Deploying Intel® vPro™ Technology with Microsoft* System Center Configuration Manager 2007

Troubleshooting Guide

Revision 1.20

April 01, 2011

Revision History

Revision	Revision History	Date
0.55	Initial Draft – Steve Davies	1.28.2009
0.6	Edits, Template, Trademarking – Michele Gartner	2.9.2009
0.7	Add additional tips – Steve Davies	2.16.2009
1.0	First Release	2.17.2009
1.1	Add DHCP option 81 requirement – Steve Davies	2.18.2009
1.12	Add additional tips and re-order – Steve Davies	2.24.2009
1.13	Edits for consistent terminology – Steve Davies	2.24.2009
1.14	Corrections for KB960804 – Steve Davies	3.01.2009
1.15	Add additional tips – Steve Davies	3.11.2009
1.20	Re-organized entries, updated certain tips	4.1.2011

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The Intel® Active Management Technology may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web Site.

Intel® Active Management Technology requires the computer system to have an Intel(R) AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/technology/platform-technology/intel-amt/

Throughout this document Intel ME refers to Intel® Management Engine and Intel® AMT refers to Intel® Active Management Technology.

Intel , the Intel logo, Intel® AMT, Intel vPro, Centrino, Centrino Inside, and vPro Inside are trademarks or registered trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2009 Intel Corporation. All rights reserved.

Contents

Introduction 5
Troubleshooting by Provisioning Stage 6
Stage 1 - Installation Pre-Requisites Met 6
Tested Functionality 6
Verification Checks 6
Stage 2 - Provisioning Requests Received at ConfigMgr Server 8
Tested Functionality 8
Verification Checks 8
Corrective Actions 9
Stage 3 - Provisioning Process Starts and Completes Successfully 12
Tested Functionality 12
Verification Checks 12
Corrective Actions 16
Stage 4 - Collection Initiated Power Control is Operational 19
Tested Functionality 19
Verification Checks 19
Corrective Actions 19
Stage 5 - ConfigMgr Out of Band Console Connects to Client and is Operational 20
Tested Functionality 20
Verification Checks 20
Corrective Actions 20
Stage 6 - Intel AMT client WebUI Available and Login Successful (Optional) 22
Tested Functionality 22
Verification Checks 22
Corrective Actions 22
Stage 7 - Client Un-Provisioning Successful 24
Tested Functionality 24
Verification Checks 24
Corrective Actions 25
Troubleshooting by Component 26
Client 26
Network 28
ConfigMgr Servers 28
Active Directory 30
Certificate Authority 30
Other 30
References 30
Appendix A – Hot Fixes Applicable to Windows Server 2003 / ConfigMgr SP1 31
Appendix B – Hot Fixes Applicable to Internet Explorer 32

Figures

Figure 1 - Trace32 view of AMTOPMGR.LOG showing incoming 'hello' packets during ConfigMgr Out-of-Band provisioning 8
Figure 2 - Trace32 view of AMTOPMGR.LOG showing incoming ZTC request during ConfigMgr In-Band provisioning 9
Figure 3 - Trace32 view of AMTOPMGR.LOG showing provisioning process starting and continuing to completion 16

Figure 4 - Trace32 view of AMTOPMGR.LOG showing un-provisioning process starting and continuing to completion 25

Introduction

This guide contains troubleshooting and corrective action tips to help successfully deploy Intel® vPro™ technology PC's with Microsoft* System Center Configuration Manager (ConfigMgr).

These tips were compiled over a seven month period of deployment projects. The number of tips is a measure of the comprehensive nature of this document, rather than a measure of difficulty or lack of robustness during deployment.

This guide contains two troubleshooting sections: Troubleshooting by Provisioning Stage and Troubleshooting by Component. The sections contain the same corrective action tips; however, the tips are organized differently to accommodate different troubleshooting approaches.

For best results, the following tools and infrastructure access should be available during deployment:

- Microsoft Management Console (MMC) tool with Certificates snap-in, Active Directory Users and Computers (ADUC) snap-in, Certificate Authority snap-in, DNS snap-in, DHCP snap-in, Active Directory Service Interface Editor (ADSIEdit) and Enterprise PKI snap-in for reviewing infrastructure components.
- Microsoft Trace32 tool for viewing Microsoft ConfigMgr log files (available from the Microsoft ConfigMgr 2007 Toolkit).
- Access to Active Directory, the network, DNS and DHCP servers and Enterprise PKI.
- Network packet capture tool for capturing Intel AMT 'hello' packets.
- Microsoft TOKENSZ tool for calculating Kerberos ticket sizes and evaluating Windows group membership (available from Microsoft download site)
- Intel® vPro™ Activator Utility or ZTCLOCALAGENT tool for initiating Intel® AMT 'hello' packets.
  - Download the Intel vPro Activator Utility from the Intel® Software Network at http://software.intel.com/en-us/articles/intel-vpro-technology-activator-utility/.
  - Locate ZTCLOCALAGENT in the Manageability Developer Toolkit. Download the DTK at http://software.intel.com/en-us/articles/download-the-latest-version-of-manageability-developer-tool-kit/.

In addition to the tools listed above, a number of Kerberos debugging tools are available in the Windows Server 2003 resource kit that may be helpful, although none of the tips included in this document specifically requires those tools.

Troubleshooting by Provisioning Stage

This section verifies functionality at key stages of the provisioning, management, and un-provisioning process

Work through the stages below in sequence. Each stage describes functionality being tested, verification checks to test functionality and suggested corrective actions if any verification checks fail.

Functionality verification is cumulative; be sure to successfully verify each stage before proceeding to the following stages.

Some corrective action checks will take more effort to perform than others; for expediency, perform the simple ones first. Where possible, corrective actions for each stage are arranged to address functionality for that stage; however, if verification checks continue to fail after performing corrective actions for a specific stage, then review the corrective actions for all stages to ensure all possible corrective actions are exhausted.

Stage 1 - Installation Pre-Requisites Met

Tested Functionality

Microsoft ConfigMgr pre-requisites reviewed, understood, and completed.

Verification Checks

- Baseline Microsoft ConfigMgr installation performed in accordance with Microsoft supported hardware and software recommendations.
- Microsoft ConfigMgr SP1 or preferably SP2 installed on both ConfigMgr servers and client agents.
- Clients using in-band provisioning (i.e. using the ConfigMgr agent) have the Intel MEI driver (formerly known as the HECI driver) is installed.
- When using ConfigMgr SP1 rather than SP2 or hosting ConfigMgr on Windows Server 2003, the required hot fixes are installed on ConfigMgr servers (see Appendix A).
- Intel AMT web server certificate template created and configured to grant read and enroll permissions to ConfigMgr servers.
- Microsoft Enterprise issuing CA available with Issue and Manage Certificates permission granted to ConfigMgr servers. This pre-requisite is optional. If this permission is not available ConfigMgr will not revoke certificates when clients are un-provisioned.
- Active Directory OU or CN created to hold objects representing client Management Controllers and configured to grant full control to the OU or CN and full control over objects within the OU or CN to ConfigMgr servers.
- Microsoft ConfigMgr Out of Band service point installed on all ConfigMgr primary sites responsible for provisioning clients (i.e., primary sites that receive 'hello'

packets from clients using out-of-band provisioning and/or primary sites with clients assigned that use in-band provisioning).

- Clients and ConfigMgr servers responsible for provisioning and managing those clients reside in the same Active Directory forest.
- Clients and ConfigMgr servers responsible for provisioning those clients share DNS namespace.
- Provisioning certificates procured and both certificate and full signing chain installed on all ConfigMgr servers responsible for client provisioning.
- Clients use dynamic IP allocation.
- DNS servers support dynamic updates from DHCP servers. This requirement is optional. If this requirement is not met then the client Operating System is responsible for registering the client hostname in DNS
- DHCP servers support DHCP option 81 to perform dynamic DNS updates. This requirement is optional. If this pre-requisite is not met then the client Operating System is responsible for registering the client hostname in DNS
- DHCP servers allocating IP addresses to clients also provide DNS domain information to those clients (using DHCP option 15).
- Clients using in-band provisioning (i.e. using the ConfigMgr agent) are domain members.
- Firewalls located between ConfigMgr servers or ConfigMgr consoles and clients allow access for ports 9971 and 16992-16995 and any other ports specified in ConfigMgr documentation.
- Intel WS-MAN Translator is installed on any ConfigMgr servers responsible for provisioning 'legacy' clients (Intel AMT clients using firmware earlier than V3.2.1).
- Intel WS-MAN Translator is installed on any ConfigMgr servers responsible for provisioning clients using Pre Shared Keys (PSK) rather than PKI. PSK provisioning is only supported when provisioning 'legacy' clients (Intel AMT clients using firmware earlier than V3.2.1).
- If Intel WS-MAN Translator is being used to support provisioning using PSK's, the same PSK is used across all clients using PSK's.
- When using Internet Explorer to access the Intel AMT WebUI, the required hot fixes are installed on systems hosting Internet Explorer (see Appendix B).

Stage 2 - Provisioning Requests Received at ConfigMgr Server

Tested Functionality

- Clients being provisioned using ConfigMgr in-band provisioning have received the provisioning policy from ConfigMgr and have requested provisioning
- Clients being provisioned using ConfigMgr out-of-band provisioning have located the ConfigMgr provisioning server and are sending 'hello' packets to request provisioning

Verification Checks

- Check AMTOPMGR.LOG file on the ConfigMgr server and verify receipt of 'hello' packets for clients using ConfigMgr out-of-band provisioning or receipt of Zero Touch Configuration (ZTC) requests for clients using ConfigMgr in-band provisioning (use Trace32 to view the AMTOPMGR.LOG file and see examples in Figure 1 and 2).

