Sun StorageTek™ Business Analytics Remote Host Agent Installation Guide

Release 5.0 SP1

Sun Microsystems, Inc.
www.sun.com

Part No. 819-6239-10
March 2006, Revision 01

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

COPYRIGHT

English:

French:

Table of Contents

Introduction to the Remote Host Agent

The Sun StorageTek Business Analytics Remote Host Agent (RHA) provides an interface to collect data from different Windows servers through the Windows Management Instrumentation (WMI)/Web Based Enterprise Management (WBEM) protocol.

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.

WBEM (Web Based Enterprise Management) is an industry initiative to provide management of systems, networks, users and applications across multiple vendor environments. WBEM simplifies system management, providing better access to both software and hardware data that is readable by WBEM compliant applications. WMI is Microsoft's implementation of WBEM.

WMI is a component of the Windows operating system. The WMI uses a proprietary protocol whereas WBEM uses xml over http protocol. The following notes apply to installing and configuring the Remote Host Agent:

- Refer to the *Sun StorageTek Business Analytics Support Matrix* located on the Documentation CD to confirm the latest features and support requirements.
- Is provided on the Sun StorageTek Business Analytics Central Manager and Local Manager Installation Media.
- The Remote Host Agent and Host Agent can be installed on the same Windows computer.

To upgrade the Remote Host Agent, uninstall the previously installed Remote Host Agent before you install the current Sun StorageTek Business Analytics Remote Host Agent. The decision to upgrade an existing Remote Host Agent to the current Sun StorageTek Business Analytics Remote Host Agent may be performed because:

- The Sun StorageTek Business Analytics Release Notes indicate a problem has been fixed or a new feature added.
- The upgrade is recommended by your Sun representative.

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 Remote Host 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

REMOTE HOST AGENT MATRIX

Item	Description
HBAs	Currently the Remote Host Agent does not report on Host Bus Adapters because of limitations in WMI/WBEM.
Operating Systems	
Windows	• InstallShield-based installation. • Required Server Access: Administrator privileges
Configuration Parameters	• **Local Manager** – Specifies the IP address or host name of the Local Manager to be contacted for agent auto registration. The default value is local host (meaning the Host Agent contacts the Routing Agent on its server for agent auto registration). • **Local Manager Registration Port** – Specifies the TCP port number used by the Local Manager for auto registration. The default port number is 17146 for agent auto registration. • **IP** – Specifies the IP address of the remote machine the agent is to connect to. • **Port** - Defines the TCP port number of the CIM (Common Information Model) server running on the remote host machine. The default port number for CIM is 5988. • **Namespace** – Specifies access to the default namespace on the remote computer. For example, root/cimv2 for Windows 2000 or Solaris 9 or root\cimv2 for Windows 2003. • **Domain** – Specifies the domain name of the remote computer. • **Enable Auto Registration** – Turns agent auto registration on (default) or off.

Table 1 – Remote Host Agent Matrix

REMOTE HOST AGENT REQUIREMENTS FOR WINDOWS 2003

Whenever the Remote Host Agent is installed as a service, by default it runs with the privilege of Local System Account. On Windows 2003, this account does not have privileges to connect to a remote machine using the Distributed Common Object Model (DCOM) which is required by WMI. As a result, you need to set up the Remote Host Agent to run under a user account having privileges to connect to other machines.

To do so, proceed as follows:

1. Select Start->Settings-> Control Panel -> Administrative Tools -> Services applet.
2. Select the service named "Storability Remote Host Agent".
3. Right click and select Properties.
4. Select "Log On" tab.
5. Select "This Account".
6. Enter the username and password whose privilege the RHA service should run. This can be system administrator or any other user of the machine.
7. Click **OK**.
8. Record the user account for convenient reference when you configure the Remote Host Agent to connect to remote machines.

REMOTE HOST AGENT OBJECTS

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

Currently, the Remote Host Agent does not report HBA, Logical Volume Manager (LVM), or end-to-end mapping data because of WMI/WBEM limitations.

