Sun StorageTek™ Business Analytics NAS Agents Installation Guide

Release 5.0 SP1

Sun Microsystems, Inc.
www.sun.com

Part No. 819-6238-10
March 2006, Revision A

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

COPYRIGHT

English:

French:

Table of Contents

INTRODUCTION TO NAS AGENTS

Sun Storagetek Business Analytics provides NAS agents supporting Network Appliance systems and the EMC Celerra. **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.

Refer to the *Sun Storagetek Business Analytics Support Matrix* that is located on the Documentation CD to obtain the latest information on supported NAS systems as well as their support requirements. Sun Storagetek Business Analytics 5.0 SP1 provides three agent installation CDs for supported platforms: Windows Local Manager, Solaris Local Manager, and UNIX Agents (HP-UX and IBM AIX).

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

- The Sun StorageTek Business Analytics Release Notes indicate a problem has been fixed or a new feature added (e.g., support for hard and soft quotas).
- 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.

The Sun StorageTek Business Analytics Network Appliance (NetApp) Agent does not auto-register with the Routing Agent and, therefore, needs to be registered statically.

To register the NAS 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

NAS AGENT OBJECTS

Table 1 – NAS Agent Objects lists the objects that the NAS Agents publish. The Celerra Agent does not populate the **gsa_nas_physicalvolume_path** object. For the NetApp Agent, the gsa_nas_quotas-2_1 object contains two new columns, quota_kb_slimit and quota_files_slimit. Their column values identify the quota limit (Kb) and the 'number of files' limit for soft quotas, respectively.

Table	Columns
alerts-3-0	sourceip, priority, alert_id, progname, alert, time, firsttime, refreshedtime, int1, text1, text2.
agent_version	ip_address, agent_name, version, compile_time, managed_entities, tz_name, tz, timestamp
gsa_nas_component	ip_address, gsa_id, component_id, name, serial, type, model, software_name, software_version, software_version_minor, firmware_version, numcpus, volatile_memory, nonvolatile_memory, power_status, fan_status, battery_status, disk_status, temperature_status, timestamp
gsa_nas_component_perf	ip_address, gsa_id, component_id, cpu_percent_busy, cpu_percent_idle, uptime, cifs_ops_sec, nfs_ops_sec, http_ops_sec, lan_inbound_kb_sec, lan_outbound_kb_sec, lan_inbound_io_sec, lan_outbound_io_sec, disk_read_kb_sec disk_write_kb_sec,, disk_read_io_sec, disk_write_io_sec, nvram_write_kb_sec, cache_hits_sec, cache_miss_sec,timestamp
gsa_nas_config	ip_address, nas_ip_address, gsa_id, system_id, nodename, vendor, product, model, cluster_status, cluster_partner, cluster_partner_status, timestamp
gsa_nas_filesystem	ip_address, gsa_id, filesystem_name, filesystem_type, mount_device, blocksize, total_blocks, blocks_available, blocks_used, snapshot_reserved, snapshot_used, total_files, files_used, files_available, lvm, logical_device_group, logical_device_name, timestamp.
gsa_nas_filesystem_mapping	ip_address, gsa_id, destination_name, destination_path, source_name, mapping_type, mapping_status, last_sync_time, schedule, timestamp
gsa_nas_filesystem_options	ip_address, gsa_id, filesystem_name, option_name, option_value, timestamp
gsa_nas_interfaces_ip	ip_address, gsa_id, component_id, if_name, if_ipaddr, if_netmask, timestamp
gsa_nas_lan_perf	ip_address, gsa_id, component_id, if_name, outbound_kb_sec, inbound_kb_sec, inbound_io_sec, outbound_io_sec, errors, collisions, drops, timestamp
gsa_nas_logicalvolume_config	ip_address, gsa_id, lvm, lvm, logical_device_group, logical_device_name, type, raw_blocks, capacity, blocksize, device_layout, logical_device_status, timestamp.