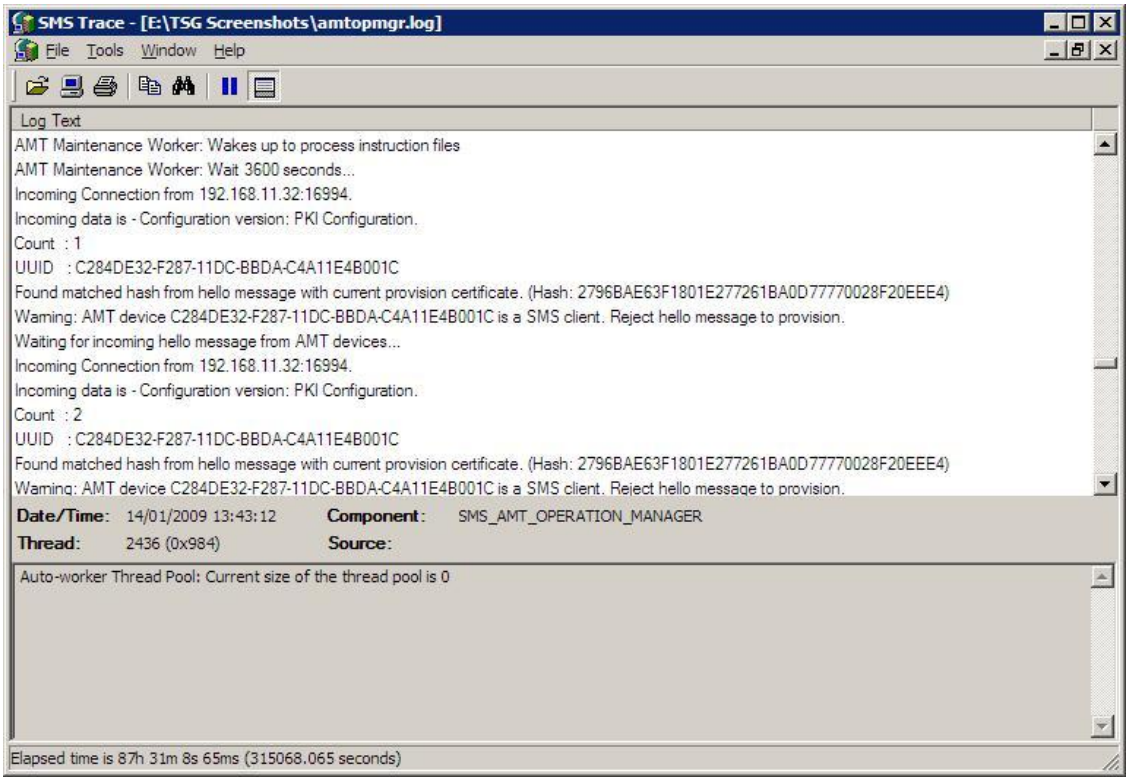


Figure 1 - Trace32 view of AMTOPMGR.LOG showing incoming 'hello' packets during ConfigMgr Out-of-Band provisioning

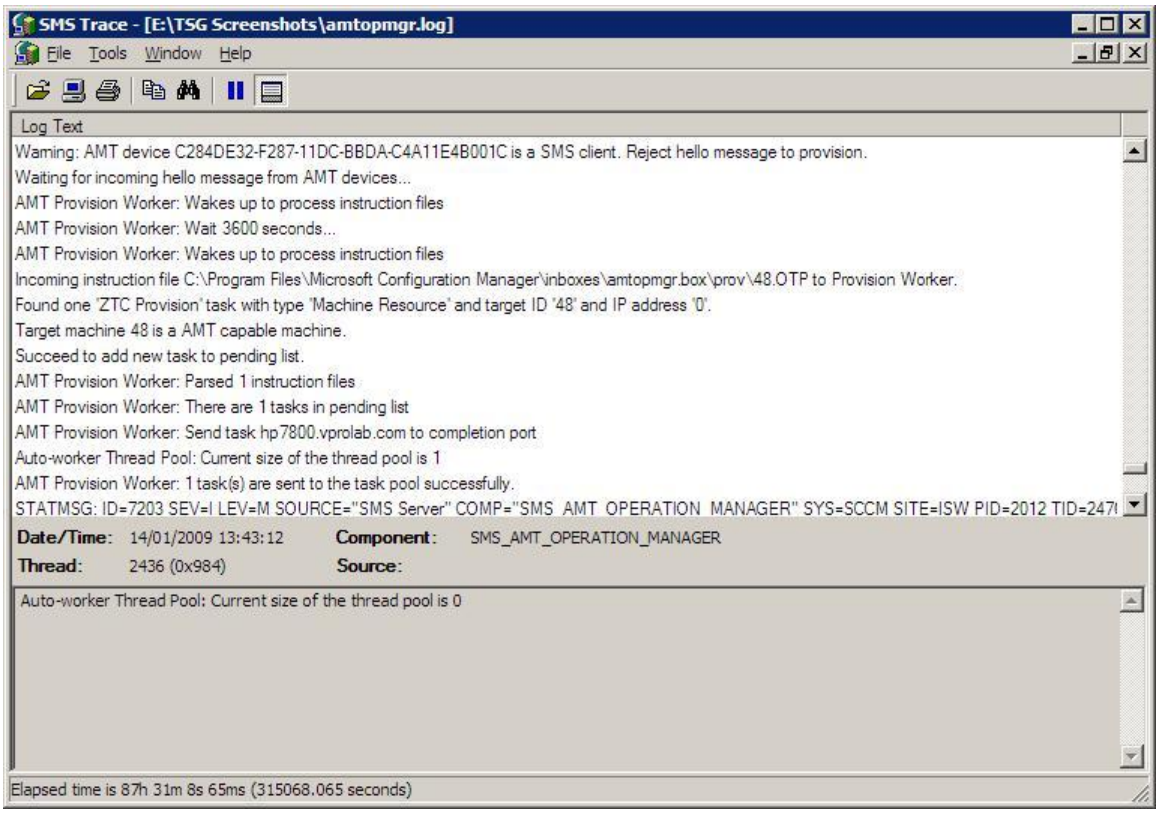


Figure 2 - Trace32 view of AMTOPMGR.LOG showing incoming ZTC request during ConfigMgr In-Band provisioning

Corrective Actions

- Check all ConfigMgr servers that will perform provisioning and verify the Out of Band service point is installed (use ConfigMgr Console to check site system roles).
- When using ConfigMgr in-band provisioning, check the Intel MEI (formerly Intel HECI) driver is installed and started on the client (check using Windows driver manager)
- When using ConfigMgr in-band provisioning, check the ConfigMgr agent is installed and assigned to a ConfigMgr site code with the Out of Band Service Point installed (check using Configuration Manager on the client).
- When using ConfigMgr in-band provisioning, check the ConfigMgr agent is from ConfigMgr SP1 or later.
- When using ConfigMgr in-band provisioning, check the ConfigMgr automatic provisioning policy has been downloaded by the ConfigMgr agent and is enabled (check using OOBMGMT.LOG file on client).
- When using ConfigMgr out-of-band provisioning, check the currently selected Intel® Management Engine (Intel® ME) power package allows the Intel ME to be active in the desired client power states to send 'hello' packets. If the selected Intel ME power package configures the Intel ME to be active in client power state S0 only, power on the client to send 'hello' packets. If 'hello' packets must be sent in

other client power states select a different power package so the ME is active in other client power states (check using the Intel MEBX).

- Check Intel AMT is enabled in BIOS (check using BIOS Setup).
- Check Intel ME management mode is set to 'Intel AMT' (check using MEBX).
- Check Intel ME is configured for DHCP and is receiving a dynamic IP address (check using Intel MEBX and DHCP server).
- Check Intel ME is un-provisioned (use Intel MEBX to check for the presence of a provisioning record or to perform a full un-provision. Performing a full un-provision erases any existing MEBX data so should be used with caution; if the client is pre-provisioned with PSK or custom certificate hash information this will need to be re-entered after a full un-provision).
- Check Intel ME is configured for Enterprise mode and either PKI provisioning is enabled or a PSK has been loaded (check using Intel MEBX).
- When using ConfigMgr out-of-band provisioning, verify the Intel AMT client is sending 'hello' messages (use a network packet capture tool to monitor the network, use an agent like ZTCLOCALAGENT to restart packets, or perform a full un-provision to restart packets. Performing a full un-provision erases any existing MEBX data and should be used with caution; if the client is pre-provisioned with PSK or custom certificate hash information this will need to be re-entered after a full un-provision. Also note that certain OEM's have configured their platforms so they no longer send hello packets automatically - in such a situation, use ZTCLOCALAGENT to initiate 'hello' packets).
- Check clients have had sufficient time to request provisioning; when using ConfigMgr Out of Band provisioning, clients send 'hello' packets at a decreasing frequency the longer they are turned on and eventually stop sending 'hello' packets; when using ConfigMgr in-band provisioning ConfigMgr agents may take up to 25-hours to recognize the automatic in-band provisioning setting on the ConfigMgr server depending on collection membership update frequency and client policy update period. If using ConfigMgr Out of Band provisioning, restart the 'hello' packet sequence. If using ConfigMgr in-band provisioning, enable automatic in-band provisioning for an ConfigMgr collection containing the client, update ConfigMgr collection membership to re-generate client policy, download the ConfigMgr machine policies to the client and force the ConfigMgr agent to restart the in-band provisioning process. (See Intel® vPro™ Expert Center article "Using WMI to force the SCCM Agent to check for its AMT Auto Provisioning Policy" for details of restarting ConfigMgr in-band provisioning).
- When using ConfigMgr out-of-band provisioning, check client 'hello' packets are directed to the correct ConfigMgr server (use NSLOOKUP at the client to lookup 'ProvisionServer' and verify the IP address matches the ConfigMgr server IP address, or check DNS for a 'ProvisionServer' record with the correct ConfigMgr server IP address, or check MEBX for correct Provision Server IP address, or check any Operating System hosted ACTIVATOR is using the correct ConfigMgr server IP address).

- Check network firewalls and firewalls on ConfigMgr servers allow ports 9971, 16992-16995 and any other ConfigMgr required ports (check with network administrator, or use a packet capture tool to confirm transit of packets between clients and ConfigMgr server. Microsoft ConfigMgr help files have port information).

