Symantec™ IT Management Suite 7.6 powered by Altiris™ technology

QuickStart Migration Guide: 6.x to 7.6

Introduction

Symantec™ IT Management Suite 7.6 powered by Altiris™ technology is all about IT flexibility and user freedom. It provides more flexibility than ever before while giving users more freedom to choose where and how they work. IT can now securely manage remote users, rapidly deploy and support new devices, platforms, and applications while also working smarter with simplified administration and reporting tools.

This QuickStart Migration Guide is designed for IT professionals to outline the steps required for successful migration to IT Management Suite 7.6 from an Altiris 6.x infrastructure.

Server OS Considerations

Windows Server 2012 R2 is the preferred host operating system. The process of moving to Windows Server 2012 R2 might vary greatly depending on the current operating system and the chosen upgrade pathway. Use the following link to determine the optimal upgrade path: https://technet.microsoft.com/en-us/library/dn303416.aspx

Hardware Considerations

It is important to review the hardware requirements for both the ITMS server and SQL Server. It is recommended that organizations larger than 5,000 endpoints dedicate separate servers for ITMS and SQL. Also note that while virtual environments are supported, the overall success and performance in virtual environments depends on proper management and resource allocation to the entire ITMS infrastructure – in particular the SQL and ITMS Servers.

Additional Considerations

Changes in Symantec Installation Manager

The Symantec Installation Manager (SIM) is used to install the Symantec Management Platform and IT Management Suite solutions. During the installation process, the Symantec Installation Manager verifies hardware and software prerequisites. The new SIM will ensure the following prerequisites are met for a successful migration:

- Checks whether there is sufficient OS drive space on the server to store the logs and data that is posted by the agent or Notification Server.
- Checks the database collation during an upgrade that uses an existing database. The collation for the database server and the existing database need to match, otherwise the installation cannot continue.
- Integration of the KMS store utility with the SIM. This utility can restore backed-up cryptographic keys. The KMS restore utility: \Program Files\Altiris\Symantec Installation Manager\KMSRestoreUtility\ KMS_Utility
- Integration of IT Analytics, Report Server and Analysis Server configuration through SIM. Configuration is optional and can still be done later in the management console.
- New install readiness checks are added and upgraded for ASP.NET 4.5.1, SQL 2014, WCF4.5.1, Java 8, and Migration Wizard IRC.

For more information about Symantec Installation Manager, see the Symantec Installation Manager Getting Started Guide at the following URL: http://www.symantec.com/docs/DOC6717

Legacy Agent Communication

Some agent communication and connectivity options have changed. The Legacy Agent Communication (LAC) mode allows computers that use older versions of Symantec Management Agent to communicate with the upgraded 7.6 Notification Server. This option also allows agents to be updated in phases rather than updating all of them immediately after the upgrade of Notification Server. When performing an upgrade or redirection of agents from a 6.x system, agents should first be pointed to a 7.1 SP2 MP1.1 install. Once upgraded to this intermediate step, enabling legacy agent communication mode is required on the 7.6 install. This ensures proper communication between the 7.1 SP2 MP1.1 agents and the 7.6 server. Depending on the installation method selected within the SIM, this functionality may need to be enabled *after* 7.6 is installed. If an upgrade installation is performed, legacy communication should be enabled by default.

Cloud-Enabled Management (CEM)

Cloud-enabled Management (CEM) allows for remote endpoint management when endpoints are not connected directly to the corporate network or through VPN. This functionality helps to improve inventory, software and patch deployment coverage of mobile workforces and telecommuting employees. CEM requires fully secure communication between roaming endpoints and Notification Server(s) on the internal network and supports most ITMS solutions. CEM is supported on Windows and Mac clients only.

Clients that utilize Cloud-enabled Management are required to use SSL. SSL communications are required between the SMP, the Internet Gateway and the CEM endpoint. This does not mean all clients are required to use SSL. While enabling all clients to utilize SSL may be easier, it may also increase processing of SSL based communications. It is possible to configure an explicit group of CEM clients for SSL while allowing others to communicate over regular http. This requires multiple client policies – at least one for CEM based endpoints requiring communications via https and one for non-CEM based endpoints allowing for http communications. To allow both http and https traffic to the SMP server, perform the install in SIM without the https/ssl required option.