Table	Columns
gsa_nas_logicalvolume_relation	ip_address, gsa_id, lvm, lvm, logical_device_group, logical_device_name, uses_lvm, uses_logical_device_group, uses_logical_device_name, timestamp.
gsa_nas_options	ip_address, gsa_id, option_type, option_name, option_value, timestamp.
gsa_nas_physicalvolume_config	ip_address, gsa_id, physical_device_name, vendor, product, serial_number, location_1, location_2, location_3, volume_id, array_id, physical_device_status, timestamp.
gsa_nas_physicalvolume_path	ip_address, gsa_id, path_device_name, physical_device_name, ctrl_instance, if_name, target, channel, lun, array_wwpn, timestamp.
gsa_nas_physicalvolume_perf	ip_address, gsa_id, physical_device_name, read_kb_sec, write_kb_sec,, read_io_sec, write_io_sec, read_time_usec, write_time_usec, percent_busy,timestamp.
gsa_nas_quota-2_1	ip_address, gsa_id, quota_type, quota_id, quota_volume, quota_tree, quota_kb_used, quota_kb_limit, quota_kb_slimit, quota_kb_threshold, quota_files_used, quota_files_limit, quota_files_slimit, quota_specifier, timestamp.
gsa_nas_share	ip_address, gsa_id, share_type, share_name, share_path, filesystem_name, options, timestamp.

Table 1 - NAS Agent Objects

NETAPP AGENT

The Sun StorageTek Business Analytics NetApp Agent reports configuration, allocation, and performance information on supported Network Appliance Filers. The agent communicates to the array using both CLI (via RSH or SSH access method) and Simple Network Management Protocol (SNMP).

NETAPP AGENT MATRIX

Feature	Description
Support Prerequisites	

Verify RSH or SSH access to the array	`rsh <netapp_filer>  -l root sysconfig –v`
	`rsh <netapp_filer>  -l root sysconfig –v`
	
	Or:
	
	`ssh <netapp_filer>  -l root sysconfig –v`
	
	Notes:
	• SSH client is a prerequisite and is supported. However, Cygwin SSH client on any NAS agent installation and configuration is not supported by StorageTek. It is only supported for the Sun StorageTek Business Analytics Compaq (HSG80) agent.
	
	• Beginning with NetApp ONTAP Version ONTap 6.4 and the associated SecureAdmin 3.0, the nonstandard username: password command-line format is **not** supported. Instead of password authentication, you can configure the NetApp Agent to authenticate to SecureAdmin 3.0 using public key authentication. Refer to the **Requirements to Use SSH** section that follows.
	
	• Some versions of "rsh" require the –l option to follow the hostname; others accept either.

Ethernet Connectivity to NetApps Filer	To verify the agent has connectivity to the filer: `ping <file_IP_address>`
Verify SNMP is enabled on the Filer	Use the Local Manager utility, bulkAll.exe. For example: `bulkall  -IP 10.250.1.57 –o c:\temp\netapp.txt` Verify that data appears in the output file (e.g., netapp.txt)
Agent Installation	
Windows	• Windows Local Manager Installation CD (InstallShield) • Windows Administrator privileges
Solaris	• Solaris Local Manager Installation CD (package installation) • root user account

Feature	Description
Configuration Parameters	
ssh/rsh Command Path	Fully-qualified path to the access method to be used (rsh or ssh); must have working version of rsh or ssh for the agent to work properly.
User Name	User name for agent authentication
Password	Password for agent authentication
SNMP Read Community	SNMP read community (e.g., public) Note: This configuration setting is case-sensitive. If you enter "Public" instead of "public", for example, agent data collection will not work properly.
Local Manager	IP address or network resolvable host name of Local Manager to contact for agent auto registration.
Local Manager Registration Port	TCP port number the Local Manager uses for agent auto registration. The default TCP port number is 17146.
Enable Auto Registration	Specifies auto registration is enabled (true) by default; set to false to disable auto registration.

Table 2 - NetApp Agent Matrix

NETAPP AGENT AND AGGREGATE SUPPORT

NetAPP Data ONTAP v7.0 introduces the concept of aggregate, which is a storage virtualization method to collectively represent groups of raid disks. Aggregates combine all the physical storage resources managed by a NetApp appliance into a single virtualized storage pool, regardless of the types of storage in the pool.

An aggregate consists of a collection of one or two plexes. If the aggregate is unmirrored, it contains a single plex. A plex is a collection of one or more RAID groups that together provide the storage for one or more Write Anywhere File Layout (WAFL) file system volumes.