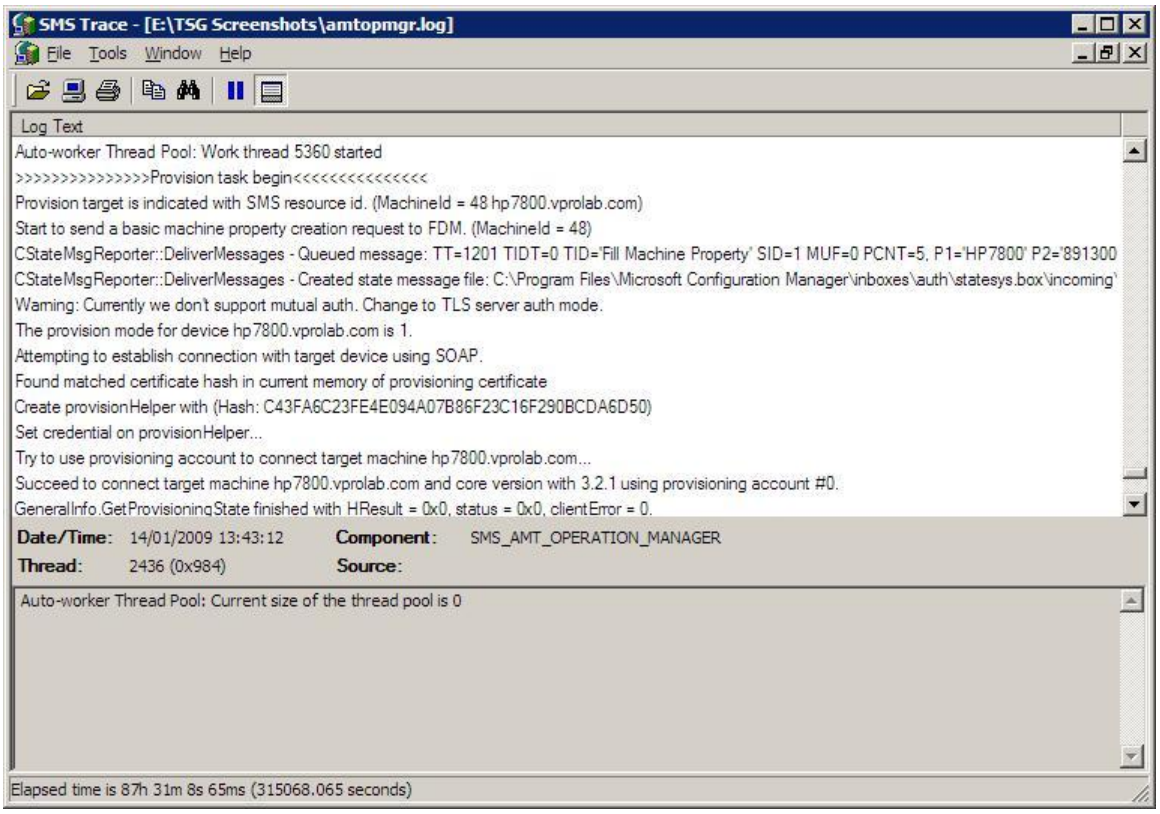
Stage 3 - Provisioning Process Starts and Completes Successfully

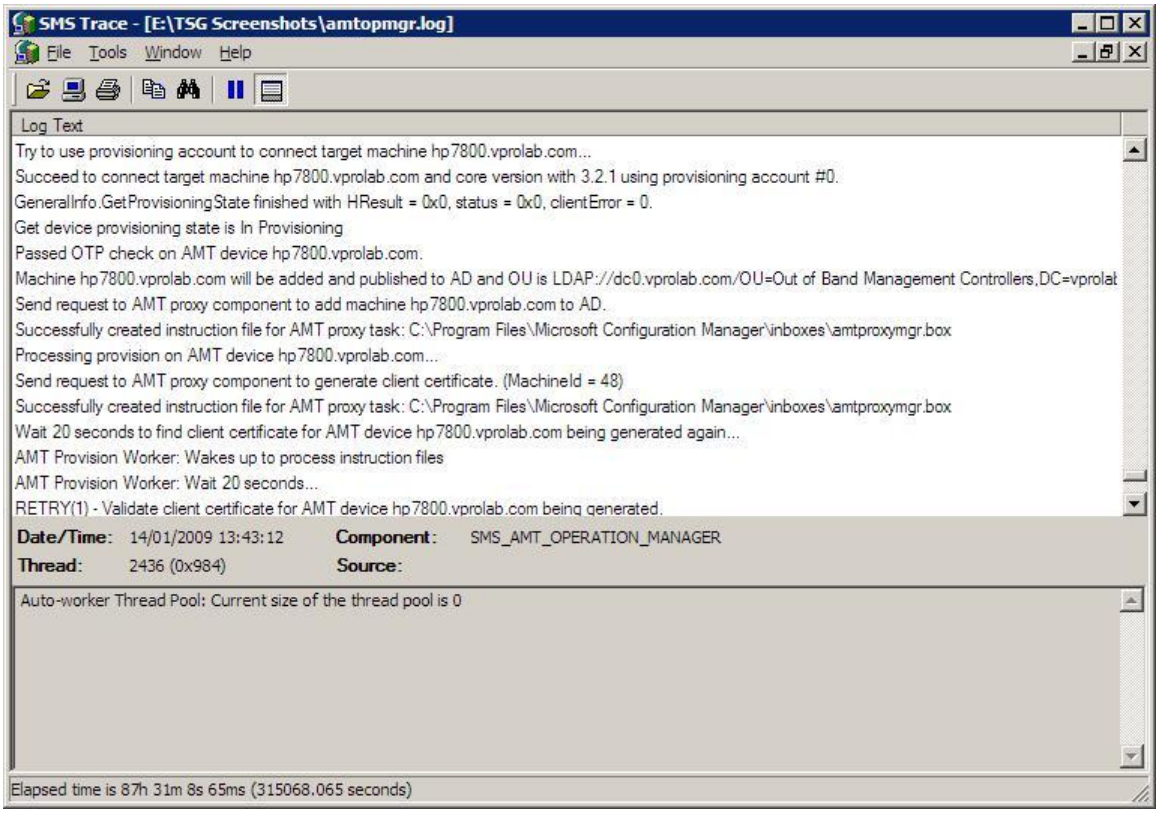
Tested Functionality

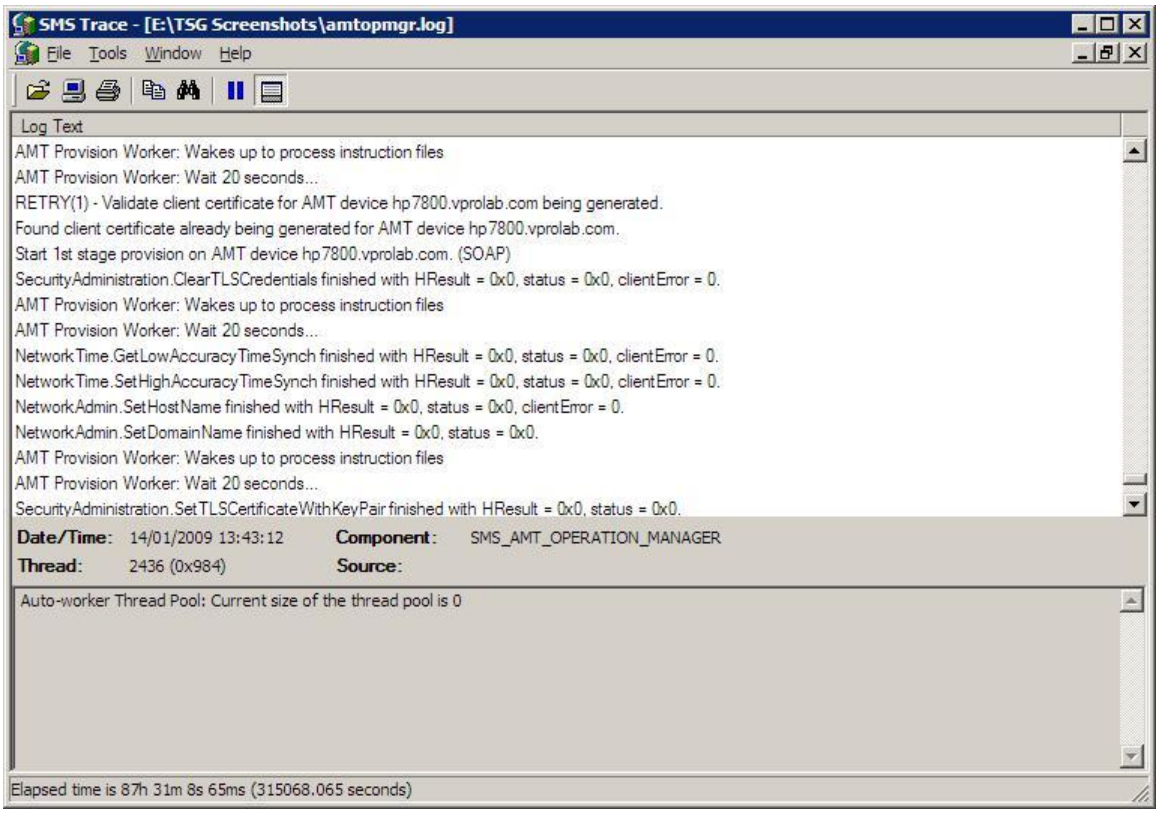
- Client name resolution is operational
- Client to ConfigMgr server connectivity is operational
- Provisioning certificate and signing chain is operational or PSK is operational
- Intel WS-MAN Translator is operational for 'legacy' Intel AMT clients or clients using PSK
- Provisioning and Discovery accounts are correctly configured into ConfigMgr Out of Band Out of Band Service Points for access to Intel AMT during provisioning
- ConfigMgr Out of Band Service Point permissions to Active Directory allow objects representing the Intel Management Engine to be correctly created during provisioning
- Intel AMT web server certificate template is correctly configured in the issuing CA

