# Sun StorageTek™ Business Analytics SRM Agent Installation Guide

Release 5.1

Sun Microsystems, Inc.
www.sun.com

Part No. 819-7208-10
November 2006, Revision 01

Submit comments about this document at: `http://www.sun.com/hwdocs/feedback`

# COPYRIGHT

## English:

## French:

# Table of Contents

# Introduction to the SRM Agent

The Sun StorageTek Business Analytics SRM Agent provides optimized disk scanning based upon disk layout.

**Note**: With the acquisition of StorageTek, Sun Microsystems has re-branded and re-named Global Storage Manager (GSM) as Sun StorageTek Analytics, a member of the Enterprise Storage Manager portfolio of software solutions. The functionality of Business Analytics is identical to GSM, only the name has changed.

Sun StorageTek Business Analytics 5.0 SP1 provides three agent installation CDs for the supported platforms: Windows Local Manager, Solaris Local Manager, UNIX Agents (HP-UX and IBM AIX). To upgrade an existing SRM Agent, uninstall the previously installed SRM Agent before you install the current Sun StorageTek Business Analytics SRM Agent.

**Notes**: Be sure to backup the SRM config_srm.xml file, the config_srm.xsd file, and the srmAgentPubCache.xml file before you upgrade the SRM Agent. The srmAgentPubCache.xml file is located where specified in the config_srm.xml file. The uninstallation of the SRM Agent on Solaris or other UNIX servers does not delete the srmAgentPubCache.xml file and older versions of the srmAgentPubCache.xml file are not compatible with the SRM Agent currently supplied with Sun StorageTek Business Analytics.

The following notes apply to installing and configuring the SRM Agent:

- Refer to the *Sun StorageTek Business Analytics Support Matrix* to confirm the server hardware/software configuration is supported.
- Consult the *Sun StorageTek Business Analytics Agent Features Quick Facts Sheet* for a summary of the features supported by a particular SRM agent, which may vary depending on data collection access method, platform or software components present.
- Requires the Host Agent.
- Allows optional scanning of network-mounted file-systems.
- Supports a user-definable scan schedule.
- Base behavior is controlled by storability.ini.
- Typical filtering rules can be configured using the Management Console's **SRM Agent Configuration** menu.
- Other complex filtering rules can be manually configured in the SRM Configuration File (config_srm.xml).
- Transform feature provides user-definable rules to facilitate user accounting.
- The SRM Agent provides support for specific file types (e.g., email archives) that affect the agent's configuration and reports.
- Agent auto registration is not supported for certain installation types (e.g., Self Extracting Agent Installation).
- Only change settings in the config_srm.xsd (schema) file if instructed to do so by your support representative.
- The Remote Share Configuration Tool (RSCT) may be used to facilitate configuring remote shares in the config_srm.xml file. Refer to the *Installation* Manual to obtain additional information on this tool.

## Solaris Installation

Effective with Sun StorageTek Business Analytics Release 5.1, all Solaris installation packages contain the prefix, SUNWbizan, within their package names. These names appear in the informational status text that is displayed when you install or uninstall a Business Analytics agent.

The Solaris Agent Installation CD provides an installation script (setup). The installation script (setup) can be used to:

- View a list of the available agents, depending on the server platform, that you can choose to install or upgrade.
- Perform agent upgrade for existing agent packages.
- Uninstall (setup –u) a previously installed agent package.

The installation script will validate that you have logged in as root, which is the required user permission to perform an agent installation. It also validates that the system is running a supported Operating System for an agent that you select for installation or upgrading.

## Automatic and Static Agent Registration

Automatic agent registration is a configuration option for agent data collection. In the storability.ini file, automatic agent registration is configured as follows:

- **Local Manager** – Specify the IP address or host name of the Local Manager to be contacted to activate agent registration.
- **Local Manager Registration Port** – Specifies the TCP port number used by the Local Manager for agent auto registration. The default port number is 17146.
- **Enable Auto Registration** – Turns agent auto registration on (default) or off.

To register the SRM Agent statically, proceed as follows:

- Enter false in the **Enable Auto Registration** field.
- Modify the Routing Agent static agent configuration to include an entry (port number|<agent IP address/name>)
- Restart the Routing Agent
- Restart the companion Central Manager agents

## SRM Agent Matrix

| Feature | Description |
|---|---|
| **Operating Systems** | |
| Windows | • InstallShield and Self-Extracting Agent Install supported<br>• Silent Installation supported for both InstallShield and Self-Extracting Agent Installation<br>• Required Server Access: Administrator privileges |
| Solaris | • Installation script<br>• Required Server Access: root access |
| AIX | • “Tar/install.sh” installation<br>• Required Server Access: root access |
| HP-UX | • Tar/install.sh” installation |

| | |
|---|---|
| | - Required Server Access: root access |

| Feature | Description |
|---|---|
| Red Hat Linux | • Tar/install.sh" installation<br>• Required Server Access: root access |
| **Configuration Parameters** | |
| *storability.ini file* | • **Local Manager** – Specifies the IP address or host name of the Local Manager to contact for agent auto registration. The default value is local host (meaning the Local Manager and SRM Agent are installed on the same server).<br>• **Local Manager Registration Port** – Specifies the TCP port number used by the Local Manager for agent auto registration. The default port number is 17146.<br>• **Enable Auto Registration** – Turn agent auto registration on (default) or off.<br>• **Location of xml schema file** – Directory/folder where the SRM Agent XSD schema file is located.<br>• **Location of xml input file** - Directory/folder where the SRM Agent XML input file (config_srm.xml) is located. |
| *config_srm.xml file* | The config_srm.xml file largely controls the behavior of the SRM Agent. The Sun StorageTek Business Analytics administrator can use the Management Console's **SRM Agent Configuration** menus to create and save the SRM Agent Configurations for their environment. These menus allow the agent's scan schedule, basic filters, and some advanced settings in a specified config_srm.xml file to be configured and saved.<br><br>Refer to the *Administration* chapter for additional information on the **SRM Agent Configuration** menus in the Management Console. |

**Table 1 - SRM Agent Matrix**

# Configuration Methods

The Sun StorageTek Business Analytics administrator can use an XML editor to manually configure the scan schedule, filters, and advanced options that control the behavior of the Sun StorageTek Business Analytics SRM Agent. These configuration settings are stored in the SRM Agent configuration file (config_srm.xml).

To greatly simplify configuring the SRM Agent, the SRM Agent Configuration window in the Management Console provides the capability to create, modify, and save configuration parameters for a SRM Agent installed on a Windows or UNIX platform.

Using the **SRM Agent Configuration** window, the Sun StorageTek Business Analytics administrator can perform the following configuration functions:

- Specify loading a file for a Windows or UNIX platform
- Choose to load a default SRM Agent Configuration or specify the location of the desired file.
- Specify the frequency (hourly, daily, weekly, and monthly) and any related frequency options (e.g., hourly, every four hours).

- Specify pre-scan and post-scan filters.
- Specify Advanced Settings (e.g., enable remote file system scan).

Using **SRM Agent Configuration**, the Sun StorageTek Business Analytics administrator can set up filters, such as to identify the largest files, the largest old files, and the general distribution of storage utilization by file type. The SRM Agent Configuration may include new filters and related reports for:

- **Email Archives** – Provides filters to report detailed information about the size and location of email archives. Default filters are provided for Outlook users' .ost and .pst files as well as for Lotus Notes users' .nsf and .nst files.
- **Unauthorized Files** – Provides filters that help to limit the storage of particular file types (.mp3, .wav, .avi) on corporate networks.
- **Largest Directory Consumers -** Provides the SRM Agent Configuration filters that can be used to identify the directories that utilized the most disk space.
- **Nth level Directories –** Provides the capability to report on directories at various levels of the hierarchy under filesystems.

Refer to the *Administration* chapter for instructions on the use of the Management Console's **SRM Agent Configuration** functionality. The file-specific reports are described in the *Sun StorageTek Business Analytics Management Console User's Guide*.

## SRM Agent Configuration File

This section describes configuration settings related to the SRM Agent Configuration File (config_srm.xml).

**Important Note**: This section is only intended for customers who need to set up filters in the configuration file beyond what can be done using the Management Console's **SRM Agent Configuration** menus, as described in the *Administration* chapter.

At the highest level, the configuration file is divided into three (3) sections:

- **Configuration** - This is the optional section containing filter definitions and declarations.
- **Agent Level Configuration** - This is a mandatory section containing scan configurations like schedules, scan-time filter configurations, and so forth.
- **Table Level Configuration** - This is a mandatory section, which involves section configuration options for output tables supported by the SRM Agent.

## Filter Section

This section describes the basic functionality of filters used in the SRM Agent. A filter has match criteria and an action to be performed, if the match criteria evaluates successfully. Each row of file detail information will consume 4KB RAM.

The match criteria can be specified for different file system objects:

- File system
- Directory on the file system
- File on the file system

The match criteria involve comparing the attribute of the file system object to the some value. For example, match all files whose size (size is one of the attributes of the file system object) is more than or equal to XXMB. The match criteria are specified through the XML configuration file installed during the SRM Agent installation.

Upon successful match, SRM Agent performs a certain action. There are three pre-defined actions:

- **Include -** Means consider the file system object (matched by the filter criteria) for further processing (e.g. if files match certain criterion of file_size > 100 MB, report them in largest files table).
- **Exclude -** Means do not consider these file system objects (matched by the filter criteria) for further processing (e.g. if the dir matches criterion of dir_name contains "administrator", do not scan further inside the dir).
- **Transform -** Means change the attribute value of the file system object (matched by the filter criteria) to a given value, before further processing (e.g. change the owner of any file under directory matching criterion dir_name contains "*george*" to "finance department").

The SRM Agent scans the file systems, processes the data, and finally publishes the data. Some examples of setting the scan time filter:

- Skip a file system
- Skip a directory on a file system

An example of a processing time filter is to skip a file while calculating usage factors (but that file will be considered for other type of processing like type distribution etc.).

Some examples of a publish time filter:

- Do not report users with less than X MB space occupied on a file system
- Do not report users, which have "ADMIN" in their username.

All the filters that are set finally affect the data being published by the SRM Agent.

## Configuration Levels

The configuration file is divided into three levels:

- Filter Configurations
- Agent Level Configurations
- Table Level Configurations

The sequence of the configuration levels must be the same as specified above.
If the configuration parameters are not specified in the XML file, the default values are used.

The Filter Level Configurations consists of filter definitions and declarations. The sequences of entries in the configuration file are as follows:

- The main tag used is <filter_config>.
- There must be at least one (1) <filter_def> tag inside <filter_config> tag.
- Every filter definition must be given a unique name.
- A filter definition tag <filter_def> contains a <filter_object> tag that specifies which file system object this filter applies to (i.e. the "match criteria".)
- There must be exactly one <filter_object> tag inside <filter_def> tag.

A sample filter definition is as follows:

```
<filter_def name="temp_data_filter_1">
      <filter_object attribute="path" operator="eq"
                            expandEnv="true">%TEMP%</filter_object
>
</filter_def>
```

The following table explains these variables.

| Attribute Name | Description |
|---|---|
| name=”temp_data_filter_1” | Name specified for the filter definition. Name can be user-dependent. |
| attribute=”path” | File system objects attribute to match. |
| operator=”eq” | Operator to be used while matching the attribute. |
| %Temp% | The pattern to be matched against given attributes value. In this case, it is a System Environment variable. |

The following attributes and the corresponding operators can be used:

| Attribute | Supported Operator |
|---|---|
| Path | eq (Equal operator) |
|  | wildcardeq (Wild card operator) |
|  | regexeq (Regular Expression operator – follows Perl Compatible Regular Expressions) |
| Owner | eq |
|  | wildcardeq |
|  | regexeq |
| Size | eq |
|  | Neq (Not Equal to) |
|  | lt (Lesser than) |
|  | lteq (Lesser than Equal To) |
|  | gt (Greater than) |

| | |
|---|---|
| | gteq (Greater than equal to) |

| Attribute | Supported Operator |
|---|---|
| access_time | eq |
|  | neq |
|  | lt |
|  | lteq |
|  | gt |
|  | gteq |
| modification_time | eq |
|  | neq |
|  | lt |
|  | lteq |
|  | gt |
|  | gte |
| creation_time | eq |
|  | neq |
|  | lt |
|  | lteq |
|  | gt |
|  | gteq |

**Note:**
The attributes and the operators are case sensitive. They should be provided in lower case letters.

## Remote File System Scan Exclusion filters

If you want to skip a folder on a remote file system, a sample filter would be:

```
          <filter_def name="remotefsskip">
            <filter_object attribute="path" operator="wildcardeq"
      caseSensitive="false">\\192.168.100.100\folder</filter_object>
          </filter_def>
```

and in the Agent or tables section use:

```
          <filter name="remotefsskip" action="exclude"/>
```

**Note**: When the SRM Agent is installed, it is registered as a service, but doesn't start scanning. It waits for the user to configure the XML file and then starts scanning when it is started.

