IT@Intel White Paper

Intel IT

Mobile PCs with Intel® vPro™ Technology

April 2012

Configuration Tips for Managing Mobile PCs with Intel® vPro™ Technology

By integrating the use of Intel® Setup and Configuration Software with our client management console solution, with Intel® Active Management Technology we are now able to successfully perform a number of critical maintenance tasks remotely on our mobile PC fleet.

Executive Overview

To improve our ability to use certain remote management features of Intel® Active Management Technology (Intel® AMT), a component of Intel® vPro™ technology, Intel IT worked with Intel's software development team to develop ways to enhance Intel® Setup and Configuration Software (Intel® SCS), a tool used with Intel AMT. By combining the updated version that resulted, Intel® SCS 7, with our existing client management console, we created a highly available, agile configuration and maintenance environment for our mobile systems. This solution improves our ability to configure and maintain mobile PCs on demand with Intel AMT and keep them configured throughout their on-the-go life cycles for our customers.

By integrating the use of Intel SCS with our client management console solution, with Intel® Active Management Technology we are now able to successfully perform a number of critical maintenance tasks remotely on our mobile PC fleet. For example, we are now using:

- Built-in Intel SCS maintenance commands to perform clock synchronization and reissue certificates.
- The Intel SCS reconfigure command, with some additional functionality added through our own coding, to resolve hostname mismatches.
- Our management console to push periodic firmware and software updates that improve overall stability of the mobile PCs.

Additionally, through the integration of Intel SCS and our management console, our technicians now have a fast, efficient configuring tool to use when configuring new and refurbished mobile PCs with Intel AMT.

Our success in keeping mobile PCs continuously configured for remote management with Intel AMT is leading us to look into more use cases for Intel vPro technology, increasing its value to Intel and our Service Desk.

Omer Livne
vPro AMT Product Manager, Intel IT

Ziv Balshai
AMT Firmware and Software Engineering Lead, Intel Architecture Group

Contents

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BACKGROUND

Intel's worldwide computing environment includes more than 109,000 PCs. More than 80 percent of them are mobile PCs that connect wirelessly to our network. In 2006, Intel developed Intel® vPro™ technology, a set of technologies built into the PC's hardware, to provide hardware-based security, manageability, and virtualization features. Recognizing Intel vPro technology's significant business value, more than four years ago Intel IT made a strategic decision to standardize its computing platform on laptop and desktop PCs that have Intel® Core™ processors with Intel vPro technology.

A component of the 2nd generation Intel® Core™ vPro™ processor family, Intel vPro technology is a combination of processor technologies, hardware enhancements, management features, and security technologies that allow remote access to a PC. Since its implementation, Intel vPro technology has become vitally important to us as a core capability for improving system defense, asset discovery, remote builds, virtualized client usages, and device-independent computing. By configuring Intel vPro technology across our highly mobile fleet, we help to improve mobile PC support, business continuity, and employee productivity.

Another key capability is Intel vPro technology's out-of-band (OOB) manageability and security component Intel® Active Management Technology (Intel® AMT). Intel AMT's OOB system, which operates out of firmware and establishes a secure communication channel, enables the control of clients from a level below the OS in a pre-boot environment. This makes client management less susceptible to issues that affect the OS and allows remote access to the PC regardless of the system's power state or OS condition. In fact, many of our mobile PCs have versions of Intel AMT that enable remote Keyboard-Video-Mouse (KVM) control capabilities, and we're adding more to their ranks through our two- to four-year PC refresh cadence.

Intel AMT-enabled clients allow our Service Desk staff to take control of a remote PC quickly.

- Unlock encrypted drives
- Manage data security settings
- Troubleshoot and repair many hardware and software issues
- Use the Integrated Drive Electronics Redirection feature to boot from an ISO image, OS build, remote drive share, or Windows* preinstallation environment.

Overall we estimate significant savings every year from Intel vPro technology's remote repair and management capabilities. A large part of these savings comes from reducing costly desk-side visits. For example, we routinely use Intel AMT to take control of PCs using KVM, to set up and manage self-encrypting drives (SEDs), and to reset security passphrases. This helps keep support costs down, resolves user issues more quickly, and helps maintain high employee productivity.

