authority`.
3. Right-click the `Certification Authority`, and click `Properties`.
4. On the `General` tab, click `View Certificate`.
5. On the `Details` tab, scroll to and select `Thumbprint`. Copy the 40-character code displayed in the details. You will add this information to the AMT BIOS later.
6. Click `OK` to close the certificate properties.
7. Click `Ok` to close the `Certification Authority` properties.

8. Expand the Certification Authority, and select Certificate Templates.
9. Right-click Certificate Templates, and select Manage.
10. Locate Web Server in the list of available certificate templates. Right-click the template, and select Duplicate Template.
11. Select Windows 2003 Enterprise, and click OK.
12. Change the template name to AMT Provisioning.
13. On the Subject Name tab, select Build from this Active Directory Information. Select Common Name, and choose the option UPN.
14. On the Security tab, add the security group you created for your SCCM site servers. Add the Enroll permission for the security group. Ensure Domain Admins and Enterprise Admins have Enroll permissions.
15. On the Extensions tab, select Application Policies, and click Edit.
16. Click Add. Click New. Type `AMT Provisioning` for the name, and `2.16.840.1.113741.1.2.3` as the Object Identifier. Click OK.
17. Ensure AMT Provisioning and Server Authentication are listed, and click OK.
18. Click OK to close the template properties.
19. Right-click the web server template, and select Duplicate Template.
20. Select Windows 2003 Enterprise, and click OK.
21. Change the template name to `AMT Web Server Certificate Template`
22. On the general tab, choose the option Publish Certificate in Active Directory.
23. On the Subject Name tab, select Supply in the request.
24. On the Security tab, ensure Domain Admins and Enterprise Admins have Enroll permissions.
25. Click OK to close the template properties.
26. Log in to the management server as `domain\administrator`.
27. Click Start→Run. Type `mmc` and press Enter.
28. In the mmc console, click File→Add/Remove Snap-in...
29. Select Certificates, and click Add. Select Computer account. Click Next.
30. Select Local computer, and click Finish.
31. Click OK.
32. Expand Certificates→Personal→Certificates.
33. In the right panel, click More Actions→All Tasks→Request a new certificate...
34. Click Next.
35. Accept the defaults, and click Next.
36. Select the new AMT Provisioning certificate. Click Enroll.
37. Click Close.

Installing System Center Configuration Manager 2012 SP1

1. Copy the SCCM installation folder to the local computer.
2. Open splash.hta.
3. Click Install.

4. Read the Before You Begin section, click Next.
5. Choose Install a primary site. Do not choose the typical options.
6. Choose the Evaluation option, or enter your license key. Click Next.
7. Click to accept the EULA, and click Next.
8. Accept the license agreements, and click Next.
9. Enter a path for the prerequisite file downloads. We used C:\Downloads.
10. Select a language, and click Next for both server and client.
11. Enter a site code for the primary site. We used PTL.
12. Enter a description.
13. Choose an install path. We accepted the default install path.
14. Ensure that the console will be installed, and click Next.
15. Install as a primary stand-alone site.
16. Enter the SQL server name and instance, and click Next.
17. Accept the default SMS provider, and click Next.
18. Select the option to configure the communication method on each site system role.
19. Select HTTPS, and click Next.
20. Select HTTP for Management Point and Distribution point, and click Next.
21. Enable CEIP if you wish to participate, and click Next.
22. Run the prerequisites check, and resolve any issues displayed.
23. Click Begin Install, and click Close when the installation is complete.
24. Update the installation upon completion.

Adding site system roles for OOB management

1. Open the Configuration Manager console.
2. Click Administration in the lower left panel of the console.
3. Expand Site Configuration. Select Sites.
4. Right-click the management server, and select Add Site System Roles.
5. Click Next.
6. Accept the default for Proxy, and click Next.
7. From the list of available roles, choose the options Enrollment point and Out of band service point. Click next.
8. Accept the defaults for the AMT Service Point, and click Next.
9. Click Browse to select the AMT provisioning certificate you created in the previous steps.
10. Clear the checkbox for Enable CRL checking for the AMT provisioning certificate. Click Next.
11. Accept the defaults for the enrollment point, and click Next.
12. Review the summary, and click Next.
13. Click Close to exit the wizard.