With Data ONTAP v7.0, the NAS administrator uses aggregates to manage plexes and RAID groups. In previous versions of ONTAP, volumes were tied to fixed physical entities, whether a single RAID or a group of RAID sets. Aggregates allow combining multiple storage resources into a single storage pool and, thereby, allowing volumes to grow or decrease in size as needed.

Traditional and Flexible Volumes

Prior versions of Data ONTPAP allowed creation of volumes that were dedicated to the containing aggregate, meaning no other volumes could obtain storage from this container. Such volumes are called traditional volumes.

A flexible volume is a volume that is loosely coupled to its containing aggregate. This means a flexible volume can share its containing aggregate with other flexible volumes. As this volume is managed separately from the aggregate, you can have smaller size volumes that can grow in small increments up to the size of the aggregate. You can also clone flexible volumes.

Some characteristics are described as follows:

- An aggregate can only be used by flexible volumes.
- A flexible volume can only contain one aggregate while an aggregate can be used by many flexible volumes.
- An aggregate has "options" that can be set or unset.
- An aggregate cannot be exported as a share.
- An aggregate has no file-system associated with it.

The Sun StorageTek Business Analytics assurent database contains the gsa_nas_logicalvolume_config table. In a NetApp Data ONTAP 7.0 environment, a volume that that is listed in this table and that has no associated file system is an aggregate.

NetApp Agent and Aggregate Support

As implemented by NetApp filers, quotas are primarily used to:

- Limit the consumption of storage resource by the amount of disk-space or the number-of-files.
- Track disk-space/number-of-files usage without imposing any limits.
- Alert administrators when quota thresholds are crossed.

Quota targets can be assigned to users, groups or qtrees. User and group quotas are applied on a per volume or per qtree basis.

Some terminology regarding quotas is discussed below.

- qtree - Is a logically defined file system that can exist as a special subdirectory of the root directory within either a traditional volume or a flexible volume. For NetApp devices, you can have a maximum of 4,995 qtrees on any volume.

- Hard quota - Is a limit that cannot be exceeded. If an operation, such as a write, causes a quota target to exceed a hard quota, the operation fails and a warning message is logged to the filer console and an SNMP trap is issued.
- Soft quota - Is a limit that can be exceeded. When a soft quota is exceeded, a warning message is logged to the filer console and an SNMP trap is issued. When the soft quota limit is no longer being exceeded, another syslog message and SNMP trap are generated. You can specify both hard and soft quota limits for the amount of disk space used and the number of files created. In order for quota settings to take effect, they have to be "turned on" or activated on a per-volume basis. When

applying a user quota, Data ONTAP distinguishes one user from another based on their ID, which can be a UNIX ID (UID) or a Windows ID (SID).

Requirements to Use SSH - NetApp Agent

When configuring the Storability NetApp agent to use SSH, there is a complication if NetApp SecureAdmin 3.0 is installed on the filer. SecureAdmin 3.0, which began shipping with OnTap 6.4, is a complete rewrite based on OpenSSH. The previous SecureAdmin 2.x accepted the `-l username:password` format, which the new version does not support. When connecting to a filer running SecureAdmin 3.0 or higher in the default configuration, the ssh client will prompt for a password interactively. The agent will not handle the interaction, and the command will time out.

Instead of password authentication, the agent can authenticate to SecureAdmin 3.0 using public key authentication; SecureAdmin 2.x did not support this mode. With public key authentication, the password configured in storability.ini must be empty (no spaces, just empty), the ssh client has to be set up properly for public key authentication for the NetApp agent service user, and SecureAdmin must be configured to accept public key authentication. Setup instructions for the NetApp side are contained in the **SecureAdmin 3.0** manual. This can be very complicated to get working properly, but it is the only way the agent can communicate with this filer software version using SSH. We summarized the necessary steps below.

storability.ini File change

Add the following entry to the storability.ini file:

```
SSH_OPTIONS = -o protocol=2 -o BatchMode=yes -o StrictHostKeyChecking=no
```

The previous version of SecureAdmin required the ssh client to use protocol 1, which this option will override. The **BatchMode** and **StrictHostKeyChecking** options will help avoid problems that could interfere with non-interactive use. (Turning StrictHostKeyChecking off is not a security hole when using public key authentication; it would be if we were using password authentication.)