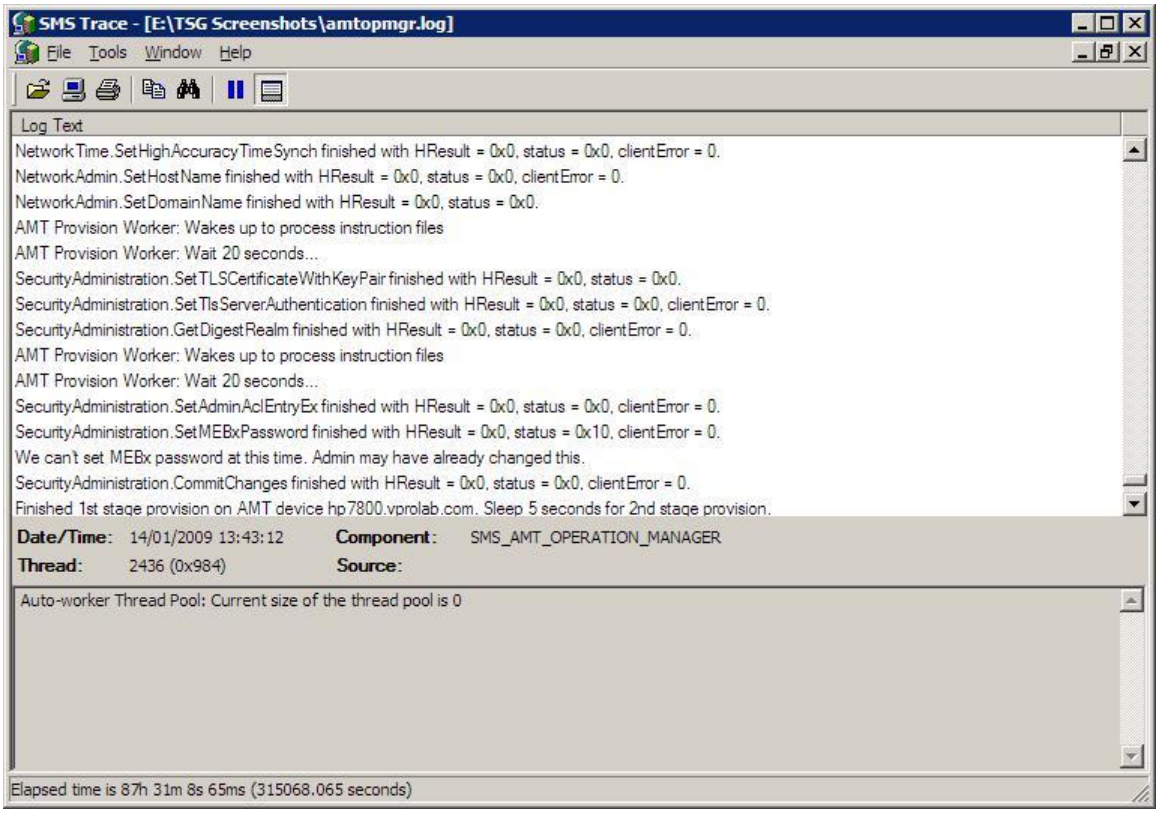
Verification Checks

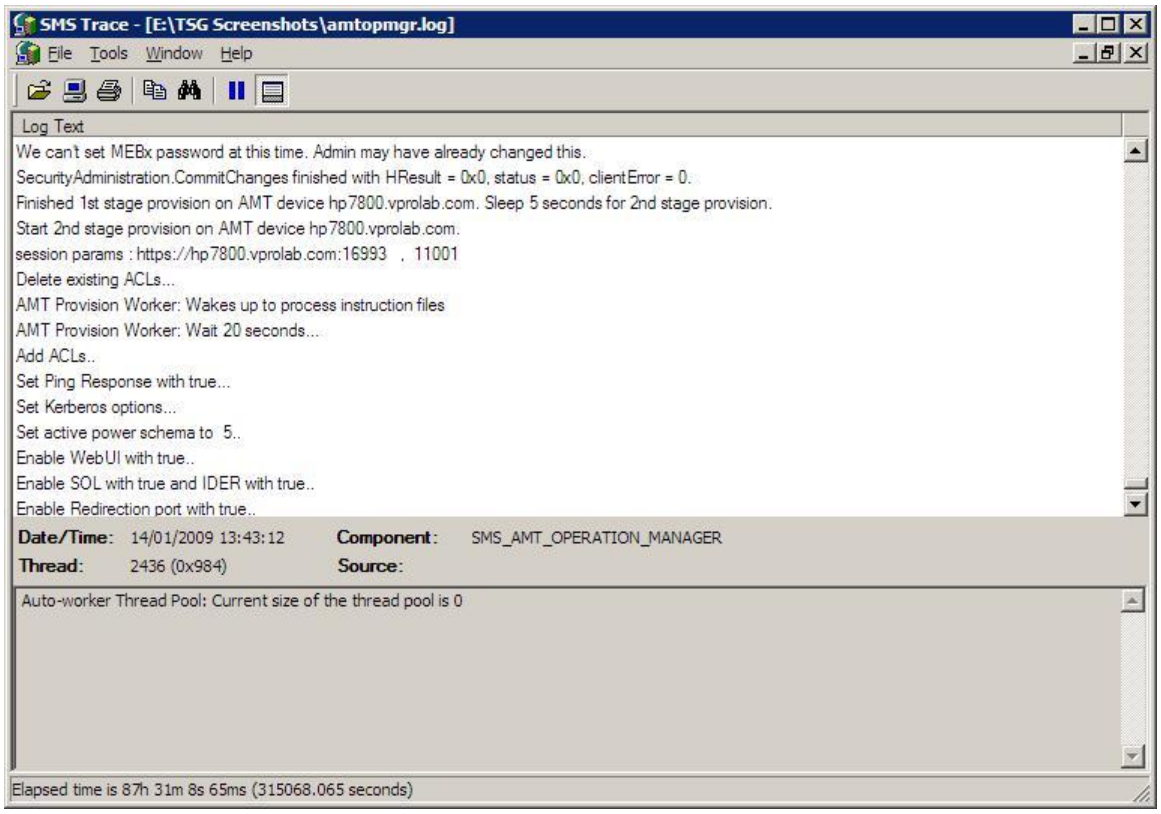
- Check AMTOPMGR.LOG file on the ConfigMgr server and verify the provisioning process starts and both first and second stage provisioning completes successfully (use Trace32 to view log file and see example in Figure 3 below).
- Check computer objects are created for each provisioned client in the Active Directory OU or CN used to hold objects representing client Management Controllers (use MMC with ADUC snap-in).
- Check computer objects representing client Management Controllers are not marked with a cross or exclamation mark and check that Service Principal Names have been correctly written into those objects (use MMC with ADUC and ADSIEdit snap-in).


SMS Trace - [E:\TSG Screenshots\amtopmgr.log]
File Tools Window Help
Log Text
Auto-worker Thread Pool: Work thread 5360 started
>>>>>>>>>>>>>>>Provision task begin<<<<<<<<<<<<<<<
Provision target is indicated with SMS resource id. (MachineId = 48 hp7800.vprolab.com)
Start to send a basic machine property creation request to FDM. (MachineId = 48)
CStateMsgReporter::DeliverMessages - Queued message: TT=1201 TIDT=0 TID='Fill Machine Property' SID=1 MUF=0 PCNT=5, P1='HP7800' P2='891300
CStateMsgReporter::DeliverMessages - Created state message file: C:\Program Files\Microsoft Configuration Manager\inboxes\auth\statesys.box\incoming\
Warning: Currently we don't support mutual auth. Change to TLS server auth mode.
The provision mode for device hp7800.vprolab.com is 1.
Attempting to establish connection with target device using SOAP.
Found matched certificate hash in current memory of provisioning certificate
Create provisionHelper with (Hash: C43FA6C23FE4E094A07B86F23C16F290BCDA6D50)
Set credential on provisionHelper...
Try to use provisioning account to connect target machine hp7800.vprolab.com...
Succeed to connect target machine hp7800.vprolab.com and core version with 3.2.1 using provisioning account #0.
GeneralInfo.GetProvisioningState finished with HResult = 0x0, status = 0x0, clientError = 0.
Date/Time: 14/01/2009 13:43:12
Component: SMS_AMT_OPERATION_MANAGER
Thread: 2436 (0x984)
Source:
Auto-worker Thread Pool: Current size of the thread pool is 0
Elapsed time is 87h 31m 8s 65ms (315068.065 seconds)


SMS Trace - [E:\TSG Screenshots\amtopmgr.log]
File Tools Window Help
Log Text
Try to use provisioning account to connect target machine hp7800.vprolab.com...
Succeed to connect target machine hp7800.vprolab.com and core version with 3.2.1 using provisioning account #0.
GeneralInfo.GetProvisioningState finished with HResult = 0x0, status = 0x0, clientError = 0.
Get device provisioning state is In Provisioning
Passed OTP check on AMT device hp7800.vprolab.com.
Machine hp7800.vprolab.com will be added and published to AD and OU is LDAP://dc0.vprolab.com/OU=Out of Band Management Controllers,DC=vprolat
Send request to AMT proxy component to add machine hp7800.vprolab.com to AD.
Successfully created instruction file for AMT proxy task: C:\Program Files\Microsoft Configuration Manager\inboxes\amtproxymgr.box
Processing provision on AMT device hp7800.vprolab.com...
Send request to AMT proxy component to generate client certificate. (MachineId = 48)
Successfully created instruction file for AMT proxy task: C:\Program Files\Microsoft Configuration Manager\inboxes\amtproxymgr.box
Wait 20 seconds to find client certificate for AMT device hp7800.vprolab.com being generated again...
AMT Provision Worker: Wakes up to process instruction files
AMT Provision Worker: Wait 20 seconds...
RETRY(1) - Validate client certificate for AMT device hp7800.vprolab.com being generated.
Date/Time: 14/01/2009 13:43:12
Component: SMS_AMT_OPERATION_MANAGER
Thread: 2436 (0x984)
Source:
Auto-worker Thread Pool: Current size of the thread pool is 0
Elapsed time is 87h 31m 8s 65ms (315068.065 seconds)


