UPL08 – Symantec Management Platform Troubleshooting Hands-On Lab

Description	In this session, you will learn the methodologies behind the troubleshooting of common agent, site server and platform challenges that may arise in your Symantec Management Platform environment. You will also learn about the tools and utilities available to you to aid in resolving these issues. This lab assumes a prerequisite knowledge of basic Microsoft networking skills, Symantec Management Platform component communications and operations.

At the end of this lab, you should be able to	▪ Learn the troubleshooting methodology applied at the agent, platform and site server levels. ▪ Understand the tools, reports and utilities available for resolving common SMP issues. ▪ Review critical areas to observe to provide a logical path when troubleshooting Agent, Site Server and Platform issues.

Notes	▪ A brief presentation will introduce this lab session and discuss key concepts. ▪ This lab is designed to aid in facilitating troubleshooting discussions with your customer to broker the discussion with support resources in order to reduce the time to resolution. ▪ The lab will **NOT** provide you with complete step-by-step procedures, but rather a tactical approach to resolving the problem. ▪ Feel free to follow the lab using the instructions on the following pages. You can optionally perform this lab at your own pace. ▪ Be sure to ask your instructor any questions you may have. ▪ Thank you for coming to our lab session.

Contents

The Lab Environment

The lab environment consists of a headless Domain Controller, Symantec Management Platform Server with ITMS 7.5 installed, Site Server with Task & Package Services loaded. A single Windows 7 professional system is also included to demonstrate all of the functions found in this SMP Troubleshooting Lab.

- **DC** – Headless Domain Controller
- **NS75** – Notification Server 7.5
- **WIN7** – Windows 7
- **MONITOR** – Windows Server 2008 R2 SP1 (Site Server)

SMP Troubleshooting Methodology

When critical problems arise in your Production Environment the following steps may help to resolve them:

SMP Environment

- **Identify the cause**
  - Is it environmental? (Firewalls, file system lockdown etc.)
  - Where is it failing? (w3wp.exe, sqlservr.exe, AeXSvc.exe etc.)
  - Which product is failing? (Core, Patch, Inventory etc.)
- **Remediation**
  - What can be done to get the system running again? (process restart, system reboot?)
  - Is this a short-term fix or can it be applied indefinitely?
- **Support Case**
  - What data needs to be gathered? (SMP version, Operating System info, stack traces, etc.)
  - Prioritization of incidents.

SMP Server

- **Non-invasive troubleshooting**
  - Inspecting aspects of the system without affecting it.
    - Reviewing log files.
    - Running various traces. (Altiris Profiler, SQL Server Profiler, Debug View)
    - Monitoring communications. (Web debugging proxies like Fiddler)
    - Running SQL Queries. (nolock hint, execution plans)
- **Invasive troubleshooting**
  - Diagnosing problems that may adversely affect the running system.
    - Attaching a debugger. (Visual Studio, WinDbg, MDbg, MSE)
    - Modifying the CMDB. (UPDATE/DELETE statements, altering stored procedures, views etc)
    - Making changes to CoreSettings.config
    - Making changes to registry keys

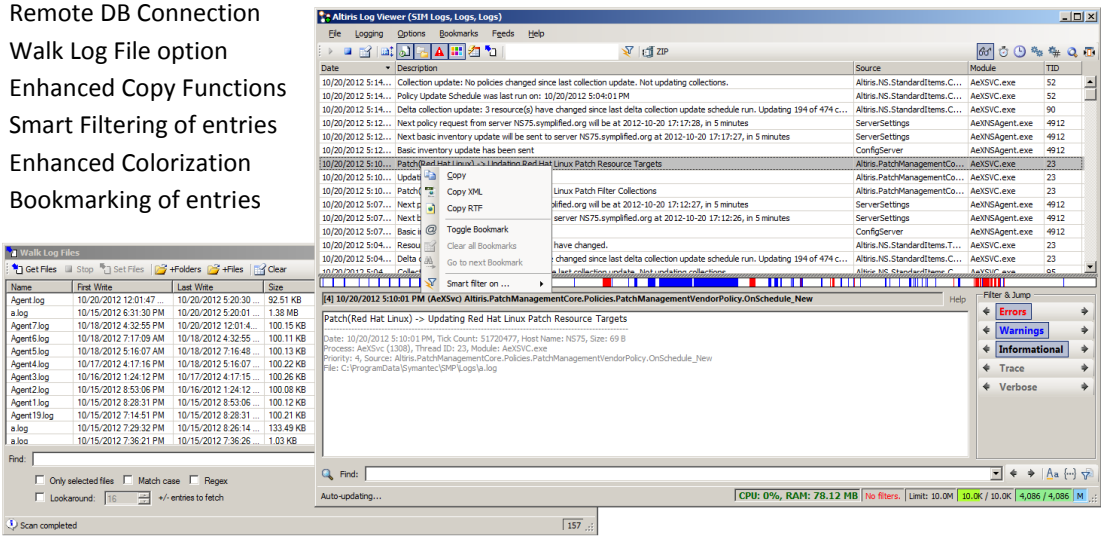
Available Troubleshooting Tools

The Altiris Log Viewer

The purpose of this lab is to provide you with

The Altiris Log Viewer is installed by default as part of the Symantec Management Platform and it provides the following capabilities:

- Provides a convenient way to browse the SMP and Symantec Management Agent logs.
- Highlights important information.
- Filters on severity.
- Can be set to auto-update will keep the log viewer up to date
- Will auto-refresh current log files or can be pointed to a folder or log file to monitor
- Can Register shell extensions for right click open with log viewer
- Change the default file location
- Can turn on trace and informational messages
- Has been updated in SMP 7.5 to include:
    - Enhanced Log View, GUI, and filter options
    - Remote DB Connection
    - Walk Log File option
    - Enhanced Copy Functions
    - Smart Filtering of entries
    - Enhanced Colorization
    - Bookmarking of entries

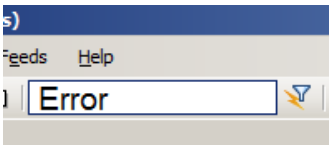


☐ Lab Exercise 1: Altiris Log Viewer

The purpose of this lab is to provide an overview of the Altiris Log Viewer found in the upcoming release of the Symantec Management Platform and to highlight some of the new features.

1. Switch to the **NS75** VM
2. Open the Symantec Management Console (Link on Desktop)
3. Start the **Altiris Log Viewer** in Windows Start Menu under "**All programs > Symantec > Diagnostics**".
4. You will notice that there are possibly red and blue entries in the log. These represent Errors and Warnings in the log. These are the types of entries you would be most interested in when troubleshooting SMP Servers.

5. On the right side of the viewer, under the **Filter & Jump** section, press the **Informational** link. These entries will now appear in black text and would be reviewed by an administrator to troubleshoot the actions happening on the SMP Server.
6. **To enable Smart Filtering:**
    a. Type **Error** or any other text you would like into the Smart Filter Box
    b. Press the **Filter** button next to it



    c. Notice how the content changes to reflect the results you entered.
7. **To Set Enhanced Colorization options:**
    a. Scroll through the log and look under the **TID** Column for a number that seems to be seen multiple times. Remember this number for a later step.
    b. In the main menu choose **Options > Colorization Options**
    c. Press the **Add** button
    d. Select the **Active** checkbox
    e. Select **TID** in the dropdown
    f. Enter the **number** you picked in step a) into the empty field
    g. Press the **'B'** beside the last entry
    h. Choose a bright color like green, then press **OK**
    i. Press the **Colorization** button on the top tool bar. (Looks like a color palette)
    j. Press **OK** – Notice all of the Green Entries. If the color does not appear, make sure the
8. **To Utilize Bookmarks:**
    a. Right click on a log entry and select **Toggle Bookmark**
    b. You will notice a small red triangle on the upper left side of the log entry
    c. Bookmark a few more entries
    d. Right Click and entry and select **Go to Next Bookmark** – repeat to see the next one.
    e. Right Click an entry and select **Clear All Bookmarks** to clear them
9. **To use the Walk Log File function:**
    a. Under the main menu choose **File > Walk Log Files**. The Walk Log Files interface opens
    b. Press the **Get Files** Button. Notice how the window populates all **SMP** Related log files on this system
    c. Double Click on any log file listed and notice how the content now appears in the **Altiris Log Viewer**
    d. Press the **+Files** Button
    e. Browse to **\\MONITOR\c$\ProgramData\Symantec\Symantec Agent\Logs**
    f. Select the any **Agent*xx*.log** file (Not Agent.log)
    g. Select this file in the list – notice that a remote log has appeared in the Altiris Log Viewer. This is an excellent way of walking through remote SMP Servers or endpoint agent logs.
    h. Close the Walk Log File interface
10. You will notice that most of the functions seen in this version of Altiris Log Viewer are very similar to the version 6.x – 7.1 versions.

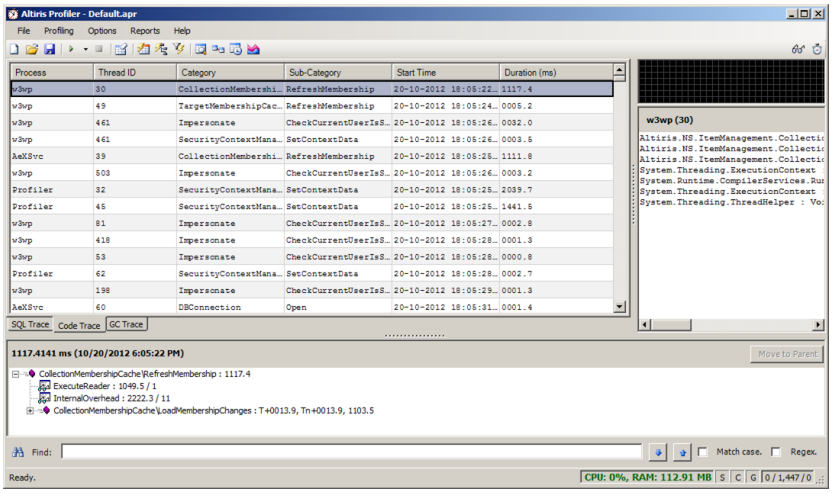
Altiris Profiler

Altiris Profiler is a simple yet powerful tool for analyzing SQL queries and code blocks executing in Notification Server and its associated processes. As well you will be able to do:

- See the .NET stack trace associated with database queries
- Filter collected data based on timing constraints, or substring or regular expression matches
- Copy and paste logged SQL straight into the Microsoft Query Analyzer, complete with pre-substituted command parameters
- Track database errors as they occur with a life profile session
- Set up a zero impact trace from Profiler to run on a schedule
- Search your data with powerful .NET style regular expressions and watch the results appear on your screen live
- Profile executing queries without access to the database server

As well as profiling SQL, it receives, filters, and records information about executing code blocks. With Altiris Profiler you can:

- Instrument your code with a simple but powerful API and immediately see performance results within the profiler,
- Gather information about SQL queries and remoting calls, within the context of executing code blocks,
- Safely profile your code within a production environment.