BUSINESS CHALLENGE

Our decision to standardize our computing platform on PCs with Intel vPro technology continues to deliver many security, manageability, and cost benefits. We continue to improve our management console to expand our ability to use Intel AMT in our wireless environment.

In order to use Intel AMT, we first configure PCs with Intel vPro technology over a wired LAN.[1] Once configured, these systems must be regularly accessed to perform trust-related maintenance, such as clock synchronization, password reset, and firmware updates.

[1] There is an option to configure Intel® Active Management Technology in Client Control Mode over a wireless LAN, but for greater control over the process, we don't use that feature.

These services are fully supported on a stationary network connection where PCs always have the same IP address. However remotely managing and reconfiguring systems in a mobile work environment can present challenges, including dealing with the following:

- **IP addresses that frequently change.** This may occur as users move around an office building, connect at home, or use private or public hotspots. In this situation, the PC discovery process may attempt to communicate with the mobile PC using the IP address recorded in the management database but may be unable to connect because a different IP address is in use.
- **Multiple IP addresses in use at the same time.** This can happen when a mobile PC is connected to both a wired and wireless connection, and perhaps even through a VPN adapter. The client discovery process can miss the client because an IP address is in use that is different from the one last reported.

Challenges related to managing a large mobile workforce environment can also arise.

- **Hostname mismatch between the name of the host and the name of the Intel® Management Engine (Intel® ME).** Intel® ME is built into an Intel vPro technology-based PC's hardware and firmware. Hostname mismatches can result from the PC repair process where a user's hard drive is inserted into a new laptop. They can also occur when an old laptop receives a new hard drive, is issued to a different employee, and receives a new hostname. In the first scenario, placing a hard drive in a new system creates a mismatch between the OS hostname and the Intel ME hostname. In the second scenario, giving a repaired system to a new user creates a mismatch by changing the fully qualified domain name, which uniquely identifies a device by specifying its exact location in the tree hierarchy of the Domain Name System (DNS).
- **Out-of-sync clocks and out-of-date Intel AMT certificates.** The Intel ME protected real-time clock is important for the date and time checks required for certain types of authentication, time stamps for events and logging, and maintaining alarms for the Alarm Clock feature. Thus it needs to synchronize periodically with a server's time. We also found that periodically reissuing certificates is an important best practice for maintaining trust.

The IP address challenges and hostname mismatches we were experiencing in our mobile PC fleet frequently made it difficult to maintain best practices and, in turn, the out-of-sync clocks and out-of-date certificates made it difficult to authenticate and maintain trust with a number of systems.

A Deeper Look at Hostname Mismatches

When a PC configured for the dynamic host configuration protocol (DHCP) wants to connect to a network, the PC sends a broadcast query requesting necessary information from a DHCP server. The DHCP server manages a pool of IP addresses and information about PC configuration parameters, such as default gateway, domain name, name servers, and time servers. After receiving a valid request, the server assigns the computer an IP address, a lease for the length of time the allocation is valid, and other IP configuration parameters.

When an OS is running on a mobile PC, it is responsible for managing the DHCP lease and registering the PC's hostname in the domain name system (DNS), which is the hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. This ensures that there is a DNS record for the hostname.

When trying to manage the system through Intel® Active Management Technology from a management console, the OS and Intel® Management Engine (Intel® ME) hostnames must match.[2] If the hostnames are different because something has changed within the PC, such as a hard drive replacement, two manageability issues can arise.

- A management request will fail if a PC has connected and registered with the DNS an OS hostname different from the Intel ME hostname. In this case, the DNS will not return an IP address.
- Using the hostname or recorded IP address will fail the required Transport Layer Security (TLS) because the certificates are issued on the Intel ME hostname. Furthermore, Kerberos, another computer network authentication protocol,[3] will fail because it must use the Intel ME hostname to successfully complete the authentication.