SMS Trace - [E:\TSG Screenshots\amtopmgr.log]
File Tools Window Help
Log Text
AMT Provision Worker: Wakes up to process instruction files
AMT Provision Worker: Wait 20 seconds...
RETRY(1) - Validate client certificate for AMT device hp7800.vprolab.com being generated.
Found client certificate already being generated for AMT device hp7800.vprolab.com.
Start 1st stage provision on AMT device hp7800.vprolab.com. (SOAP)
SecurityAdministration.ClearTLSCredentials finished with HResult = 0x0, status = 0x0, clientError = 0.
AMT Provision Worker: Wakes up to process instruction files
AMT Provision Worker: Wait 20 seconds...
NetworkTime.GetLowAccuracyTimeSynch finished with HResult = 0x0, status = 0x0, clientError = 0.
NetworkTime.SetHighAccuracyTimeSynch finished with HResult = 0x0, status = 0x0, clientError = 0.
NetworkAdmin.SetHostName finished with HResult = 0x0, status = 0x0, clientError = 0.
NetworkAdmin.SetDomainName finished with HResult = 0x0, status = 0x0.
AMT Provision Worker: Wakes up to process instruction files
AMT Provision Worker: Wait 20 seconds...
SecurityAdministration.SetTLSCertificateWithKeyPair finished with HResult = 0x0, status = 0x0.
Date/Time: 14/01/2009 13:43:12 Component: SMS_AMT_OPERATION_MANAGER
Thread: 2436 (0x984) Source:
Auto-worker Thread Pool: Current size of the thread pool is 0
Elapsed time is 87h 31m 8s 65ms (315068.065 seconds)


SMS Trace - [E:\TSG Screenshots\amtopmgr.log]
File Tools Window Help
Log Text
NetworkTime.SetHighAccuracyTimeSynch finished with HResult = 0x0, status = 0x0, clientError = 0.
NetworkAdmin.SetHostName finished with HResult = 0x0, status = 0x0, clientError = 0.
NetworkAdmin.SetDomainName finished with HResult = 0x0, status = 0x0.
AMT Provision Worker: Wakes up to process instruction files
AMT Provision Worker: Wait 20 seconds...
SecurityAdministration.SetTLSCertificateWithKeyPair finished with HResult = 0x0, status = 0x0.
SecurityAdministration.SetTlsServerAuthentication finished with HResult = 0x0, status = 0x0, clientError = 0.
SecurityAdministration.GetDigestRealm finished with HResult = 0x0, status = 0x0, clientError = 0.
AMT Provision Worker: Wakes up to process instruction files
AMT Provision Worker: Wait 20 seconds...
SecurityAdministration.SetAdminAclEntryEx finished with HResult = 0x0, status = 0x0, clientError = 0.
SecurityAdministration.SetMEBxPassword finished with HResult = 0x0, status = 0x10, clientError = 0.
We can't set MEBx password at this time. Admin may have already changed this.
SecurityAdministration.CommitChanges finished with HResult = 0x0, status = 0x0, clientError = 0.
Finished 1st stage provision on AMT device hp7800.vprolab.com. Sleep 5 seconds for 2nd stage provision.
Date/Time: 14/01/2009 13:43:12 Component: SMS_AMT_OPERATION_MANAGER
Thread: 2436 (0x984) Source:
Auto-worker Thread Pool: Current size of the thread pool is 0
Elapsed time is 87h 31m 8s 65ms (315068.065 seconds)


SMS Trace - [E:\TSG Screenshots\amtopmgr.log]
File Tools Window Help
Log Text
We can't set MEBx password at this time. Admin may have already changed this.
SecurityAdministration.CommitChanges finished with HResult = 0x0, status = 0x0, clientError = 0.
Finished 1st stage provision on AMT device hp7800.vprolab.com. Sleep 5 seconds for 2nd stage provision.
Start 2nd stage provision on AMT device hp7800.vprolab.com.
session params : https://hp7800.vprolab.com:16993 , 11001
Delete existing ACLs...
AMT Provision Worker: Wakes up to process instruction files
AMT Provision Worker: Wait 20 seconds...
Add ACLs..
Set Ping Response with true...
Set Kerberos options...
Set active power schema to 5..
Enable WebUI with true..
Enable SOL with true and IDER with true..
Enable Redirection port with true..
Date/Time: 14/01/2009 13:43:12
Component: SMS_AMT_OPERATION_MANAGER
Thread: 2436 (0x984)
Source:
Auto-worker Thread Pool: Current size of the thread pool is 0
Elapsed time is 87h 31m 8s 65ms (315068.065 seconds)

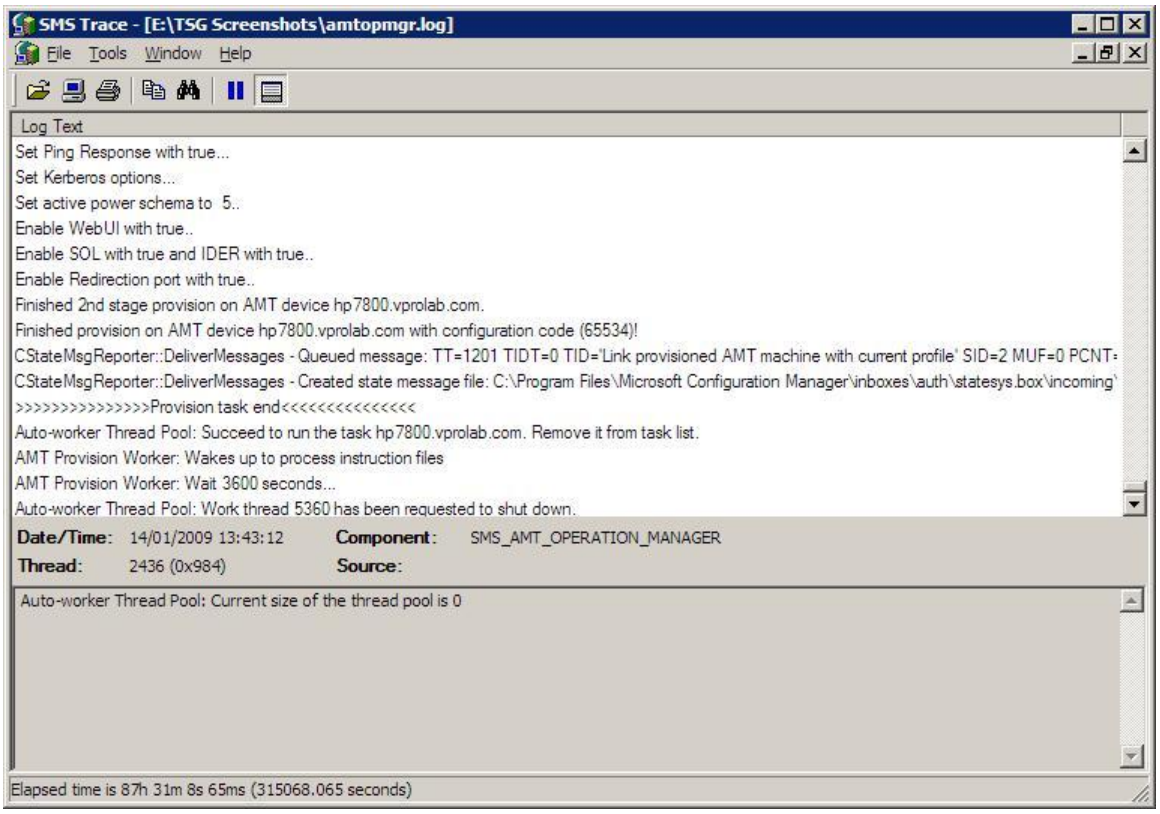


Figure 3 - Trace32 view of AMTOPMGR.LOG showing provisioning process starting and continuing to completion

Corrective Actions

- When using ConfigMgr out-of-band provisioning for clients, verify the ConfigMgr agent is not installed on those clients. If the ConfigMgr agent has been installed on clients and the agent has been detected by ConfigMgr, then only ConfigMgr in-band provisioning can be used with those clients (check using ConfigMgr Console to view the 'Client' column of ConfigMgr collections).
- When using ConfigMgr out-of-band provisioning, check that clients have been imported into the ConfigMgr server responsible for client provisioning using "Import Out of Band Management Controller Wizard" (check ConfigMgr collections using ConfigMgr Console) and the Intel ME hostname matches the client OS hostname.
- Check client FQDN does not include any special characters. FQDN should be composed of characters A-Z, a-z, 0-9, minus '-' and period '.'. Underscore characters are not supported and will cause provisioning failure
- Check Intel ME Admin credentials are known by ConfigMgr (check Provisioning and Discovery accounts in Intel AMT Component configuration in ConfigMgr Console). Normally this only needs doing if MEBX credentials have changed from default 'admin/admin'.
- Check hot fixes are installed on ConfigMgr servers (see Appendix A).

- Check forward and reverse client name resolution is working consistently, and resolves to the correct client (use NSLOOKUP on ConfigMgr server).
- Check the provisioning certificate includes server authentication.
- Check the provisioning certificate includes special Intel AMT OU and/or OID.
- Check the provisioning certificate was accepted by ConfigMgr server during configuration of the Out of Band Component and not rejected due to a missing OID or a subject CN domain name that differs from ConfigMgr server domain (check AMTOPMGR.LOG using Trace32
- Check the provisioning certificate has a signing chain that terminates with a trusted root certificate authority (check root certificate thumbprint and use MEBX to compare with client certificate hash list).
- Check the provisioning certificate subject domain or FQDN is trusted by Intel AMT client (check DHCP option 15, or MEBX PKI Domain or MEBX Provision Server FQDN).
- Check full provisioning certificate signing chain is available on the ConfigMgr Out of Band service point (use MMC to check Windows certificate store).
- Check all certificates in the provisioning certificate signing chain have valid dates (use MMC to check signing chain certificates).
- Check the provisioning certificate and all certificates in the signing chain have key length >=1024-bits and <= 2048-bits (use MMC to check provisioning and signing chain certificates).
- In non-COM and non-NET domains, if clients to be provisioned are located in third level DNS domains or below, check child domains are trusted by the client ME (evaluate DNS topology, DHCP option 15, provisioning certificates and Intel AMT firmware version, MEBX DNS Suffix and Provision Server FQDN settings and see Intel® vPro™ Expert Center article "Intel® AMT Remote Configuration Certificate Selection Whitepaper"
- Check clients are not impacted by self-signed certificate behavior (upgrade to Intel AMT firmware V3.2.2 or later or apply workarounds documented in Intel® vPro™ Expert Center article "Intel AMT 3.2.1 Self-signed certificate issue and working around it for Microsoft System Configuration Manager SP1").
- When using legacy clients (i.e., using Intel AMT firmware earlier than V3.2.1), check Intel WSMAN Translator is installed on ConfigMgr servers responsible for provisioning those legacy clients.
- When using PSK provisioning, check that Intel WSMAN Translator is installed on ConfigMgr servers responsible for provisioning and all clients are using identical PSK.
- Check ConfigMgr servers have full permission to the Active Directory OU or CN used to hold objects representing client Management Controllers and full control over objects in the OU or CN.