The Altiris Log Viewer is located under ***Start>All Programs>Symantec>Diagnostics***. The actual files used for it are located under …*Program Files**Altiris**Diagnostics* as Profiler.exe. The fully featured guide and other information are available at the following links:

http://www.symantec.com/business/support/index?page=content&id=HOWTO75167

http://www.symantec.com/business/support/index?page=content&id=HOWTO1673

www.symantec.com/docs/HOWTO75156

Altiris Profiler Tips:

- Ignore the performance graph
- Watch for red (failed) SQL commands when viewing the SQL trace
- Ensure your Filters are configured correctly before leaving Altiris Profiler for an extended period
- Log messages appear (in context) in the code block tree. You can get the stack trace for these
- Fast import is much faster than standard import, but it requires that you lose any data already in the grid
- Filter collected data based on timing constraints, or substring or regular expression matches
- Copy and paste logged SQL straight into the Microsoft Query Analyzer, complete with pre-substituted command parameters
- Don't leave Altiris Profiler running or open. It may cause high memory usage.
- After using Altiris Profiler, clear the trace. It may use unnecessary hard drive space.

☐ Lab Exercise 2: The Altiris Profiler

When errors occur on the Symantec Management Platform, they are not always self-explanatory. In this Lab we will review how to get started with the Altiris Profiler to troubleshoot a particular problem.

Starting the profiler for the first time

1. Switch to the NS75 VM
2. Start the Altiris Profiler in Windows Start Menu under "**All programs > Symantec > Diagnostics**".
3. Press Next. The Basic Options settings window opens. This allows you to choose how detailed you need your profile.
4. Choose **Detailed code and database timings, as well as all SQL Query data.**
5. Press **Next**
6. Check the **Collect Group Communications data** box
7. Press **Next**
8. Press **Next** on **Advanced Options**
9. Enter **0** hours, **2** Minutes and **0** seconds on the **Scheduling** Page
10. Press **Next**
11. Press **Finish** to start the Profiling
12. Open the Symantec Management Console (Link on the Desktop)
13. Select **Reports | All Reports** from the main console menu
14. On the left pane, select the **LAB - Troubleshooting Reports** folder
15. Select the **BAD SQL REPORT** on the List
16. Allow it to display the data in the report
17. Scroll down to the bottom of the data with the vertical bar on the left side of the report. This will produce an error "The data could not be loaded" will occur
18. Press **OK** to the error
19. Close the Symantec Management Console
20. Go to the **Altiris profiler** window and Press Enter. The Command window should eventually close
21. Allow the profiler to finish compiling its data. The Altiris Profiler will be shown in a few minutes
22. Switch to the **Altiris Profiler** and Maximize the window

23. Review the items in the Profiler window
24. Select the **SQL Trace Tab** (middle left side) and select an entry in the top left pane and review the data that appears in the in the other panes
25. Select the **Code Trace Tab** and select an entry in the top left pane and review the data that appears in the in the other panes
26. On the Main Menu, select **Profiling > Stop Profiling**
27. Switch to the **Performance Report** from the tray
28. Select the **Get Item Summary** in the left pane and notice that the BAD SQL REPORT is at the top of the list showing how long it ran – its duration is longer than most items in this table. This is good for seeing long running reports.
29. Switch to the **Executive Summary Report** from the tray and select each of the items in the left pane while viewing the information in the right pane. Notice the wealth of SMP Specific information that comes out of this report.

    If a case is opened with Symantec Support, certain Profiler files will be needed. They will normally be found in the same directory from which the profiler.exe was run. The following are the files that are generated during the course of the profile:

    - **default.apr**
    - **GCCache_<number>_0.buffer**
    - **SqlCache_<number>_0.buffer**
    - **CodeCache_<number>_0.buffer**

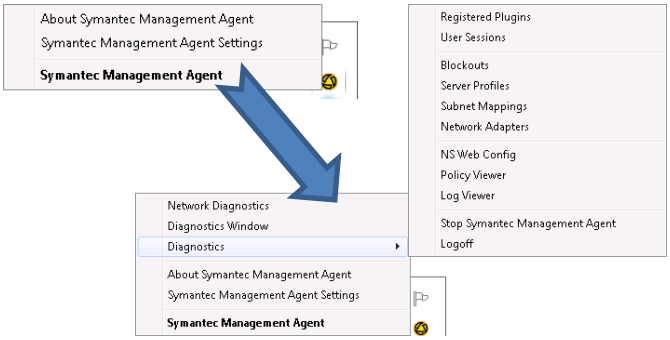
    There are two .buffer files which support directly needs. There are also two reports that the profiler can generate. They are .htm files and give some general information gathered during the profile and regarding some performance of the server on which the profile was run. Here are the names of these two files:

    - **"Executive Summary Report-<today's date>.htm"**
    - **"Performance Report-<today's date>.htm"**

    They should be collected and sent in to the support group or saved with the two .buffer files or can be simply stored for your future reference.

Symantec Management Agent Diagnostics

- Register 'AeXAgentDiagnostics.dll' to access additional information on the agent
  - Register with regsvr32.exe AeXAgentDiagnostics.dll
  - Unregister with regsvr32.exe /u AeXAgentDiagnostics.dll



- Capture agent requests and responses to disk.
- HKLM\SOFTWARE\Altiris\Altiris Agent\Save Policy Requests (DWORD = 1)
- Latest request and response from the server are saved in the Client Policies folder with extension .request.xml and .response.xml respectively.

☐ Lab Exercise 3: Symantec Management Agent Diagnostics

This phase of the lab will walk you through common tools used in the evaluation and diagnosis of endpoint management challenges. These tools will aid you in discovering the problem/symptoms through the use of various tools/utilities to find the root cause, and then finally resolve the specific issue.

1. Switch to the **WIN7 VM**
2. In Windows, click **Start > Run**
3. Type the following:

```
Regsvr32 "c:\program files\altiris\altiris agent\aexagentdiagnostics.dll"
```

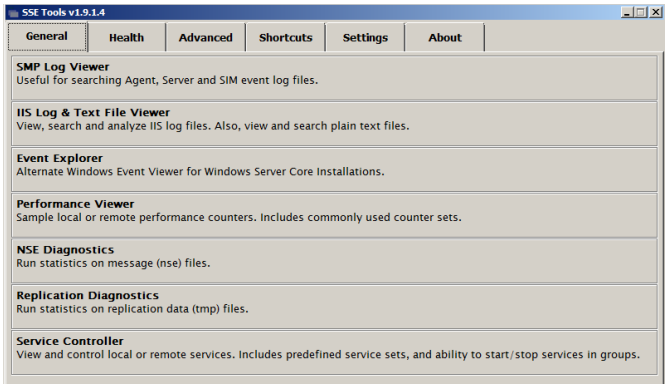
4. You should get a message indicating the DLL was successfully registered. Press **OK**.
5. Right-click on the Symantec Management Agent icon in the system tray, it will display additional diagnostics items.
6. Choose **Diagnostics > Log Viewer**
7. Browse through the tabs and review the information. You can see how useful this can be for diagnosing communication and other errors.
8. Return to the **Logs Tab**
9. Right-click on the Altiris Agent icon in the system tray and choose **Software Management Agent Settings**
10. Press the **Update** button
11. Press the **Send** button
12. Return to the **Logs Tab** and press the **Refresh** Button
13. You should notice that entries have appeared in the log and there are no errors
14. Press the Network Icon on the Windows task tray and select "**Open Network and Sharing Center**"
15. Select **Change Adapter Settings**
16. Right click on **Local Area Connection** and select **Disable.** This will disable the network card.
17. Notice that the Symantec Management Agent icon has changed to a **Red** circle indicating no communications
18. Return to the Agent Diagnosics window and press the **Settings** button
19. Press the **Update** button
20. Press the **Send** button
21. Return to the **Logs Tab** and press the **Refresh** Button
22. Notice that there are communication errors appearing in the log. Review them to get a better understanding of what network communication errors look like.
23. Return to the **Network Card** window
24. Right click on **Local Area Connection** and select **Enable.** This will enable the network card.
25. Close all windows on the desktop

ITMS Technical Resource Kit

SSETools - http://www.symantec.com/docs/HOWTO77027

The SSE Tools were developed by the ITMS SSE Team at Symantec as an aid in troubleshooting many aspects of the SMP Environment. The SSE Tools primary objectives are:

- Save time and effort in identifying common issues.
- Reduce the time required to troubleshoot issues
- Create a platform for tool development and re-use
- Improve both the quality and quantity of diagnostic information available for troubleshooting
- Provides new tool features and maintenance fixes more frequently than in the past
- Very useful in identifying common areas that Symantec Support usually looks at:
    - SMP logs, IIS Logs, SQL Performance, Process Manager, Database and IIS Health, capture memory dumps.
- Provides Links commonly used Microsoft Tools:
    - IIS Manager, Services Console, Windbg, and additional tools from Sysinternals.



SSE Tools Included Utilities

SMP Log Viewer

- Useful for searching Agent, Server and SIM logs where the Altiris Log Viewer is either unavailable or not parsing log files correctly
- Live monitoring of Altiris logs, load logs from a folder, clear current log set, export logs in XML format compatible with SMP Log Viewer, and import logs that have been previously exported
- Find-as-you type filtering with the ability to include, exclude and OR terms on-the-fly using a built-in micro search engine
- Pre-defined buttons to load:
    - Agent logs
    - SIM (Symantec Installation Manager) logs
    - Server (Symantec Management Platform (SMP)/Altiris a*.log files)
    - Server Installs
- Use this to quickly review all component installation logs.
- Connect to any SMP SQL Server\Instance\Database for GUID resolution
    - Database selection persists through all applicable tools once selected here
- Compress the log files that are currently being displayed and store to date/time folder

IIS Log and Text file Viewer

- View, search and analyze IIS logs. Can be used for viewing and searching text files as well
- IIS log file statistics feature
    - Count of page accesses
    - Count of website accesses by IP
    - Count of hits over time
    - Drill downs between the previous three statistics to narrow down problems
    - Ability to filter statistics by any field found within an IIS - formatted log file
- Live monitoring of text files for changes
- Open very large log files when used on x64 Windows
    - Ability to filter and load only log entries earlier or later than a given date/time
- Convenient drop-down access to five most recent IIS log and HTTP error log files
- Find in file capability with hit counts
- Screen capture of the current window is available

Event Explorer

- Enhanced Windows Event Viewer. Especially useful on Core machines
- Displays all Event Logs registered with Windows
- Search and Filter windows events based on:
    - Search criteria
    - Severity criteria
    - Click on the "?" icon for search syntax details
- Configure:
    - Severity highlighting
    - Maximum rows to display
- Screen capture of the displayed information is available.