The TLS errors could be simply ignored, but many management consoles will not ignore them and thus communication fails. There is no such workaround for Kerberos. Since Intel IT uses both TLS and Kerberos to access Intel AMT-based systems, any time an Intel ME hostname is not registered properly for any reason in DNS, a hostname failure occurs, and the PC cannot be managed remotely.

[2] Intel® Active Management Technology (Intel® AMT) 6.x and above includes a mode called a dedicated fully qualified domain name (FQDN) that allows the OS and Intel® Management Engine to be different. In the FQDN mode Intel AMT registers itself in the domain name system. Intel IT currently doesn't use the FQDN mode.

[3] Kerberos works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

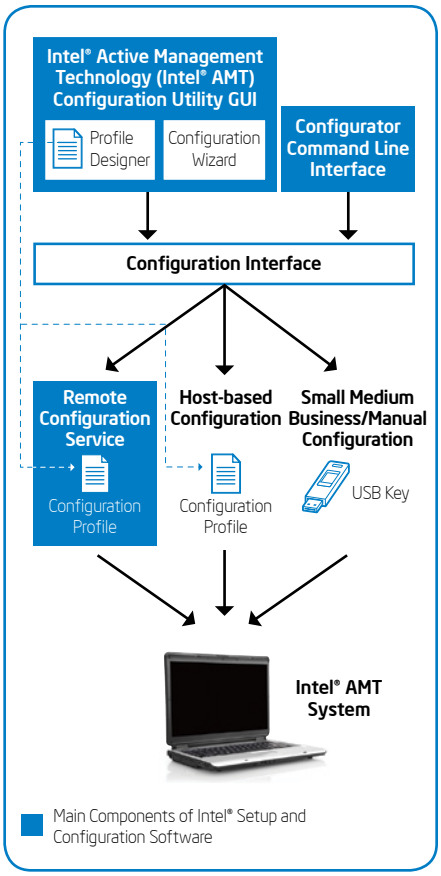

Figure 1. Main components of Intel® Setup and Configuration Software 7.0 and methods for configuring clients based on Intel® Active Management Technology.

SOLUTION

To improve the implementation and operation of Intel AMT in our mobile fleet, Intel IT worked with Intel's software development team to develop ways to enhance Intel® Setup and Configuration Software (Intel® SCS), a tool used with Intel AMT. These improvements were implemented beginning with Intel SCS 7. By combining Intel SCS 7 with existing technologies, we created a highly available, highly agile configuration and maintenance environment for mobile systems running Intel vPro technology.

Intel SCS provides the tools to set up and configure Intel AMT devices. The service package consists of a configuration engine and installer in source and binary form, plus a reference graphical user interface, available from the Intel web site, that ISVs can integrate into their own software.

Prior to the development of Intel SCS 7, Intel IT used a commercial client management console to configure and manage its Intel AMT-based mobile PCs. However, as it became increasing difficult to reconfigure and manage many of these mobile PCs on demand, we began to look for a different solution.

An Improved Intel SCS

Improvements in version 7 of Intel SCS add flexibility to configuring mobile PCs with Intel AMT (see Figure 1). A revised configuration utility enables the initial configuring of systems and then enables reconfiguration later without having to unconfigure first. A Remote Configuration Service runs on a server and handles the communication with the Intel AMT clients. Digest passwords can be randomized and retrieved later using a master password, without the need to go through a database. This enables remote system configuration even if inaccuracies are present in the database.

A New Way to Manage Intel AMT-based Clients

In the past, we used a commercial client management console to handle all configuration and maintenance tasks for mobile and desktop clients (see Figure 2). After realizing we needed to improve client management console support of our environment, we researched ways to separate out the configuration and maintenance tasks using a different software solution.