- Check the Intel AMT Web Server certificate template includes server authentication and indicates the subject name is supplied in certificate requests (use MMC with Certificate Template snap-in).
- Check the full certificate chain for the Enterprise issuing CA is available on the ConfigMgr Out of Band service point (use MMC to check Windows certificate store)
- Check all certificates in issuing CA signing chain on the ConfigMgr Out of Band service point have valid dates (use MMC to check signing chain certificates)
- Check ConfigMgr servers have read and enroll permissions to the Intel AMT Web Server certificate template (use MMC with Certificate Authority snap-in).
- Check valid Certificate Revocation Lists (CRL) and certificates are available from the Enterprise PKI at CRL Distribution Points (CDP) and Authority Information Access (AIA) points (use MMC with Enterprise PKI snap-in).
- Check network firewalls and firewalls on ConfigMgr servers allow ports 16992-16995, 9971 and any other ConfigMgr required ports (check with network administrator, or use a packet capture tool to confirm transit of packets between clients and ConfigMgr server. Microsoft ConfigMgr help files have port information).

Stage 4 - Collection Initiated Power Control is Operational

Tested Functionality

- Randomized digest credentials for Intel AMT access are functional.
- Client Management Controller has correct power scheme to permit Out of Band power control.

Verification Checks

- From the ConfigMgr Console, select provisioned clients in the ConfigMgr collection, right-click and perform power control operations. Verify that clients can be powered down correctly. If power control operations are not available in the menu, perform a Discover Management Controllers operation for clients and update ConfigMgr collection membership before retrying the power down operation.
- Select provisioned clients in the ConfigMgr collection, right-click and perform power control operations. Verify that previously powered down clients can be powered-up correctly after the power down operation.

Corrective Actions

- After provisioning, check the Intel ME power package is set so Intel ME is ON when the client is powered on (S0 state), in sleep (S3 state), hibernate (S4 state) and powered off (S5 state). Use MEBX or Intel AMT WebUI to set ME power package so ME remains active in sleep, hibernate and power-down states. For volume environments, if the power package is incorrectly set after provisioning, use a post-provisioning script to set the correct power package.
- Check hot fixes are installed on ConfigMgr servers (see Appendix A).

Stage 5 - ConfigMgr Out of Band Console Connects to Client and is Operational

Tested Functionality

- Kerberos authentication is operational.
- SOL / IDER functionality is operational.
- Multi-tier PKI (where applicable) certificates configured correctly in ConfigMgr Console certificate stores.

Verification Checks

- Select a provisioned client in ConfigMgr collection, right click and open the ConfigMgr Out of Band Management Console.
- Verify the ConfigMgr Out of Band console correctly connects to the client.
- Verify the ConfigMgr Out of Band console correctly displays the system status of the client.
- Verify power control can be used to power down and power up the client.
- Verify SOL / IDER can be used to display the client BIOS console output and boot the client from an IDE image.

Corrective Actions

- Check the Intel AMT Web Server certificate template includes server authentication and indicates the subject name is supplied in certificate requests (use MMC with Certificate Template snap-in).
- Check domain controller replication has occurred after provisioning if there are multiple domain controllers in the environment.
- Check client/server times and time zones are synchronized.
- Check access to the appropriate Intel AMT realms is enabled if functions are unavailable from the ConfigMgr Out of Band console when managing clients (check Intel AMT component configuration in ConfigMgr Console).
- Check the current Windows user (operating the ConfigMgr Out of Band console) is included in the Intel AMT ACL (check Intel AMT component configuration in ConfigMgr Console).
- If SOL / IDER is not operational, check SOL / IDER is enabled in MEBX and client BIOS (check using MEBX and BIOS Setup and review AMTOPMGR.LOG for success when this capability was enabled during provisioning).
- In a multi-tier PKI environment with intermediate CA's, if SOL / IDER is not operational, check that both root and all subordinate CA certificates from the Enterprise PKI are in the local machine Trusted Root Certificate Authority store on systems hosting the ConfigMgr Out of Band Console (check using MMC certificates snap-in).

- If SOL is not operational, check the Windows telnet client is installed on the system hosting the ConfigMgr Out of Band Console.
- If the ConfigMgr Out of Band console will not connect to the client, try logging off the system hosting the ConfigMgr Out of Band, logging back on again and retrying the ConfigMgr Out of Band console. The logoff and logon operation forces new Kerberos tickets to be generated. KerbTray or KerbList utilities from Microsoft Windows Server 2003 resource kit can also be used to flush cached Kerberos tickets.
- Check the current Windows user (operating the ConfigMgr Out of Band console) is not a member of a large number of Windows groups. Intel AMT limits Kerberos ticket size so membership of a large number of groups may cause Kerberos authentication to fail. Use TOKENSZ tool and see Microsoft article "Troubleshooting Kerberos Errors" to determine group membership and ticket size. Newer Intel AMT firmware supports larger Kerberos ticket sizes. Firmware can be remotely upgraded.

Stage 6 - Intel AMT client WebUI Available and Login Successful (Optional)

Tested Functionality

- Kerberos authentication operational.
- Intel AMT WebUI operational.

Verification Checks

- Open Microsoft* Internet Explorer, enter the URL for the provisioned client in this format: https://ClientFQDN:16993. Verify the browser connects to the Intel AMT WebUI.
- Click the logon button and enter credentials in the format DOMAIN\Username with password. DOMAIN\Username should represent a Windows domain account with access to Intel AMT.

Corrective Actions

- Check the Intel AMT WebUI option is enabled in the AMT Component configuration in ConfigMgr Console.
- Check the Intel AMT WebUI URL is specified using the client FQDN and not an IP address or other address alias otherwise Kerberos authentication will fail.
- When using Microsoft Internet Explorer to connect to the Intel AMT WebUI, enable Integrate Windows Authentication in the browser's Advanced Internet Options and restart the browser.
- For browsers hosted on Windows Server 2003 SP1 or earlier or Windows XP SP2 or earlier, check hot fix KB908209 is installed and check the registry entry associated with KB908209 is added. For browsers hosted on Windows Server 2003 SP2 or later or Windows XP SP2, KB908209 is already included but the registry entry associated with KB908209 must still be added for Windows XP, Windows Vista, Windows 7, Windows Server 2003 and Windows Server 2008.
- Check the Intel AMT Web Server certificate template includes server authentication and indicates the subject name is supplied in certificate requests (use MMC with Certificate Template snap-in).
- Check domain controller replication has occurred after provisioning if there are multiple domain controllers in the environment.
- Check that times / time zones are synchronized.
- Check access to Intel AMT realms is enabled if functions are unavailable from the WebUI when managing clients (check Intel AMT component configuration in ConfigMgr Console).
- Check the current Windows user (operating the WebUI) is included in the Intel AMT ACL clients (check Intel AMT component configuration in ConfigMgr Console).
- Check the current Windows user (operating the ConfigMgr Out of Band console) is not a member of a large number of Windows groups. Intel AMT limits Kerberos ticket size so membership of a large number of groups may cause Kerberos

authentication to fail. Use TOKENSZ tool and see Microsoft article "Troubleshooting Kerberos Errors" to determine group membership and ticket size. Newer Intel AMT firmware supports larger Kerberos ticket sizes. Firmware can be remotely upgraded.

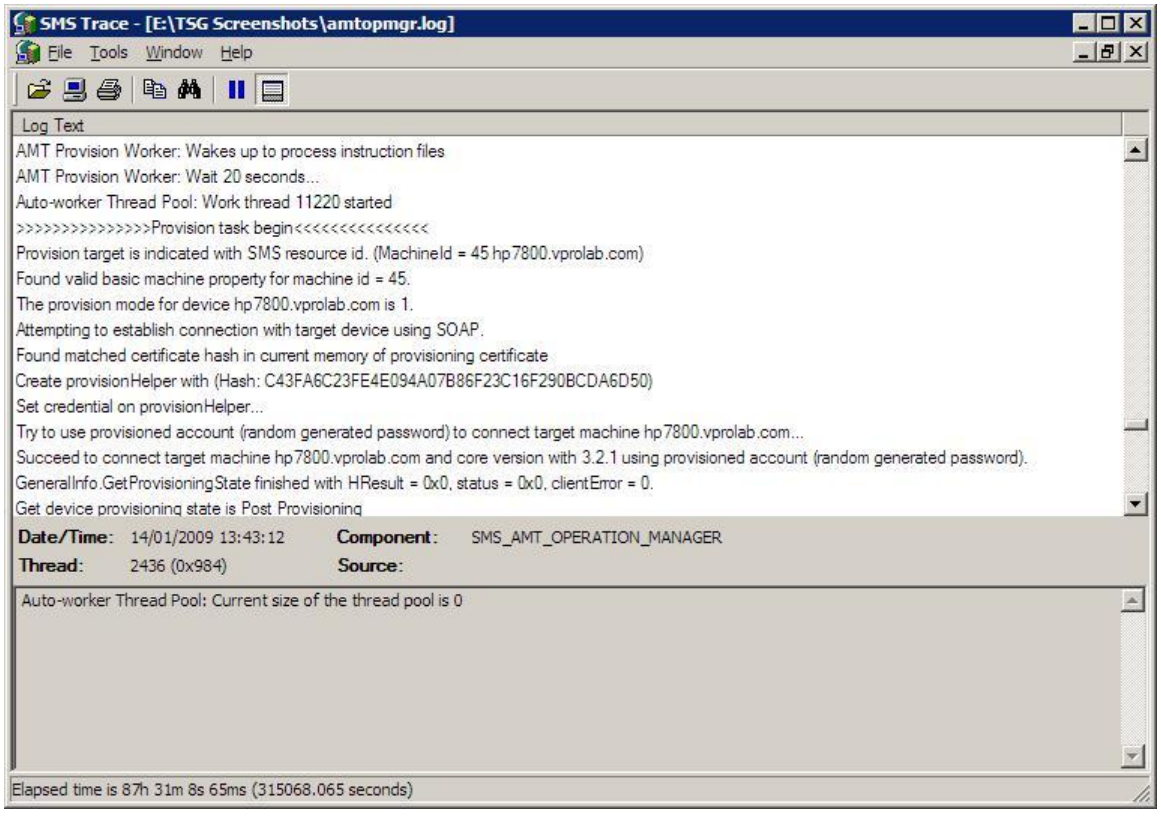
Stage 7 - Client Un-Provisioning Successful

Tested Functionality

- ConfigMgr permissions to Enterprise issuing CA are sufficient to revoke certificates.
- ConfigMgr permissions to Active Directory OU or CN are sufficient to allow Management Controller objects to be deleted.