Performance Viewer

- Sample local or remote performance counters. Includes commonly used counter sets by product/component
- Load all counters registered with Windows into a tree for more convenient access over Windows' Perfmon tool
- Ability to log counter values to CSV file
- Displays Min/Max/Average/Current counter information
- Export and import custom counter sets in XML format
- Pre-defined buttons for SMP, SMP Agent and SQL
- Screen capture of the displayed information is available.

NSE Diagnostics

- Allows reading of .nse and .tmp files used for client/server messaging
- Summary statistics include Scenario GUID counts, Resource counts and message count
- Breaks NSEs down by
    - Scenario GUIDs
    - Resource GUID
- Displays list of each message

- Ability to filter by Scenario GUID or Resource GUID
- Ability to double-click a message and jump to the actual XML Replication Diagnostics
- Allows reading of .tmp files used for server replication
- Summary statistics include Class Type GUID counts, Resource Type GUID counts and item/object/resource counts
- Breaks replication data down by
    - Class Type GUIDs
    - Resource Type GUID
- Ability to filter by Class Type GUID or Resource Type GUID
- Ability to double-click an object and jump to the actual XML
- Services Controller
- View and control local or remote services. Includes predefined service sets, and the ability to start/stop services in groups.
- Filterable by group (EMG, EMG + Related, All)
- Copy currently selected service row information
- Screen capture of the current window is available.

Database Health

- Check an SMP database for configuration or performance issues
- Displays frequently needed SQL configuration information such as:
    - Collation
    - Maintenance Plan activity
    - Locates SQL data files (*.MDF) or log files (*.LDF) files and where they are stored
- Lists very large tables
- Lists index fragmentation
- Lists membership object update duration, filters and targets
- Lists Stored Procedure execution statistics
- Lists blocked SQL Process IDs (SPIDS) and blocking SPID
- Lists potentially helpful new indexes

IIS Health

- IIS Metabase viewer and health checker. Helps find configuration, performance and consistency issues with IIS configuration
- Displays IIS metabase information in a tree similar to the Windows IIS Manager
- Checks Virtual Directories for missing physical directories
- Checks Application Pool performance attributes such as Kernel Request Queue Length
- Checks for missing Windows and .NET performance hot fixes
- Checks for Applications that are in debug mode

Queue Monitor

- Monitors Agent and Server NSE queue directory activity
- Monitors Replication directory activity

SQL Test Tool

- Contains 4 simple Network and Database performance tests:
- CMDB + Network
    - Select approximately 16KB of data from vItem
    - Measures time for SQL to service query and time to return 16KB of across network to the tool
- Network
    - Generate 16KB of using a SQL function so it's done in memory only
    - Measures only the time to return 16KB of data across the network to the tool (very slight amount of SQL CPU required, should be nearly negligible latency in most cases)
- tempdb + Network
    - Creates a temp table, populates it, then reads all the data in it
    - Measures time for tempdb to do the work, and return the data across the network to the tool
- tempdb Only
    - Loops a simple select statement from tempdb.sys.objects over a specified duration
    - Measures how quickly tempdb can service simple selects from existing tables

☐ Lab Exercise 4: SSETools Overview

This Lab exercise is intended to provide an introduction to the SSE tool, hopefully providing sufficient detail about each of the individual utilities to allow a moderately technical individual to navigate and use it successfully. You will find that some of the enhancements to utilities such as Event Explorer and IIS Health will be useful beyond their intended scope.

NOTE: *Some of the utilities in the SSE toolkit may seem redundant if you are running a "Full" installation of windows server. It is not intended to re-invent the wheel, rather it is to help provide access to system information that would ordinarily remain "obfuscated" behind a windows Core Server installation.*

NOTE: *Some of the utilities in the SSE toolkit may not present data or run on the upcoming SMP Server installation due to recent changes in core structure like Event Queues and Locations of log files.*

1. Switch to the **NS75 VM**
2. In Windows, press **Start > Programs > ITMS Technical Resource Kit > SSE Tools**
3. Click on **SSE Tools**. SSE Tools opens
4. Select the **SMP Log Viewer** link. Notice that it appears different than the 7.5 Version we just reviewed.
5. On the top menu, choose the drop down list for **Open…** and choose the **Agent** logs. Notice that this drop down list provides quick access to the Server, Agent, SIM and Install logs.
6. Review some of the options in this application especially the simple interface and filtering functions
7. Close the **SMP Log Viewer**
8. Click the **IIS Log and Temp File Viewer** link
9. On the top menu, choose the drop down list for **Open…** and choose the **Agent** logs. Notice that this drop down list provides quick access to many Symantec and IIS logs.
10. Select a file that has the **u_ax…** prefix. View the file contents

11. Close the **IIS Log and Temp File Viewer** windows
12. Press the **Event Explorer** link
13. Review some of the Events and options in this application, especially the simple interface and filtering functions
14. Search on the word “error” in a particular Event log
15. Close the **Event Explorer** windows
16. Open the **Service Controller** link
17. Notice that it has the ability to filter Endpoint Management related services. Review the functions available, but do not stop any services
18. Close the **Service Controller** windows
19. Press the **Health** TAB
20. Press the **Database Health** link
21. Press the **Connect** Button
22. Press the **Connect** Button to close the connection option
23. Select **Symantec_CMDB** in the dropdown box
24. Press the green **>** arrow
25. Review the various tab options and buttons like **Defragmentation** and **SQL Test**
26. Close the **Database Health** windows
27. Press the **Application Health** Link
28. Review the IIS Health, Consistency and Performance tab data and note the results they return
29. Close the **Application Health** interface
30. Open the **Queue Monitor**
31. Review the functions available, you will notice that the queues are empty and there may not be a lot to see, but in the case of a very busy SMP server, this tool is invaluable.
32. You may certainly browse through the other tabs to see what other utilities are available.

Task Services Troubleshooting

This section will serve as valuable information in regards to Task Services and how they operate in the SMP environment. The following subjects will cover how the Task Service registers endpoints, gets loaded on the SMP, and is installed on the Site Servers and how it communicates.

Task service registration

An Agent on a client computer must be registered with a Task Server in order for it to receive and execute tasks. (In NS 7, a Task Server does not necessarily refer to a dedicated computer that is running only task services. Task services can now run on Notification Server, on a Site Server dedicated to task services, or on a Site Server that is running task services in addition to other services, such as package services. For the sake of simplicity, the term Task Server in this Lab Guide refers to NS 7.x task services.)

When the Agent plug-in (Client Task Agent) starts, it connects to the SMP Server (NS) to retrieve a list of Site Servers with Task Services installed. When the Agent has received this list, it attempts to connect to one of the Task Servers. The Agent registers itself with the first server with which it is able to connect.

How Task Services Automatically Appear on the SMP Server

Symantec Installation Manager (SIM) installs TS during Symantec Management Platform (SMP) installation right after installation of TM. There is a problem that TS starts activity before Notification Server (NS) and NS Agent installed and configured. Site Service controller has InstallOnNSByDefault property that by default is true. That means that during importing of this controller's item a site service of corresponding type will be added to the NS. This is how Task Services "automatically" appear on NS machine.

How Task Services get installed on remote Site Servers

When a customer adds Task Service on some computer, the platform creates new ***TaskService*** resource with parent resource association (SiteServiceComputerResourceAssociationTypeGuid) to the assigned computer.

RM_ResourceTaskService is auto generated table for the TaskService resource and vRM_TaskService is auto generated view for this table. There are two enabled, hidden Software Delivery (SWD) policies - "Task Service Install (x86)" and "Task Service Install (x64)", corresponding for 32 and 64 bit windows platforms. These policies have corresponding resource targets "x86 Site Servers Requiring Task Service Install" and "All x64 Site Servers Requiring Task Service Install".

These resource targets contain all computers that have TaskService resource association - collection "Computers Assigned Task Services" and don't have installed TS Agent - collection "Computers without Task Services Installed" plus dependencies to installed Symantec Management Agent. This resource target is evaluated to so the 64-bit TS will be installed on machine with 64-bit Symantec Management Agent and a 32-bit TS should be installed on machine with 32-bit Symantec Management Agent. It also ensures that a SMP Server is not listed to prevent the installation of the Task Service on the SMP Server.

How the Task Service is uninstalled from Site Server

When a customer deletes Task Service, the corresponding TaskService resource is marked as deleted (field Deleted in RM_ResouceTaskService set to 1). After that corresponding computer resource becomes member of "Computers with Deleted Task Service entries" (f26ebf91-c7c7-4921-8f3f-61070cf8c40d) collection.

There is hidden, enabled policy "Task Service Uninstall" with resource target "Computers Requiring Task Service Uninstall") based on the previous collection.

☐ Lab Exercise 5: Site Server Troubleshooting – Task Services

This phase of the lab will walk you through common methods used in the evaluation and diagnosis of Task Services. This should aid you in discovering the problem/symptoms through the use of various tools/utilities to find the root cause, and then finally resolve the specific Task Service related issue.

Task Service Operations

One important item to note is that the Symantec Management Agent (SMA) must have registered itself with NS before it can request a list of Task Servers.

During Agent Rollout, the Agent is not instantaneously registered with a Task Server. The Agent will make a request to the SMP Server for a new resource via CreateResource.aspx page. The SMP

Server will then return XML from CreateResource.aspx with a Resource GUID that will be assigned to the endpoint on which the Agent is installed. If The SMP Server is paused, it will not respond with a Resource GUID.

After an endpoint has its own unique Resource GUID, the Agent will send its initial inventory. After SMP Server receives the inventory, SMP Server will be able to manage the endpoint and can return a list of Task Servers via GetClientTaskServers.aspx.