Installing System Center Operations Manager 2012 SP1

1. Copy the SCOM installation folder to the desktop, and run setup.exe.
2. Click Install.

3. Click the following options:
 - a. Management Server
 - b. Operations Console
4. Accept the default installation path, and click Next.
5. If there are Prerequisite error messages, remedy them and then continue.
6. On the Proceed with Setup screen, click Next.
7. On the Specify an Installation screen, create the first management server in the management group.
8. Name the management group, and click Next.
9. Accept the license agreement, and click Next.
10. On the Configure the Operational Database screen, enter the SQL database server name and instance.
11. Leave the database size, and database and log location settings at their defaults. Click Next.
12. On the Configure the Data Warehouse Database, enter the SQL database server name and instance.
13. Leave the database size, and database and log location settings at their defaults. Click Next.
14. On the Accounts screen, select Domain Account for all services.
15. Enter the domain administrator. Click Next.
16. Select whether or not to participate in CEIP.
17. On the Microsoft Update screen, enable updates. Click Next.
18. Click Install.
19. Once install is complete, close the installer, and run updates.

Installing Intel vPro add-on for System Center Configuration Manager

1. Download the Intel Core™vPro processor add-on for System Center Configuration Manager from downloadcenter.intel.com/Detail_Desc.aspx?agr=Y&DwnldID=21835&lang=eng
2. Extract the downloaded zip file to a location on your SCCM server. We used c:\IntelvProSCCMAddOn-v2.
3. Browse to c:\IntelvProSCCMAddOn-v2\x64\, and double-click setup.
4. Select I Agree, and click Next.
5. Accept the default installation location. Select Everyone, and click Next.
6. Click Next to begin installation.
7. Click Close.

Installing Intel SCS 8.2

1. Download IntelSCS_8.2.zip. Extract the contents to C:\IntelSCS_8.2.
2. Browse to C:\IntelSCS_8.2\IntelSCS\RCS.
3. Double-click IntelSCSInstaller.exe
4. Check the boxes for Database, Service, and Console. Click Next.
5. Select I accept the terms of the license agreement, and click Next.
6. Enter the credentials of the Domain account that will run the service. We used domain\administrator. Click next.
7. Select the SQL server you want to use for the SCS database. This information may populate automatically. Click next.

8. For Installer SQL Server Authentication, select Windows authentication (integrated security), and click Next.
9. For Service SQL Server Authentication, select Windows authentication (integrated security), and click Next.
10. Review and confirm the setup information, and click Install.
11. Click Finish.

Deploying Configuration Manager and Operations Manager agents

1. Launch the Configuration Manager Console
2. Select Assets and Compliance. Expand Overview→Devices.
3. In the Home menu, click Import Computer Information.
4. Select Import single computer
5. Enter the Computer name and the MAC address of the target server. Click Next.
6. Click Next. Select Add computers to the All Systems Collection. Click Next.
7. Review the Summary, and click Next.
8. Click Close to finish.
9. Right-click on the newly imported server. Select Install Client. Click Next.
10. Choose all three client push options, and click Next.
11. Review the Summary, and click Next.
12. Review the status messages, and click Close.
13. Launch the Operations Manager Console.
14. Click Administration in the lower left corner of the console.
15. Click Discovery Wizard...
16. Select Windows Computers. Click Next.
17. Select Automatic computer discovery. Click Next.
18. Select Other user account. Enter the credentials for a Domain Administrator. Click Discover.
19. Choose the device you want to manage. Click Next.
20. Under Agent Action Account, select Other, and provide a domain account with administrative access to the target computer. We used domain\administrator. Click Next.
21. Click Close. The health state will change to Healthy when the agent deployment and configuration is complete.

Setting up AMT provisioning with Intel SCS Remote Configuration Service

Creating the configuration profile

1. Launch the Intel Setup and Configuration Console.
2. Click the Profiles button.
3. Click the New button to construct a profile for deployment.
4. For Profile Name, enter the name of your target server. We used TS440-SUT. Click Next
5. Choose the options Active Directory Integration, Access Control List (ACL), and Transport Layer Security (TLS) and click Next.
6. Browse for the OU created for the AMT managed devices. We used OU=AMT,DC=iAMT,DC=test. Click Next.
7. Click Add.
8. Select Active Directory User/Group. Click Browse.