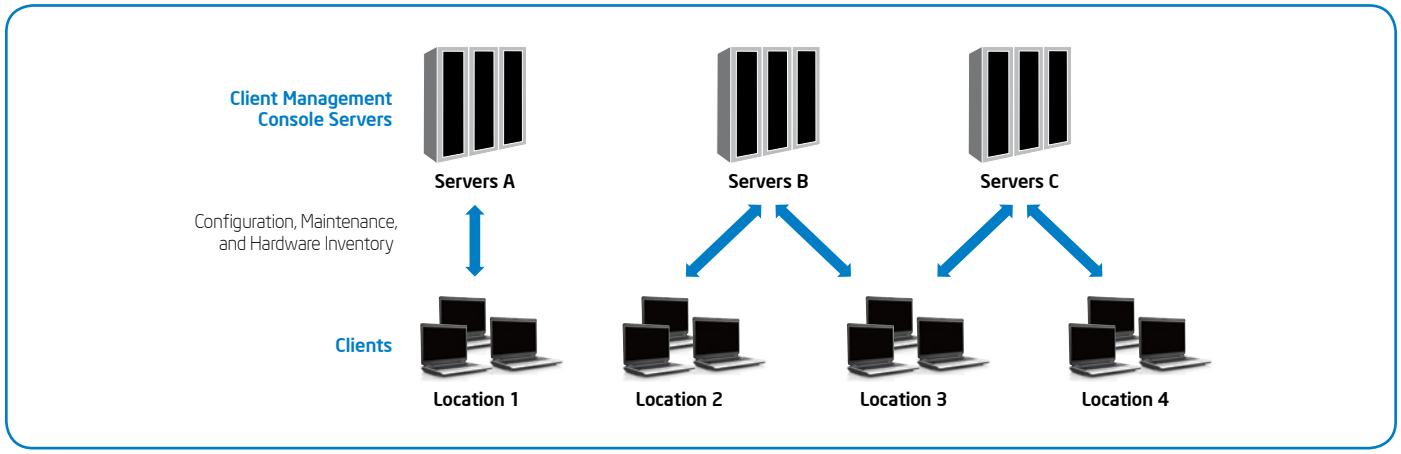

Figure 2. Previously we performed configuring, maintenance, and other client IT tasks using a commercial client management console.

In adding Intel SCS 7 to our overall management solution, we set up Intel SCS to run on separate servers (see Figure 3). This allowed us to physically isolate the functionality.

- We use the client management console for monitoring, database functions, and software distribution, preserving its use for select services.
- We use Intel SCS for configuration and other maintenance tasks related to Intel AMT, such as clock synchronization and password maintenance.

This separation of function enables us to make the best use of each software product. One advantage of the client management console is that it communicates well with Intel AMT and can read its data even when a client is not configured and can collect this information in the console's database.

Intel® Setup and Configuration Software

Intel® Setup and Configuration Software (Intel® SCS) automates the process of populating clients equipped with Intel® Active Management Technology (Intel® AMT) with the necessary user names, passwords, and network parameters for remote, out-of-band administration through a management console. IT departments can use Intel SCS to connect Intel AMT-based hardware to the network infrastructure using common technologies such as Dynamic Host Configuration Protocol, Domain Name Services, Public Key Infrastructure, and Microsoft Active Directory*. Management setup and configuration solutions can use Intel SCS to provide the management console with the necessary information to communicate with the managed hardware, including Intel AMT credentials, hostname data, and connection requirements. The setup and configuration process is secured by means of Transport Layer Security. Microsoft's Certificate Authority provides certificate services, automatically generating a certificate each time an Intel AMT device is set up. User names and passwords can be integrated with Microsoft Active Directory using Kerberos, a computer network authentication protocol. By providing the ability to readily implement a secure setup and configuration infrastructure for Intel AMT devices, Intel SCS makes it easier to activate this technology across thousands of client devices.

To take advantage of additional capabilities, Intel IT plans to upgrade to the next version of Intel SCS. Intel SCS 8 adds new features, including automatic maintenance and discovery enhancements that further improve the ability to remotely monitor, manage, and control mobile PCs equipped with Intel AMT.