In order for GetClientTaskServers.aspx to return a list of Task Servers, at least one Task Server must be installed and managed by SMP Server. By default, the local SMP Server has the Task Service installed. You can view a listing of Task Servers from the Jobs and Tasks Portal (Manage > Jobs and Tasks) or from the Site Services page (Settings > Notification Server > Site Server Settings > Site Management > Site Servers) in the Console.

The Agent will '"tickle" a Task Server at a set interval to verify that it still has a connection with SMP Server. By default, this interval is set at every five minutes and is configurable in the Site Service options in the SMP Server Console. If the Agent has not been able to tickle a Task Server successfully, it will query SMP Server for the list of Task Servers and register with another Task Server.

In this scenario, the **WIN7** agent has not been able to register with a non-SMP Task Server (MONITOR) in quite some time. The following steps will walk you through the stages of Task Server troubleshooting:

1. **Is the SMP Server paused?**
    a. Go to the NS75 VM
    b. Open the Symantec Management Console (Link On Desktop)
    c. In the main menu press **Settings | All Settings**
    d. In the left pane expand **Settings > Notification Server**
    e. Select **Notification Server Settings** (Below the folders)
    f. Under the **Processing Tab,** check that the **Notification Server Processing** is **ON**
    g. You observe that the Processing is running.
2. **Are any SMP Server services Paused?**
    a. In windows, press **Start > Run**
    b. Type in **services.msc.** This is where you would check the “Altiris” named services
    c. Just observe the services named AeX… or Altiris… and make sure they are started, and Ignore the AltirisAgentProvider service that is set to manual.
    d. You observe that all services are running.
3. **Has the Agent recently been able to send inventory and receive its configurations?**
    a. Switch to the **WIN7** VM
    b. Right Click on the Symantec Management Agent
    c. Select Symantec Management Agent Settings
    d. Press the **Update** and **Send** Buttons – NOTE THE TIME THAT YOU PRESSED THEM
    e. Switch to the **NS75** VM
    f. Open the Symantec Management Console
    g. In the main menu press **Manage | Computers**
    h. Select **Installed Agent** on the left pane
    i. Right click on **WIN7 in the middle pane**, then select **Resource Manager**
    j. Scroll through the right pane information and locate **Symantec Management Agent Details**

k. The **Last Configuration…, Last Basic Inventory…** and **Last Event Received** entries should be around the time you pressed the Update and Send buttons on Win7.
l. You notice that the time and dates are very close to when you pressed the Update/Send buttons on WIN7, so the agent is sending information to the SMP Server. In practice;
    - If the Agent is unable to send inventory or receive its configurations, you should review the Agent logs.
    - If the Agent can send inventory and can receive its configurations, you should also review the Agent logs for items that may indicate different symptoms.

4. Is at least one additional Task Service registered with SMP Server?

a. Switch to the **NS75** VM
b. Open the Symantec Management Console (Link On Desktop)
c. In the main menu press **Settings > Notification Server > Site Server Settings**
d. Expand the **Site Management** item
e. Expand **Site Servers**
f. Expand **MONITOR** (This is our Lab Site Server)
g. Select the **Services** icon
h. Look for **Task Service.** This is where you would look for irregularities in the Task Service. You notice that there are task services installed for **MONITOR.**
i. In the left pane, choose sites under **MONITOR**. This is where you would check to make sure it is assigned to a site and Subnet that the affected endpoint belongs to.
j. You notice that Task Services and the proper Site and Subnet is assigned to MONITOR VM

5. Reset the WIN7 Agent to register to another Task Server

a. Switch to the WIN7 VM
b. Right Click on the Symantec Management Agent
c. Select **Symantec Management Agent**
d. Press the **Task Status** tab
e. Note that the Site Server it is registered to is NS75 and not MONITOR
f. Press **Reset Agent**. You should see the status change to: **Received request to stop…**
g. The **Task Server:** field should be changing to **MONITOR.symplified.org**, but it will not.

6. Investigate Agent Communications

a. Switch to the WIN7 VM
b. Right Click on the Symantec Management Agent and choose **Diagnostics Window.** *If you do not have this option go into windows and press **Start > Run**, then enter the following command:* **Regsvr32 "c:\program files\altiris\altiris agent\aexagentdiagnostics.dll"**
c. Press the **Clear** button
d. Double click on the Symantec Management Agent in the tray
e. Press the **Task Status** tab
f. Press **Reset Agent**. You should see the status change to: **Received request to stop…** wait until the **Task Server:** field shows **NS75.symplified.org**
g. Return to the Agent Diagnostics window and press the **Refresh** button
h. Read through the log and try and get a sense of why the Agent is not connecting to MONITOR Site Server. Here are a few items you will observe:
    i. The Agent Clears the existing Task Server list
    ii. The Agent finds NS75 and MONITOR as valid Task Services
    iii. The Agent tries to connect to MONITOR via HTTPS and fails

iv. The Agent tries to connect to MONITOR via HTTP and fails
v. The Agent tries to connect to NS7 via HTTPS and Succeeds
vi. The Agent Successfully Registers to the NS7

i. Knowing this information, we can now see that MONITOR cannot be connected to by HTTP or HTTPS to complete the registration. We must now check web connectivity on the MONITOR VM.

j. Switch to the **MONITOR** VM

k. Right click on the Computer icon on the desktop and select Manage

l. Expand **Server Manager > Roles > Web Services (IIS)**

m. In the middle pane, select **MONITOR (SYMPLIFIED\Administrator)**

n. In the **Actions** pane, make sure it is started. You notice that it is set properly.

o. Expand **MONITOR (SYMPLIFIED\Administrator) > Sites**

p. Select **Default Web Site** and make sure it is started. You notice that it is set properly.

q. In the **Actions** pane, press the **Advanced** button

r. Check that the **Application Pool** setting is set for **"Classic .NET AppPool".** This is a common mistake when setting up Site Servers. You notice that it is set properly.

s. Press **Cancel**

t. In the **Actions** pane, press the **Bindings** button. You notice that HTTP is set, but HTTPS is not. You note that this setting is OK because HTTPS is not in use in the environment.

u. Press **Close**

7. With the IIS Configuration seemingly OK, you move on to possible Firewall conflicts

a. In the left pane of the Server Manager, expand the **Configuration >Windows Firewall…** Folder.

b. Select Inbound Rules, and review the items that relate to Altiris or Web Services

c. You notice that some of the **Altiris Client Task Data Loader Service** rules are disabled

d. Re-enable these 2 rules by right clicking on them and selecting **Enable Rule**

e. You notice that the **WWW Services (HTTPS Traffic IN)** policy is enabled, but this is not a factor as HTTPS is not used on the Site Servers in this environment.

f. You notice that the **WWW Services (HTTP Traffic IN)** policy is Disabled. This is a major factor that contributes to the registration of agents on the Task Service. Other common mistakes are setting Firewall Policies that block the Task Services communications ports.

g. Re-enable the World Wide Web Services (HTTP Traffic In) rule by right clicking on it and selecting **Enable Rule**

8. Reset the WIN7 Agent to register to another Task Server

h. Switch to the WIN7 VM

i. Double Click on the Symantec Management Agent

j. Press the **Task Status** tab

k. Note that the Site Server it is registered to is NS75 and not MONITOR

l. Press **Reset Agent**. You should see the status change to: **Received request to stop…**

m. The **Task Server:** field changes to **MONITOR.symplified.org**

a. Switch to the Agent Diagnostics window and press the **Refresh** button

b. Review the log to show that it still has some errors connecting to HTTPS but it will now connect successfully through HTTP and register this agent to MONITOR thus reducing the load on the SMP Server.

Package Services Troubleshooting

This section will serve as valuable information in regards to Package Services and how they operate in the SMP environment. The following subjects will cover key concepts in how the Package Service operates in the SMP Environment and how this information pertains to common troubleshooting methods.

Updated Packages:

Below is an example of where a particular package is stored. Each package is stored underneath their own GUID folder. The actual package files reside inside the cache folder.

C:\Program Files\Altiris\Altiris Agent\Package Delivery{6C821F5E-5BF4-407F-A6FF-ABB85EEE0418}\cache

Below is what occurs when Package Server receives configuration about an updated package.

- The Agent Access Credentials (ACC) on the package root folder under 'cache' will be temporarily removed so only System and Local Administrator rights remain.
- (Agents using the ACC will be unable to reconnect).
- The files in the package are scanned and all open files are closed.
- Any Agents that are currently downloading the package will be disconnected from the download, and will retry at the usual interval.
- The updated Package is downloaded to the Package Server.
- The ACC is restored to the 'cache' folder

Invalid Packages

The following are symptoms that will cause packages to show as invalid inside the Package Server UI on the Site Server:

- Creating a SWD Package and specifying a non-default download location that does not exist on the PS
- Creating a SWD Package and Specifying a non-default download location that exists but is not shared.
- If there is not enough disk space to download a packages to Package Server
- Anonymous access to package codebases setting has been disabled and the specified ACC cannot be applied to the downloaded files i.e. ACC is an untrusted account.

Deletion of Unused Packages

The setting for when Package Servers should delete unused packages exists on the **Settings** tab of the **Package Server** page.

The countdown to remove package files on a Package Server will only begin when either; the package is unassigned from the Package Server, or the package is deleted from the NS database. Both of these situations result in the package no longer being sent down to the Altiris Agent in the Package Server node of the configuration XML file.

Once this occurs the Package Server updates the PackageStatus.xml file that it stores for each individual package and sets the ‘Status’ flag to ‘Deleted’ and the ‘Time’ flag to that of when it was removed from the configuration file.

The package status files are located (on a default install) at the following location:

C:\Program Files\Altiris\Altiris Agent\Package Server Agent\Package Status

At each Package Server refresh the Package Server will check for a Deleted flag inside all the Package Status files and if the corresponding Time flag has past the duration configured for deletion of unused packages, then the package files will be removed.

Disk Space Check

The Altiris Agent and Package Server calculate the space requirement for package download based on a couple of things. There is a registry key called 'Min Disk Free Space (Mbytes)' at the following location on the Agent machine.

HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Communications\Package Delivery

This key is set to 500MB by default. It works out to be 500MB+120% of the package size.

So for example, if the package is 100Mb in size, it first checks to see whether there is 620MB of free space available at the default install location, if there is not it will check whether any other drive has this space available and download there, if no other drive has this space then it will not download the package.