Table	Description
alerts-3_1	ip_address, port, when, application, severity, id, description
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_hba_config	ip_address, nodename, host_id, vendor, model, serial_number, port_num, driver_version, wwnn, wwpn, firmware_version, port_fcid, port_type, effective_speed, max_speed, link_status, fabric_wwn, ctrl_instance, ctrl_num, hardware_path, timestamp
gsa_host_config	ip_address, nodename, host_id, osname, vendorname, model, version_number, release_level, numcpus, memory, timestamp.
gsa_host_filesystem-2_3	ip_address, nodename, host_id, device, filesystem name, filesystem_type, blocksize, total_blocks, blocks_ used, blocks_ available, files_used, files_available, filesystem _id lvm, logical_device_group, logical_device_ name, timestamp.
gsa_host_interfaces	ip_address, nodename, host_id, interface_name, mac_ address, interface_ip, interface ip_name, subnet *mask,* default_gateway, interface_status, timestamp.
gsa_host_netshares	ip_address, nodename, host_id, share_name, share_ type, share_path, filesystem name, options, timestamp.
gsa_ini_control-2_0	ip_address, port, domain, parameter, value, status, timestamp
gsa_logical_volume_config-2_1	ip_address, nodename, host_id, lvm, logical_device_ group, logical_device_name, type, device_layout, capacity, blocksize, logical_device-status, timestamp.
gsa_logical_volume_relation	ip_address, nodename, host_id, lvm, logical_device_ group, logical_device_name, uses_lvm, uses_logical_device_group, uses_ logical_device name, timestamp.
gsa_parm_info	ip_address, port, object, parm_name, value_syntax, description

Table	Description
gsa_physicalvolume_config	ip_address, nodename, host_id, physical_device name, vendor, product, serialnum, volume_id, array_ id, physical_device_status, timestamp.
gsa_physical_volume_path-2_1	ip_address, nodename, host_id, physical_device _name, path_device_name, ctrl_instance, ctrl_number, channel, target, LUN, array_wwpn, path_status, path_ software_name, path_software_version, timestamp.

Table 2 - Host Agent Objects

WINDOWS LOCAL MANAGER INSTALLATION CD - INSTALLSHIELD

1. Insert the 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. Click **Next>**.
5. Review/modify the informational **User Name** and **Company Name** and click **Next>**.
6. On the screen that allows you to select agents to be installed, select **Remote Host Agent** and click **Next>**.

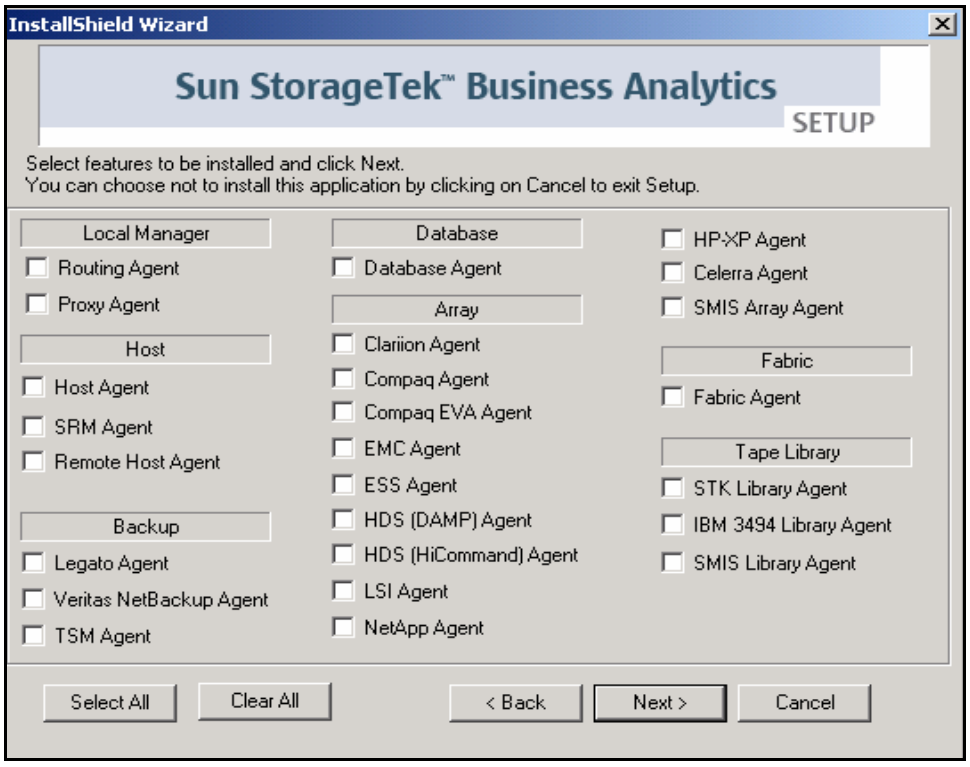

Figure 1 - Agent Selection Dialog

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

8. If prompted, specify whether (yes/no) to install the new version of the Configuration Tool. The *Sun StorageTek Business Analytics Release Notes* will specify any agent whose configuration requires a new release of the Configuration Tool.