Internet Gateway

Symantec recommends having at least two Internet gateways to provide failover options, load balancing, and to maintain communication continuity. Each Internet gateway can serve multiple Notification Servers. This configuration is supported even if Notification Servers are organized in a hierarchy. Each Internet gateway supports 1- 60,000 endpoints and 3,000 concurrent connections. Installing Internet Gateway on a virtual computer is not recommended. Running Internet gateway on virtual hardware can lower its scalability by up to 40%.

Site Server Services

Consider deployment locations for site server services. In ITMS 7.6 it is possible to install individual services, such as task, package and NetBoot service (NBS/PXE). A general recommendation is to consider concentrating task services in a central location while deploying package and NBS services to locations in closer proximity to managed endpoints. As an example, NBS services require traffic forwarded between subnets if the NBS services are not on the same network segment as the computer PXE booting.

Mac Management

In order to perform Mac management, OS X Server Tools as well as an OS X source computer are required to create NetBoot and NetInstall packages. Once these are created NBS services are utilized for imaging and installation tasks.

System Requirements

For complete details on platform and OS support, please review the Platform Support Matrix.

Management Server OS

Windows Server 2008 R2, 2008 R2 SP1
Windows Server 2012 R2
VMware ESX 3.5, 4.0, 5.0, 5.1, ESXi 5.5
Windows Hyper-V Server 2008 R2, 2012
Microsoft SQL Server 2008 SP2, 2008 SP3
Microsoft SQL Server 2008 R2, 2008 R2 SP1, 2008 R2 SP2
Microsoft SQL Server 2012
Microsoft SQL Server 2014

Management Server Software

- Microsoft IIS 7.5 (IIS 6 compatibility), Microsoft IIS 8.5 Native
- Java 8
- Microsoft Internet Explorer: 7, 8, 9, 10, 11
- Microsoft .NET Framework 4.5.1
- Microsoft Silverlight 5.0

Workflow Server

- Windows Server 2008 R2, 2008 R2 SP1 (64-bit only)
- Windows Server 2012 R2

Agents

The following applies to Client Management Suite and Server Management Suite. Asset Management Suite does not have an agent.

Windows Agent

- Windows 8, Windows 8.1
- Windows 7, Windows 7 SP1, Windows 7 Embedded SP1
- Windows Vista SP2
- Windows XP SP3 (x86), Windows XP SP2 (x64)

- Windows Server 2003 SP2 or later
- Windows Server 2008, 2008 R2, 2008 R2 SP1
- Windows Server 2012, 2012 R2
- Windows Hyper-V Server 2008
- Windows Small Business Server (SBS) 2003 R2, 2008

Mac Agent

- OS X 10.8, 10.9, 10.10
- OS X Server 10.9, 10.10

Linux Agent

- Red Hat Enterprise Linux Desktop: 5.10, 6-6.5, 7(partial)
- Red Hat Enterprise Linux Server: 5.10, 6-6.5, 7(partial)
- SUSE Linux Enterprise Desktop: 10, 11, 11 SP1, 11 SP2
- SUSE Linux Enterprise Server: 10, 11, 11 SP1, 11 SP2
- VMware ESX/ESXi (agentless): 3.5, 4.0, 4.1, 5.0, 5.1, 5.5

UNIX Agent

- IBM AIX 6.1, 7.1
- HP HP-UX 11i (PA-RISC), 11i v2 (PA-RISC), 11i v3 (PA-RISC /IA-64)
- Oracle Solaris 9 (SPARC), 10 (SPARC/x86/x64), 11 (SPARC/x86/x64)

Minimum Hardware Recommendations

Symantec Management Platform

SMP Hardware:

Component	**Evaluation**	**100-1,000 endpoints**	**1,000 – 5,000**	**5,000 – 10,000**	**10,000 - 20,000**
Processors	Two Cores\2.4 Ghz or more	Eight Cores\2.4 Ghz or more	Eight Cores\2.4 Ghz or more	Eight Cores\2.4 Ghz or more	8-12 Cores\2.4 Ghz or more
Disk Speed (in IOPS)	180 – C: OS, SMP	180 – C: OS, SMP	180 – C: OS, SMP	180 – C: OS 130 – D: SMP	180 – C: OS 130 – D:SMP 130 – E:Storage
Disk Capacity	80GB	80GB	200GB	400GB	600GB