## Agent Level Configuration

The Agent Level configuration specifies the following:

- Scan schedule
- Scan Configuration
- Publisher Configuration
- Remote Command Configuration

### Scan Schedule

The scan schedule configuration section contains the periodic scan specification for the SRM Agent. The agent is configured to scan the file system based upon the scheduling parameters passed in the configuration file.

The sequences of entries in the configuration file are as follows:

- The main tag used is <agent_config>.
- The <schedule> tag is used to specify the schedule for the scanning process
- The <schedule> tag can contain one or more instances of the <scan> tag.

Sample entries are listed as follows:

```
<schedule disablePeriodicScans=”false”
                 disableScanOnAgentStart=”false”>
  <scan type=”exhaustive”> 1 2 * * 1</scan>
</schedule>
```

| Attribute Name | Description |
|---|---|
| disablePeriodicScans=”false” | If ‘false’ then the SRM Agent periodic scheduler is enabled otherwise vice versa |
| disableScanOnAgentStart=”false” | If ‘false’ then it means the Agent will automatically scan the host once when the service/daemon is started and resumes normal schedule. If’ ‘true’ then the agent will not start the scan on the start up. |
| Type=’exhaustive” | Must be always ‘exhaustive’ |
| Value (1 2 * * 1) | This is the crontab value passed to the attribute |

The crontab format is briefly explained as follows:

- There are five elements in the value.
- 1st element: Minute of the hour. Allowed values: 0 to 59
- 2nd element: Hour of the day: Allowed values: 0 to 23
- 3rd element: Day of the month: Allowed values: 1 to 31
- 4th element: Month of the year: Allowed values: 1 to 12 (no month names allowed)
- 5th element: Day of the week: Allowed values 0 (Sunday) to 6 (Saturday)
- If the value is greater than the allowed maximum value for an element, the current element is “rolled over” and the “extra” or the “difference” is carried over to the next element. If all values are to be specified for an element, use *.

### ***SCAN CONFIGURATIONS***

The scan configuration specifies the following information:

- Filter Application - Specifies which filters defined earlier in the <filter_config> have to be used at scan time.
- Remote file system configuration - Specifies which remote file system to scan.
- Multithreading scan options  - Specifies the level of multi-threading for scanning local and remote file systems

Scan Configuration has an option to specify how to handle the compressed NTFS files. A sample entry is as follows:

```
<scan_config handleCompressedData=”true”>
 …
 </scan_config>
```

| Attribute Name | Description |
|---|---|
| handleCompressedData=”true” | If ‘true’ (default), the compressed file size is considered for calculations for all compressed files on NTFS file system (and not the actual size, which could be larger than compressed file size). |
| handleCompressedData=”false” | If ‘false’, the actual file size is used for calculations for all compressed files on NTFS file system (and not the compressed file size) |

For uncompressed files, the actual file size is used.

## Filter Application Section

The <Filters> section refers to one or more filters defined previously in the <filter_config> section.

There can be one or more <filter> tags inside <filters>. Each filter refers to a previously defined filter definition by name and specifies the action to be taken if the filter matches successfully.

A sample entry is listed as follows:

```
<filters>
  <filter name="orphan_user_data_3"
            action=" transform ">%Computername%\administrator
</filter>
</filters>
```

| Attribute Name | Description |
|---|---|
| name ="orphan_user_data_3” | The filter name already defined in the xml file. |
| action="transform" | |
| action="transform">%Computername%\administrator | Filter action value (if this ‘transform’ filter matches, use this owner ‘administrator’ instead of the existing owner of the file system object. |

## Remote File System Scan Configuration

For Windows, perform the following steps to configure and use the remote file system scan capabilities of the SRM Agent:

- As a system administrator, set up security to enable the SRM Agent to access the network share (Windows).
- Define the remote file system configuration settings for your environment (see also the following **Remote File System Configuration** section).

### Set Up System Security

The following general security guidelines must be followed:

- Only ‘auth_userName’ must have read permissions on the remote machine to read the share specified in the ‘share_name’ setting.
- The ‘imp_user’ need not have access permissions on the remote machine to be scanned by the SRM Agent.
- The ‘imp_user’ must be manually registered in Windows Local Security policy to possess “Log On as Service Rights” privileges on the server running the SRM Agent.
- If the impersonating user is not an administrator on the computer that is running the scan, the permissions for the C:\Program Files\Storability\GSM\Agents\Storability SRM Agent (or where ever the SRM agent is running from) need to be updated so that the impersonating user had read-write permissions to the directory and the files in it. Otherwise, some of the possible error messages regarding impersonating user will not be written to the Message log.

### *Windows Security – Add User*

The following steps summarize adding a user on a Windows 2000 computer.

1. Log on to the Windows system using a local/domain administrative user account.
2. Select Start**-> Settings ->Control Panel-> Users and Passwords**.
3. Click the **Advanced** tab. In the Advanced User Management section, click **Advanced**.
4. Click the **Users** folder. The current users are displayed in the right pane.
5. On the **Action** menu, click **New User**.
6. In the User Name box, type the user name and the password (the password is case-sensitive) in the Password and Confirm Password boxes.
7. Click to clear the **User must change password at next logon** check box. Click **Create**.

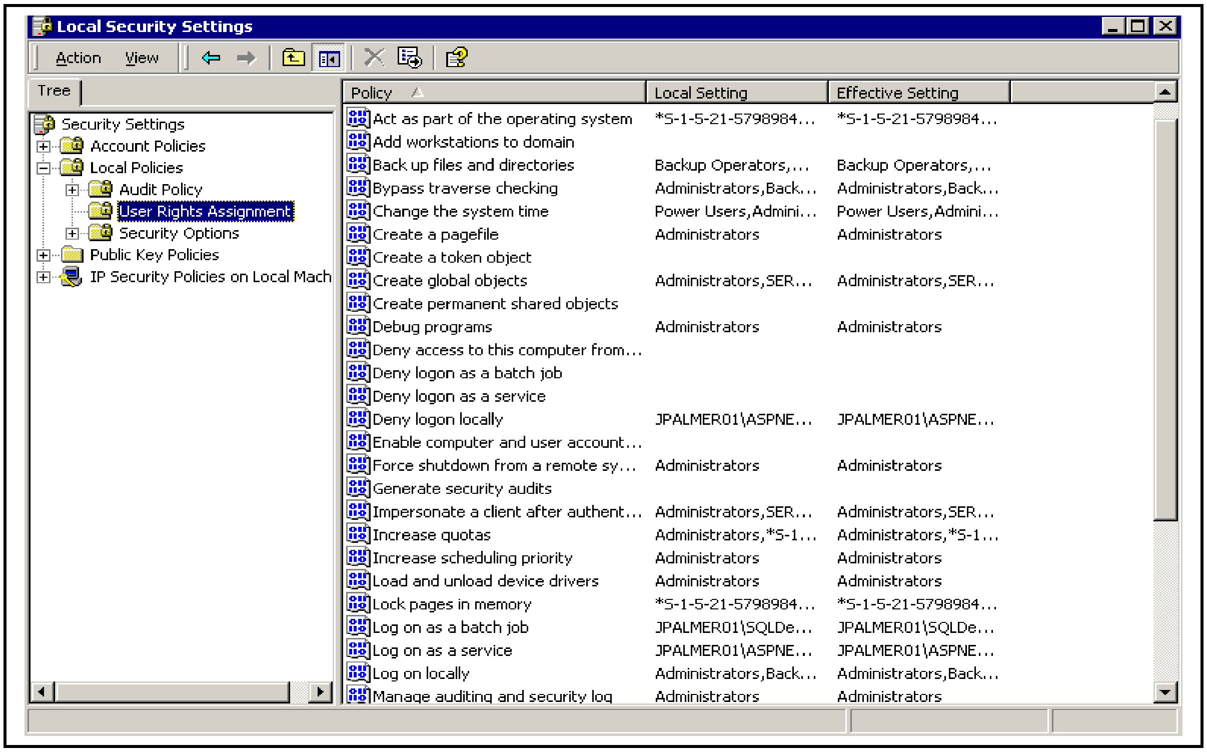
### Logon as service user

The Windows user to be configured as the impersonating user must be assigned the security right, “Logon as service user”, defined under Local Security Settings. A sample procedure follows.

1. Locate **secpol.msc** on your computer. The following example assumes you located the c:\C:\WINNT\SYSTEM32 folder.
2. Open a DOS command window and change launch secpol.msc to open the Local Security Settings window. For example, type:

   *C:\WINNT\SYSTEM32\secpol.msc /s*

3. Expand **Local Policies** and click **User Rights Assignment**.



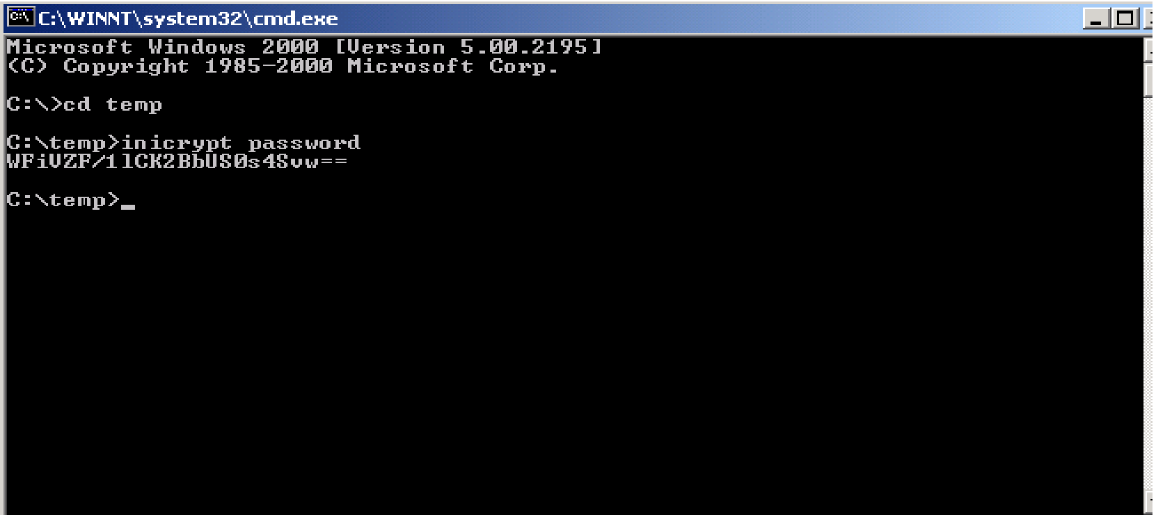
| Policy | Local Setting | Effective Setting |
|---|---|---|
| Act as part of the operating system | *S-1-5-21-5798984... | *S-1-5-21-5798984... |
| Add workstations to domain | | |
| Back up files and directories | Backup Operators,... | Backup Operators,... |
| Bypass traverse checking | Administrators,Back... | Administrators,Back... |
| Change the system time | Power Users,Admini... | Power Users,Admini... |
| Create a pagefile | Administrators | Administrators |
| Create a token object | | |
| Create global objects | Administrators,SER... | Administrators,SER... |
| Create permanent shared objects | | |
| Debug programs | Administrators | Administrators |
| Deny access to this computer from... | | |
| Deny logon as a batch job | | |
| Deny logon as a service | | |
| Deny logon locally | JPALMER01\ASPNE... | JPALMER01\ASPNE... |
| Enable computer and user account... | | |
| Force shutdown from a remote sy... | Administrators | Administrators |
| Generate security audits | | |
| Impersonate a client after authent... | Administrators,SER... | Administrators,SER... |
| Increase quotas | Administrators,*S-1... | Administrators,*S-1... |
| Increase scheduling priority | Administrators | Administrators |
| Load and unload device drivers | Administrators | Administrators |
| Lock pages in memory | *S-1-5-21-5798984... | *S-1-5-21-5798984... |
| Log on as a batch job | JPALMER01\SQLDe... | JPALMER01\SQLDe... |
| Log on as a service | JPALMER01\ASPNE... | JPALMER01\ASPNE... |
| Log on locally | Administrators,Back... | Administrators,Back... |
| Manage auditing and security log | Administrators | Administrators |

**Figure 1 - Local Security Settings**

4. Click the Log on as a service icon and the Local Security Policy Setting window opens.
5. Click Add to open the Select Users or Groups window.
6. Locate and select (highlight) the user you added and click Add.
7. Click OK to return to the Local Security Policy Setting window.
8. Click OK to return to the Local Security Settings window.
9. Close the Local Security Settings window.