Windows with OpenSSH client version 3.x

Perform the following tasks as the local Administrator or a local account in the administrators group.

1. Generate Public/Private Keys using the Administrator account (or whatever account you're logged in as).

   ```
   C:\> ssh-keygen -t dsa
   Generating public/private dsa key pair.
   Enter file in which to save the key
   (/home/Administrator/.ssh/id_dsa):
   Enter passphrase (empty for no passphrase):
   Enter same passphrase again:
   Your identification has been saved in .../id_dsa
   Your public key has been saved in .../id_dsa.pub.
   The key fingerprint is:
   27:0a:c3:58:2d:91:db:0f:c1:df:0b:97:72:49:91:cb username@yourhost
   ```

   This will generate two files, id_dsa (private key) and id_dsa.pub (public key) for the Administrator (or whatever user you're logged in as). Note that the directory specified above, /home/Administrator/.ssh is actually C:\Documents and Settings\Administrator\.ssh)

Note: You can also repeat this step to generate rsa keys by changing the option above to "`-t rsa`" (generates `id_rsa` and `id_rsa.pub`).

If you already use public key authentication, an alternative to running `ssh-keygen` is to copy an existing `id_dsa` and `id_dsa.pub` that are already accepted by the NetApp filers to the appropriate SSHDIR directory on the agent host. You can still determine SSHDIR from `ssh-keygen`, and then interrupt with control-C.

2. Put the public key(s) on Netapp filer.

   - If multiple public keys were generated in Step 1, combine them into one file. Name the file containing the public key(s) "authorized_keys".
   - Put the authorized_keys file in \\<filer address>\C$\etc\.sshd\root\.ssh
   - For each Netapp filer, put the authorized_keys file in \\<filer address>\C$\etc\.sshd\root\.ssh

3. Mount the Netapp C$ filesystem locally. (Note, this is easier from a UNIX NFS client, but that process is not described here.)

4. Create a directory <C$ mount point>: \etc\sshd\NETAPPUSER\.ssh. Replace NETAPPUSER by the login name you use to connect to the Netapp, e.g. "root". The file manager will not allow you to name a directory ".ssh" so you will have to do that from a command window: `mkdir .ssh`

5. Copy or append the resulting id_dsa.pub file (the public key) to a Netapp file named <C$ mount point>: \etc\sshd\NETAPPUSER\.ssh\authorized_keys, where NETAPPUSER is replaced by the NetApp username (e.g. "root"). Do not copy the private key file (id_dsa), only the public key file (id_dsa.pub). The format of this file is one very long line, which must not be broken up, so copy-and-paste is not advised.

Warning: if the authorized_keys file already exists, the customer is probably already using public key authentication. In this case, you must APPEND the new id_dsa.pub to this file, by using >> redirection from a command-line. **Do not overwrite an existing id_dsa.pub file** or you will interfere with other filer administrators.

6. Test the connection using your current login. To do so, open a command window and type: `C:\> ssh -l root <netapp address> sysconfig -A`

   You should get the output from that command without being prompted for a password.

7. Copy the private key file(s) to the Base SSH directory. To do so, copy the entire .ssh directory containing the key(s) above to the Base SSH directory (probably C:\Program Files\OpenSSH).
8. Verify that the keys exist in the proper place (default C:\Program Files\OpenSSH\.ssh).

INSTALLING THE NETWORK APPLIANCE AGENT - WINDOWS

1. Insert the Sun StorageTek Business Analytics Windows Local Manager Installation 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. Check the **NetApp Agent** checkbox on the screen that lists the agents for installation and click **Next>**.