9. After the Configuration Tool is automatically launched, click **File->Edit->Smart Agent Configuration**.

10. Click the **Remote HostAgent** tab in the main window.

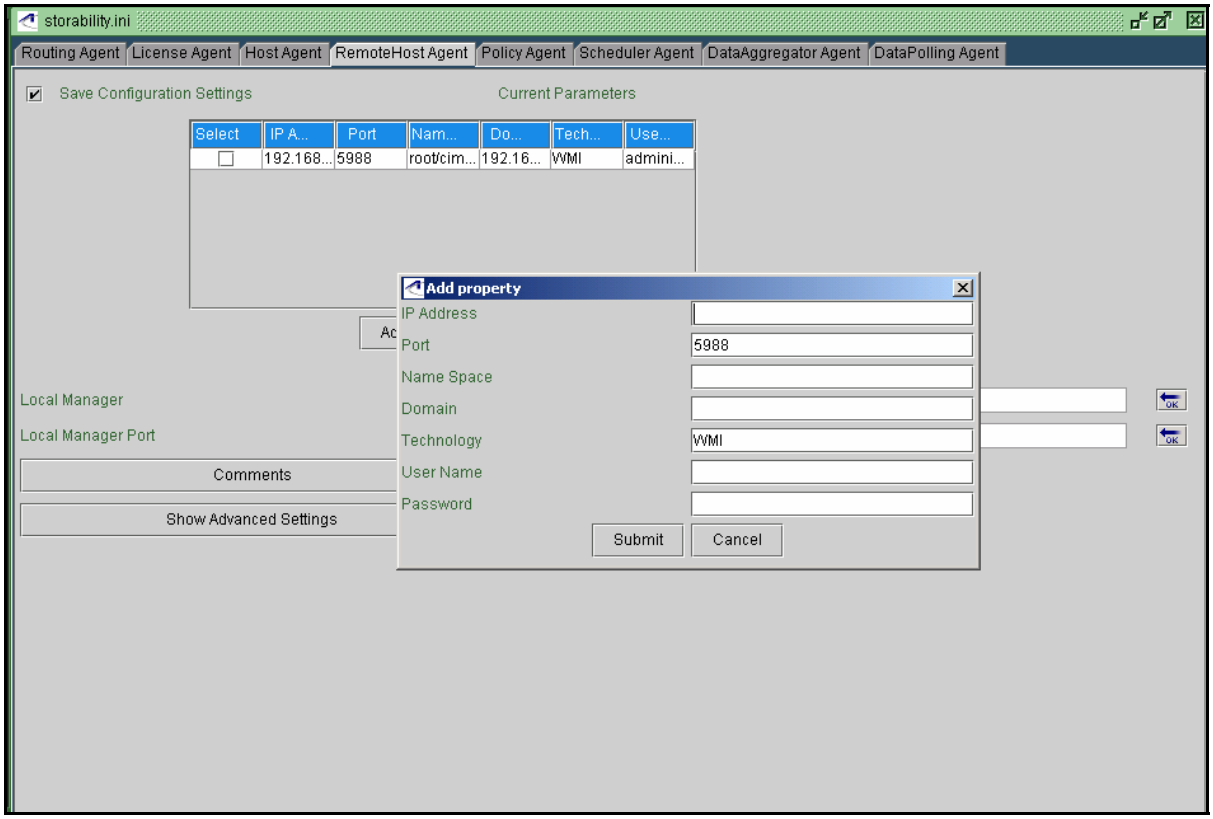

Figure 2 - Remote Host Agent Configuration Window

11. Click **Add** and the **Add property** dialog opens**.** Enter the following information for each server connection:

    - **IP Address** – Specify the IP address of a remote host machine that the RHA connects to.

    - **Port** – Specify the TCP port number of the CIM (Common Information Model) or WBEM server running on the remote host machine. The default port number for CIM is 5988.