Drive Overflow

The Altiris Agent and Package Server have a package download drive overflow method. If there is not enough space to download a package to the default install location (e.g., C drive) then the Altiris Agent or Package Server will download the package to the next available drive with the required space.

Package Snapshots - If Package Server packages are stored on an alternate drive or an alternate download destination, the package snapshots for these packages always remain at the default Altiris Agent install location.

Packages stored in non-default locations

When specifying a non-default location for package server to download to, if a local path is specified i.e. C:\folder and the folder does not exist then package server will create it when downloading the package.

A share for this package will not be created, so therefore a UNC codebase for this type of package will not be sent to the server, only HTTP will be sent.

Specifying a non-default location on the Advanced tab when creating a SWD Package The location can be \\%computername%\share

%computername% is substituted for the name of the localhost computer name. 'Share' is a shared folder that already exists on the hard-drive of each Package Server receiving the package.

A Package Server does not create shares, (except the primary share PkgSvrHostC$) so if the folder specified does not exist or is not shared, the PS will not download the package and will set the status to invalid. If the shared folder does exist then the Package Server will send UNC codebases to the NS for this UNC alternate download location.

Package Access

The Altiris Agent cannot download a package via UNC from a Package Server on a non-trusted domain. An 'Access Denied' error occurs. In this case you must set the Package Service Setting - 'Allow anonymous access to package codebases'

Anonymous access effectively means all authenticated users are allowed when downloading via UNC. Even if a Package Server in a non-trusted domain has anonymous access enabled on its files, if the ACC account that the Altiris Agent uses to connect anonymously to the UNC source cannot be authenticated, then access with be denied and no download will occur.

When attempting to download via HTTP from a Package Server in a non-trusted domain using anonymous access, the download should occur with no access issues.

Site Severs with IIS7

Package Server is unable to host its packages within IIS 7 unless the IIS 6.0 Compatibility Tools are installed as part of the Web Service role configuration. This is a common mistake and it is important to have the Role: Web Server (IIS), Role Services: ASP, Windows Authentication, and all IIS6 Management Capability options present.

☐ Lab Exercise 6: Site Server Troubleshooting – Package Services

This phase of the lab will walk you through common tools used in the evaluation and diagnosis of package services issues. This example should aid you in discovering the problem/symptoms through the use of various tools/utilities to find the root cause, and then finally resolve the specific issue.

Scenario: Package is not Deliverable (Multiple problems)

The customer has created a Thunderbird 4.42 Software Resource and has tried to distribute it to a group of computers with no success. The customer mentions that they never see it appear on the Site Server and the client never receives the software to install it. They have also tried to distribute it to an endpoint that is registered to the SMP Server with no success.

- When it is sent using the **Quick Delivery** method the endpoint shows a Task Status of "New Thunderbird Delivery Task" is "Running" for 20 minutes then it exits with a Code 3.
- When it is sent using the **Managed Software Delivery** method the endpoint receives the software policy, checks the prerequisites, but the Download task sits at "In Progress". When they investigate the problem at the agent they notice that there are no Codebases listed in the download task. Both Methods are showing errors in the Agent and Server Logs.

We have duplicated this real world scenario in this Lab and will attempt to walk you through the steps that would be required to solve the issue. The possible areas of concern relating to the Package Server known issues could be related to Invalid Packages, Packages stored in non-default locations, site server configuration and software package configuration.

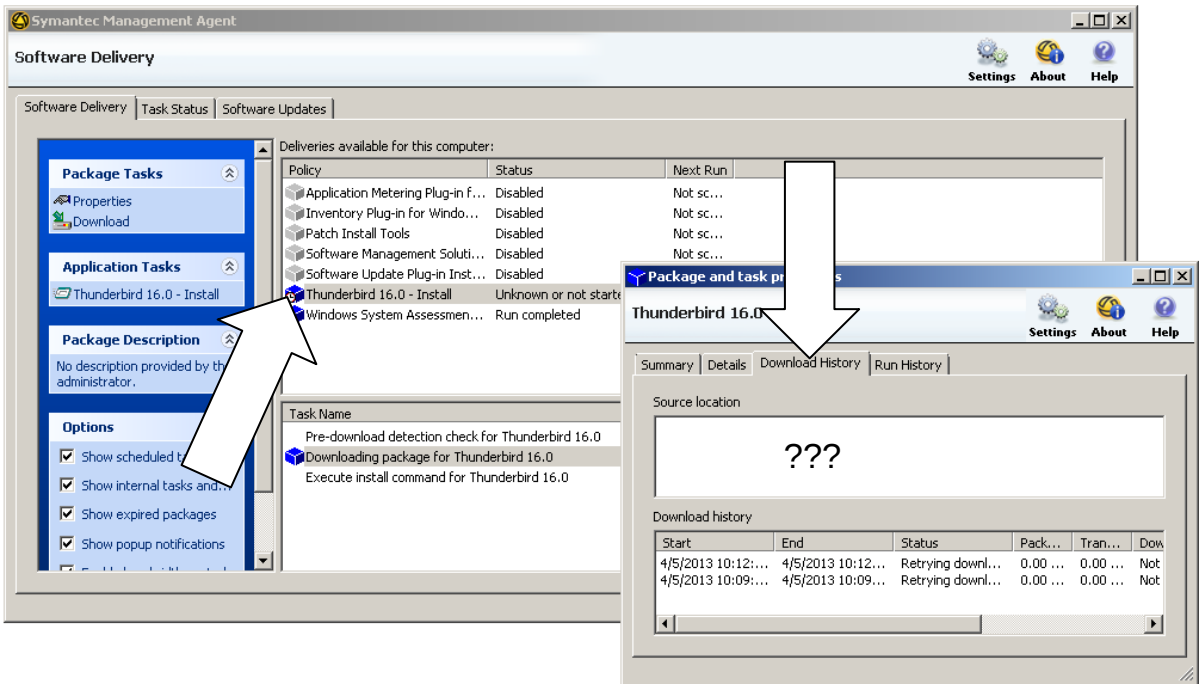
Problem Duplication:

1. **Switch to the NS75 VM**
2. Open the **Symantec Management Console**
3. Select **Manage | Software** on the main menu
4. Select **Software Resources** under the **Deliverable Software** area on the left pane
5. In the middle pane, right click on **Thunderbird 16.0** and select Managed Software Delivery. The **Managed Software Delivery** interface appears
6. Click **Next**
7. Select the **Apply to** button and select **Quick Apply**
8. Type **Windows 7**, select the Dropdown arrow, then click **Apply**
9. Click **Next**
10. Select the **Add Schedule** button and Select **Schedule Window**
11. Enter **5 minutes** in the **"During window, check every:"** time field
12. Click **Next**
13. Press the **Deliver Software** button
14. In the main console menu, select **Settings | Notification Server | Resource Membership**
15. Press the **RUN** button under the **Policy Update Schedule** section, and wait for the "**Policy Update Schedule has Completed**" message at the top left.
16. **Switch to the WIN7 VM**
17. Double Click on the **Symantec Management Agent** in the tray
18. Select the **Software Delivery** tab and keep this window open.
19. Select the **Settings** Icon on the top right
20. Press the **Update** Button
21. Close the **Settings** window
22. Return to the other agent window, and look in the **Software Delivery** area for the "**Thunderbird 16.0 Install**"
23. Select the **Thunderbird 16.0** item in the list
24. Press the "**Thunderbird 16.0 Install**" entry under the **Application Tasks** pane on the left side

25. Observe the progress of the software delivery in the **Task Status** pane (Lower Right)
26. You should notice that the Download Task is sitting at "In Progress" – it will sit in this status indefinitely.

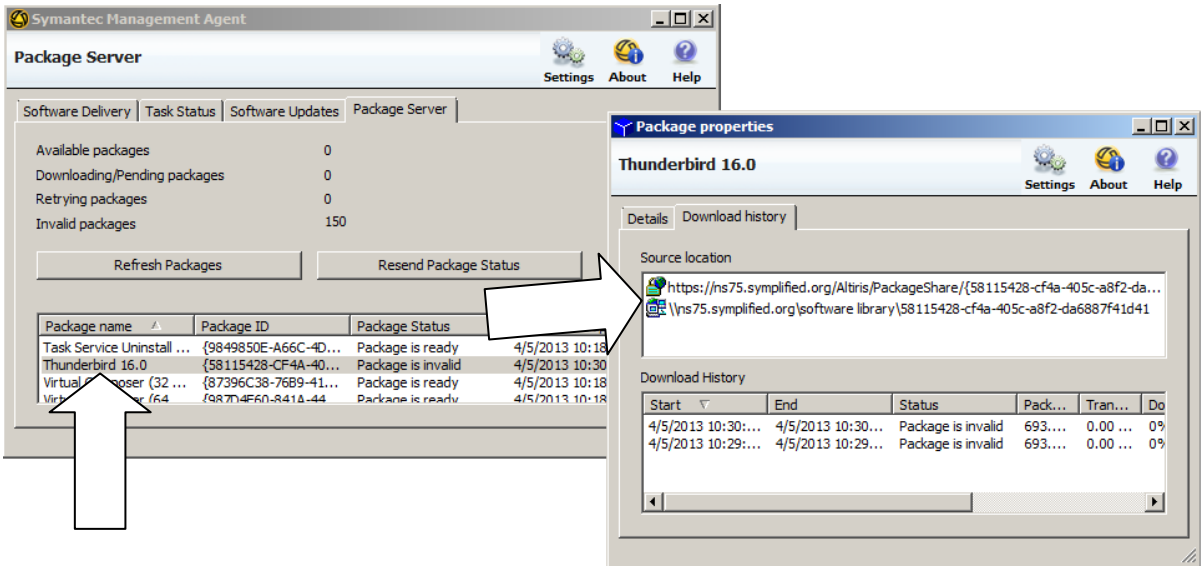
Troubleshooting Steps:

1. Stay on the **WIN7** VM
2. Right click on the **Symantec Management Agent** and select **Diagnostics Window**. *If you do not have this option go into windows and press Start > Run, then enter the following command:* ***Regsvr32 "c:\program files\altiris\altiris agent\aexagentdiagnostics.dll"***
3. Press the **Refresh** button, and look for any entries that indicate package issues. You may notice a few items about missing codebases and many package retry attempts.
4. Go to the **Software Delivery** tab on the **Symantec Management Agent** window
5. Double click on the "**Downloading package for Thunderbird 16.0**" task in the task status pane on the lower right pane.