Verification Checks

- Select a provisioned client in the ConfigMgr collection, right-click and use Delete provisioning data from the management controller option to delete all data from Intel AMT memory. Check the AMTOPMGR.LOG file on the ConfigMgr server and confirm the un-provisioning process completed successfully (use Trace32 to view log file and see example in Figure 4 below).
- Check the Enterprise issuing CA and confirm the Intel AMT web server certificate issued to the client Management Controller was successfully revoked.
- Check the Active Directory OU or CN and confirm the Management Controller object was deleted.



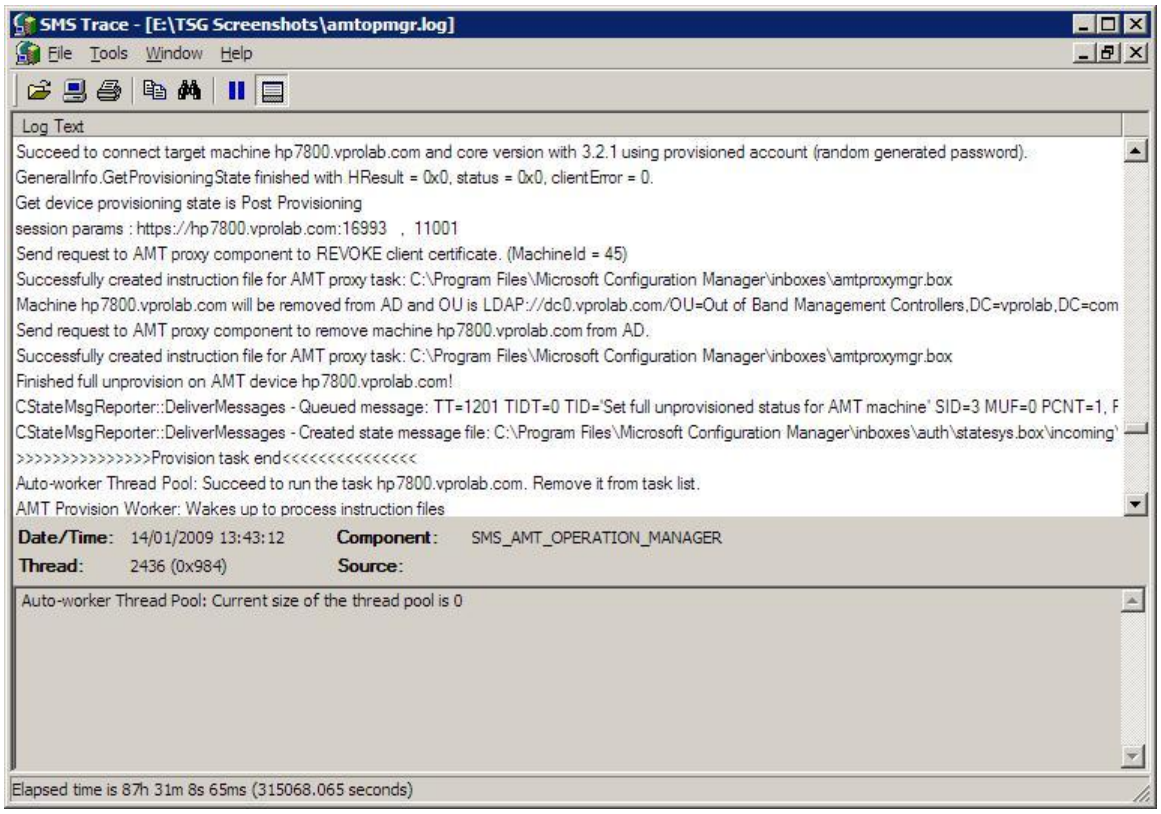


Figure 4 - Trace32 view of AMTOPMGR.LOG showing un-provisioning process starting and continuing to completion

Corrective Actions

- Check ConfigMgr servers have full permission to the Active Directory OU or CN used to hold objects representing client Management Controllers and full control over objects in the OU or CN.
- Check ConfigMgr servers have permission to Issue and Manage certificates for the Enterprise issuing CA (use MMC with Certificate Authority snap-in).

Troubleshooting by Component

This section contains a checklist of tips for major solution components. Work through the checklist for each major component.

Client

- When using ConfigMgr out-of-band provisioning, check the currently selected Intel® Management Engine (Intel® ME) power package allows the Intel ME to be active in the desired client power states to send 'hello' packets. If the selected Intel ME power package configures the Intel ME to be active in client power state S0 only, power on the client to send 'hello' packets. If 'hello' packets must be sent in other client power states select a different power package so the ME is active in other client power states (check using the Intel MEBX).
- Check Intel AMT is enabled in BIOS (check using BIOS Setup).
- Check the Intel ME management mode is set to 'Intel AMT' (check using MEBX).
- Check the Intel ME is configured for DHCP and is receiving a dynamic IP address (check using MEBX and DHCP server).
- Check the Intel ME is un-provisioned (use MEBX to check for presence of provisioning record or perform a full un-provision. Performing a full un-provision erases any existing MEBX data so should be used with caution; if the client is pre-provisioned with PSK or custom certificate hash information this will need to be re-entered after a full un-provision).
- Check the Intel ME is configured for Enterprise mode and either PKI provisioning is enabled or a PSK has been loaded (check using MEBX).
- When using ConfigMgr out-of-band provisioning, check that the Intel AMT client is sending 'hello' messages (use a network packet capture tool to monitor the network, use an agent like ZTCLOCALAGENT to restart packets, or perform a full un-provision to restart packets. Performing a full un-provision erases any existing MEBX data and should be used with caution; if the client is pre-provisioned with PSK or custom certificate hash information this will need to be re-entered after a full un-provision. Also note that certain OEM's have configured their platforms so they no longer send 'hello' packets automatically - in such a situation, use ZTCLOCALAGENT to initiate 'hello' packets).
- Check clients have had sufficient time to request provisioning; when using ConfigMgr Out of Band provisioning clients send 'hello' packets at a decreasing frequency the longer they are turned on and eventually stop sending 'hello' packets; when using ConfigMgr in-band provisioning ConfigMgr agents may take up to 25-hours to recognize the automatic in-band provisioning setting on the ConfigMgr server depending on collection membership update frequency and client policy update period. If using ConfigMgr Out of Band provisioning, restart the 'hello' packet sequence. If using ConfigMgr in-band provisioning, enable automatic in-band provisioning for an ConfigMgr collection containing the client, update ConfigMgr collection membership to re-generate client policy, download the ConfigMgr machine policies to the client and force the ConfigMgr agent to restart

the in-band provisioning process. (See Intel® vPro™ Expert Center article "Using WMI to force the SCCM Agent to check for its AMT Auto Provisioning Policy" for details of restarting ConfigMgr in-band provisioning).

- When using ConfigMgr out-of-band provisioning, check client 'hello' packets are directed to the correct ConfigMgr server (use NSLOOKUP at the client to lookup 'ProvisionServer' and verify the IP address matches the ConfigMgr server IP address, or check DNS for a 'ProvisionServer' record with the correct ConfigMgr server IP address, or check MEBX for correct Provision Server IP address, or check any Operating System hosted ACTIVATOR is using the correct ConfigMgr server IP address).
- When using ConfigMgr in-band provisioning, check the Intel MEI (formerly Intel HECI) driver is installed and started on the client (check using Windows driver manager).
- When using ConfigMgr in-band provisioning, check the ConfigMgr agent is installed and assigned to an ConfigMgr site code with the Out of Band Service Point installed (check using Configuration Manager on the client).
- When using ConfigMgr in-band provisioning, check the ConfigMgr agent is from ConfigMgr SP1 or later.
- When using ConfigMgr in-band provisioning, check the ConfigMgr automatic provisioning policy has been downloaded by the ConfigMgr agent and is enabled (check using OOBMGMT.LOG file on client).
- When using ConfigMgr out-of-band provisioning for clients, verify the ConfigMgr agent is not installed on those clients. If the ConfigMgr agent has been installed on clients and the agent has been detected by ConfigMgr, then only ConfigMgr in-band provisioning can be used with those clients (check using ConfigMgr Console to view the 'Client' column of ConfigMgr collections).
- Check client FQDN does not include any special characters. FQDN should be composed of characters A-Z, a-z, 0-9, minus '-' and period '.'. Underscore characters are not supported and will cause provisioning failure
- Check clients are not impacted by self-signed certificate behavior (upgrade to Intel AMT firmware V3.2.2 or later or apply workarounds documented in Intel® vPro™ Expert Center article "Intel AMT 3.2.1 Self-signed certificate issue and working around it for Microsoft System Configuration Manager SP1"
- After provisioning, check the Intel ME power package is set so Intel ME is ON when the client is powered on (S0 state), in sleep (S3 state), hibernate (S4 state) and powered off (S5 state). Use MEBX or Intel AMT WebUI to set ME power package so ME remains active in sleep, hibernate and power-down states. For volume environments, if the power package is incorrectly set after provisioning, use a post-provisioning script to set the correct power package.
- If SOL / IDER is not operational, check SOL / IDER is enabled in MEBX and client BIOS (check using MEBX and BIOS Setup).