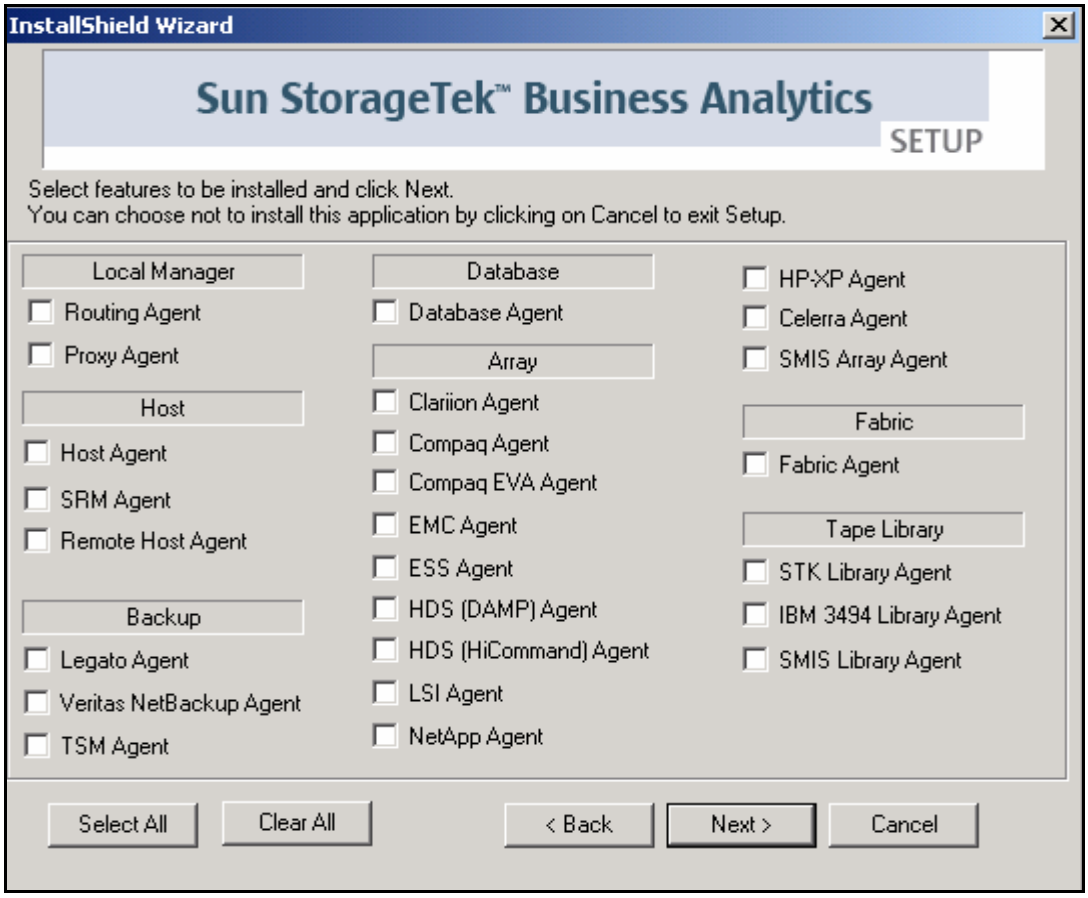


Figure 1 - Agent Selection Dialog

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

7. Specify whether or not to install the new version of the Configuration Tool, if prompted.

8. When the Configuration Tool is automatically launched, select **File** -> **Edit** -> **Smart Agent Configuration**.

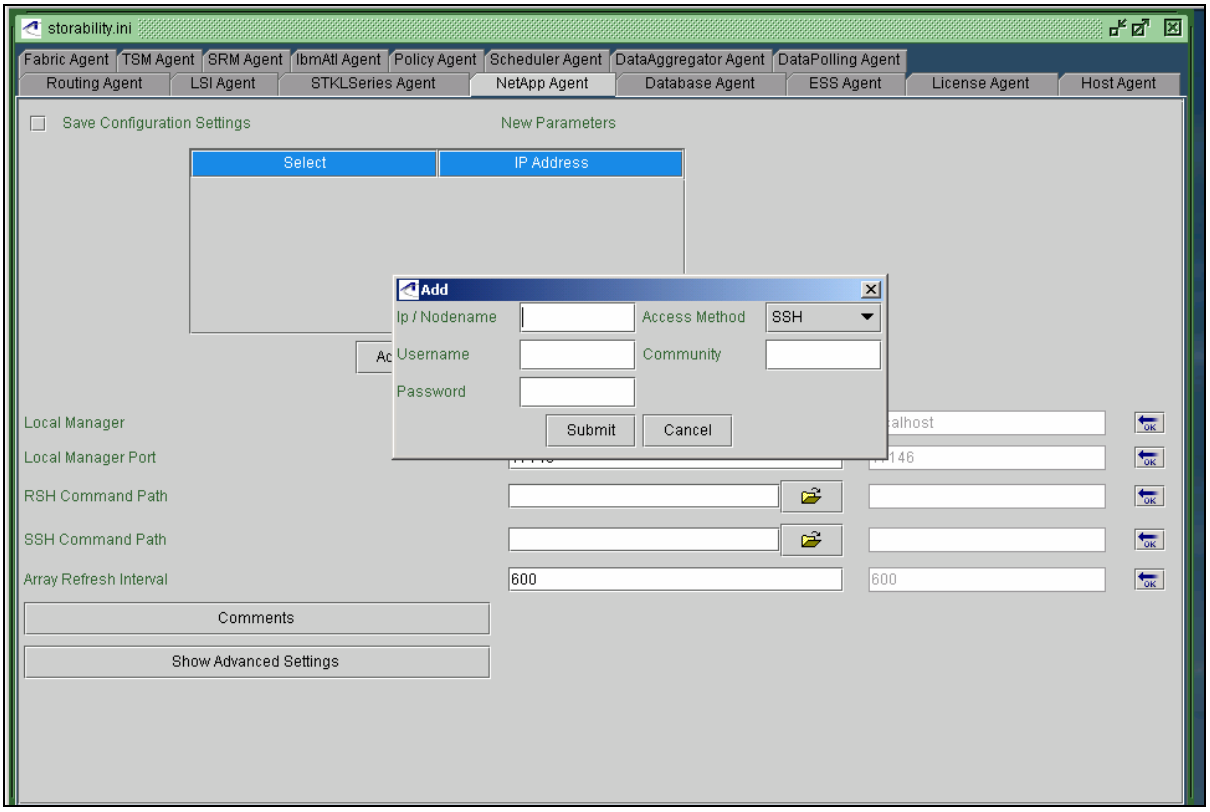


Figure 2 - NetApp Configuration Window

9. Click the **NetApp Agent** tab and then click **Add** to enter the configuration variables:

   - **IP/Nodename** – The IP address or network resolvable name of the Filer.
   - **User name** – User name for agent authentication.
   - **Password** – Password associated with the user name. May be blank to meet the requirements for using SSH as the access protocol.
   - **Access Method –** Use the drop down box to select the access method of RSH or SSH for the agent.
   - **Community** - The SNMP read community (e.g., public).

11. Click **Submit.**

12. Review/modify the following variables:

   - **Local Manager –** Specify the IP address or host name of the Local Manager the NetApp Agent will contact for agent auto registration.

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

   - **RSH Command Path** – The fully qualified path to the rsh executable. This is a global parameter that only appears once in the storability.ini file. It will be used only if the RSH access method is specified for at least one NetApp device. You may click the **Folder** icon to browse directories.

   - **SSH Command Path** – The fully qualified path to the ssh or ssh2 executable. This is a global parameter that only appears once in the storability.ini file. It will