6. Press the **Download History** tab on the package properties
7. Notice that there are missing codebases in the **Source Location** area
8. Feel free to investigate the other tabs for further information
9. **Switch to the MONITOR VM**
10. Double Click on the **Symantec Management Agent**
11. Select the **Package Server Tab**
12. Look for **Thunderbird 16.0** in the list of software. *Notice that it is missing. If the software does not exist on the package server, then it can't be downloaded by agents that rely on it.*
13. At this point we might do an update on this Agent to see if it needs to be downloaded
    a. Press the **Settings** Icon
    b. Press **Update**
    c. Close the **Settings** window
14. Return to the Agent window and press the **Resend Package Status** button in the **Package Server** Tab
15. You notice that the **Available packages** total stays the same (154 Packages)
16. Right click on the **Symantec Management Agent** and select **Diagnostics Window**
17. In the **Log Tab**, Look for any entries that indicate package issues. The entries for ***HttpTransfer*** have nothing to do with this package service issue, and only relate to the fact that MONITOR uses HTTP.
18. You notice that there are no errors indicating communication or package services issues. This might indicate that the Software Package may not be set for this site server. It could also be a result of a site server configuration error that does not have the Site Server in the proper site.
19. **Switch to the NS75 VM**
20. Select **Manage | Software** from the main menu
21. Select **Software Resources** under the **Installable Software** area on the left pane
22. Double Click on the **Thunderbird 16.0** package in the middle pane
23. Review the tabs in the **Software Package** for any irregularities. The causes are usually in:
    - Packages Tab: You would check that there is a package and install command line
    - Rule Tab: You would investigate the validity of the detection and applicability rules

24. You don't notice any obvious problems in the information in these tabs, so you dig deeper:
25. Press the **Package Tab**
26. Double click on the **Thunderbird 16.0** title under the Packages section to edit it
27. Select the **Package Server** Tab
28. Review the items in the **Package Server** settings
29. You notice that MONITOR is not selected as an assignable package server.
30. You have 2 choices to resolve the issue; Check the MONITOR site server or change the **Assign Packages To:** setting to a new choice. In our case we will choose to change "**Assign Packages to:**" to "**All Package Servers**" as this is a globally delivered package.
31. Change "**Assign Packages to:**" to "**All Package Servers**"
32. Press **OK**
33. Press **OK** to close the Software Resource
34. **Switch to the MONITOR VM**
35. At this point we might do an update on this Agent to see if the package needs to be downloaded
36. Press the **Settings** Icon on the Symantec Management Agent window
37. Press **Update**
38. Close the Settings window
39. Return to the Symantec Management Agent window,
40. Select the **Package Server** tab, and press the **Resend Package Status** button
41. Notice that **Thunderbird 16.0** appears in the list
42. It attempts to download, but it has a status of "**Package is Invalid**"



43. Double click on the **Thunderbird 16.0** package in the list and select the **Download History** Tab. Notice that it is showing proper codebases for NS75. This status does not indicate a communication issue or package distribution problem. This indicates that there is a problem creating the package on the Site Server to be distributed – At this point the **Thunderbird 16.0** Package should be investigated further.

44. **Switch to the NS75 VM**
45. Select **Manage | Software** from the main menu
46. Select **Software Resources** under the **Deliverable Software** area on the left pane
47. Double Click on the **Thunderbird 16.0** package in the middle pane
48. Press the **Package Tab**
49. Double click on the **Thunderbird 16.0** title under packages (to Edit it)
50. Select the **Package Server** Tab
51. Review the items in the **Package Server** settings
52. You notice that customer wants to redirect the package location to: **\\%COMPUTERNAME%\SOFTWARE**
53. You must make sure that that location exists on the **MONITOR** site server
54. In Windows, Select **Start > Run**, then Type: **\\MONITOR\c$\Software** in the box and press **enter**
55. You notice that the directory does not exist, so you must create it on the Site Server
56. **Switch to the MONITOR VM**
57. Open Windows Explorer
58. Browse to C: and create a folder called **Software** on the root
59. Right Click on the **Software Folder** and select **Share With > Specific People**
60. Select **Administrators**
61. Select the **Share** Button
62. Press **Done**
63. At this point we might do an update on this Agent to see if the package downloads
64. Press the **Settings** Icon on the Symantec Management Agent window (or Double Click on the Agent)
65. Press **Update**
66. Close the Settings window and return to the Symantec Management Agent window
67. Press the **Resend Package Status** button on the Symantec Management Agent **Package Server** Tab
68. The **Thunderbird 16.0** appears in the list as a valid package with "Package is Ready"
69. **Switch to the WIN7 VM**
70. Double Click on the **Symantec Management Agent** in the tray
71. Select the **Software Delivery** tab and make sure you can see all of the items listed
72. Select the **Settings** Icon on the top right
73. Press the **Update** Button
74. Close the **Settings** window
75. Look in the **Software Delivery** List for "**Thunderbird 16.0**"
76. You should notice that the Thunderbird install is completing. If not, simply press the "**Thunderbird 16.0**" entry under the **Application Tasks** pane

77. Observe the progress of the software delivery in the Task Status pane (Lower Right)
78. The software installs successfully and you should see Mozilla Thunderbird on the desktop

SUPPLIMENTAL: SMP Performance Tuning and Optimization

Common Configuration Issues

- **Common SMP Server Issues**
  - Managed nodes should not be checking in every hour
    - Recommend setting this to 4 hours for twice daily updates
  - Collection and Policy Update schedules shouldn't be running every 5 minutes
    - Increase the interval, and stagger so they aren't running concurrently
  - Re-evaluate the agent intervals for each solution
    - Inventory recommendation weekly deltas and monthly full inventories
    - Application metering data is truly useful for long term trending
    - Do you really need to know that I opened up Word 4 times this morning?
    - Patch inventory summaries should be changed, most of the time there is not a need to send a summary every 4 hours

- **Common issues seen with IIS**
  - Multiple worker processes servicing the same application pool
    - Configured through the 'Advanced Settings…' of the application pool.
    - Session state not shared across the worker processes.
  - Application pool has been shut down due to repeated errors
    - If any hosted application within an app pool fails several times (5 by default) within a certain period (5 minutes by default), IIS Rapid-Fail Protection will shut down the entire app pool.
    - Configurable within IIS Manager under app pools advanced settings also.
    - Returns 503. (Service unavailable)
  - Windows authentication not installed/enabled
    - SMP supports both Windows authentication (default) and Forms authentication.
    - Returns 401.2. (Unauthorized)
  - Custom error pages can be replaced with the actual error information.
  - Modify the web.config file.
    - Locate the <customErrors mode="On" defaultRedirect="error.htm"/> node.
    - Replace mode="On" with mode="Off". (or "RemoteOnly")

SQL Server Tuning

- **The top issue we see with SQL is with memory configuration**
  - SQL and the Notification Server share the user space of memory
  - If SQL and the Notification Server are on the same server, start out by setting SQL to a fixed memory value
    - The amount will depend on node count, solutions installed, etc.,
- **Review HOWTO10723** for information on SQL Server 2005 and 2008 Implementation Best Practices
- **A common bottleneck with SQL can be the disk subsystem**
  - Ideally SQL should not share the same disk channel as the Notification Server due the large amount of file I/O with the NSEs and other processing on smaller implementations (<2500 endpoints)

- **The Notification Server uses the tempdb database heavily.**
    - **Consider optimizing the tempdb Performance**
        - Allow the tempdb database to automatically expand as needed
            - This ensures that queries that generate larger than expected intermediate result sets stored in the tempdb database are not terminated before execution is complete
        - Set the original size of the tempdb database files to a reasonable size to avoid the files from automatically expanding as more space is needed
        - Set the file growth increment percentage to a reasonable size to avoid the tempdb database files from growing by too small a value
        - If the file growth is too small compared to the amount of data being written to the tempdb database, then tempdb may need to expand constantly, thereby affecting performance
        - Place the tempdb database on a fast I/O subsystem to ensure good performance
        - Use file groups to place the tempdb database on disks different from those used by user databases
- **Set Maintenance Schedules**
    - Do not enable “fix minor problems”
    - The NS will never allow the database to go into single user mode
    - dbcc_checkdb can’t perform repairs without single user mode
    - Your database will never be backed up, due to the inability to run an integrity check
    - Enable index rebuilds Every 7 days
        - Reindexing will temporarily hurt performance, but will cure heavily fragmented indexes and corrupted indexes
    - Enable the check for problems (without repair), but remember to review the SQL agent logs
    - Enable the reclaim space options

Purging Maintenance Troubleshooting

Large table sizes can affect the performance of reports, upgrades, and processing of NSEs

- If the event tables are too large, the automated purging process may suffer a database timeout
- The purging process has been rewritten to perform row purging in smaller batches, but a large table could prevent the process from finishing
- To manually correct this you may use the following:
    - Truncate large event tables
    - If there is a need to keep recent events
        - Copy by date recent rows into a temp table
        - Truncate the original table
        - Insert the data from the temp table back into the original

☐ OPTIONAL LAB 1: Reducing the Impact of Common Misconfigurations

This exercise consolidates some of the most commonly misconfigured areas of the Symantec Management Platform that can result in measurable and perceivable decreases in performance. It also presents a simplistic process that can be used to tune and troubleshoot performance of the platform. The information contained in this exercise is geared toward servers that are generally found in large customer environments.

The table below shows 4 settings that can result in high impact to the processing and communications of a SMP Server if they are incorrectly set. The following table can be used as a general guideline to ensure a reduction of impact.