9. Add Kerberos Admin, Domain Admins, or other administrative users groups. Click OK.
10. Select Remote for Access Type.
11. Choose the option for PT Administration. Click Ok.
12. Click Next.
13. Select your Enterprise Certificate Authority.
14. Select the Server Certificate Template you will use to generate certificates for your AMT devices. We selected AMTWebServerCertificate. Click Next.
15. Choose the options Web UI, Serial Over LAN, IDE Redirection, KVM Redirection. Enter the RFB Password for KVM sessions. We used Pa\$\$w0rd.
16. Enter the MEBios Extension password. We used Password1!.
17. Select Use the following password for all systems:. Enter the password for use after provisioning is complete. We used Password1!.
18. Choose the options Enable Intel AMT to respond to ping requests and Enable Fast Call for Help (within the enterprise network).
19. Click Set... to Edit IP and FQDN settings.
20. Select Use the following as the FQDN, and choose Primary DNS FQDN from the pull-down menu.
21. Choose the option The device and the OS will have the same FQDN (Shared FQDN).
22. Select Get the IP from the DHCP server.
23. Select Update the DNS directly or via DHCP option 81. Click OK.
24. Click Next. Click Finish.

Adding the enterprise certificate authority to the AMT trusted root certification authorities

1. Reboot the target server.
2. During POST, press CTRL-P to enter the Intel Management Engine BIOS settings
3. When prompted for a password, type the default password `admin`.
4. Provide and confirm a new password (required). We used Password1!
5. Select Intel AMT Configuration. Press Enter.
6. Select Remote Setup and Configuration. Press Enter.
7. Select TLS PKI. Press Enter.
8. Select PKI DNS Suffix. Press Enter.
9. Type the FQDN suffix. We used `iamt.test`. Press Enter.
10. Select Manage Hashes. Press Enter.
11. Press Insert to add a new hash.
12. Enter a descriptive name for your Enterprise Certificate Authority. We used `iAMT.test CA`. Press Enter.
13. Following the syntax example provided in the prompt, enter the 40-character thumbprint previously copied from your Enterprise CA root certificate. Press Enter.
14. Press `y` to set the hash certificate as active. `iAMT.test CA` will appear in the list of trusted root authorities. To exit, press `Esc` until prompted. Press `y` to confirm exit.

Executing the remote configuration script on the AMT managed host

1. Log in to the AMT managed target server as domain\administrator.
2. Copy the \Configurator folder from the SCS_8.2 directory located on your Management Server (SCCM-2012) to C:\ on the local host.
3. Open a command prompt.
4. Type `cd C:\Configurator` and press Enter.
5. Execute the following command (where sccm-2012.iamt.test is the fully qualified domain name of our management server:

```
ACUConfig.exe /lowsecurity /output console /verbose ConfigViaRCSOnly sccm-2012.iamt.test TS440-SUT
```
6. The Configurator utility will contact the Remote Configuration Service and apply the settings configured in the TS440-SUT profile.

Setting up AMT discovery in SCCM

1. Open the SCCM Management Console. Locate your target server in the Devices panel.
2. Right-click the headings bar in the Devices panel. Check the entries for AMT Status and AMT Version.
3. Right-click the server, and select Manage Out of Band → Discover AMT Status. Click OK to begin discovery.
4. Click refresh in the Home menu at the top of the panel.
5. When the AMT Status for the target server displays Detected, the AMT controller has been discovered.

Adjusting entry in SCCM Database

1. Log on to the SQL server using administrative credentials. We used domain\administrator.
2. Launch SQL Server Management Studio.
3. Click Connect.
4. In Object Explorer, expand Databases, and locate your configuration manager database. Our database is named CM_PTL.
5. Expand the database → Tables, and select dbo.System_DISC.
6. Right-click and select Edit Top 200 rows.
7. Locate the entry for your target server. Scroll to the column for AMTStatus0. The cell should show 1. Click that cell, and replace 1 with 4. Press Enter.
8. To execute SQL, click the red exclamation mark at the top of the object explorer.
9. At the top menu, select File → Save All.
10. Close the SQL Server management studio.

Refreshing the status in SCCM

1. In the SCCM console, refresh the devices panel. The AMT Status will change to Externally Provisioned. The Out of Band Management console is now enabled for your target server.