be used only if the SSH access method is specified for at least one NetApp device. You may click the **Folder** icon to browse directories.

- **Array Refresh Interval** – Specify the frequency the array disk performance data is refreshed. The default interval is 600 seconds.

13. Click **Show Advanced Settings** to review/modify the following variables:

- **Enable Auto Registration –** Accept that agent auto registration is enabled (true) or set this parameter to false to disable agent auto registrsation.

- **NAS NetApp Read Timeout –** The agent's timeout interval to wait for the filer to send data

- **Array Refresh Performance Interval** – The frequency that the performance data cache is refreshed.

14. With "Save Configuration Settings" turned on (check mark), click **File->Exit** to close the Configuration Tool.

15. Restart the Storability Netapp Agent before you verify agent functionality.

Solaris with OpenSSH Client Version

A configuration example for OpenSSH Client Version 3.x on Solaris follows. You run the following specified commands while logged in using the gsm user account. For example:

```
su root
su – gsm
```

1. Generate Public/Private Keys.

- **DSA public key / private key**

a. Create a dsa public key / private key pair for the gsm user with the following command.

```
ssh-keygen -t dsa -b 1024
Generating public/private dsa key pair.
```

b. When prompted to "Enter file in which to save the key (/opt/storability/gsm/.ssh/id_dsa", accept the default location.

c. When prompted to "Enter passphrase (empty for no passphrase):" , press ENTER.