Setting	< 1000 endpoints	1000 – 5000	5000 – 10,000	10,000 – 15,000	15,000 to 20,000
Agent Configuration Interval (Desktop)	Every **1** hour	Every **1** hour	Every **2** hours	Every **3** hours	Every **4** hours
All Linux/Mac Workstations	Every **1** hour	Every **1** hour	Every **2** hours	Every **3** hours	Every **4** hours
Full Resource Membership Update schedule	Daily	Daily	Daily	Daily	Daily
Delta Resource Membership schedule	15 min	30 min	30 - 60 min	1 Hour	2 Hours
Task Service task update interval	5 min	5 min	15 min	30 min	30 min

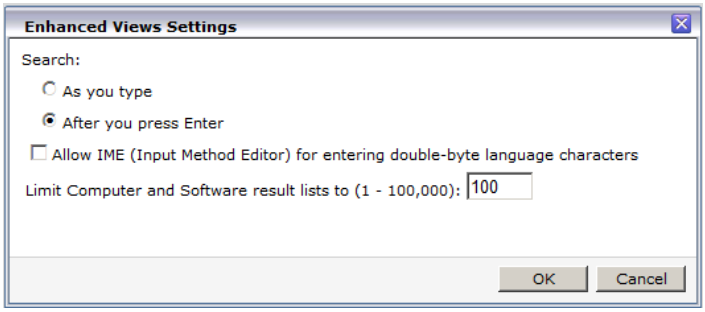
In this Exercise we will set the Notification Server to be optimally set for 20,000 endpoints:

1. Open the Symantec Management Console
2. In the main menu, select **Settings ➔All Settings**
3. In the left pane, Expand the **Settings ➔ Agents/Plugins ➔ Symantec Management Agent ➔ Settings**
4. Select **Symantec Management Agent Settings – Targeted**
5. In the right pane, select the **All Desktop computers (excluding 'Site Servers')** policy
6. Change the **Download new configuration every:** setting to **4 Hours**
7. Change the **Upload basic inventory every:** setting to **1 Days**
8. Press **Save Changes**
9. Repeat steps 5 to 8 for the **All Linux/Mac Workstations** policy
10. In the left pane, Expand the **Settings ➔ Notification Server ➔ Site Server Settings ➔ Task Service ➔ Settings**
11. Select **Task Service Settings**
12. Change the **Task Update Interval** to **30 minutes**
13. Press **Save Changes**
14. In the main menu, select **Settings ➔ Notification Server ➔ Resource Membership Update**
15. Change the **Complete Update Schedule** to **1 Day**
16. Change the **Full Update Schedule** to **2 Hours**
17. Press **OK**

☐ OPTIONAL LAB 2: SMP Console Performance Tuning

Customers with large data sets experience console slowness as a result of reports or management views automatically running or querying large amounts of rows. The following method will aid in the reduction of execution time and will allow them to limit results for quicker response.

1. In **Windows Explorer** Browse to:
   C:\Program Files\Altiris\Notification Server\Bin\Tools
2. Double Click on NSConfigurator.exe
3. Set the **SuppressAutorun** feature
   a. When SuppressReportAutorun is enabled and you open any report, the report does not run immediately. To see the results of the report, you must click Refresh. By default, the SuppressReportAutorun functionality is disabled.
   b. On the Left pane, select **CoreSettings > User Interface > Report > SuppressReportAutorun**
   c. Check the **Value** box to enable this option, then press **Save**
   d. Close the **NSConfigurator** Application
4. Set the **Enhanced View** settings:
   a. Open the Symantec Management Console
   b. In the main menu, select **Settings ➔Console ➔ Enhanced Views**
   c. Set the parameters as follows:



   d. Press **OK**
5. Test the results of these settings by:
   a. In the main console menu, select **Manage ➔ Software**
   b. Select **Newly Discovered Software** in the left pane
   c. In the middle pane (Newly Discovered Software), scroll down to the bottom of the list
   d. You should see a **"More Available… Click to Load…"** item in the list. This is a result of limiting the results to 100 in the Enhanced Views setting.
   e. Click the **"More Available… Click to Load…"** item, and notice how it loads additional software titles.
   f. Type **Apple** in the **Newly Discovered Software** search box in the middle pane
   g. Notice that a query is not running as you type…
   h. Press Enter, and notice that the query to filter the results executes
   i. In the main console menu, select **Reports ➔ All Reports**
   j. Expand **Reports ➔ Service and Asset Management ➔ Assets**
   k. Select the Assets **by Type, Status, Department, Cost Center and Location** report. Notice how it does not display any results – imagine having this report automatically running with over 100,000 assets, and you waiting for it to run before you can select any filters first.
   l. Press the **Refresh** button. You will now see the results.

☐ OPTIONAL LAB 3: Creating a Data Collector for Performance Monitoring

This phase of the lab will demonstrate the ability of the Windows Performance Monitor to collect performance trending data commonly used by Symantec Support Services and customers.

Often in trying to troubleshoot performance issues, it is very helpful to have a basic set of performance counters. Microsoft has a performance monitor tool that does real-time monitoring of a system. In addition to a real-time display of these counters in a grid, a perfmon counter can be created to collect this data in the background over time. The counters are saved to a Binary log file (.blg) which can sent to Symantec Support Services or utilized by the customer.

The counters we will create below are broken down into two groupings.

- **Counters that should be collected on any Altiris related servers (SMP Servers, Site Servers…)**
- **Counters that should be collected on SQL Servers**

Creating the Data Collector using a prebuilt XML settings file

1. Switch to the **NS75** VM
2. In Windows press **Start > Run** and type **perfmon.msc** in the box then press enter
3. In the tree Select **Data Collector Sets > User Defined**
4. Right Click on the User Defined folder and Select **New > Data Collector Set**
5. Change the Name to **SMP Data Collector**
6. Make sure "**Create from a template (Recommended)"** is selected
7. Press **Next**
8. Press the **Browse** button
9. Browse to **C:\Lab Resources\SMP Troubleshooting**
10. Select **SMP Data Collector Set.XML,** and press **Open**
11. Press **Next**
12. Press **Next**
13. Press **Finish**
14. Select **Data Collector Sets > User Defined > SMP Data Collector Set**
15. In the right pane, Right click on **DataCollector01** and select **Properties**
16. Select the **Performance Counters** Tab
17. Make sure there entries in the list
18. Press **OK**

Manually Start Collecting Metric Data

19. In the tree Select **Data Collector Sets > User Defined**
20. Right Click on the **SMP Data Collector Set** and choose **Start**
21. Once the counter is started, it will continue to run even after the Performance window is closed.
22. Open the Symantec Management Console and run through a few of the menus for about 1 minute.

Manually Stop Collecting Metric Data

23. In the tree Select **Data Collector Sets > User Defined**
24. Right Click on the SMP **Data Collector Set** and choose **Stop.** Each time the log is started again, the log number will increment.
25. Expand the **Reports > User Defined > SMP Data Collector Set**
26. Open up one of the reports and review the information gathered

27. In windows explorer go to C:\PerfLogs\Admin\SMP Data Collector Set
28. Open one of the report run folders by double clicking on the .BLG file
29. Review the various functions and close the application when finished.

NOTE: The **SMP Collector Data Set.XML** is included in Appendix B in this Guide so this exercise can be run in your test or personal environment.

SMP Counter Matrix

The following table lists the Counter names, their thresholds and the actions that should be considered if the thresholds are exceeded.

Common Counters for All Servers	Additional Counters for SQL Servers	Additional Counters for SMP Servers
Object: Memory	**Object: Physical Disk(All Instances)**	**Object: .Net CLR Memory(_Global_)**
Free System Page Table Entries	Avg. Disk Read Queue Length	#bytes in all Heaps
Pages/sec	Avg. Disk Write Queue Length	% Time in GC
Object: Physical Disk(_Total)	**Object: Process(sqlservr)**	**Object: Process(AeXSvc,W3WP, and W3WP#1)**
Avg. Disk Queue Length	%Processor Time	%Processor Time
Object: Process(_Total)	Private Bytes	Private Bytes
%Processor Time	Virtual Bytes	Virtual Bytes
Private Bytes	Working Set	Working Set
Virtual Bytes	**Object: SQLServer:Buffer Manager**	**Object: Web Service(All Instances)**
Working Set	Buffer Cache hit ratio	Current Connections
Object: Processor(_Total)	Free Pages	
% Processor Time	Page Life Expectancy	
Object: System		
Context Switches/sec		

☐ OPTIONAL LAB 4: Server Troubleshooting Reports

This lab will familiarize you with the most commonly used troubleshooting reports that can tell you a lot about the performance and state of your SMP Environment.

1. Go to the NS75 VM
2. Open the Symantec Management Console
3. Go to Reports | All Reports from the main console menu
4. On the Left pane, Browse to the Notification Server Management folder and expand it
5. Select the Server Folder
6. Review the following Reports

Report Name	Description	Useful For…
Daily Event Report	This report provides a summary of event processing per day.	Server Performance
Event History	This report lists event succeed/fail statistics over a given time period.	Server Performance
Event Queue Statistics	This report displays statistics for each event queue and the failed backup folder over the specified from-to range (last 7 days by default)	Server Performance
Event Trends Report	This report shows trends for the selected event.	Server Performance
Filter Update Duration	Lists the time taken for reports to update their membership, both by full update and delta update.	Server Performance
Package Server Account Creation Failure	Lists package servers which have failed to create ACC local accounts	Site Server TS, SWM TS, PMS TS, DS TS
Package Server Account Locked	Lists package servers which have ACC local accounts that have been locked out	Site Server TS, SWM TS, PMS TS, DS TS
Package Server DC Account Creation Failure	Lists package servers which are installed on a DC and cannot create ACC local accounts because the option is disabled	Site Server TS, SWM TS, PMS TS, DS TS
Package Server Password Expiry	Lists package servers with ACC local accounts that will expire within N days (14 days by default).	Site Server TS, SWM TS, PMS TS, DS TS
Resource Target Updates	Shows how long resource target updates are taking. Includes average, fastest and slowest times.	Server Performance
Scheduled Events	Lists the Scheduled Events run over a given period.	Server Performance
Scheduled Events Detail	Details instances of a Scheduled Event executed over a given period.	Server Performance
Site Report	This report lists configured site details.	Site Server TS, SWM TS, PMS TS, DS TS
Site Servers in Subnet Report	This report lists the configured site servers in the selected subnet.	Site Server TS, SWM TS, PMS TS, DS TS
Sites and Package Servers Report	Shows Sites with or without a particular type of Package Server.	Site Server TS, SWM TS, PMS TS, DS TS

APPENDIX A: Troubleshooting Related Links

Go to http://www.symantec.com/business/support/index?page=home **and enter reference in Search Box**

HOWTO35984 "Best Practice references for Symantec Management Platform 7.1"

DOC3464 "Altiris™ IT Management Suite 7.1 from Symantec™ Planning and Implementation Guide"

DOC3549 "Altiris™ IT Management Suite from Symantec™ Migration Guide version 6x to 7.1"

DOC3550 "Altiris™ IT Management Suite from Symantec™ Migration Guide version 7.0 to 7.1"

HOWTO45739 "How to enable a Full Dump creation for the Symantec Management Agent 7.x"

HOWTO45753 "Where is the CoreSettings.config file for Symantec Management Platform 7.1 stored?"