## *Password Encryption*

The password stored in the SRM agent configuration must be encrypted. Use the Storability-supplied **inicrypt** utility to encrypt the user's password. On Windows servers, the default location is <drive>:\Program Files\Storability\GSM\Storability Local Manager Utilities. On Solaris, the default location is /opt/storability/utilities. Record the encrypted password for reference when you set up the SRM Agent's configuration file.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>cd temp

C:\temp>inicrypt password
WFiVZF/11CK2BbUS0s4Svw==

C:\temp>_
```

**Figure 2 - Encrypting a Password**

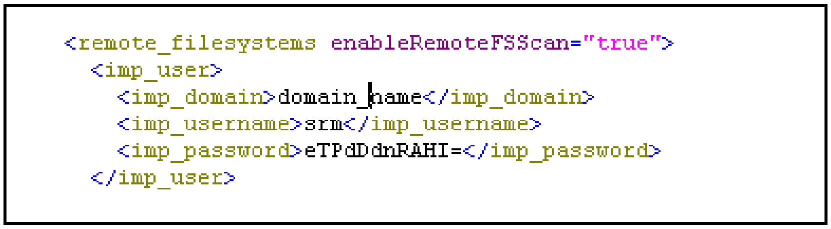
**Note**: The Management Console's SRM Agent Configuration option can be used to define an impersonating user. However, the password that is written when you save the configuration is not encrypted (plain text). Therefore, this password should be replaced with an encrypted password before the SRM agent configuration file is used.

### *Remote Scanning a Windows Share*

The remote file system scanning section of the configuration file (config_srm.xml) can be only used on a Windows-based SRM Agent. This functionality is NOT available on non-Windows SRM Agents.

**Note**: For the SRM Agent to report all the information about a file/directory, the userID used to run the agent should have the following (effective) permissions on the directory or the file:

- Traverse Folder
- List Folder
- Read Attributes
- Read Extended Attributes
- Read Permissions



```
<remote_filesystems enableRemoteFSScan="true">
  <imp_user>
    <imp_domain>domain_name</imp_domain>
    <imp_username>srm</imp_username>
    <imp_password>eTPdDdnRAHI=</imp_password>
  </imp_user>
```

The tags are briefly described as follows:

- **remote_filesystems enableRemoteFSScan** – This tag is used to enable or disable remote filesystem scans. The possible values for this tag are listed as follows:

  *<remote_filesystems enableRemoteFSScan="true">*

  Or:

  *<remote_filesystems enableRemoteFSScan="false">*

- **imp_user**- This tag is used to group and indicate that the encapsulated entries are for the impersonating user information. The impersonating user information is used by the SRM Agent for impersonating itself as a logged in user on the local machine while connecting to the remote share.

- **imp_domain**- This tag specifies the Windows Domain that has the User ID indicated by the *imp_username* tag. This configuration setting may contain the computer name - this helps when the machine is not in a domain, or alternatively, the domain name (where the user ID exists) can also be supplied.

- **imp_username**- This tag pair encapsulates the user name of the user to impersonate. The SRM Agent tries to log in as this user name on the local system before attempting the remote file system scan.

- **imp_password**- This tag indicates the encrypted password, which is obtained by supplying the password to the *inicrypt* utility, as previously described.

- **filesystem_def**- This tag pair encapsulates the share definition and the user Id information that the  SRM Agent will try to use to connect to the remote file system.

- **share_name**- This tag indicates the path to the share in UNC format. The machine name or its IP address (used if the machine is not in a domain) and the share name to scan are specified. Some examples follow.

```
<share_name>\\MACHINE_NAME\shared_folder</share_name>
                       or:
    <share_name>\\IP_ADDRESS\shared_folder</share_name>
```

- **auth_username -** This tag encapsulates the User ID that the SRM Agent uses for connecting to the remote file system or remote share. The User ID specified here is typically a local user on the remote machine where the remote file system resides, having access to the share. However, if the share name has the machine name specified in the share_name tag, the User ID can be a Windows domain user who has access rights to the remote share.

  For example, if the remote machine doesn’t belong to a Windows domain and the local user name is **abc**, **<auth_username>** would just be:

  ```
  <auth_username>abc</auth_username>
  ```

  If the remote machine belonged to a domain, DOM, and the user name is **xyz**, the **<auth_username>** would be:

  ```
  <auth_username>DOM\xyz</auth_username>
  ```

- **auth_password**- This tag specifies the authentication password used by the  SRM Agent to connect to the remote share. Again, it is in an encrypted form, using the inicrypt utility.

EXAMPLES

Assume that:

- The SRM Agent is running on MYMACHINE and that it's not in any Windows domain.
- john is a local system user on MYMACHINE.
- The remote share is \\192.168.200.4\storability and it is not in the Windows domain either.
- Scott has access to \\192.168.200.4\storability.

The config_srm.xml may be set up as follows:

```
<remote_filesystems enableRemoteFSScan="true">
<imp_user>
<imp_domain>MYMACHINE</imp_domain>
<imp_username>john</imp_username>
<imp_password>1+6TOCITbM4=</imp_password>
</imp_user>
<filesystem_def>
<share_name>\\192.168.200.4\storability</share_name>
<auth_userName>Scott</auth_userName>
<auth_password>gg3oB5JXqas=</auth_password>
</filesystem_def>
</remote_filesystems>
```

Assume that:

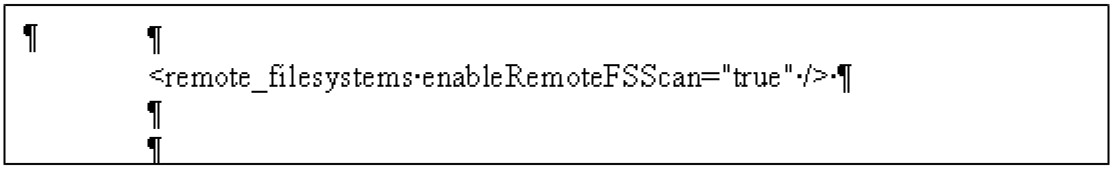
- The SRM Agent is running on MYMACHINE and its in Windows domain is UTOPIA.
- john is a domain user in UTOPIA.
- The Remote share is \\DOMSHARE\storability and it's in the domain UTOPIA.
- john has access to \\DOMSHARE\storability.

The config_srm.xml may be set up as follows:

```
<remote_filesystems enableRemoteFSScan="true">
<imp_user>
<imp_domain>MYMACHINE</imp_domain>
<imp_username>john</imp_username>
<imp_password>1+6TOCITbM4=</imp_password>
</imp_user>
<filesystem_def>
<share_name>\\DOMSHARE\storability</share_name>
<auth_userName>john</auth_userName>
<auth_password>1+6TOCITbM4=</auth_password>
</filesystem_def>
</remote_filesystems>
```

### REMOTE SCANNING THE NFS MOUNT ON SOLARIS

The section of the configuration file that pertains to remote file system scanning appears below. You must manually add this tag to your config_srm.xml file.



```
¶         ¶
          <remote_filesystems·enableRemoteFSScan="true"·/>·¶
          ¶
          ¶
```

This tag is briefly described as follows:

- **remote_filesystems enableRemoteFSScan** – This tag is used to enable or disable the remote file system scan capability. Possible values for this tag are listed as follows:

  *<remote_filesystems enableRemoteFSScan="true">*

  or:

  *<remote_filesystems enableRemoteFSScan="false">*

### Common Options

The following configuration options are applicable to both "Remote scan (Windows)" and "Remote Mount scan (NFS)".

- **multi_threading_model** – This tag dictates the number of PPUs (Parallel Processing Units) that the SRM Agent spawns to scan the file systems.
- **forRemoteFilesystems** – Is specified as either "SEQUENTIAL" or "PER_FILESYSTEM" to scan file system after file system or to start the scan of all remote file systems at once, respectively. The SEQUENTIAL configuration setting optimizes the use of system resources but takes longer to complete the scan. The PER_FILESYTEM setting can optimize scan performance at the risk of consuming a high level of system resources if many file systems are involved.

### Multi-threading Options

The multi-threading tag is listed as follows:

```
<multi_threading_model forLocalFilesystems="PER_FILESYSTEM"
forRemoteFilesystems="PER_FILESYSTEM" maxThreadLimit="3"/>
```

For Local Filesystems (forLocalFilesystems), the valid values are described as follows:

- "SEQUENTIAL" - In this mode, the SRM Agent will create one thread for scanning all local filesystems.
- "PER_DISK" - In this mode, the SRM Agent will create one thread per disk for scanning local filesystems. This is supported on a Windows server only.
- "PER_FILESYSTEM" - In this mode, the SRM Agent will create one thread per filesystem for scanning local filesystems.

For Remote Filesystems (forRemoteFilesystems), the valid values are described as follows:

- "SEQUENTIAL" - In this mode, the SRM Agent will create one thread for scanning all remote filesystems.
- "PER_FILESYSTEM" - In this mode, the SRM Agent will create one thread per filesystem for scanning remote filesystems.

The Max Thread Limit (maxThreadLimit ) parameter specifies the maximum number of threads that the SRM Agent can create while scanning local and remote filesystems combined. The default value of "maxThreadLimit" is 3, and this value can be extended to a maximum of 10.

**Note**: Any multi-threading option other than those described above is considered as "invalid". In this case, the SRM Agent will discard the invalid value and will revert to the default value of the above attributes.

# Transform Filters

Transform filters allow you to transform the owner of a directory for reporting purposes. You define the Transform filters in the SRM Agent Configuration file, which is located in the SRM Agent folder on Windows or in the /install_directory/storability/etc directory (e.g., /opt/storability/etc) on Solaris. The Transform filters are not designed to change system directory/file permissions.

## Transform Directory Owner Recursively

There are two operators that allow you to transform the owner of all files under a directory as well as those under its subdirectories: the “wildcardeq” operator and the regexeq operator.

## Using the wildcardeq Operator

A sample configuration that uses the “wildcardeq” operator follows.

```
<filter_config>

 <!--  Filters get defined here to specify the path needed for the transform filter
-->

<!—For transforming owner of files under sub-directories of dnorton directory-->
 <filter_def name="dnorton_filterR">
  <filter_object attribute="path"
operator="wildcardeq">/users/dnorton/*</filter_object>
  </filter_def>

<!—For transforming owner of files under dnorton directory-->
<filter_def name="dnorton_filter">
  <filter_object attribute="path" operator="eq">/users/dnorton</filter_object>
  </filter_def>

<filter_config>

<scan_config handleCompressedData="true">
<filters>
<!--  we use the filter here as a transform filter, where all the files defined in
dnorton_filter will be owned by the user of dnorton. It can also be changed to any
other existing user.  -->

<filter name="dnorton_filterR" action="transform">dnorton</filter>
<filter name="dnorton_filter" action="transform">dnorton</filter>

</filters>
```

## Using the regexeq Operator

A sample configuration that uses the “regexeq” operator follows.

```
<filter_config>

 <!--  Filters get defined here to specify the path needed for the transform filter
-->

 <filter_def name="dnorton_filterR">
  <filter_object attribute="path"
operator="regexeq">/users/dnorton/[.]*</filter_object>
  </filter_def>
<filter_def name="dnorton_filter">
```

```
  <filter_object attribute="path" operator="eq">/users/dnorton</filter_object>
  </filter_def>

<filter_config>

<scan_config handleCompressedData="true">
<filters>

<!--  we use the filter here as a transform filter, where all the files defined in
dnorton_filter will be owned by the user of dnorton. It can also be changed to any
other existing user.  -->

<filter name="dnorton_filterR" action="transform">dnorton</filter>
<filter name="dnorton_filter" action="transform">dnorton</filter>

</filters>
```

## Transform Directory Owner Recursively with Exception

The Transform feature also allows you to transform the owner of all files under a directory as well as the files under the subdirectories except for one directory, such as subDir1.

## Using the wildcardeq Operator

A sample configuration that uses the "wildcardeq" operator to transform the owner of all files under the dnorton directory as well as the files under the subdirectories except for one directory, subDir1, follows.