SMP Hardware (continued):

Component	Evaluation	100-1,000 endpoints	1,000 – 5,000	5,000 – 10,000	10,000 - 20,000
RAM	4GB	8GB	16GB	16GB	16GB
Cache	6MB L2 or More				
Network	Dual Gigabit – Load Balanced				
OS	Windows Server 2012 R2 Standard or Enterprise				

SMP Server Software:

Component	
OS	Recommended: 2012 R2 Standard or Enterprise Alternative: 2008 R2 Standard or Enterprise (SP1 Supported)
IIS	On 2012 R2: 8.5 Native On 2008 R2: 7.0 + 6.0 compatibility
.NET	4.5.1
IE	Internet Explorer

Service Account:

Domain Account	Local Admin
Altiris Service Account	Local Admin on the Symantec Management Platform. It is also Beneficial for the account to be a Local Admin on site Servers, however that is not a Requirement.

SQL Hardware:

Processors	Evaluation	100-1,000 endpoints	1,000 – 5,000	5,000 – 10,000	10,000 -20,000
Processors	Two Cores/2.4Ghz or More	Four Cores/2.4Ghz or More	Eight Cores/2.4Ghz or more	8-16 Cores/2.4Ghz or more	16 Plus Cores/2.4Ghz or more
Disk Speed (IOPS)	180 - C: OS, SMP 200 – D:SQL	180 - C: OS, SMP 200 – D:SQL	180 - C: OS, SQL App 300 - D: SQL DB 300 - E: Logs 200 - F: TempDB	180 - C: OS, SQL App 400 - D: SQL DB 400 - E: Logs 300 - F: TempDB	180 - C: OS, SQL App 600 - D: SQL DB 600 - E: Logs 400 - F: TempDB

SQL Hardware (Cont'd)

RAM	Evaluation	100-1,000 endpoints	1,000 – 5,000	5,000 – 10,000	10,000 -20,000
RAM (GB)	16 GB	16 GB	16+ GB	24+ GB	32+ GB
Drives	**Disk Configuration**	**IOPS**	**Write %**	**Read %**	**Drive Size**
Operating System Drive	RAID 1 (Mirrored)				
CMDB Drive	RAID 10 or RAID 0+1	250	98%	2%	=>5-8 MB Per Client
TempDB Drive	RAID 0 (Striped)	2	49%	51%	=>10% of CMDB
Transaction Log Drive	RAID 10 or RAID 0+1	600	100%	0%	=>10% of CMDB

SQL Software:

Evaluation	100-1,000 endpoints	1,000 – 5,000	5,000 – 10,000	10,000 -20,000
Microsoft SQL Server Express 2008 SP2 or higher, 2012, 2014.	Microsoft SQL Server 2008 SP2 or higher, 2012 or 2014 Standard or Enterprise. On-box SQL is supported; off-box SQL is recommended.		Microsoft SQL 2008 SP2 or higher, 2012 or 2014 Standard or Enterprise. Symantec recommends off-box SQL.	

Site Server – Package / Site / PXE

SS Hardware:

Component	10-100 endpoints	100 – 1,000	1,000 – 5,000	5,000 - 7500
Operating System	Desktop / Server OS	Server OS	Server OS	Server OS
Processors	One core	Two cores	Four cores	Four cores
Disk Capacity	100 GB – 250 GB	100 GB – 250 GB	100 GB – 250 GB	100 GB – 250 GB
RAM	4	4	4-6 GB	4-8 GB

SS Software:

Component	
OS	XP x86/x64 SP2 + Vista x86/x64 SP2 + Win 7 x86/x64 2008 SP1 +, 2008 R2 + 2012 R2
.NET	4.5.1
IIS	IIS 7 with IIS 6 compatibility components
IE	Internet Explorer

Internet Gateway:

Component	Requirement
OS	Windows 20012 R2 SP1
Processors	Dual Core CPU
RAM (GB)	8 GB
Disk Capacity	At least 40GB

Migration Paths

Starting with ITMS 7.0, the separate Notification Server and Deployment Servers have been combined into the unified Symantec Management Platform with a single console to manage endpoints. This means that a migration must be performed when transitioning from 6.x to any 7.x version. There is no direct upgrade path from 6.x to 7.6. Simply upgrading the system is not possible. This will require incremental upgrades, e.g. 6.0 > 7.1 SP2 MP1.1 > 7.6 or 6.0 > 7.5 SP1 HF5 > 7.6. Due to additional steps necessary for 7.5 SP1 HF5, the recommended upgrade path is 6.0 > 7.1 SP2 MP1.1 > 7.6.