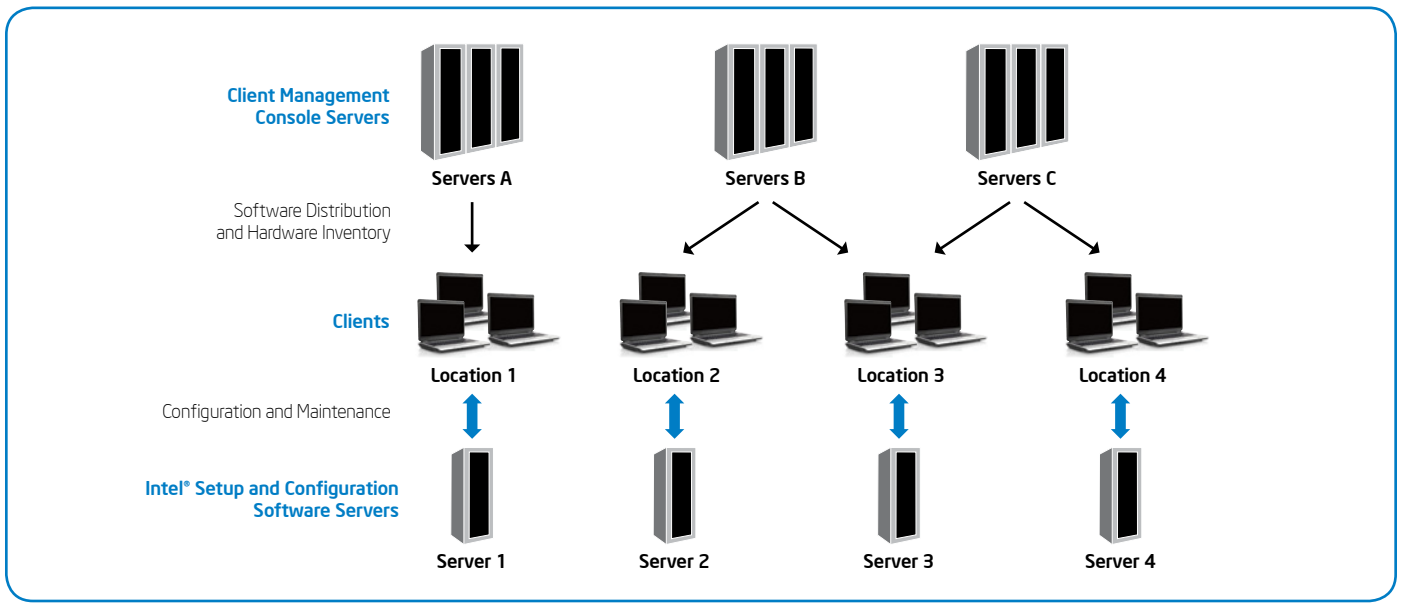

Figure 3. Our new client management solution uses the client management console for software distribution, inventory, and database functions, and uses Intel® Setup and Configuration Software for Intel® Active Management Technology configuration and maintenance.

Configuration on Demand

One important goal for us was to set up configuration on demand. This solution allows technicians to configure a system that because of special circumstances may have missed being configured, such as when a hard drive is placed in a new system.

With our new solution, the client management console monitors PCs and characterizes them according to certain criteria, including whether a PC is unconfigured. If it is, the client management console sends a custom software package we call Intel AMT Configuring On-Demand that includes the necessary Intel AMT configuration files and configures the client through Intel SCS (see Figure 4). The PC downloads and runs this software, which scans the system and configures it. This can occur even if the PCs are unattended, as long as they have a network connection and power. The advantages are that the process can happen automatically and be pushed to a PC at any time.

Resolving Hostname Mismatches

As previously explained, we found that hostname mismatches occur mainly when a system is rebuilt and the hostname changed, or when a hardware component is failing and, rather than fix the system, the hard drive is installed in a new client chassis that in the past may have been configured for another user.

Intel SCS 7 resolves these hostname mismatches by executing a simple remote reconfigure command, an operation that does not require unconfiguration and that can be executed over a wireless interface. We wrote code to handle the instances where the PC's Intel ME hostname or recorded IP address fail Transport Layer Security (TLS), or when Kerberos, another computer network authentication protocol, fails to issue a ticket because of a mismatch.