    - **Namespace** – Specify access to the default namespace on the remote computer. For example: `root/cimv2` for Solaris 9 or Windows 2000 or `root\cimv2` for Windows 2003.

    - **Domain** – Specify the domain name of the remote computer.

    - **Technology** – Specify WMI or WBEM.

- **User Name** – Enter the user name used by the agent for authentication. By default, users that are members of the **administrators** group have full local and remote access to WMI.

- **Password** – Enter the above user's password.

12. Click **Submit** after you have finished configuring the remote server.

13. Repeat the above procedure until you have added all the desired remote servers.

14. For **Local Manager**, enter the IP address or host name of the Local Manager to be contacted for agent auto registration.

15. For **Local Manager Registration Port**, specify the TCP port number the Local Manager uses for agent auto registration.

16. Click Show Advanced Settings to review/modify these configuration parameters.

    - For **Enable Auto Registration**, accept that agent auto registration is turned on (default) or disable it by setting this configuration parameter to false.

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

18. Click **File->Exit** to close the Configuration Tool.

19. View and then close the **Readme** file and click **Finish**.

VERIFYING REMOTE HOST AGENT

Use the GSM Agent Diagnostic Tool to verify the Remote Host Agent functionality. This diagnostic utility is installed in the Storability Local Manager Utilities folder as part of the Sun StorageTek Business Analytics Central Manager or Local Manager software installation. It represents the primary tool to verify agent functionality or troubleshoot agent problems.

Proceed as follows:

1. Wait approximately 30 seconds after you start the Sun StorageTek Business Analytics Remote Host Agent to allow it to initialize before querying it with the GSM Agent Diagnostic Tool.

    a. Launch the GSM Agent Diagnostic Tool from the Storability Program Folder.

    b. 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.

    c. Set the port to 17173 (or select the Remote Host Agent from the drop down list of service names).

    d. Click the **Get Object List** button and you should receive a list of objects published by the Host Agent.

e. Select the **gsa_host_config** object and it should list the IP address, node name, host ID of the host server as well as additional fields.

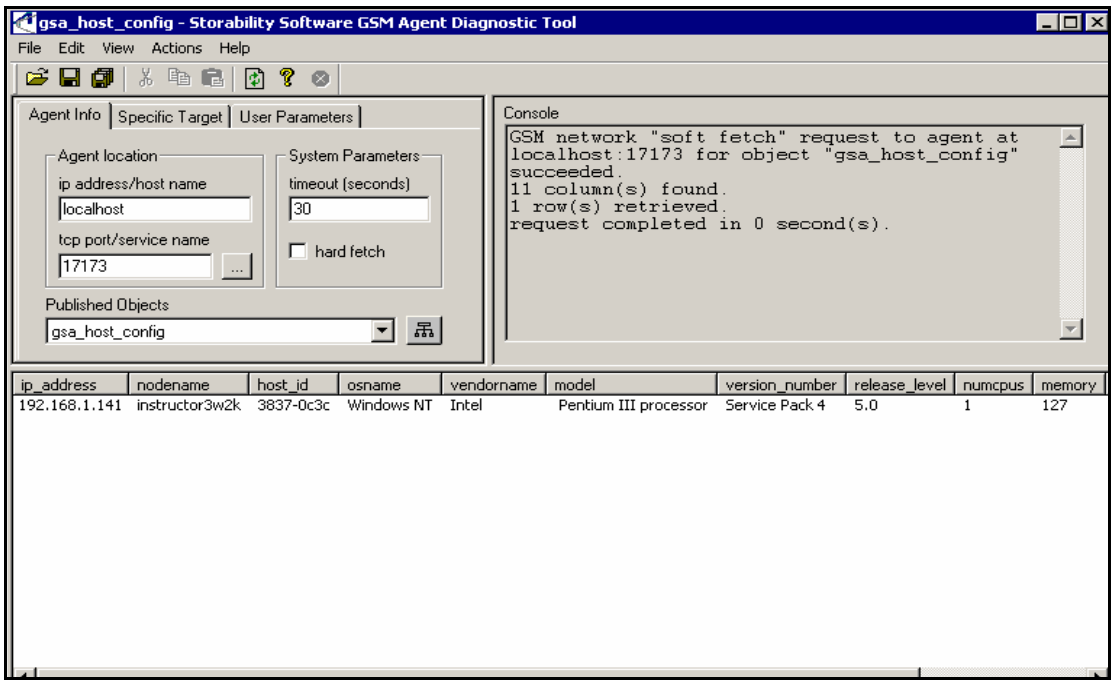

Figure 3 – Sample Host Configuration Object

f. Proceed to collect all other objects published by the agent keeping in mind some objects (e.g., gsa_hba_config) will not be populated with data because of WMI/WBEM limitations.