For more information about upgrade path requirements and the recommended upgrade paths visit: http://www.symantec.com/docs/DOC7718

Migration Tips

Use a test environment

Before installing Symantec Management Platform 7.6 in a production environment, create a test environment for evaluating and validating the entire installation and migration process. Symantec recommends maintaining the test environment for ongoing validation.

Use a pilot test group

Use a small group of managed computers as a pilot group to test the migration to Symantec Management Platform 7.6. During this pilot test, allow the remaining managed computers to be supported by the previous version of Notification Server.

Make note of all configuration settings before migrating

Examples to document before the migration process include:

- All Task Server settings
- All agent communication settings
- All policy refresh settings
- All membership update settings

After a successful migration use these settings to configure the new environment.

Ensure that Legacy Agent Communication (LAC) mode is enabled

To allow complete management of legacy agents when the upgrade is in progress, ensure that Legacy Agent Communication mode is enabled.

Redirect managed computers in small groups

Redirect a group of *8,000 or less computers at a time to a single Notification Server. After successfully redirecting a group of computers, upgrade the Symantec Management Agent and agent plug-ins for that group. To upgrade an agent or agent plug-in, enable the upgrade policy for the agent or the agent plug-in.

*Note: If redirecting more than 8,000 computers at a time, disable any policies and tasks that communicate frequently with the Symantec Management Agent. For example, disable the inventory, software delivery, and patch policies. Disabling the policies and tasks prevents Notification Server from being overly taxed and potential latency issues in the management console.

Keep the 6.x Notification Server.

Maintain the previous Notification Server as a baseline for historical data, policy configuration details, and other settings and data. Decommissioning the old server may be considered in the following circumstances:

- After the business functional uses on the old server are matched on the new server.
- After the data saturation on the new server has the needed depth.
- When the data in the new Configuration Management Database (CMDB) qualifies against company regulatory standards

Migrate to new hardware

Install the Symantec Management Platform 7.6 products on a server running Windows Server 2012 R2. Because this operating system is *different from the requirements for 6.x, Symantec recommends installing ITMS 7.6 on new server hardware.

*Note: As Notification Server 6.x is installed on a 32-bit server, the operating system requires upgrade or replacement. Upgrading the operating system is not a recommended migration path, as this complicates the upgrade of the Symantec Management Platform and the Notification Server itself. New hardware will help to ensure best practices are met and migration is successful.

Upgrading the agent

The 6.x AClient and DAgent can co-exist with the SMA. While this approach requires careful consideration of PXE/NBS services it allows for a rip-and-replace style migration of the agent. Create a script that will remove the 6.x Altiris Agent and associated components and install a clean 7.6 Symantec Management Agent pointing to the new server.

- After the upgrade, make sure the Legacy Agent Communication mode is set to enabled.
- After the upgrade is completed and all agents are upgraded to the latest version, disable the Legacy Agent Communication mode.
- Consider uninstalling all agent plug-ins (sub-agents) on the 6.x Altiris Agent prior to migrating.
- To perform this automatically, make use of the sub-agent uninstall policies. Create a collection to track all endpoints which meet the criteria of “no sub-agents” installed and use this as a basis to target with a new policy to re-direct/migrate the agent.
- Consider utilizing DS 6.x in the environment to migrate Altiris Agents from 6.x to Symantec Management Agents on 7.6

Hierarchy Migration

If migrating into a hierarchy, map out which clients will be managed by which SMP servers. Consider an intermediate 7.1 SP2 MP1.1 system to first migrate and update endpoints to a state allowing upgrade to 7.6 or alternatively build out the hierarchy as 7.1 SP2 MP1.1, then upgrade it and all endpoints to 7.6 after verifying all connected clients have graded to 7.1 SP2 MP1.1.
Additional logic and policies will be required to migrate clients to specific SMP servers. Typical scenarios include assigning a client’s 7.6 SMP based on geographical proximity.