The code adds an entry to the host's file on the server that runs Intel SCS, and then lets Intel SCS perform its task, invoking an Intel SCS configure Windows Management Instrumentation command and removing the record from the host's file. To invoke this flow on a specific system, we implemented the code as a web service and wrote a small client software script which was executed on the system with the hostname mismatch. This script collects and sends the data needed for the web service to complete its operation (see Figure 5).

One of the challenges in solving the hostname mismatch is how to detect this condition in order to trigger the remediation flow. To accomplish this we wrote a small script that retrieves the Intel ME hostname and compares it to the hostname. If there is a mismatch, the script adds an entry to the registry, which is monitored by our client management console. If a host has a hostname mismatch, it meets the client manageability criteria to send the software code and have Intel SCS resolve the issue.

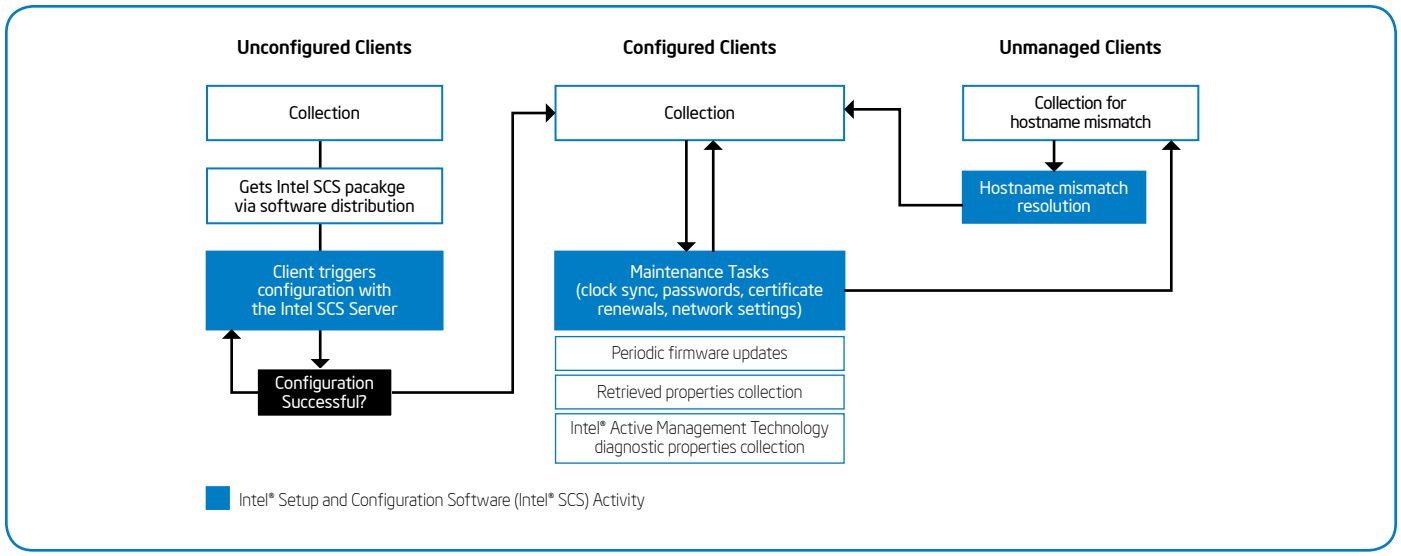

Figure 4. This diagram shows the Intel® Active Management Technology flow for unconfigured, configured, and unmanaged clients.