HOWTO45754 "Where are the event queues (EvtQueue, EvtQFast, etc.) for Symantec Management Platform 7.1 located?"

HOWTO45755 "Where is the Replication folder for Symantec Management Platform 7.1 located?"

HOWTO47803 "Installing Package Server in IIS 7.0"

HOWTO47804 "Installing Task Server in IIS 7.0“

HOWTO9965 "Symantec Management Platform Support Matrix"

HOWTO36974 "Replication FAQ and Known Issues"

HOWTO42291 "Hierarchy and Replication"

HOWTO42359 “Hierarchy Replication process and Troubleshooting tips”

APPENDIX C: SMP Data Collector Sets

Copy contents into Notepad and save as ***SMP Data Collector Set.xml***

```
<?xml version="1.0" encoding="UTF-16"?>
<DataCollectorSet>
	<Status>0</Status>
	<Duration>0</Duration>
	<Description>
	</Description>
	<DescriptionUnresolved>
	</DescriptionUnresolved>
	<DisplayName>
	</DisplayName>
	<DisplayNameUnresolved>
	</DisplayNameUnresolved>
	<SchedulesEnabled>-1</SchedulesEnabled>
	<LatestOutputLocation>
	</LatestOutputLocation>
	<Name>SMP Data Collector Set</Name>
	<OutputLocation>C:\PerfLogs\Admin\SMP Data Collector Set\NS75_20130404-000001</OutputLocation>
	<RootPath>%systemdrive%\PerfLogs\Admin\SMP Data Collector Set</RootPath>
	<Segment>0</Segment>
	<SegmentMaxDuration>0</SegmentMaxDuration>
	<SegmentMaxSize>0</SegmentMaxSize>
	<SerialNumber>1</SerialNumber>
	<Server>
	</Server>
	<Subdirectory>
	</Subdirectory>
	<SubdirectoryFormat>3</SubdirectoryFormat>
	<SubdirectoryFormatPattern>yyyyMMdd\-NNNNNN</SubdirectoryFormatPattern>
	<Task>
	</Task>
	<TaskRunAsSelf>0</TaskRunAsSelf>
	<TaskArguments>
	</TaskArguments>
	<TaskUserTextArguments>
	</TaskUserTextArguments>
	<UserAccount>SYSTEM</UserAccount>
	<Security>O:BAG:DUD:AI(A;;FA;;;SY)(A;;FA;;;BA)(A;;FR;;;LU)(A;;0x1301ff;;;S-1-5-80-2661322625-712705077-2999183737-
3043590567-590698655)(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;0x1200ab;;;LU)(A;ID;FR;;;AU)(A;ID;FR;;;LS)(A;ID;FR;;;NS)</Security>
	<StopOnCompletion>0</StopOnCompletion>
	<PerformanceCounterDataCollector>
		<DataCollectorType>0</DataCollectorType>
		<Name>DataCollector01</Name>
		<FileName>DataCollector01</FileName>
		<FileNameFormat>0</FileNameFormat>
		<FileNameFormatPattern>
		</FileNameFormatPattern>
		<LogAppend>0</LogAppend>
		<LogCircular>0</LogCircular>
		<LogOverwrite>0</LogOverwrite>
		<LatestOutputLocation>
		</LatestOutputLocation>
		<DataSourceName>
		</DataSourceName>
		<SampleInterval>15</SampleInterval>
		<SegmentMaxRecords>0</SegmentMaxRecords>
		<LogFileFormat>3</LogFileFormat>
		<Counter>\.NET CLR Memory(_Global_)\# Bytes in all Heaps</Counter>
		<Counter>\.NET CLR Memory(_Global_)\% Time in GC</Counter>
		<Counter>\Memory\Free System Page Table Entries</Counter>
		<Counter>\Memory\Pages/sec</Counter>
```

<Counter>\PhysicalDisk(_Total)\Avg. Disk Queue Length</Counter>
<Counter>\Process(_Total)\% Processor Time</Counter>
<Counter>\Process(_Total)\Private Bytes</Counter>
<Counter>\Process(_Total)\Virtual Bytes</Counter>
<Counter>\Process(_Total)\Working Set</Counter>
<Counter>\Process(AeXSvc)\% Processor Time</Counter>
<Counter>\Process(w3wp)\% Processor Time</Counter>
<Counter>\Process(w3wp#1)\% Processor Time</Counter>
<Counter>\Process(AeXSvc)\Private Bytes</Counter>
<Counter>\Process(w3wp)\Private Bytes</Counter>
<Counter>\Process(w3wp#1)\Private Bytes</Counter>
<Counter>\Process(AeXSvc)\Virtual Bytes</Counter>
<Counter>\Process(w3wp)\Virtual Bytes</Counter>
<Counter>\Process(w3wp#1)\Virtual Bytes</Counter>
<Counter>\Process(AeXSvc)\Working Set</Counter>
<Counter>\Process(w3wp)\Working Set</Counter>
<Counter>\Process(w3wp#1)\Working Set</Counter>
<Counter>\Processor(_Total)\% Processor Time</Counter>
<Counter>\System\Context Switches/sec</Counter>
<Counter>\Web Service(*)\Current Connections</Counter>
<CounterDisplayName>\.NET CLR Memory(_Global_)\# Bytes in all Heaps</CounterDisplayName>
<CounterDisplayName>\.NET CLR Memory(_Global_)\% Time in GC</CounterDisplayName>
<CounterDisplayName>\Memory\Free System Page Table Entries</CounterDisplayName>
<CounterDisplayName>\Memory\Pages/sec</CounterDisplayName>
<CounterDisplayName>\PhysicalDisk(_Total)\Avg. Disk Queue Length</CounterDisplayName>
<CounterDisplayName>\Process(_Total)\% Processor Time</CounterDisplayName>
<CounterDisplayName>\Process(_Total)\Private Bytes</CounterDisplayName>
<CounterDisplayName>\Process(_Total)\Virtual Bytes</CounterDisplayName>
<CounterDisplayName>\Process(_Total)\Working Set</CounterDisplayName>
<CounterDisplayName>\Process(AeXSvc)\% Processor Time</CounterDisplayName>
<CounterDisplayName>\Process(w3wp)\% Processor Time</CounterDisplayName>
<CounterDisplayName>\Process(w3wp#1)\% Processor Time</CounterDisplayName>
<CounterDisplayName>\Process(AeXSvc)\Private Bytes</CounterDisplayName>
<CounterDisplayName>\Process(w3wp)\Private Bytes</CounterDisplayName>
<CounterDisplayName>\Process(w3wp#1)\Private Bytes</CounterDisplayName>
<CounterDisplayName>\Process(AeXSvc)\Virtual Bytes</CounterDisplayName>
<CounterDisplayName>\Process(w3wp)\Virtual Bytes</CounterDisplayName>
<CounterDisplayName>\Process(w3wp#1)\Virtual Bytes</CounterDisplayName>
<CounterDisplayName>\Process(AeXSvc)\Working Set</CounterDisplayName>
<CounterDisplayName>\Process(w3wp)\Working Set</CounterDisplayName>
<CounterDisplayName>\Process(w3wp#1)\Working Set</CounterDisplayName>
<CounterDisplayName>\Processor(_Total)\% Processor Time</CounterDisplayName>
<CounterDisplayName>\System\Context Switches/sec</CounterDisplayName>
<CounterDisplayName>\Web Service(*)\Current Connections</CounterDisplayName>
</PerformanceCounterDataCollector>
<TraceDataCollector>
<DataCollectorType>1</DataCollectorType>
<Name>DataCollector02</Name>
<FileName>DataCollector02</FileName>
<FileNameFormat>0</FileNameFormat>
<FileNameFormatPattern>
</FileNameFormatPattern>
<LogAppend>0</LogAppend>
<LogCircular>0</LogCircular>
<LogOverwrite>0</LogOverwrite>
<LatestOutputLocation>
</LatestOutputLocation>
<Guid>{00000000-0000-0000-0000-000000000000}</Guid>
<BufferSize>8</BufferSize>
<BuffersLost>0</BuffersLost>
<BuffersWritten>0</BuffersWritten>
<ClockType>1</ClockType>
<EventsLost>0</EventsLost>
<ExtendedModes>0</ExtendedModes>
<FlushTimer>0</FlushTimer>

```
                <FreeBuffers>0</FreeBuffers>
                <MaximumBuffers>0</MaximumBuffers>
                <MinimumBuffers>0</MinimumBuffers>
                <NumberOfBuffers>0</NumberOfBuffers>
                <PreallocateFile>0</PreallocateFile>
                <ProcessMode>0</ProcessMode>
                <RealTimeBuffersLost>0</RealTimeBuffersLost>
                <SessionName>DataCollector02</SessionName>
                <SessionThreadId>0</SessionThreadId>
                <StreamMode>1</StreamMode>
        </TraceDataCollector>
        <ConfigurationDataCollector>
                <DataCollectorType>2</DataCollectorType>
                <Name>DataCollector03</Name>
                <FileName>DataCollector03</FileName>
                <FileNameFormat>0</FileNameFormat>
                <FileNameFormatPattern>
                </FileNameFormatPattern>
                <LogAppend>0</LogAppend>
                <LogCircular>0</LogCircular>
                <LogOverwrite>0</LogOverwrite>
                <LatestOutputLocation>
                </LatestOutputLocation>
                <QueryNetworkAdapters>0</QueryNetworkAdapters>
                <FileMaxCount>0</FileMaxCount>
                <FileMaxTotalSize>0</FileMaxTotalSize>
                <FileMaxRecursiveDepth>0</FileMaxRecursiveDepth>
                <RegistryMaxRecursiveDepth>0</RegistryMaxRecursiveDepth>
                <SystemStateFile>
                </SystemStateFile>
        </ConfigurationDataCollector>
        <DataManager>
                <Enabled>0</Enabled>
                <CheckBeforeRunning>0</CheckBeforeRunning>
                <MinFreeDisk>0</MinFreeDisk>
                <MaxSize>0</MaxSize>
                <MaxFolderCount>0</MaxFolderCount>
                <ResourcePolicy>0</ResourcePolicy>
                <ReportFileName>report.html</ReportFileName>
                <RuleTargetFileName>report.xml</RuleTargetFileName>
                <EventsFileName>
                </EventsFileName>
        </DataManager>
</DataCollectorSet>
```