Network

- DNS servers support dynamic updates from DHCP servers
- DHCP servers support DHCP option 81 to perform dynamic DNS updates
- DHCP servers allocating IP addresses to clients also provide DNS domain information to those clients (using DHCP option 15).
- Check network firewalls and firewalls on ConfigMgr servers allow ports 9971, 16992-16995 and any other ConfigMgr required ports (check with network administrator, or use a packet capture tool to confirm transit of packets between clients and ConfigMgr server. Microsoft ConfigMgr help files have port information).
- Check forward and reverse client name resolution is working consistently, and resolves to the correct client (use NSLOOKUP on ConfigMgr server).
- Check the provisioning certificate subject domain or FQDN is trusted by Intel AMT client (check DHCP option 15, or MEBX PKI Domain or MEBX Provision Server FQDN).

ConfigMgr Servers

- Check all ConfigMgr servers that will perform provisioning and verify the Out of Band service point is installed (use ConfigMgr Console to check server roles).
- When using ConfigMgr out-of-band provisioning, check clients have been imported into the ConfigMgr server responsible for client provisioning using "Import Out of Band Management Controller Wizard" (check ConfigMgr collections using ConfigMgr Console) and the Intel ME hostname matches the client OS hostname.
- Check Intel ME Admin credentials are known by ConfigMgr (check Provisioning and Discovery accounts in Intel AMT Component configuration in ConfigMgr Console). Normally this only needs doing if MEBX credentials have changed from default ‘admin/admin’.
- Check hot fixes are installed on ConfigMgr servers (see Appendix A).
- Check the provisioning certificate includes server authentication (check the provisioning certificate).
- Check the provisioning certificate includes special Intel AMT OU and/or OID (check the provisioning certificate).
- Check the provisioning certificate was accepted by ConfigMgr server during configuration of the Out of Band Component and not rejected due to a missing OID or a subject CN domain name that differs from ConfigMgr server domain (check AMTOPMGR.LOG using Trace32
- Check the provisioning certificate has a signing chain that terminates with a trusted root certificate authority (check root certificate thumbprint and use MEBX to compare with client certificate hash list).
- Check the full provisioning certificate signing chain is available on the ConfigMgr Out of Band service point (use MMC to check Windows certificate store).

- Check all certificates in the provisioning certificate signing chain have valid dates (use MMC to check signing chain certificates).
- Check the provisioning certificate and all certificates in the signing chain have key length >=1024-bits and <= 2048-bits (use MMC to check provisioning and signing chain certificates).
- Check the full certificate chain for the Enterprise issuing CA is available on the ConfigMgr Out of Band service point (use MMC to check Windows certificate store)
- Check all certificates in issuing CA signing chain on the ConfigMgr Out of Band service point have valid dates (use MMC to check signing chain certificates)
- In non-COM and non-NET domains, if clients to be provisioned are located in third level DNS domains or below, check child domains are trusted by the client ME (evaluate DNS topology, DHCP option 15, provisioning certificates and Intel AMT firmware version, MEBX DNS Suffix and Provision Server FQDN settings and see Intel® vPro™ Expert Center article "Intel® AMT Remote Configuration Certificate Selection Whitepaper").
- When using legacy clients (i.e. using Intel AMT firmware earlier than V3.2.1), check Intel WSMAN Translator is installed on ConfigMgr servers responsible for provisioning.
- When using PSK provisioning, check Intel WSMAN Translator is installed on ConfigMgr servers responsible for provisioning and all clients are using identical PSK.
- Check access to Intel AMT realms is enabled if functions are unavailable when managing clients (check Intel AMT component configuration in ConfigMgr Console).
- Check the ConfigMgr Console user is included in Intel AMT ACL.
- In a multi-tier PKI environment, if SOL / IDER is not operational, check that root and all subordinate CA certificates are in the local machine Trusted Root Certificate Authority store on systems hosting the ConfigMgr Out of Band Console (using MMC certificates snap-in).
- If SOL is not operational, check the Windows telnet client is installed on the system hosting the ConfigMgr Out of Band Console.
- Check the current Windows user (operating the ConfigMgr Out of Band console) is not a member of a large number of Windows groups. Intel AMT limits Kerberos ticket size so membership of a large number of groups may cause Kerberos authentication to fail. Use TOKENSZ tool and see Microsoft article "Troubleshooting Kerberos Errors" to determine group membership and ticket size. Newer Intel AMT firmware supports larger Kerberos ticket sizes. Firmware can be remotely upgraded.
- Check that the Intel AMT WebUI option is enabled in Intel AMT Component configuration in ConfigMgr Console.
- Check that access to Intel AMT realms is enabled if functions are unavailable when managing clients (check Intel AMT component configuration in ConfigMgr Console).

Active Directory

- Check ConfigMgr servers have full permission to the Active Directory OU or CN used to hold objects representing client Management Controllers and full control over objects in the OU or CN.
- Check domain controller replication has occurred after provisioning if there are multiple domain controllers in the environment.

Certificate Authority

- Check ConfigMgr servers have read and enroll permissions to the Enterprise issuing CA Intel AMT Web Server certificate template (use MMC with Certificate Authority snap-in).
- Check valid Certificate Revocation Lists (CRL) and certificates are available from the Enterprise PKI at CRL Distribution Points (CDP) and Authority Information Access (AIA) points (use MMC with Enterprise PKI snap-in).
- Check the Intel AMT Web Server certificate template includes server authentication and indicates the subject name is supplied in certificate requests (use MMC with Certificate Template snap-in).
- Check ConfigMgr servers have permission to Issue and Manage certificates for the Enterprise issuing CA (use MMC with Certificate Authority snap-in).

Other

- Check client/server times and time zones are synchronized.
- Check the Intel AMT WebUI URL is specified using the client FQDN and not an IP address or other address alias otherwise Kerberos authentication will fail.
- When using Microsoft Internet Explorer to connect to the Intel AMT WebUI, enable Integrate Windows Authentication in the browser's Advanced Internet Options and restart the browser.
- For browsers hosted on Windows Server 2003 SP1 or earlier or Windows XP SP2 or earlier, check hot fix KB908209 is installed and check the registry entry associated with KB908209 is added. For browsers hosted on Windows Server 2003 SP2 or later or Windows XP SP2, KB908209 is already included but the registry entry associated with KB908209 must still be added for Windows XP, Windows Vista, Windows 7, Windows Server 2003 and Windows Server 2008.

References

1. Microsoft Corporation (1 December 2008), *Configuration Manager Documentation Library*, [Online document], Available from: http://technet.microsoft.com/en-us/library/bb680651.aspx (accessed 16 February 2009)
2. Microsoft Corporation (March 2004), *Troubleshooting Kerberos Errors*, [Online document], Available from:

http://www.microsoft.com/DOWNLOADS/details.aspx?FamilyID=7dfeb015-6043-47db-8238-dc7af89c93f1&displaylang=en (accessed 24 February 2009)

Appendix A – Hot Fixes Applicable to Windows Server 2003 / ConfigMgr SP1

- KB899900

  Windows HTTP Services does not let you append a port number to the service principal name in a program or service when you use Kerberos authentication on a Windows Server 2003 SP1-based computer.

  Note: This hot fix is included in Windows Server 2003 SP2.

- KB932303

  WMI service stops responding on a computer that is running the .NET Framework 2.0 and System Center Configuration Manager 2007.

- KB936059

  Update for Windows Remote Management (WinRM) feature in Windows Server 2003 and Windows XP.

- KB940848

  Hot fix rollup package for Microsoft Management Console (MMC) in Windows Server 2003, Windows XP and Windows Vista.

- KB942841

  Windows Server 2003-based computer cannot make an SSL connection or a TLS connection to the out-of-band interface on an Intel AMT-enabled computer.

- KB960804

  Hot fix rollup package containing KB954718, KB955126, KB955114, KB955355, KB956337, KB957183, KB957469 and KB959040.

- KB954718

  Cannot use the Out of Band Management console in Configuration Manager 2007 to connect to computers that use versions of Intel AMT earlier than version 3.2.1.

- KB955126

  The SMS_Executive service process (Smsexec.exe) in System Center Configuration Manager 2007 may crash if you have Intel AMT-related software installed.

- KB955114

  The SMS_Executive service process may crash when the System Center Configuration Manager 2007 SP1 Hierarchy Manager handles the site control (.ct2) file from child sites that are running the RTM version of Configuration Manager 2007.

- KB955355

  A distinguished name that contains more than 100 characters and that is discovered from Active Directory for an Intel AMT host causes the SMS_EXECUTIVE service to crash in System Center Configuration Manager 2007.

- KB956337

  System Center Configuration Manager 2007 Service Pack 1 is unable to remove Intel AMT user ACLs during the provisioning process for Intel AMT 2.x computers.

- KB957183

  Cannot add a group as an Intel AMT user account in Configuration Manager 2007 Service Pack 1 if the group name has more than 20 characters.

- KB957469

  Out of Band Power control function does not work for clients that have Intel AMT 4 or Intel AMT 5 chipset in System Center Configuration Manager 2007 Service Pack 1.

- KB959040

  System Center Configuration Manager 2007 Service Pack 1 systems cannot provision Intel AMT 2.2/2.6 clients in PKI mode and Intel AMT 2.1/2.5 clients in PSK mode.

Appendix B – Hot Fixes Applicable to Internet Explorer

- KB908209

  Internet Explorer 6, 7 or 8 cannot use the Kerberos authentication protocol to connect to a Web site that uses a non-standard port (i.e. port 16992 or 16993 used by Intel AMT).

  Note: The binary portion of this hot fix is required for versions of Windows XP prior to SP3 and versions of Windows Server 2003 prior to SP2. The binary portion of this hot fix is already included in Windows XP SP3, Windows Vista, Windows 7, Windows Server 2003 SP2 and Windows Server 2008. There is an associated registry entry which must be added for the binary portion of the hot fix to be effective. This registry entry is not included in any Windows Operating System and must be added to use Internet Explorer 6, 7 and 8.