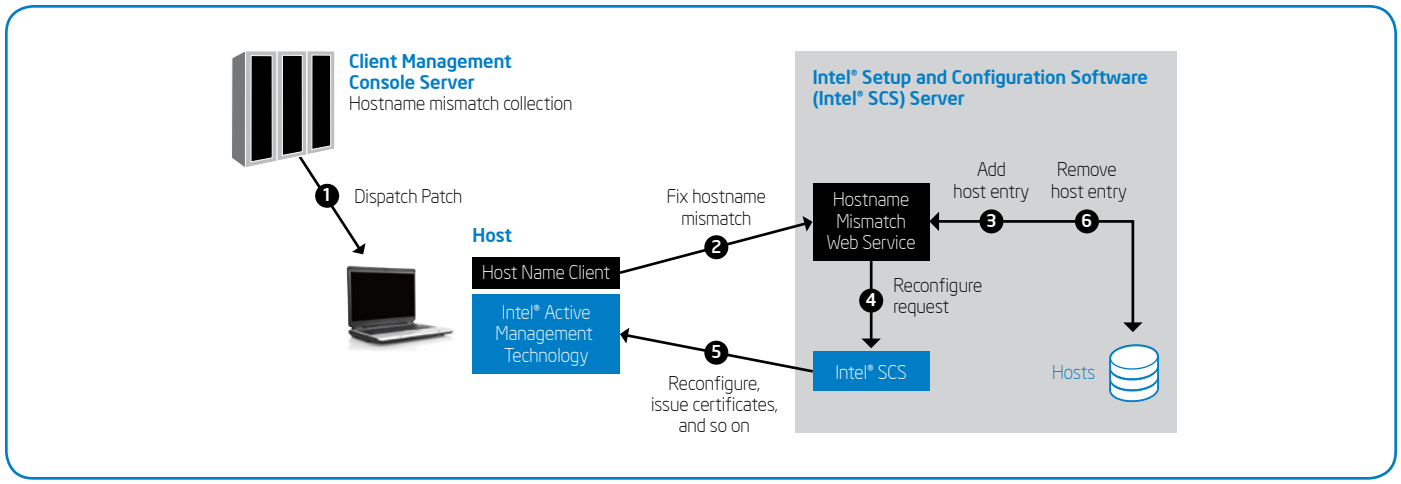

Figure 5. To resolve the issue of hostname mismatches, we wrote code that adds an entry to the host's file on the server that runs Intel® Setup and Configuration Software (Intel® SCS) and then lets Intel SCS perform its task.

CONCLUSION

By adding Intel SCS 7 to our client management console, we now have a solution that improves our ability to configure and maintain mobile PCs on demand with the Intel AMT component of Intel vPro technology. This solution also helps keep the mobile PCs configured throughout their on-the-go life cycles with our customers.

One of the key benefits of this new solution is the mechanism we devised to resolve hostname mismatches using the built-in capabilities of Intel SCS. This mechanism provides a significant improvement in managing mobile fleets, eliminating the need to unconfigure and then reconfigure the client on a wired connection.

We also now have a customized, fast configuration tool—Intel AMT Configuring On-Demand—that technicians can download onto systems and run. We are including this tool in our client build process, allowing us to quickly deliver a configured system to our customers and reducing our dependency on network and LAN connections.

We have also created tools that enable technicians to troubleshoot and fix Intel AMT configuration issues. As part of our proactive PC management strategy, this data is being collected and analyzed to help reduce and eliminate potential future problems.

We are now looking into ways to use Intel AMT's remote OOB capabilities to improve support to our worldwide customers and continue reducing operating costs. For increased security and flexibility, we plan to implement these capabilities through web services and manage them through web portals.

FOR MORE INFORMATION

Visit www.intel.com to find additional information on this and related topics:

- "Achieving Long-term Business Value with Intel® vPro™ Technology", download the pdf at http://download.intel.com/it/pdf/Achieving_Long-term_Business_Value_with_Intel_vPro_Technology.pdf
- To learn more about Intel SCS, visit www.intel.com/go/scs

For more information on Intel IT best practices, visit www.intel.com/it.

CONTRIBUTORS

Elkana Asulin

Gavin Morriss

Tal Tamir

ACRONYMS

DHCP	dynamic host configuration protocol
DNS	domain name system
FQDN	fully qualified domain name
KVM	Keyboard-Video-Mouse
OOB	out of band
TLS	Transport Layer Security

Printed in USA
0412/JGLU/KC/PDF

♻ Please Recycle
327181-001US