```
<filter_config>

 <!--  Filters get defined here to specify the path needed for the transform filter
-->

<filter_def name="dnorton_filterR">
  <filter_object attribute="path"
operator="wildcardeq">/users/dnorton/*</filter_object>
  </filter_def>
<filter_def name="dnorton_filter">
  <filter_object attribute="path" operator="eq">/users/dnorton</filter_object>
  </filter_def>

<filter_def name="subDir1_filter">
  <filter_object attribute="path" operator="eq">/users/dnorton/subDir1</filter_object>
  </filter_def>

<filter_config>

<scan_config handleCompressedData="true">
<filters>

<!--  we use the filter here as a transform filter, where all the files defined in
dnorton_filter will be owned by the user of dnorton. It can also be changed to any
other existing user.  Order is important, transform filter for subDir1 must come prior
to dnorton-->

<filter name="subDir1_filter" action="transform">subDiruser</filter>

<filter name="dnorton_filterR" action="transform">dnorton</filter>
<filter name="dnorton_filter" action="transform">dnorton</filter>

</filters>
```

## Using the regexeq Operator

A sample configuration that uses the "regexeq" operator to transform the owner of all files under the dnorton directory as well as the files under the subdirectories except for one directory, subDir1, follows.

```
<filter_config>
```

```
 <!--  Filters get defined here to specify the path needed for the transform filter
-->

 <filter_def name="dnorton_filter">
  <filter_object attribute="path"
operator="regexeq">/users/dnorton/[.]*</filter_object>
  </filter_def>
<filter_def name="dnorton_filter">
  <filter_object attribute="path" operator="eq">/users/dnorton</filter_object>
  </filter_def>

<filter_def name="subDir1_filter">
          <filter_object attribute="path"
        operator="eq">/users/dnorton/subDir1</filter_object>
          </filter_def>


        <filter_config>

        <scan_config handleCompressedData="true">
        <filters>

        <!--  we use the filter here as a transform filter, where all the files
        defined in dnorton_filter will be owned by the user of dnorton. It can also be
        changed to any other existing user.  Order is important, transform filter for
        subDir1 must come prior to dnorton-->

        <filter name="subDir1_filter" action="transform">subDiruser</filter>

        <filter name="dnorton_filterR" action="transform">dnorton</filter>
        <filter name="dnorton_filter" action="transform">dnorton</filter>


        </filters>
```

## Transform Directory Owner Non-Recursively

The Transform feature may also be used to transform the owner of directory non-recursively. You set up the non-recursive transform of directory ownership as shown below.

```
<filter_config>

   <!--  Filters get defined here to specify the path needed for the transform filter
-->

 <filter_def name="dnorton_filter">
  <filter_object attribute="path" operator="eq">/users/dnorton/</filter_object>
  </filter_def>

<filter_config>

<scan_config handleCompressedData="true">
<filters>

<!--  we use the filter here as a transform filter, where all the files defined in
dnorton_filter will be owned by the user of dnorton. It can also be changed to any
other existing user.  -->

<filter name="dnorton_filter" action="transform">dnorton</filter>

</filters>
```

## Sample Transform Filter Settings for Windows

Sample Transform filter settings for use on a Windows server appear below.

```
<filter_def name="t1_r"> <!--filter for transforming owner of subdirectories-->
<filter_object attribute="path" operator="wildcardeq" expandEnv="true">C:\Program
Files\*</filter_object>
    </filter_def>
<filter_def name="t1">  <!-- while specifying directory name, don't append "\" at the
end -->
      <filter_object attribute="path" operator="eq" expandEnv="true">C:\Program
Files</filter_object>
    </filter_def>
```

```
      <scan_config handleCompressedData="true">
            <filters>
              <filter name="sys_data_filter_1" action="exclude"/>
              <filter name="sys_data_filter_2" action="exclude"/>

      <filter name="t1" action="transform">all</filter>
      <filter name="t1_r" action="transform">all</filter>
      </filters>
```

### Sample Transform Filter Settings for Solaris

Sample Transform filter settings for use on a Solaris server appear below.

```
            <filter_def name="tmp_dir_r">
              <filter_object attribute="path" operator="wildcardeq">/tmp/*</filter_object>
            </filter_def>
             <filter_def name="tmp_dir">
              <filter_object attribute="path" operator="eq">/tmp</filter_object>
            </filter_def>

<filter name="sys_data_filter_1" action="exclude"/>
        <filter name="sys_data_filter_2" action="exclude"/>
        <filter name="sys_data_filter_3" action="exclude"/>
        <filter name="root" action="exclude"/>
        <filter name="tmp_dir" action="transform">mandar</filter>
        <filter name="tmp_dir_r" action="transform">mandar</filter>
      </filters>
```

### Verifying Transform Filters

To verify Transform filters are working properly, use the Agent Diagnostic Tool (gsmdiag.exe).

- Collect the gsm_srm_largest_files (or gsm_srm_largest_old_files) table and examine the **owner** column data.
- Collect the gsm_srm_user table and examine the srm_user_id and srm_user_name columns' data

## Publisher Configuration Section

This section sets the options for the publisher behavior.

| Attribute Name | Description |
|---|---|
| publishDataPerFilesystemScanUpdate<publisher_config publishDataPerFilesystemScanUpdate="true" enableDiskCache="true"/> ="true" | If 'true' (default), as soon as a scan for a file system finishes, the data in SRM Agent tables is immediately updated.<br>If 'false', SRM Agent waits for the entire scan to complete (for all file systems) to update data. |
| publisher_config enableDiskCache ="true" | If 'false' (default), SRM Agent will not update/create local disk cache. If 'true', whenever table data is updated, it is synched with a local disk cache (so that when the SRM Agent is restarted, it can still serve last scan data. |

### Remote Command Configuration Section

This section contains a list of users and their encrypted password (<auth_user> elements), which will be allowed to use the remote commands (one of the username-password pair from this list in the configuration must be specified as table request parameters while sending remote commands to the SRM Agent). Optionally, the user can specify which OS group should be allowed to use remote commands.  A sample entry follows:

```
<remote_command_config>
  <auth_user>
    <auth_username>srmAdmin1</auth_userName>
    <auth_pass>OKQWJE9WQE91== </auth_password>
  </auth_user>
   …
   …
  <os_auth_group>GSM SRMAdmin</os_auth_group>
</remote_command_config>
```

| Tag Name | Description |
|---|---|
| <auth_username>srmAdmin1</auth_userName> | UserName. |
| <auth_pass>OKQWJE9WQE91== </auth_password> | Encrypted Password. |
| <os_auth_group>GSM SRMAdmin</os_auth_group> | OS users, which are members of this OS group will be allowed to send remote commands (if they specify their valid password along with the remote command). |

## Table Level Configuration

The filters applied at publishing time are called Table Filters. Hence table filters are applied after scan filters. Some examples of table filters are listed as follows:

- Skip temporary directories when reporting data for largest files.
- Do not report users with less than X MB space used on a file system.

The regexeq operator is not supported for "gsa_srm_temporary_directories" table filters.

| Filter Tag name | Filter Description | Examples |
|---|---|---|
| <gsa_srm_temporary_directories><br>A | Identify certain directories on a file system as a “temporary directory”. Report these in gsa_srm_temporary_directories table. | Temp folders like C:\temp, c:\tmp or /tmp, /var/tmp |
| <gsa_srm_largest_files> & <gsa_srm_largest_old_files> | Threshold filter that skips certain files or folders while reporting data on largest files on file system. Allows, “exclude” action filters. | Do not report c:\pagefile.sys or any file under c:\WINNT as largest files. |
| <gsa_srm_usage_factors> | Skip files or directories while calculating usage<br>Allows, “exclude” action filters. | Skip pagefile.sys on all drives while calculating |

| | | |
|---|---|---|
| | | usage factor. |

| Filter Tag name | Filter Description | Examples |
|---|---|---|
| <gsa_srm_usage_details> | Report data related to Specific File Types based on configuration parameters specified in the configuration file | Report all email archives (*.pst, *.ost, .nsf). Report all unauthorized files (*.mp3, *.mpeg, *.avi) |
| <gsa_srm_type_distribution> | Files of these types (ex exe, EXE) are treated case insensitive | Report all .exe and .EXE file tyes. |

Besides these generic filters, there are few additional filters available, such as gsa_srm_user, gsa_srm_size_distribution and gsa_srm_filesystem.

The sections below describe table filter tags in detail.

### GSA_SRM_LARGEST_FILES SECTION

This section specifies the criteria for selecting "largest files" on a file system. A sample entry is as follows:

```
<gsa_srm_largest_file   rowsPerFileSystem=”25”
                   fileSizeThreshold=”5242880”/>
```

| Attribute Name | Description |
|---|---|
| rowsPerFileSystem=”25” | Report only specified number of rows (at max) per file system, that is, 25. The default range is zero (0) to 3000 rows. |
| fileSizeThreshold=”5242880” | Only consider files whose size (in bytes) is greater than the specified threshold (i.e. 5242880). The default range is zero to "9223372036854775807" or signed int64. |

### GSA_SRM_LARGEST_OLD_FILES SECTION

This section specifies the criteria for "largeness" as well as "oldness" of files on a file while selecting them for this table

A sample entry is listed as follows:

```
         <gsa_srm_largest_old_file     rowsPerFileSystem=”25”
                     fileSizeThreshold=”5242880”

                   fileAgeThreshold=”P3M”/>
```

| Attribute Name | Description |
|---|---|
| rowsPerFileSystem=”25” | Report only specified number of rows (at max) per file system (i.e. 25). |
| fileSizeThreshold=”5242880” | Only consider files whose size (in bytes) is greater than the specified threshold (i.e. 5242880). |
| fileAgeThreshold=”P3M” | Only consider files, which are not modified after the timestamp (scan start – fileAgeThreshold). |

### GSA_SRM_USAGE_FACTORS SECTION

The element <time_spans> specifies the time span ranges for usage factor calculations.

```
<time_spans>PT1H P1D P7D P1M P3M P1Y P2Y</time_ spans>
```

| Tag Name | Description |
|---|---|
| <time_spans>PT1H P1D P7D P1M P3M P1Y P2Y</time_ spans> | A space-separated list of “XML duration”. |

A duration has the following format:

```
PnYnMnDTnHnMnS
```

Where:

- n is an integer.
- Value must begin with P…
- Year, Month, Day are optional (at least hour or minute or second part must be present). In that case, the value must begin with PT…
- Hour, Minute, Seconds are optional (at least year or month or day part must be present).

The SRM Agent takes these durations and subtracts them from the scan start time to generate a list of durations for reporting (these durations then become “buckets” in which the files are categorized for access timestamp, creation timestamp and modification timestamp).

### GSA_SRM_TYPE_DISTRIBUTION SECTION

This section contains filtering information for type distribution. If you do not want all the file types found on the filesystem, you can limit the file types using this element. You can ask the agent to either exclude the given file types and report all other file types, or only include the given file types and aggregate together all other file types under a single "OTHER" file type.

If the attribute ignoreTypeCase is true, the agent will ignore the case when analyzing the data. E.g. it will consider .Exe, .EXE, .exe as the same file types and report a single row for .exe (all lower case).

If desired, you can specify (using the fileCountPerType attribute) to report the file type only if the number of files for this type are greater than the specified value.

Also, you can specify (using the consumedSpacePerType attribute) to report the file type only if the space consumed by files of this file type is greater than the specified value. If both attributes (i.e., fileCountPerType and consumedSpacePerType) are specified, the agent will do a logical AND operation for these two criteria. If any one of these two is specified, only that criterion will be applied.

```
<gsa_srm_type_distribution    ignoreTypeCase=”true”>
…
</gsa_srm_type_distribution>
```

| Attribute Name | Description |
|---|---|
| ignoreTypeCase=”true” | If true (default), types (file extensions) are treated in case insensitive manner (e.g. .Exe, .EXE, .exe are same). |
| consumedSpacePerType= | Optional. Report the file type only if the number of files for this type are greater than the specified value. The minimum value is zero (0) and the maximum value is 9223372036854775807. |
| fileCountPerType= | Optional. Report the file type only if the consumed space is greater than the specified value. The minimum value is zero (0) and the maximum value is 9223372036854775807. |

## Specific File Type Filters

The creation of user-defined filters is a two step process:

- Define the filter in the `<! Define Filters for Specific File Type Report here` → section
- Enable the filter by adding it to the `<! Define Filters for Specific File Type Report here` → section of the SRM Agent Configuration File

Default specific file type filters are supplied for email archives and unauthorized files. Additional user-defined, specific file type filters can be manually added to the SRM Agent Configuration File.