d. When prompted to "Enter same passphrase again:", press ENTER. Command output similar to the following is displayed:

```
Your identification has been saved in
/opt/storability/gsm/.ssh/id_dsa.
Your public key has been saved in
/opt/storability/gsm/.ssh/id_dsa.pub.
The key fingerprint is:
d4:9d:b5:9d:44:de:f3:5c:a3:be:e1:31:e3:95:9a:7f gsm@yourhost
```

RSA public key / private key

1. Create a rsa public key / private key pair for the gsm user with the following command.

```
ssh-keygen -t rsa -b 1024
Generating public/private rsa key pair
```

2. When prompted to "Enter file in which to save the key (/opt/storability/gsm/.ssh/id_rsa):", accept the default location.

3. When prompted to "Enter passphrase (empty for no passphrase):", press ENTER.

4. When prompted to "Enter same passphrase again:", press ENTER. Command output similar to the following is displayed:

```
Your identification has been saved in
/opt/storability/gsm/.ssh/id_rsa
Your public key has been saved in
/opt/storability/gsm/.ssh/id_rsa.pub
The key fingerprint is:
7c:d6:ba:27:a3:e3:73:d3:c2:e3:b8:c5:da:9f:5d:16 gsm@yourhost
```

5. Copy the generated public key to the NetApp system default directory and append it to the /etc/sshd/*NetApp_User*/.ssh/authorized_keys file.

The following commands append the public keys to the /etc/sshd/*NetApp_User*/.ssh/authorized_keys file on NetApp system sys1:

- `mount sys1:/netapp_filer/mnt_sys1`
- `cat id_rsa.pub >> /mnt_sys1/etc/sshd/root/.ssh/authorized_keys`
- `cat id_dsa.pub >> /mnt_sys1/etc/sshd/root/.ssh/authorized_keys`

Caution: Public Keys Generated by Secure CRT and SSH.com Clients:
SSH 2.0 public keys generated by SecureCRT and ssh.com clients contain comments and line breaks that make the public keys useless. You must make the following edits to the generated public keys before SecureAdmin can use them:

- Remove any text that is not part of the public key.
- Remove line breaks and spaces to make the public key one continuous string of characters.
- Before the first character of the public key, add ssh-rsa followed by a space.

The following is an example of an SSH 2.0 public key generated by a SecureCRT client. The generated public key contains extra text and line breaks at the end of each line.

```
---- BEGIN SSH2 PUBLIC KEY ----
Subject: john
Comment: "john@johnnt"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDJhJ6nk+2hm5iZnx737ZqxFgksPl3+OY1cP8
0s
1amXuUrwBp3/MUODEP5E51lzqjO0w5kyJlvPjCiLg9UqS7JeY5yd/6xyGarsde26De
1E
rbVJ1uqnxyAOlV9A1hjBE8TbI+lyYBH+WezT0nySix6VBQTAWhv43r9lSudswYV80Q
```

```
==
---- END SSH2 PUBLIC KEY ----
```

The following is the public key after:

- Removing text that is not part of the public key
- Rmoving line breaks at the end of each line
- Adding `ssh-rsa` at the beginning of the public key.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDJhJ6nk+2hm5iZnx737ZqxFgksPl
3+OY1cP80s1amXuUrwBp3/MUODEP5E51lzqjO0w5kyJlvPjCiLg9UqS7JeY5yd/6xy
Garsde26De1ErbVJ1uqnxyAOlV9A1hjBE8TbI+lyYBH+WezT0nySix6VBQTAWhv43r
9lSudswYV80Q==
```

6. Test the connection using your current login:

```
ssh -l root <netapp address> sysconfig -A
```

You should obtain the output from that command without being prompted for a password

INSTALLING THE NETAPP AGENT – SOLARIS

If you have not already installed the GSMbase and GSMlmutil packages, install these packages before you install the NetApp Agent. Refer to the *Installation* chapter for step-by-step instructions on installing GSMbase and GSMlmutil on a Solaris server

1. Insert the Sun StorageTek Business Analytics Solaris Local Manager Installation CD into the CD-ROM drive.
2. Mount the CD using the command:

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

3. Change to the directory corresponding to the host's Solaris Operating System version.
4. Run the package installation utility. The main package installation menu is displayed.