2. To verify the Remote Host Agent has registered successfully with its configured Local Manager:

   a. In the **Agent location** window, enter the IP Address or network resolvable Host Name of the Local Manager in the **ip address/host name** input box and set the port to 17146 (or select the Storability Routing Agent from the drop down list of service names).

   b. Click the **Get Object List** button and you should receive a list of objects published by the Routing Agent.

   c. Select the **gsa_agent_register** table.

   d. Verify this collected object reports the Host Agent using the following fields:

   - port – 17173 (Remote Host Agent default TCP port number)
   - peer_list – IP Address or Host Name of the server where the Host Agent is running
   - last_freshened – Date/time agent last registered
   - application_status – Should be 'ACTIVATED'
   - network_status – Should be 'Up'

VERIFYING MANAGEMENT CONSOLE FUNCTIONALITY

The following procedure describes how the Sun StorageTek Business Analytics administrator verifies the server 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.

Note: The same Server reports are used both for the Remote Host Agent and the Host Agent. Similarly, both agents use the same polling schedules.

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. Verify that your customized Home Page includes the **Host Filesystem Utilization** pane (or use **Change Dashboard** to select one that includes this pane).
3. Select **Tools->Data Polling Schedule.**
4. Use the **Collect Now** button to collect the Host (collection type) **Filesystem** (Collection Metric) data using a polling schedule that includes all sites.
5. Wait approximately thirty seconds and then use the **Collect Now** button to collect the Host (collection type) **Configuration** (Collection Metric) data using a polling schedule that includes all sites.
6. Wait approximately thirty seconds and then use the **Collect Now** button to collect the Host (collection type) Logical VM (Collection Metric) data using a polling schedule that includes all sites.
7. Close the **Data Polling Schedule** window.
8. Verify the **Host Filesystem Utilization** dashboard reports information on the server whose installed Remote Host Agent you are verifying.
9. Click the **Host Name** link in the pane and the **Detailed Host Configuration and Utilization** report appears.
10. Verify the Server, Platform, IP, and Site information is report with the **General** tab enabled.
11. Verify all the tabular device reports by clicking the respective tabs.

    Note: Keep in mind that some device-specific tabs may display no report data because they do not apply (e.g., Topology tab) for that server. For example, since the Remote Host Agent does not collect HBA information, selecting the Topology tab will not display data. In these instances, the window typically displays the "No Data Found" informational text.
12. Close the browser session with the Management Console as the above steps complete verifying the Management Console functionality.

REMOTE HOST AGENT TROUBLESHOOTING

1. **Verify system/agent prerequisites** – Refer to the *Sun StorageTek Business Analytics Support Matrix* that is located on the Documentation CD to verify the most recent support requirements for the agent. The main requirement is to have WMI support on the remote Windows servers from which RHA will collect data.
2. **Verify Remote Server Authentication** - If the Remote Host Agent is unable to authenticate to the remote computer, verify that the domain administrator account has privileges to the WMI namespace to which you are trying to connect on the agent computer.
   - WMI security can be configured using the **WMI Control**.
     1. Open a DOS command Window.
     2. Type:

```
wmimgmt.msc
```

and press **Ente**r.

3. Right-click **WMI Control.**
4. Click **Properties**.
5. You can verify or configure namespace-specific security from the **Security** tab.