Monitoring Intel LMS service in SCOM

1. Open the SCOM console.
2. In the lower left panel of the console, click Authoring.
3. Expand Management Pack Objects → Monitors.
4. In the list of monitors in the right pane, expand Windows Computer → Entity Health → Security.

5. Right-click on Security, and select Create a Monitor→Unit Monitor.
6. Expand Windows Events→Simple Event Detection→Timer Reset.
7. Select the Default Management Pack from the pull-down menu, and click Next.
8. Enter a descriptive name, such as AMT Event Reporter. Click Next.
9. Verify the Application Log is selected, and click Next.
10. Select the entry for Event ID. Click Delete at the top of the pane.
11. For the Event Source parameter, change the Operator to Contains, and type LMS into the value field. Click Next.
12. Accept the default for wait time, and click Next.
13. Accept the defaults for Configure Health, and click Next.
14. Choose the option for Generate alerts for this monitor.
15. Deselect the option Automatically resolve the alert when the monitor returns to a healthy state.
16. Choose the Alert description field.
17. Delete the text in the value field. Click Data→Event Description. Click Ok.
18. Select Information in the Severity pull-down menu. Click Create.

ABOUT PRINCIPLED TECHNOLOGIES



Principled Technologies, Inc.
1007 Slater Road, Suite 300
Durham, NC, 27703
www.principledtechnologies.com

We provide industry-leading technology assessment and fact-based marketing services. We bring to every assignment extensive experience with and expertise in all aspects of technology testing and analysis, from researching new technologies, to developing new methodologies, to testing with existing and new tools.

When the assessment is complete, we know how to present the results to a broad range of target audiences. We provide our clients with the materials they need, from market-focused data to use in their own collateral to custom sales aids, such as test reports, performance assessments, and white papers. Every document reflects the results of our trusted independent analysis.

We provide customized services that focus on our clients' individual requirements. Whether the technology involves hardware, software, Web sites, or services, we offer the experience, expertise, and tools to help our clients assess how it will fare against its competition, its performance, its market readiness, and its quality and reliability.

Our founders, Mark L. Van Name and Bill Catchings, have worked together in technology assessment for over 20 years. As journalists, they published over a thousand articles on a wide array of technology subjects. They created and led the Ziff-Davis Benchmark Operation, which developed such industry-standard benchmarks as Ziff Davis Media's Winstone and WebBench. They founded and led eTesting Labs, and after the acquisition of that company by Lionbridge Technologies were the head and CTO of VeriTest.

Principled Technologies is a registered trademark of Principled Technologies, Inc.
All other product names are the trademarks of their respective owners.

Disclaimer of Warranties; Limitation of Liability:

PRINCIPLED TECHNOLOGIES, INC. HAS MADE REASONABLE EFFORTS TO ENSURE THE ACCURACY AND VALIDITY OF ITS TESTING, HOWEVER, PRINCIPLED TECHNOLOGIES, INC. SPECIFICALLY DISCLAIMS ANY WARRANTY, EXPRESSED OR IMPLIED, RELATING TO THE TEST RESULTS AND ANALYSIS, THEIR ACCURACY, COMPLETENESS OR QUALITY, INCLUDING ANY IMPLIED WARRANTY OF FITNESS FOR ANY PARTICULAR PURPOSE. ALL PERSONS OR ENTITIES RELYING ON THE RESULTS OF ANY TESTING DO SO AT THEIR OWN RISK, AND AGREE THAT PRINCIPLED TECHNOLOGIES, INC., ITS EMPLOYEES AND ITS SUBCONTRACTORS SHALL HAVE NO LIABILITY WHATSOEVER FROM ANY CLAIM OF LOSS OR DAMAGE ON ACCOUNT OF ANY ALLEGED ERROR OR DEFECT IN ANY TESTING PROCEDURE OR RESULT.

IN NO EVENT SHALL PRINCIPLED TECHNOLOGIES, INC. BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH ITS TESTING, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL PRINCIPLED TECHNOLOGIES, INC.'S LIABILITY, INCLUDING FOR DIRECT DAMAGES, EXCEED THE AMOUNTS PAID IN CONNECTION WITH PRINCIPLED TECHNOLOGIES, INC.'S TESTING. CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES ARE AS SET FORTH HEREIN.