```
         <!-- Show Email Archive File Usage -->
         <!-- Show Unauthorized File Usage -->
         <! -- Show Graphic File Usage -->
……

<filter_def name="Email_Archives"><filter_object attribute="path"
operator="wildcardeq" expandEnv="true">*.pst,*.nsf,*.ost,*.nst
</filter_object></filter_def><filter_def
name="Unauthorized_Files"><filter_object attribute="path"
operator="wildcardeq"
expandEnv="true">*.mpeg,*.mp3,*.avi,*.mov,*.wma,*.wmv,*.aiff,*.wav
</filter_object></filter_def></filter_config>


  <gsa_srm_usage_details rowsPerFilter="25" fileSizeThreshold="5242880">
```

```
      <filters>
        <!-- Apply Filters For Specific File Type Report Here -->
        <!-- Show Email Archive Usage -->
        <filter name="Email_Archives" action="include" />
        <!-- Show Unauthorized Files Usage -->
        <filter name="Unauthorized_Files" action="include" />
      </filters>
    </gsa_srm_usage_details>
```

| Attribute Name | Description |
|---|---|
| Filter_def_name= | Filter name enclosed in quotation marks. |
| Filter_object_attribute= | Specifies the filter's file path (may be wild carded), whether case-sensitivity is observed, and the filename extensions separated by a comma. |
| rowsPerFilter | The number of rows that will be reported per filter, per filesystem that is applied to this table. The default value is "25". |
| fileSizeThreshold | The file size threshold that will be maintained when reporting data. The default value is "5242880". |
| Email Archive | Specify the file types to include such as .pst, .ost, .nsf, .nst. The name SHOULD NOT be modified, as it is used in the reports. This filter is specific to the gsa_srm_usage_details table ONLY. |
| Unauthorized Files | Specify the file types to include such as .mpg, .jpg, .exe. The name SHOULD NOT be modified, as it is used in the reports. This filter is specific to the gsa_srm_usage_details table ONLY. |

### Sample User-Defined Specific File Type

The following example shows how you can set up the SRM Agent Configuration File to add a user-defined report for graphic files.

1. Open the config_srm.xml file on the machine with the SRM Agent with a text editor or .xml editor.
2. Add a new filter definition under <!-- `Define Filters for Specific File Type Report here -->`. An easy way to do this is to copy one of the existing filters and change the name and file extension list. For example:

```
      <!-- Show Graphic File Usage -->
                     <filter_def name="Graphic_Files">
                             <filter_object attribute="path"
   operator="wildcardeq"
   caseSensitive="false">*.jpg,*.psd,*.gif,*.bmp,*.tif,*.ai,*.pdf,*.png
   </filter_object>
                     </filter_def>
```

3. Enable the filter by adding it to `<!-- Apply Filters For Specific File Type Report Here -->` section of the .xml file (close to the end of the file). For the example above, the entry would be:

   ```
       <!-- Show Graphic Files Usage -->
            <filter name="Graphic_Files" action="include"/>
   ```
4. Restart the SRM Agent, to initiate a new data collection. The filesystem scanning process can take some time. You can check the progress by opening the agent's Message.log. When the SRM Agent finishes scanning, it will write an entry like:

   ```
   12/19/2004 15:37:12PM|INFO|0|jobManager:Scanning finished for
   filesystem : C:\|srmAgent|CJob.cc|172
   12/19/2004 15:37:12PM|INFO|0|Notify() method Called|srmAgent|
   CResourceManager.cc|441
   12/19/2004 15:37:12PM|INFO|0|jobManager:Finished job to scan
   filesystems after agent was started as per config option|srmAgent|
   CJobManager.cc|143
   12/19/2004 15:37:12PM|INFO|0|jobManager:Next scheduled scan time is Sun
   Dec 26 00:00:00 2004|srmAgent|CJobManager.cc|186
   ```
5. Run GSMdiag.exe located in the Storability Local Manager Utilities folder.
   a. In the **Agent location** window, enter the IP Address or network resolvable Host Name of the Local Manager where the agent has registered itself and set the port number to 17130.
   b. Select **gsa_register** table and verify it shows a SRM Agent row (port 17152) specifying it is active and registered from the particular host.
   c. Click **Published Objects** and scroll down to select the **gsa_usage_details** object.
   d. Verify that the **gsa_usage_details** object reports data in the **resource_name** column.

## Nth Level Directory Reporting

The SRM Agent can report on directories at various levels of the hierarchy under filesystems. The directory level at which data can be obtained can be configured by modifying the config_srm.xml file. The directory data will be reported in the gsa_srm_temporary_directories table.

### How to Configure Nth Level Directory Reporting

You can configure the SRM Agent configuration file (config_srm.xml) using the methods that are described below to obtain Nth level directory reporting. The recursion limit is 256 directories.

#### Obtaining First Level Directory Data

To get the first level directory data, perform the following steps.

1. Add the following filter in the <filter_config> section.

   ```
   <filter_def name="temp_data_dirs_level_one">
     <filter_object attribute="path" operator="wildcardeq"
   caseSensitive="false">*\*</filter_object>
   </filter_def>
   ```

2. Add the above-defined filter to the  <filter> *section* of the gsa_srm_temporary_directories configuration.

   ```
   <filter name=" temp_data_dirs_level_one" action="include"/>
   ```

**Note:**
First level directories are obtained by specifying the filter name as "*" on UNIX. When Windows reports a directory called test located on c:, for example, it reports that directory  as "C:\test". In this case, we need to specify "**" as the filter to see the first level directories on ALL existing drives that are going to be scanned. If you want to see the first level directories on C:, your filter would be "C:\*".
On UNIX, however, only "*" works for directories being reported as "/etc", for instance.

### Obtaining Second Level Directory Data

To get the second level directory data, perform the following steps.

1. Add following filter in the <filter_config> section.

```
<filter_def name="temp_data_dirs_level_two">
<filter_object attribute="path" operator="wildcardeq"
caseSensitive="false">*\*\*</filter_object>
  </filter_def>
```

2. Add above defined filter to <filter> section of gsa_srm_temporary_directories configuration.

```
<filter name=" temp_data_dirs_level_two" action="include"/>
```

### Obtaining First and Second Level Directory Data

To get the first and second level directory data, perform the following steps.

1. Add the following filters in the <filter_config> section.

```
 <filter_def name="temp_data_dirs_level_one">
    <filter_object attribute="path" operator="wildcardeq"
caseSensitive="false">*\*</filter_object>
 </filter_def>
<filter_def name="temp_data_dirs_level_two">
   <filter_object attribute="path" operator="wildcardeq"
caseSensitive="false">*\*\*</filter_object>
 </filter_def>
```

2. Add the above-defined filters to the <filter> section of the gsa_srm_temporary_directories configuration.

```
<filter name=" temp_data_dirs_level_one" action="include"/>
<filter name=" temp_data_dirs_level_two" action="include"/>
```

### Obtaining First and Second Level Subdirectories Data

To get the first and second level subdirectories under a directory C:\Storability, perform the following steps.

1. Add the following filters in the <filter_config> section.

```
  <filter_def name="temp_data_dirs_level_one">
    <filter_object attribute="path" operator="wildcardeq"
caseSensitive="false">C:\Storability\*</filter_object>
```

```
     </filter_def>
     <filter_def name="temp_data_dirs_level_two">
    <filter_object attribute="path" operator="wildcardeq"
   caseSensitive="false">C:\Storability\*\*</filter_object>
     </filter_def>
```

2. Add the above-defined filters to the <filter> section of the gsa_srm_temporary_directories configuration.

```
    <filter name=" temp_data_dirs_level_one" action="include"/>
     <filter name=" temp_data_dirs_level_two" action="include"/>
```

### Obtaining First, Second, and Third Level Directory Data

To get the first, second, and third level directory data, perform the following steps.

1. Add the following filters in <filter_config> section

```
     <filter_def name="temp_data_dirs_level_one">
        <filter_object attribute="path" operator="wildcardeq"
caseSensitive="false">*\*</filter_object>
    </filter_def>
    <filter_def name="temp_data_dirs_level_two">
      <filter_object attribute="path" operator="wildcardeq"
caseSensitive="false">*\*\*</filter_object>
    </filter_def>
    <filter_def name="temp_data_dirs_level_three">
      <filter_object attribute="path" operator="wildcardeq"
caseSensitive="false">*\*\*\*</filter_object>
    </filter_def>
```

2. Add the above-defined filters to the <filter> section of the gsa_srm_temporary_directories configuration.

```
<filter name=" temp_data_dirs_level_one" action="include"/>
<filter name=" temp_data_dirs_level_two" action="include"/>
<filter name=" temp_data_dirs_level_three" action="include"/>
```

## Nth Level Directory Configuration Summary

Directories at any level can be obtained by increasing the number of wildcards "*" preceded by the backward slash "\" in the filter definition. Another example is listed as follows:

```
*\*\*\*\*\*,
*\*\*\* ,  C:\Storability\*\*\*\*\*
```

## SRM Agent Objects

The following table describes the objects that the Sun StorageTek Business Analytics SRM Agent publishes. You can use the Agent Diagnostic Tool (gsmdiag.exe) to collect any and all of these tables. See also the **Verifying SRM Agent** section.

**Note**: The **gsa_srm_usage_details** object supports the new specific file (e.g., email archive) reports. The report_name field will be populated by the matching file type extension to the report, as defined by the SRM Agent Configuration tab. The values for report_name are added to the report list in the **File Level Details** report.

| Object | Description |
|---|---|
| alerts-3_1 | ip_address, port, when, application, severity, id, description, timestamp |
| gsa_agent_version-2_0 | ip_address, port, agent_name, version, compile_time, managed_entities, tz_name, tz, timestamp |
| gsa_cache_control-2_0 | ip_address, port, table_name,  cache_age, last_update_request_length, update_request_pending, group_name, group_master, timestamp |
| gsa_parm_info | ip_address, port, object,  parm_name, value_syntax, description_required |
| gsa_srm_command | ip_address, nodename, host_id, command, params, arrival_time, status, status_description, timestamp. |
| gsa_srm_filesystem | ip_address, nodename, host_id, filesystem_id, filesystem_type, filesystem_attributes, block_size, total_capacity, used_capacity, file_count, directory count, average_file_size, median_ file_size, user_ data_size, metadata_size, block_size overhead, last_ scan_time, timestamp. |
| gsa_srm_filesystem_consumers | ip_address, nodename, host_id, filesystem_id, owner, consumed_blocks, consumed_space, last_scan_time, timestamp. |
| gsa_srm_largest_files-2_1 | ip_address, nodename, host_id, filesystem_id, file_ name, type, owner, time, size, last_scan_time, access_time, creation_time, timestamp. |
| gsa_srm_largest_old_files-2_1 | ip_address, nodename, host_id, filesystem_id, file _name, type, owner, time, size, last _scan_ time, access_time, creation_time, timestamp. |
| gsa_srm_mount_points | ip_address, nodename, host_id, mount_point, last_ scan_time, timestamp. |
| gsa_srm_size_distribution | ip_address, nodename, host_id, filesystem_id, range_start, range_stop, file_count, average_file_ size, median_file_size, consumed_ blocks, consumed_space, last_scan _time, timestamp. |
| gsa_srm_temporary_directories | ip_address, nodename, host_id, filesystem_id, directory_name, owner, consumed_space, last_scan_ time, timestamp. |
| gsa_srm_type_distribution | ip_address, nodename, host_id, filesystem_id, type, file_count, consumed_blocks, consumed_space, last _scan_time, timestamp. |
| gsa_srm_usage_details-2_1 | ip_address, nodename, host_id, filesystem_id, resource_name, extension, owner, time, size, filter_name, last_scan_time, access_time, creation_time, timestamp |
| gsa_srm_usage_factors | ip_address, nodename, host_id, filesystem_id, factor_type, time_span_type, time_span, user _data_factor_percentage, file_count_factor _percentage, last_scan_time, timestamp. |

| Object | Description |
|---|---|
| gsa_srm_user | ip_address, nodename, host_id, srm_owner_type, srm_user _d, srm_user_name, srm_group_id, srm_ group_name, allocated_quota, used_quota, last_ scan_time, timestamp. |

**Table 2 - SRM Agent Objects**

## Local Manager Installation CD (Install Shield)

Besides the SRM Agent, the installation program (Install Shield) installs the current version of the Host Agent if it detects a previous version exists on the system.

1. Insert the Sun StorageTek Business Analytics Windows Local Manager CD into the CD-ROM drive.

2. Click **Next** on the **Welcome** menu to continue the installation.

3. Click **Yes** to accept the terms of the software license agreement.

4. Review/modify the **User Name** and **Company Name** and click **Next>.**

5. Select the **SRM Agent** under the **Host** heading on the screen that lists the Sun StorageTek Business Analytics Agents for installation (and the Host Agent if not already installed) and click **Next>**.

6. Click **Next>** to accept the default destination folder or specify a different installation path.

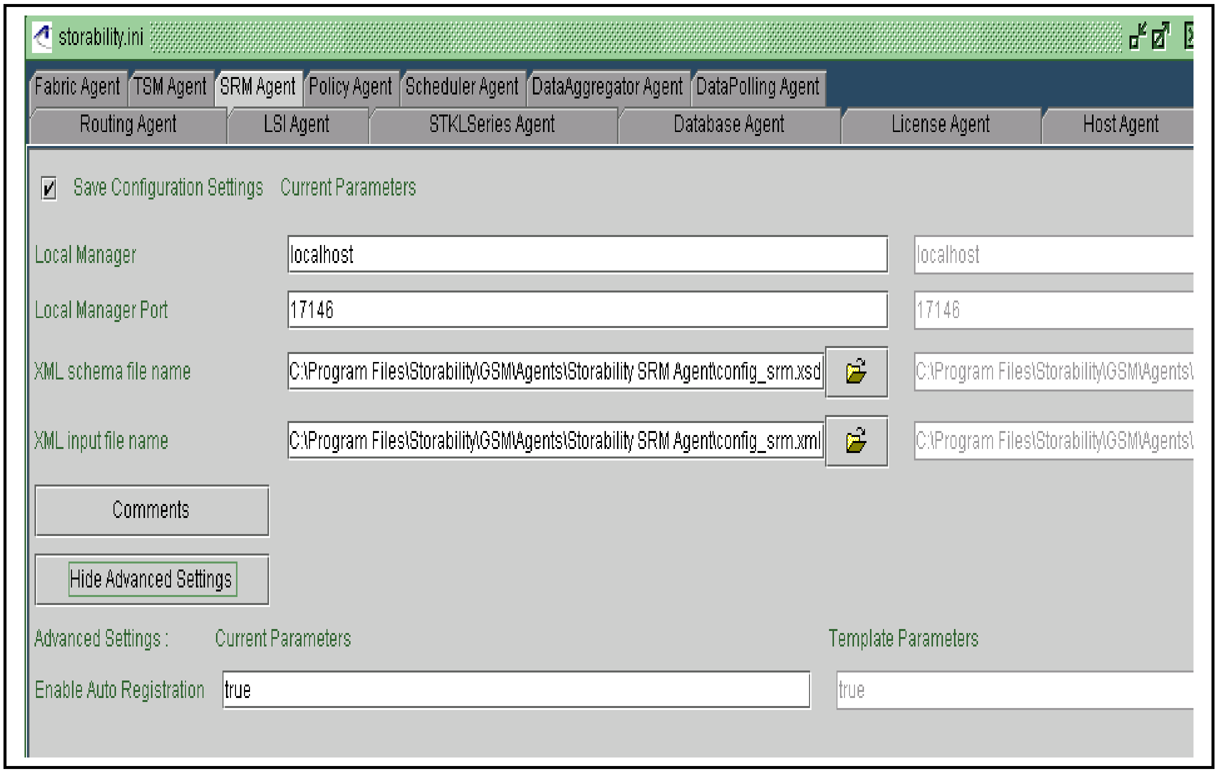
7. Review the installation settings and click **Next** to continue.

8. If the Host Agent is already installed, specify whether or not to reinstall this agent.

9. Specify whether or not to install the new version of the Configuration Tool.

10. When the Configuration Tool is launched, click **File->Edit->Smart Agent Configuration**.

11. Click the **SRM Agent** tab in the main window.



☑ Save Configuration Settings Current Parameters

| | | |
|---|---|---|
| Local Manager | localhost | localhost |
| Local Manager Port | 17146 | 17146 |
| XML schema file name | C:\Program Files\Storability\GSM\Agents\Storability SRM Agent\config_srm.xsd | C:\Program Files\Storability\GSM\Agents\ |
| XML input file name | C:\Program Files\Storability\GSM\Agents\Storability SRM Agent\config_srm.xml | C:\Program Files\Storability\GSM\Agents\ |

| Advanced Settings : | Current Parameters | Template Parameters |
|---|---|---|
| Enable Auto Registration | true | true |

**Figure 3 - SRM Agent Tab in Configuration Tool**

12. In the **Local Manager** field, type the network resolvable name or IP address of the Local Manager to contact for agent auto registration. The default value is "localhost".

13. Specify the TCP port number that the Local Manager uses for agent auto registration. The default port number is 17146.

14. For the **XML schema file name**, setting click the **Folder** icon and browse to the folder where the config_srm.xsd file is installed. The default location is c:\Program Files\Storability\Agents\Storability SRM Agent.

15. Select the file and click **Open**.

16. For the **XML input file name** setting, the **Folder** icon and browse to the folder where the config_srm.xml file is installed. The default location is c:\Program Files\Storability\Agents\Storability SRM Agent.

17. Select the file and click **Open**.

18. Click **Advanced Settings** to review/modify the "Enable Auto Registration" configuration setting. This configuration parameter turns agent auto registration on (default) or off.

19. With the "Save Configuration Settings" check box enabled (check mark), click **File->Save** and then confirm saving the storability.ini file.

20. Select **File->Exit** to close the Configuration Tool.

21. To complete the installation, view and then close the **Readme** file and click **Finish**.

22. Work with your Sun StorageTek Business Analytics administrator to:

    a. Verify the Sun StorageTek Business Analytics administrator has used the Management Console's **SRM Agent Configuration** menus to configure the SRM Agent Configuration and downloaded/copied the SRM Agent Configuration file to the SRM Agent folder

    Or:

    b. Set up the SRM Agent Configuration File (config_srm.xml) using another method, such as an XML Editor.

23. Use the Windows **Services** panel to start the configured SRM Agent.

24. Proceed to the **Verifying SRM Agent** section.

## SRM Agent Standalone InstallShield Installation

1. Insert the Sun StorageTek Business Analytics Local Manager CD into the CD-ROM drive. If the InstallShield-based installation program is automatically launched, close the program.

2. Open a DOS Command Window.

3. Change directory to Win32\SrmAgentSetup.

4. Type **setup.exe** and press **Enter**. The **SRM Agent Welcome** screen appears. Click **Next>** to continue.

5. Click **Yes** to accept the terms of the software license agreement.

6. Review/modify the informational User Name and Company Name and click **Next>**.

7. Click **Next>** to accept the default destination folder (i.e., <drive>:\Program Files\Storability) or click **Browse** to select another destination folder. Note that the \GSM folder will be created under the destination folder that you specify.

8. Review the settings and click **Next>** to continue. The Installation in progress splash screen appears.

9. When the **InstallShield Wizard Complete** screen appears, click **Finish**. At this point, the Storability SRM Agent is installed and running on the Windows server.

## Installing the SRM Agent on Solaris

Follow the procedure outlined below to install the SRM Agent on a Solaris host server. The installation script (setup) is supplied on the Solaris Local Manager Installation CD. **Note**: The SRM Agent must be run in Administrative user privileges for full functionality.

1. Open a terminal window on the desktop of the Sun host.

2. Mount the Local Manager installation CD in your CD-ROM drive. For example:

```
mount –o ro –F hsfs /dev/dsk/c0t6d0s0 /cdrom
```

3. Change directory to the mount point, such as /cdrom in this example.

4. Run the installation script to access the main agent installation main menu.

```
./setup
```

5. Select to install the **SRM Agent**.

6. Type zero (0) and press Enter to specify that you have finished selecting agents for installation.

7. The informational text "The srmAgent can be controlled by remote requests.  Such requests, if enabled, must be authenticated with a username and password." appears.

8. Allow remote srmAgent commands with a specific user/password pair? [n] [y,n,?]. Specify **y**(es) to allow the SRM Agent to be managed through remote commands or press **Enter** to accept the default value of not enabling this feature.

9. The informational text "Alternately, permission may be granted to members of a specific group to issue commands to the srmAgent, by giving their own username and password (as determined by PAM(3))." appears.

10. Allow authentication to system accounts? [n] [y,n,?] Enter **y**(es) to enable this authentication method or press **Enter** to not enable it.

11. Type **y** and press **Enter** to review/modify the **Advanced Settings**.

    - Allow the agent to be restarted by Agent Monitor (default) if the agent is detected as not running, or type **n** and press **Enter** to not use this feature.

    - Specify whether (y/n) agent auto registration is enabled. This feature is enabled by default.

    - Specify the IP address or network resolvable host name of the Local Manager to be contacted for agent auto registration. The default value is local host.

    - Specify the TCP port number the Local Manager uses for agent auto registration. The default port number is 17146.

    - Read the informational text that specifies why you will want to customize the settings in the config_srm.xml file.

    - Specify whether (y/n) you want all agents on the Solaris server to be restarted after the installation has completed.

    - Specify whether (y/n)to configure the SRM Agent to run scans weekly starting at midnight on Sunday as one of its "scan schedules".

12. When prompted, type **y** and press **Enter** to confirm continuing the installation of the SRM Agent.

13. The installation will complete and return you to the command line.

14. Use the process status (ps) command to verify the SRM Agent is running before you verify agent functionality.

> **Notes**:
> The run scripts (start/stop) for all Business Analytic agents are installed into the /etc/init.d directory. The agent will log a message in the message log that indicates the filesystem scanning has been completed.

### Installing SRM Agent on IBM AIX

All currently supported AIX agents are provided with both the .tgz (gzipped tar) file and the install script. Ensure that the "srmAgent-install.sh" and srmAgent-AIX.tgz files reside in the same location. If the Host Agent is not installed, it will be installed before the SRM Agent is installed. If the Host Agent is installed, the installation script will stop and then restart it.

1. Mount the UNIX Agent Installation CD. For example:

```
mount -v cdrfs -r /dev/cd0 /mnt # /mnt directory must exist
```

2. Change directory to the software installation directory. For example:

   *cd /mnt/Unix/AIX/5.x*

3. Run the installation script:

```
srmAgent-install.sh
```

4. The installation script installs the SRM agent and returns you to the command line.

**Agent Auto Registration on IBM AIX**
To configure agent auto registration, you can manually add the SRM Agent to a Local Manager Routing Agent configuration as a SUB_AGENT entry or add the required entries to the storability.ini file. Sample storability.ini settings for the agent appear below.

```
 GSM_LM_HOST = 10.192.1.56
 GSM_LM_PORT = 17146
GSM_ENABLE_LM_REGISTRATION = true
```

## Installing the SRM Agent on HP-UX

The following notes apply to installing Sun StorageTek Business Analytics agents on this platform:

- The Sun StorageTek Business Analytics Agent installation must be carried out locally by root.
- You may mount the software media directly using the local CD-ROM drive or copy the CD contents to some location on the server.
    - # ioscan –funC disk  # Identifies cdrom device
    - Sample mount command:

      # pfs_mount –o xlat=unix /dev/rdsk/cXtXd0 /SD_CDROM

      (where /dev/rdsk/cXtXd0 is the cdrom device)

- Depending on which filesystem extensions are recognized by the host, the location, relative to the CD root, will be:

```
 UNIX/HP-UX/<version>    (basic ISO 9660 filesystem)
Unix/HP-UX/<version>    (ISO 9660 with extensions)
```

- The software installation directory contains both the .tgz (gzipped tar) file and the install script.
- To install individual agents, simply run the corresponding installation Script, for example:

```
srmAgent-install.sh       (ISO 9660 with extensions)
```

- The agent should be started and stopped using the init scripts in the /sbin/init.d directory.
- Use the following command to confirm which agents are running:

```
$ ps -ef | grep Agent
```

- Refer to the READ.TXT file on the installation CD for additional information on installing Sun StorageTek Business Analytics agents on a HP-UX server.

1. Mount the installation CD in the CD-ROM drive of the HP-UX server.
2. Change directory to the software installation directory. For example:

```
cd /cdrom/UNIX/HPUX/11.00
```

3. Run the GSM SRM Agent installation script. For example:

```
./srmAgent-install.sh
```

The installation script installs and starts the SRM Agent.

**Agent Auto Registration on UNIX Servers (non-Solaris)**
To configure agent auto registration after installation, you can manually add the SRM Agent to a Local Manager Routing Agent configuration as a SUB_AGENT entry or add the required entries to the storability.ini file. Sample storability.ini entries for the SRM Agent appear below.

```
GSM_LM_HOST = 10.192.1.15
GSM_LM_PORT = 17146
GSM_ENABLE_LM_REGISTRATION = true
```

## Red Hat Linux SRM Agent Installation

On Red Hat Linux, the SRM Agent is provided as a simple "Tarball" or zipped tar archive. To install the agent, simply unpack the "Tarball" (<agent>-rh<version>.tgz) and start the agent using the startup script (located in /etc/rc.d/init.d on Red Hat servers).

1. Mount the Sun StorageTek Business Analytics Agent Installation CD to cdrom. For example:

   /mount/mnt/cdrom

2. Change directory to the Linux directory:

/mnt/cdrom/Unix/Linux

```
[root@Linux]# ls -al
total 10
dr-xr-xr-x   5 root    root       2048 Nov  1 03:24 .
dr-xr-xr-x   6 root    root       2048 Oct 13 16:47 ..
dr-xr-xr-x   2 root    root       2048 Oct 25 00:28 RedHat-7.2
dr-xr-xr-x   2 root    root       2048 Nov  1 03:24 RedHat-EnterpriseEdition
dr-xr-xr-x   2 root    root       2048 Oct 25 00:25 Suse-8.0
```

3. The installation files are listed as follows:

   RedHat-7.2: srmAgent-install.sh   srmAgent-rh72.tgz
   RedHat Enterprise Edition 3.0 or 4.0: srmAgent-install.sh   srmAgent-rhee.tgz

4. To install the agent, simply run the installation script srmAgent.sh as shown below.