Altiris 6.x to ITMS 7.6 Migration Steps

Upgrade options from 6.x to 7.6 vary depending on what Operating System is desired to host the final 7.6 Notification Server. Due to unsupported direct migration paths from 6.x to 7.6, the upgrade requires two version steps: One from 6.x to 7.1 SP2 MP1.1, and another from 7.1 SP2 MP1.1 to 7.6. The following steps assume Windows 2012 R2 as the chosen Notification Server OS and require an intermediary 2008 R2 Server to host the 7.1 SP2 MP1.1 installation.

1. Back up the 6.x Notification Server
2. Back up the 6.x Notification Server Database
3. Prepare for the migration
    a. On the 6.x Notification Server, complete the precautionary steps before starting the migration process.
4. Prepare the 7.1 SP2 MP1.1 server for installation
    a. The 7.1 server must be running the Microsoft Windows 2008 R2 operating system. Symantec recommends giving the 7.1 server a different name and IP address from the name and IP address of the 6.x server. Because the Windows server user accounts are not migrated during the migration, recreate them on the 7.1 server after the migration process. The following items must also be installed:
        i. ■ SSL and certificates if required.
        ii. ■ Third-party plug-ins required by the selected products. These may include Microsoft Silverlight, Adobe Flash Player, and Java.
5. Install Symantec Installation Manager on the 7.1 server
6. Select the Symantec Management Platform 7.1 components
    a. Install the Symantec Management Platform 7.1 products with Symantec Installation Manager. Install the same or the equivalent products already installed on the 6.x server.
    b. Install the migration wizard components from the Optional Installations page. The migration wizard components can be installed at any time using Symantec Installation Manager.
    c. At the end of the installation process, Symantec Installation Manager will prompt for applicable licenses based on the installed solutions. Licenses may also be applied within Symantec Installation Manager at a later time. See the ITMS 7.1 Planning and Implementation Guide for more details on licensing.
7. Migrate Notification Server 6.x data to the 7.1 server
    a. Use the migration wizard to migrate 6.x data to the new server.
    b. Note: The migration wizard verifies the success of the data it imports. Browse through the migrated data such as policies, reports, and packages to verify accuracy and completion.
8. Move solution-specific items from the 6.x server to the 7.1 server and configure the solutions
    a. Some solution-specific items are not migrated with the Notification Server Database or with the migration wizard. These items must be manually moved from the 6.x server to the 7.1 server.

   b. Each of the 7.1 solutions must be configured as applicable for the intermediary infrastructure. For more detailed information on configuration see the applicable 7.1 Configuration Guide for each solution.

9. Configure and upgrade site servers

   a. Before configuring site servers, first determine how many site servers are required. Then create the sites and configure the site servers. For recommendations on the number of site servers need, refer to the IT Management Suite 7.1 Planning and Implementation Guide.

   b. Note: A Site Server with Task Service must have the .NET Framework feature enabled.

   c. 6.x package servers must be redirected to the 7.1 Notification Server to upgrade to the latest Symantec Management Agent. The agent upgrade also upgrades the site server.

10. Download packages to upgraded package servers

    a. If the agent on a package server is upgraded from a 32-bit to 64-bit, all packages must be downloaded again.

11. Migrate managed endpoints

    a. Redirect all endpoints from the 6.x Notification Server to the new 7.1 Notification Server.

    b. Upgrade all agents and agent plug-ins on managed endpoints.

12. Prepare the 7.6 server for installation

    a. The 7.6 server should be running the Microsoft Windows 2012 R2 operating system (2008 R2 is also supported, but not recommended). Symantec recommends that giving the 7.6 server a different name and IP address from the name and IP address of the 6.x and 7.1 server. Because the Windows server user accounts are not migrated during the migration process, recreate them on the 7.6 server after the migration process. The following items must also be installed:

       i. ■ SSL and certificates if required.

       ii. ■ Third-party plug-ins required by the selected products. These may include Microsoft Silverlight, Adobe Flash Player, and Java.