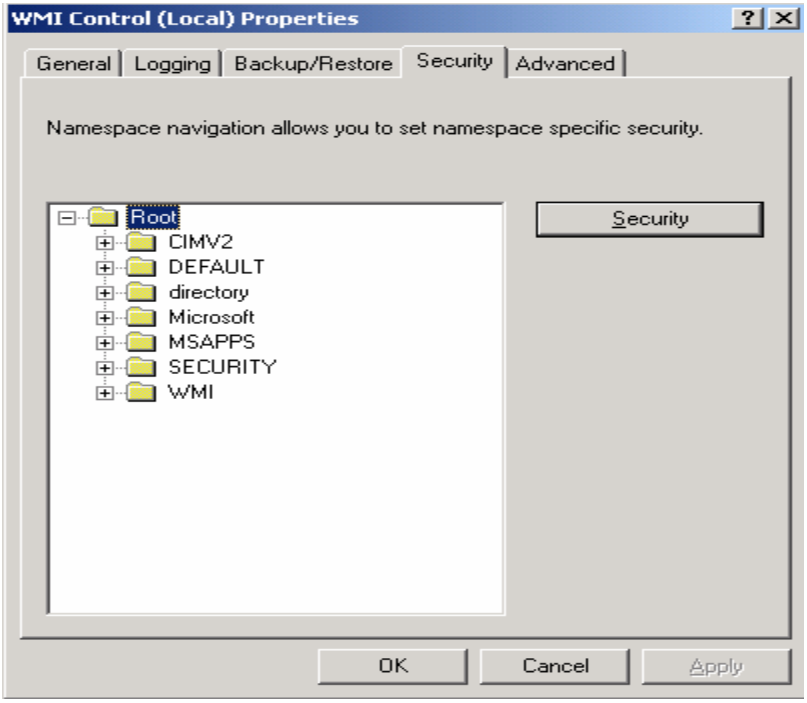

Figure 4 - WMI Control

3. For a Solaris 9 (or higher) computer, verify with the Solaris administrator that the WBEM package is installed and running.
4. Use **GSMdiag** to save the output for all the tables if escalating a problem to StorageTek Support (Technical Excellence Center).
   a. Run the Agent Diagnostic Tool from the Storability Program Folder.
   b. Enter the **IP Address** or **Hostname** of the server where the agent is installed and set the port to 17132 (or select the Remote Host 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 Host Agent. If unsuccessful, verify the Ethernet connectivity to the server running the Remote Host Agent and that the Remote Host 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**.
5. **Review the Message Log** – Review/collect the Message.log file that can contain information on startup errors, configuration errors, or errors regarding accessing data or parsing output.

Windows

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

6. **Verify Local Manager Registration -** The configured Routing Agent's **gsa_agent_register** table displays Storability agents that have registered with the Routing Agent.

   The **Type** field indicates the type of registration. If the agent registered using agent auto registration, "AUTO_NET" is displayed in the **Type** field. If the agent was defined manually as a SUB_AGENT entry in the Routing Agent's storability.ini file, the **Type** field will display "STATIC".

7. **Review the Routing Agent Message Log** – Review/collect the Routing Agent Message Log to check for errors related to Ethernet connectivity problems contacting the Remote Host Agent.
8. **Confirm Polling Schedules** – Using the Management Console's **Data Polling Schedule** menu, review/modify the existing Polling Schedules for the **Collection Type** of Host and the Filesystem, LVM, and Configuration metrics for the specific site (or all sites).
9. **Review Aggregator Message Log** – Open the Aggregator's Message Log in a text editor. Verify that the Host Tables were requested and that rows were inserted into the database. If you perform an on-demand (Collect Now) request in the **Polling** menu, look for timestamps in the log that closely approximate when that request occurred.
   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 Polling 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.
10. **Check the assurent database** – The assurent database is the data repository for your Sun StorageTek Business Analytics application. For the Remote Host Agent, use any MS SQL Query interface, such as isql, to verify rows have been inserted into the host-related tables, such as the **gsa_host_config** table.
11. **Verify Management Console Functionality** – As a final step in the agent troubleshooting procedure, minimally verify that the host server now appears in the Management Console's **Host Filesystem Utilization** dashboard on the Home Page.

UNINSTALL REMOTE HOST AGENT - INSTALLSHIELD

1. Select **Start->Program Files->Storability->Uninstall->Uninstall Local Manager**
   Or:
   Start->Program Files->Storability->Uninstall->Uninstall Remote Host Agent. The Storability Uninstall dialog appears.
2. Click the checkbox for the **Remote Host Agent**.
3. Click **Next>**. The **Question** dialog appears.
4. Click **Yes** to confirm uninstalling the agent. An uninstalling agent splash box appears as each selected agent is uninstalled.

At this point, you may update your existing Remote Host Agent version by installing the Remote Host Agent supplied with your version of Sun StorageTek Business Analytics.