```
./srmAgent-install.sh
```

This script will look for the "Tarball" in its current directory default or in the path specified as the first argument.

**Note**: The same installation files are used to support RedHat Edition 3.0 and RedHat Edition 4.0.

5. Verify the srmAgent started.

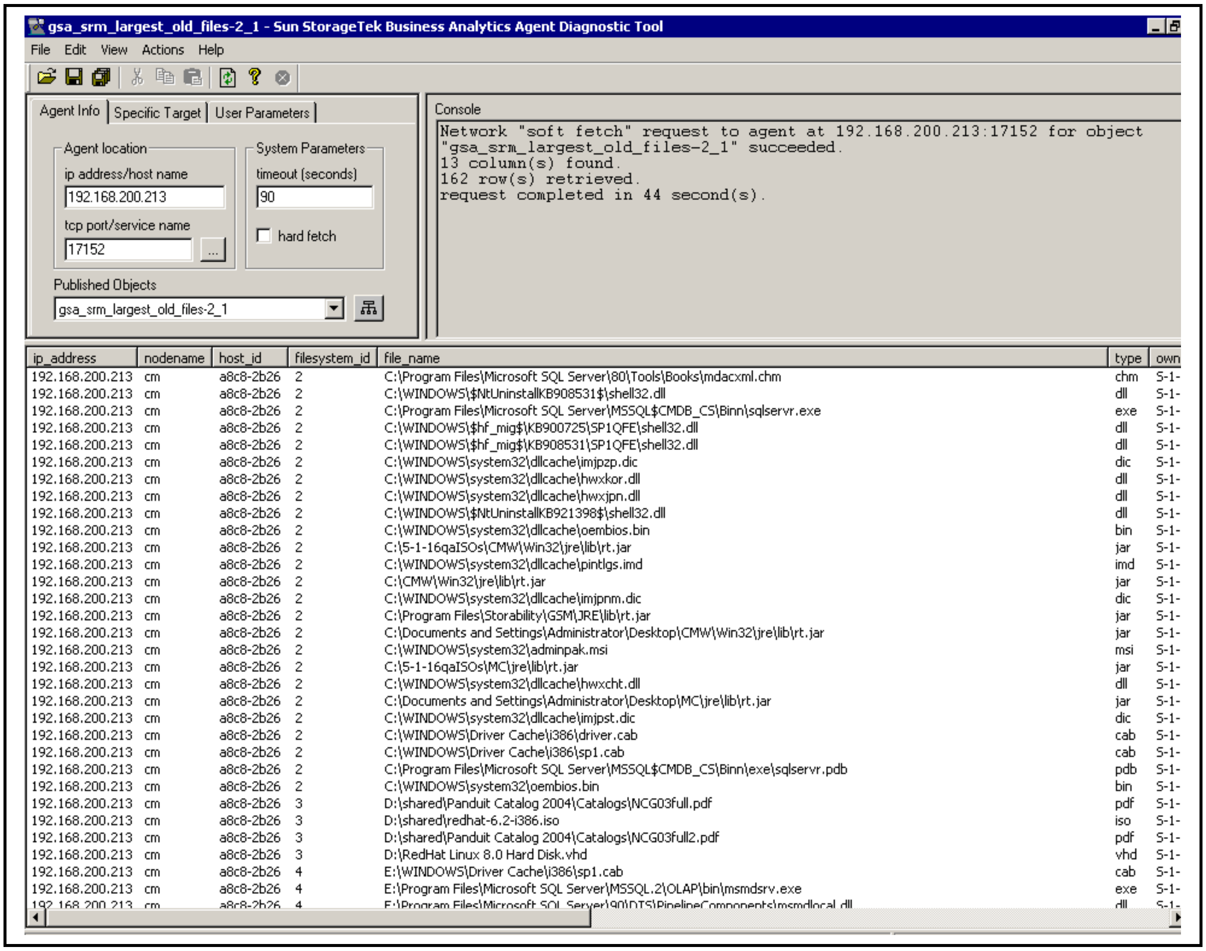
6. To start/stop the agent, simply run the startup script as shown below.

```
etc/rc.d/init.d/srmAgent   start
etc/rc.d/init.d/srmAgent   stop
```

## Verifying SRM Agent

Use the Sun StorageTek Business Analytics Agent Diagnostic Tool to verify the SRM Agent functionality. This diagnostic utility is installed as part of the Sun StorageTek Business Analytics Central Manager or Local Manager Software installation.

1. Wait until after the SRM Agent logs a message that it has completed the filesystem scan before querying the agent using the Business Analytics Agent Diagnostic Tool.
2. Launch the Business Analytics Agent Diagnostic Tool from its Program Folder.
   a. In the **Agent location** window, enter the IP Address or network resolvable Host Name of the server where the agent is installed in the ip address/host name input box.
   b. Set the port to 17152 (or select the SRM agent from the drop down list of service names).
   c. Click the **Get Object List** button and you should receive a list of objects published by the SRM Agent.
   d. Select the **gsa_srm_largest_files-2_1** object and it should report the ip_address, nodename, and hostid of the server.


gsa_srm_largest_old_files-2_1 - Sun StorageTek Business Analytics Agent Diagnostic Tool
File Edit View Actions Help
Agent Info
Specific Target
User Parameters
Console

Agent location

ip address/host name: 192.168.200.213

tcp port/service name: 17152

System Parameters

timeout (seconds): 90

☐ hard fetch

Published Objects: gsa_srm_largest_old_files-2_1