13. Install Symantec Installation Manager on the 7.6 server

14. Select the Symantec Management Platform 7.6 components

    a. Install the Symantec Management Platform 7.6 products with Symantec Installation Manager. Install the same or the equivalent products that are installed on the 7.1 server.

    b. Install the migration wizard components from the Optional Installations page. The migration wizard components can be installed at any time using Symantec Installation Manager.

   c. At the end of the installation process, Symantec Installation Manager will prompt for applicable licenses based on the installed solutions. Licenses may also be applied within Symantec Installation Manager at a later time. See the ITMS 7.6 Planning and Implementation Guide for more details on licensing.

15. Migrate Notification Server 7.1 data to the 7.6 server
    a. Use the migration wizard to migrate 6.x data to the new server.
    b. Note: The migration wizard verifies the success of the data it imports. Browse through the migrated data such as policies, reports, and packages to verify accuracy and completion.
16. Move solution-specific items from the 7.1 server to the 7.6 server and configure the solutions
    a. Some solution-specific items are not migrated with the Notification Server Database or with the migration wizard. These items must be manually moved from the 6.x server to the 7.6 server.
    b. Each of the 7.6 solutions must be configured. For more detailed information on configuration see the applicable 7.6 Configuration Guide for each solution.
17. Ensure that that the Legacy Agent Communication (LAC) mode is enabled on Notification Server
    a. The LAC mode allows computers that use older versions of the Symantec Management Agent to communicate with the upgraded Notification Server. If LAC mode is turned on, the legacy agents can communicate with Notification Server and upgrade accordingly.
18. Define the Agent Registration Policies (Optional)
    a. After upgrading the Symantec Management Agent, the agent sends out registration request to Notification Server to establish the communication. A predefined agent registration policy that is enabled by default allows all computers to register at Notification Server. To restrict access to Notification Server, configure custom agent registration policies.
    b. Note: Agent registration policies are applied only to those agents that are upgraded to the 7.6 version.
19. Configure and upgrade site servers
    a. Before configuring site servers, first determine how many site servers are required. Then create the sites and configure the site servers. For recommendations on the number of site servers need, refer to the IT Management Suite 7.6 Planning and Implementation Guide.
    b. Note: A Site Server with Task Service must have the .NET Framework 4.5.1 feature enabled. Windows Server 2012 R2 has .NET 4.5.1 enabled by default.
    c. 7.1 package servers must be redirected to the 7.6 Notification Server to upgrade to the latest Symantec Management Agent. The agent upgrade also upgrades the site server.

20. Download packages to upgraded package servers
    a. If the agent on a package server is upgraded from a 32-bit to 64-bit, all packages must be downloaded again.
21. Migrate managed endpoints
    a. Redirect all endpoints from the 7.1 Notification Server to the new 7.6 Notification Server.
    b. Upgrade all agents and agent plug-ins on managed endpoints.
22. View and manage the agent registration status to verify successful registration
    a. Use the Agent Registration Status Report to view and manage all registration requests and completed registrations from Symantec Management Agents. This report also displays whether site servers have successfully established communication with the new Notification Server.

For more detailed information on the topics above, refer to the Symantec Management Platform 7.6 Planning and Implementation Guide and the ITMS 7.6 Configuration Guides.

Migration Notes

Required version of Notification Server 6.x

Notification Server must be at least 6.0 R13 and the latest solutions must be installed before migrating from Notification Server 6.x to Symantec Management Platform 7.x. Upgrade to the latest 6.x version prior to beginning 7.1 upgrade activities. For example, if Notification Server 6.0 R11 is installed, an upgrade to 6.0 R13 is required before migrating to Symantec Management Platform 7.1 then > 7.1 SP2 MP1.1 or 7.5 SP1 HF5 > 7.6. None of the 7.1 or 7.5 platforms support installation to a 32-bit operating system.

Database and server backup

Before beginning the migration, back up the 6.x Notification Server Database and the 6.x Notification Server to a secure and accessible location. If problems occur during the migration process, simply revert to these backups.. Making backups before major migration steps provides more granular recovery options from any issues or unplanned outages that might occur during the migration process.

New database requirement

When installing Symantec Management Platform 7.6, a new database must be created due to schema changes in the database. Performing an update to the 6.x database is not possible. These schema changes were made to increase speeds and unify the database structure.

Product parity

Before beginning the migration, create a list of the 6.x products currently installed. When installing the Symantec Management Platform 7.6 products, install at minimum the equivalent products installed on the 6.x Notification Server.

Warning: Failure to have minimum product parity can result in the inability to migrate 6.x data to the 7.6 database. Keep in mind that some products have been replaced or absorbed by another product, or have a new product name. Some examples of this are below:

- Application Management Solution is now part of Software Management Solution
- Application Metering Solution is now part of Inventory Solution
- Helpdesk Solution is now ServiceDesk
- Real-Time System Manager Solution is now part of Client Management Suite
- Software Delivery Solution is now part of Software Management Solution
- Software Virtualization Solution is now Workspace Virtualization

Server name and IP address

Give the ITMS 7.6 and intermediary 7.1/7.5 server a unique name and IP address; different from the name and IP address of the 6.x server.

Mixed mode

Symantec Management Platform 7.6 does not support mixed mode. A Symantec Management Platform 6.x server cannot communicate with a Symantec Management Platform 7.6 server.

Gotchas

Server Rebuild Required

Altiris 7.6 will require a server rebuild to Windows Server 2012 R2 or 2008 R2. No on box migration is possible. Package data can be migrated with the software replicator tool.
http://www.symantec.com/business/support/index?page=content&id=TECH166711

PXE (NBS)

PXE (NBS) service names have changed. Jobs to restart these services will need to be recreated.

Cloud Enabled Management

- (CEM) requires HTTPS and the use of SSL certificates. These can be self-signed, third-party commercial or internally issued using a Certificate Authority. In all cases the certificates must be trusted by all cloud-enabled endpoints for a successful CEM deployment.
- External remote package servers for CEM may require name changes to match the internal DNS names.
- The CEM Package Server publishes https codebases using the internal FQDN- http://www.symantec.com
- Certificates can only be issued for publicly resolvable domains.

  Example, Company XYZ owns xyz.com, but uses xyz.local inside the corporate network. A certificate for cem.xyz.local cannot be purchased or issued as it will not be resolvable to the cloud-enabled agent.

Solutions

When upgrading to 7.6, any solutions that have not yet been updated to 7.6 (i.e. - Mobile Management), will be uninstalled if the upgrade is allowed to proceed.

ServiceDesk is upgraded to version 7.6. A warning will be displayed in the SIM. For more information, visit http://www.symantec.com/docs/TECH200807

Patch Management Import requires ICMP request to access solutionsam.com (if proxy being used). If ICMP traffic cannot reach solutionsam.com, Patch Management Import will fail.

Out of Band Management (OoB)

This product is no longer bundled with ITMS. The latest OoB component can be obtained directly from Intel at http://www.intel.com/go/scs. Although the OoB provisioning component is no longer bundled, existing RTSM features will continue to function on supported AMT computers. When upgrading from previous versions of ITMS, the OoBRemover utility performs a removal of OoB items from the Notification Server and Site Servers. The Intel SCS/RCS database will remain and provisioned computers will be unaffected by the OoBRemover utility. The Symantec OoB discovery tool can then be used to populate provisioned computers into the CMDB.

Helpful Links

- Symantec IT Management Suite 7.6 Documentation: http://www.symantec.com/docs/DOC8146
- IT Management Suite 7.6 Planning for Implementation Guide: http://www.symantec.com/docs/DOC8038
- IT Management Suite 7.6 Installation and Upgrade Guide: http://www.symantec.com/docs/DOC8039
- Symantec Connect page: http://www.symantec.com/connect/endpoint-management
- Knowledge Base: http://www.symantec.com/page.jsp?id=support-knowledgebase
- SQL 2008 Optimizing: http://www.symantec.com/business/support/index?page=content&id=HOWTO8589
- Software Replicator Tool: http://www.symantec.com/.../index?page=content&id=TECH166711
- Symantec Management Platform Support Matrix: http://www.symantec.com/docs/HOWTO9965