```
Network "soft fetch" request to agent at 192.168.200.213:17152 for object
"gsa_srm_largest_old_files-2_1" succeeded.
13 column(s) found.
162 row(s) retrieved.
request completed in 44 second(s).
```

| ip_address | nodename | host_id | filesystem_id | file_name | type | own |
|---|---|---|---|---|---|---|
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\Program Files\Microsoft SQL Server\80\Tools\Books\mdacxml.chm | chm | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\$NtUninstallKB908531$\shell32.dll | dll | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\Program Files\Microsoft SQL Server\MSSQL$CMDB_CS\Binn\sqlservr.exe | exe | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\$hf_mig$\KB900725\SP1QFE\shell32.dll | dll | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\$hf_mig$\KB908531\SP1QFE\shell32.dll | dll | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\system32\dllcache\imjpzp.dic | dic | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\system32\dllcache\hwxkor.dll | dll | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\system32\dllcache\hwxjpn.dll | dll | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\$NtUninstallKB921398$\shell32.dll | dll | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\system32\dllcache\oembios.bin | bin | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\5-1-16qaISOs\CMW\Win32\jre\lib\rt.jar | jar | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\system32\dllcache\pintlgs.imd | imd | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\CMW\Win32\jre\lib\rt.jar | jar | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\system32\dllcache\imjpnm.dic | dic | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\Program Files\Storability\GSM\JRE\lib\rt.jar | jar | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\Documents and Settings\Administrator\Desktop\CMW\Win32\jre\lib\rt.jar | jar | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\system32\adminpak.msi | msi | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\5-1-16qaISOs\MC\jre\lib\rt.jar | jar | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\system32\dllcache\hwxcht.dll | dll | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\Documents and Settings\Administrator\Desktop\MC\jre\lib\rt.jar | jar | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\system32\dllcache\imjpst.dic | dic | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\Driver Cache\i386\driver.cab | cab | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\Driver Cache\i386\sp1.cab | cab | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\Program Files\Microsoft SQL Server\MSSQL$CMDB_CS\Binn\exe\sqlservr.pdb | pdb | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 2 | C:\WINDOWS\system32\oembios.bin | bin | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 3 | D:\shared\Panduit Catalog 2004\Catalogs\NCG03full.pdf | pdf | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 3 | D:\shared\redhat-6.2-i386.iso | iso | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 3 | D:\shared\Panduit Catalog 2004\Catalogs\NCG03full2.pdf | pdf | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 3 | D:\RedHat Linux 8.0 Hard Disk.vhd | vhd | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 4 | E:\WINDOWS\Driver Cache\i386\sp1.cab | cab | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 4 | E:\Program Files\Microsoft SQL Server\MSSQL.2\OLAP\bin\msmdsrv.exe | exe | S-1- |
| 192.168.200.213 | cm | a8c8-2b26 | 4 | E:\Program Files\Microsoft SQL Server\90\DTS\PipelineComponents\msmdlocal.dll | dll | S-1- |

**Figure 4 - Sample SRM Largest Files Object**

e. If you have user-defined files configured, collect the **gsa_srm_usage_details** object and examine the "filter_name" field.

f. Verify all other objects published by the agent.

3. Verify the SRM Agent is registered with the configured Local Manager:

a. Enter the **IP Address** or **Hostname** of the Local Manager and set the port to 17146 (or select the Routing Agent from the drop down list of service names).

b. Click the **Get Object List** button and you should receive a list of tables published by the Routing Agent. If unsuccessful, verify the Ethernet connectivity to the server running the Sun StorageTek Business Analytics Routing Agent and that the agent is running.

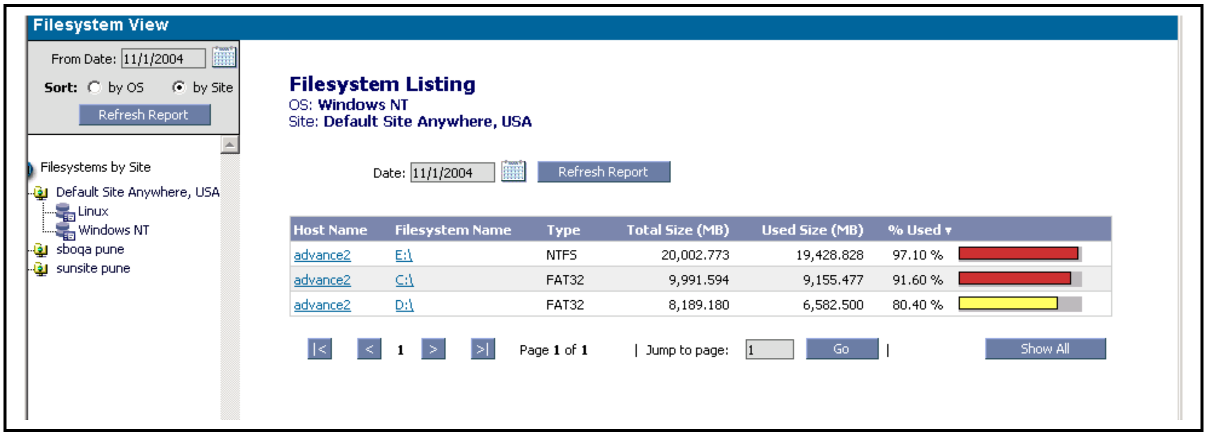
c. Collect the **gsa_agent_register** object. Verify:

- An entry is displayed with a **port** field that is 17152 and a **peer_list** field that is the host name/IP Address where the SRM Agent is running.
- The **type** field displays the expected type of agent registration where:
  - AUTO_NET indicates agent auto registration occurred
  - STATIC means registration occurred through a SUB_AGENT entry in the Routing Agent's storability.ini file.

# Verifying Management Console Functionality

The following procedure describes how the Sun StorageTek Business Analytics administrator verifies the SRM Agent's reports in the Management Console. Refer to the *Administration* chapter to obtain information on the administrative menus you can access from the **Tools** pull down menu, including the **Polling** and **Change Dashboard** menus.

1. Log in to the Management Console as an administrative user (e.g., gsmuser) whose views provide access to the desired assets (e.g., sites).
2. Select **Tools->Data Polling Schedule.** The following step assumes that a polling schedule exists for SRM for the specific site or all sites. If not, refer to the **Administration** chapter and create one before you proceed to the next step.
3. Use the **Collect Now** button to collect the **SRM** (collection type) **Configuration** (Collection Metric) data using a polling schedule that includes the specific site or all sites.
4. Wait a minute or so to allow the data to be collected and inserted into the database.
5. Repeat Step 3 for the Collection Metric of Statistics.
6. Wait a minute or so to allow the data to be collected and inserted into the database.
7. Close the **Data Polling Schedule** window.
8. Click **Servers->Filesystem Consumers** and expand the appropriate view/site in the navigation pane to locate the target server.
9. Click the server and verify the **Filesystem Consumer Listing** report is displayed.



Filesystem Listing
OS: Windows NT
Site: Default Site Anywhere, USA

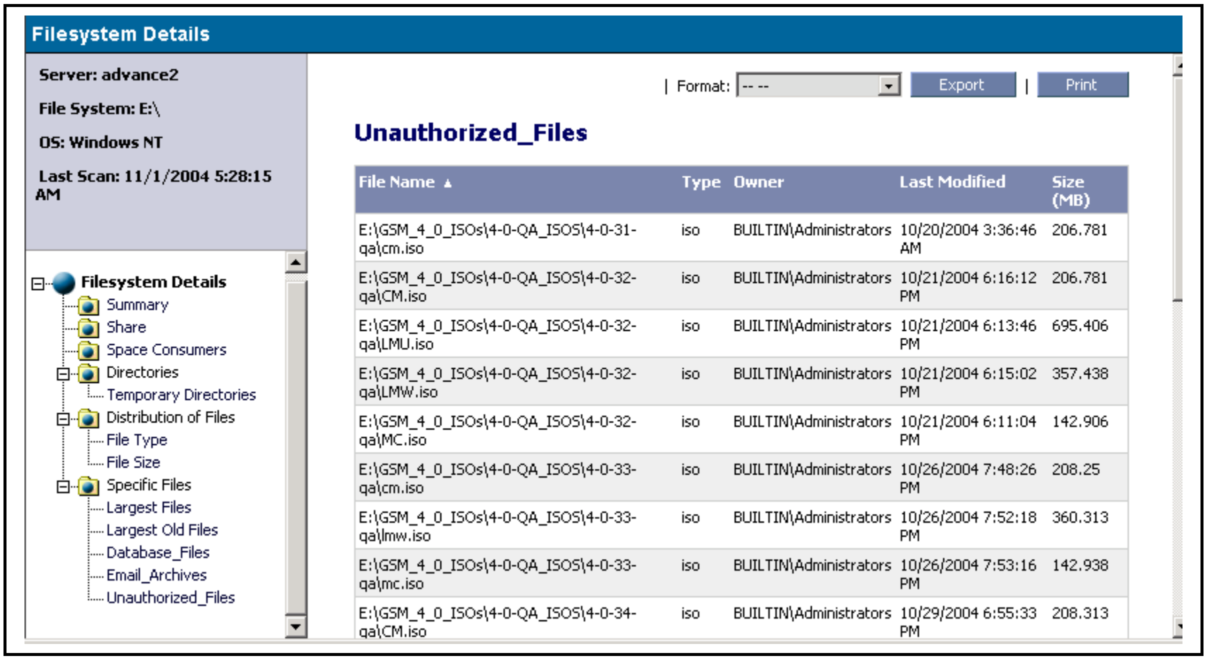
Date: 11/1/2004 Refresh Report

| Host Name | Filesystem Name | Type | Total Size (MB) | Used Size (MB) | % Used ▾ |
|---|---|---|---|---|---|
| advance2 | E:\ | NTFS | 20,002.773 | 19,428.828 | 97.10 % |
| advance2 | C:\ | FAT32 | 9,991.594 | 9,155.477 | 91.60 % |
| advance2 | D:\ | FAT32 | 8,189.180 | 6,582.500 | 80.40 % |

**Figure 5 - Filesystem Listing**

10. Click the **Filesystem Name** link and the Filesystem Details report is displayed.
11. Expand the headings and the different filters are displayed. Verify:
    - Distribution of files (file type, file size)
    - Specific files (largest files, largest old files, etc.)

    A sample Unauthorized Files report appears below.



Server: advance2

File System: E:\

OS: Windows NT

Last Scan: 11/1/2004 5:28:15 AM

Unauthorized_Files

| File Name ▲ | Type | Owner | Last Modified | Size (MB) |
|---|---|---|---|---|
| E:\GSM_4_0_ISOs\4-0-QA_ISOS\4-0-31-qa\cm.iso | iso | BUILTIN\Administrators | 10/20/2004 3:36:46 AM | 206.781 |
| E:\GSM_4_0_ISOs\4-0-QA_ISOS\4-0-32-qa\CM.iso | iso | BUILTIN\Administrators | 10/21/2004 6:16:12 PM | 206.781 |
| E:\GSM_4_0_ISOs\4-0-QA_ISOS\4-0-32-qa\LMU.iso | iso | BUILTIN\Administrators | 10/21/2004 6:13:46 PM | 695.406 |
| E:\GSM_4_0_ISOs\4-0-QA_ISOS\4-0-32-qa\LMW.iso | iso | BUILTIN\Administrators | 10/21/2004 6:15:02 PM | 357.438 |
| E:\GSM_4_0_ISOs\4-0-QA_ISOS\4-0-32-qa\MC.iso | iso | BUILTIN\Administrators | 10/21/2004 6:11:04 PM | 142.906 |
| E:\GSM_4_0_ISOs\4-0-QA_ISOS\4-0-33-qa\cm.iso | iso | BUILTIN\Administrators | 10/26/2004 7:48:26 PM | 208.25 |
| E:\GSM_4_0_ISOs\4-0-QA_ISOS\4-0-33-qa\lmw.iso | iso | BUILTIN\Administrators | 10/26/2004 7:52:18 PM | 360.313 |
| E:\GSM_4_0_ISOs\4-0-QA_ISOS\4-0-33-qa\mc.iso | iso | BUILTIN\Administrators | 10/26/2004 7:53:16 PM | 142.938 |
| E:\GSM_4_0_ISOs\4-0-QA_ISOS\4-0-34-qa\CM.iso | iso | BUILTIN\Administrators | 10/29/2004 6:55:33 PM | 208.313 |

**Figure 6 - Unauthorized Files Report**

# SRM Agent Troubleshooting

1. **Verify system/agent prerequisites** – Refer to *Sun StorageTek Business Analytics Support Matrix* to verify the most recent support requirements for the agent.

2. **Review the Message Log** – Review/collect the SRM Agent Message.log file that can contain information on startup errors, configuration errors, or errors regarding accessing data (e.g., impersonating user logon failure) or parsing output.

   **Note**: If there is a configuration error, an entry will specify the line number and other error details and indicate the "default SRM Agent Configuration settings" are being used.

   Verify that a logged entry indicates the Message log file indicates that the agent has finished the filesystem scan and specifies when the next scheduled filesystem scan is scheduled before you use the GSM Agent Diagnostic Tool to collect and verify the SRM Agent published objects.

   Windows

   - Located by default in: <drive>:\Program Files\Storability\GSM\Agents\Storability SRM Agent folder.
   - Can enable debug level logging by appending **LOG_SEVERITY=Debug** to the SRM Agent section of the storability.ini file (if your support representative requests it).

   Solaris

   - Agents common Message.log file located by default in: /opt/storability/data.

- Can enable debug level logging by appending LOG_SEVERITY=Debug to the SRM Agent section of the storability.ini file (if Storability Support requests it).

3. **Verify Local Manager Registration -** The configured Local Manager **gsa_agent_register** table should be reviewed if the auto-registration feature is enabled (default). Otherwise, verify the necessary SUB_AGENT entry has been added to the Routing Agent's storability.ini file.
4. **Review the Routing Agent Message Log** – Review/collect the configured Routing Agent's Message Log to check for errors related to Ethernet connectivity problems contacting the Storability SRM Agent.
5. Use the Business Analytics Agent Diagnostic Tool to save the output for all the tables if escalating a problem to Sun Technical Support.
   a. Run the Sun StorageTek Business Analytics Agent Diagnostic Tool (gsmdiag.exe).
   b. Enter the **IP Address** or **Hostname** of the server where the agent is installed and set the port to 17152 (or select the SRM agent from the drop down list of service names).
   c. Click the **Get Object List** button and you should receive a list of tables published by the SRM Agent. If unsuccessful, verify the Ethernet connectivity to the server running the SRM Agent and that the SRM Agent is running.
   d. Select the **alerts-3_1** table and examine the **Description** column for each reported alert.
   e. Select **File->Save All** and the "This action will network fetch all objects published by the currently specified agent and save the data to a single file." Message appears.
   f. Click **OK** and the **Save As** dialog appears.
   g. Enter a meaningful file name and click **OK** to initiate the collection.
   h. Enter the desired file name and click **OK**.

6. **Confirm Data Polling Schedules** – Using the Management Console's **Data Polling Schedule** menu, review/modify the existing Polling Schedules for the Collection Type of SRM at all sites.
7. **Review Aggregator Message Log** – Open the Data Aggregator's Message Log in a text editor and validate that the SRM Tables are being requested and that rows are being inserted into the database.

   The log contains two entries, TID (Transaction ID) and SID (Session ID), which can help you locate (e.g., Find) and view relevant logged entries. For scheduled polling requests, the TID will be equal to the Job ID in the Data Polling Schedule menu. Each SID is a unique identifier for a particular agent data collection session. For on-demand polling requests, the TID is a uniquely generated TID (not the Job ID) and SID, and the TID and SID will be equal to the same integer value.
8. **Check the assurent database** – The assurent database is the data repository for your Sun StorageTek Business Analytics application. For the SRM Agent, use any MS SQL Query interface, such as isql, to verify rows have been inserted into the SRM-related tables, such as the **gsa_srm_largest_files** table.
9. **Verify Management Console Functionality** – As a final step in the agent troubleshooting procedure, minimally verify that the File System Consumers and File System Details reports work properly.

## Upgrade SRM Agent – Non Solaris UNIX Host

To upgrade an existing SRM Agent, you perform the following tasks:

1. Stop the SRM Agent (srmAgent):

```
/etc/rc.d/init.d/srmAgent stop
```

```
[root@linux /]# /etc/rc.d/init.d/srmAgent stop
Stopping Storability SRM agent: srmAgent 939 killed
```

2. Manually remove the storability directory under /opt

```
rm -rf storability
```

3. Verify the /opt/storability directory is deleted

## Reinstalling the SRM Agent – Non-Solaris UNIX Host

The reinstallation procedure for all Sun StorageTek Business Analytics agents supported on non-Solaris UNIX hosts, such as the Host Agent on an IBM AIX server, requires that the installer perform the following steps **before** running the agent's installation script:

1. Make a backup copy of the existing agent configuration files (storability.ini and config_srm.xml).

2. Make a backup copy of the contents of /opt/storability/etc/agents.

3. Open the existing agent configuration file (storability.ini) in a system text editor.

4. Locate the configuration section for the agent to be reinstalled.

5. Delete all existing configuration settings for that Sun StorageTek Business Analytics agent.

6. Save the modified agent configuration file.

7. Remove the existing /opt/storability/etc/agents directory.

At this point, you may reinstall the agent using the agent's installation script (e.g., srmAgent-install.sh).

## Uninstall SRM Agent - InstallShield

1. Select **Start->Program Files->Storability->Uninstall->Uninstall Local Manager**
   Or:
   **Start->Program Files->Storability->Uninstall->Uninstall Host Agent and Uninstall SRM Agent.** The Storability Uninstall dialog appears.
2. Click the checkbox for the Host Agent and/or SRM Agent.
3. Click **Next>**. The **Question** dialog appears.

4. Click **Yes** to confirm the uninstallation. An uninstalling agent splash box appears as each selected agent is uninstalled.
5. When the InstallShield Wizard Complete dialog box appears, click **Finish**.

## Uninstall SRM Agent – Solaris

The setup script is used to uninstall the SRM Agent installed on a Solaris server. The installation script (setup) is supplied on the Solaris Local Manager Installation CD.

1. To view a list of installed agents, type:

   ```
   setup -u
   ```

2. Type the number corresponding to the SRM Agent and press **Enter**.

3. Type zero (0) to end the selection of agents for removal.

4. When prompted, type **y** and press **Enter** to confirm the agent removal.

## Reinstalling the SRM Agent – Non-Solaris UNIX Host

The reinstallation procedure for all Sun StorageTek Business Analytics agents supported on non-Solaris UNIX hosts, such as the Host Agent on an IBM AIX server, requires that the installer perform the following steps **before** running the agent's installation script:

1. Make a backup copy of the existing agent configuration files (storability.ini and config_srm.xml).

2. Make a backup copy of the contents of /opt/storability/etc/agents.

3. Open the existing agent configuration file (storability.ini) in a system text editor.

4. Locate the configuration section for the agent to be reinstalled.

5. Delete all existing configuration settings for that Sun StorageTek Business Analytics agent.

6. Save the modified agent configuration file.

7. Remove the existing /opt/storability/etc/agents directory.

At this point, you may reinstall the agent using the agent's installation script (e.g., srmAgent-install.sh).