```
pkgadd –d .
```

5. Select to install the **GSMnetapp** agent; type the option number and press **Enter**.
6. Specify whether (y/n) ssh is installed. If not, it is assumed that rsh is installed.
7. Specify the IP address of the NetApps array and press **Enter**.
8. Specify the user name to be used for authentication to the filer.
9. Specify that user's password.
10. Specify the SNMP Read community string or press Enter to select public.
11. Confirm the SNMP Read community string that you entered.
12. Repeat the above steps for each NetApps filer. Press **Enter** on a blank "IP address of NetApps array?" line to indicate you have finished configuring filers and to continue.

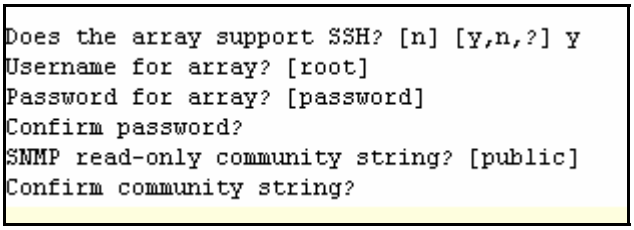


Figure 3 - Configure NetApp Agent on Solaris

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

    - Specify whether (y/n) the Agent Monitor will restart the agent if it is detected as not running.
    - Specify the frequency the agent collects disk performance data. The default value is 1800 seconds.
    - Specify how long the performance data is cached. The default value is 600 seconds.
    - Specify the frequency the controller performance data is collected. The default value is 600 seconds.
    - Specify the data collection timeout; the default timeout is 10 seconds.
    - Specify whether (y/n) agent auto registration is enabled.
    - Specify the IP address or network resolvable host name for the Local Manager to be contacted for agent auto registration.
    - Specify the TCP port number the Local Manager uses for agent auto registration. The default port is 17146.

14. Specify whether (y/n) to restart the installed agents after the installation is finished.

15. Specify whether to install (y/n) conflicting files, if prompted. The installation program displays the files that exist.

16. Specify whether (y/n) to continue with the agent's installation.

17. If continued, the installation proceeds and returns you to the main package installation menu.

18. Select another agent package for installation, or type **Ctrl-D** and **q** to exit the package installation menu.

STORABILITY CELERRA AGENT

The Storability Celerra Agent reports configuration, allocation, and performance information on EMC Celerra systems. Refer to the *Sun Storagetek Business Analytics Support Matrix* to obtain the latest information on the agent's software and hardware requirements. The agent can communicate to the array via one of the following access methods: RSH, SSH, or Telnet.

CELERRA AGENT MATRIX

Feature	Description
Support Prerequisites	
Verify Telnet, RSH or SSH access to the Control Stations	• SSH client is a prerequisite and is supported. However, Cygwin SSH Client on any NAS agent installation and configuration is not supported by StorageTek. It is only supported for the Storability Compaq (HSG80) Agent. • Refer to the **Requirements to Use Telnet, RSH, and SSH Protocol** sections that follow.

IP address/addresses or host names of the Control Station(s)	`ping <ip_address> CS1`
	Or:
	`ping <ip_address> CS2`

Verify Call Home set up	EMC Celerra administrator
Verify Celerra files located in the default /nas directory	EMC Celerra administrator
Agent Installation	
Windows	• Windows Local Manager Installation CD (InstallShield) • Windows administrator privileges
Solaris	• Solaris Local Manager Installation CD (package installation) • root user account
Configuration Parameters	
IP Addresses/Host Names	One or two IP addresses/host names to communicate with the Celerra Control Station(s)
User Name	User name for agent authentication to the Control Station

Password	Password for agent authentication (only needed for Telnet access method)
Local Manager	Network resolvable host name or IP address of the Local Manager with which the NAS agent is to register if auto registration is enabled.
Local Manager Port	Local Manager's TCP port number; default value is 17146.
Enable Auto Registration	Specifies auto registration is enabled (true) by default; set to false to disable auto registration.

EMC CELERRA AGENT ACCESS METHOD

The Sun StorageTek Business Analytics Celerra Agent collects data from the Celerra Control Station using one of three supported protocols:

- ssh (secure shell)
- rsh (remote shell)
- telnet

Note: The agent requires only one of these three communications protocols. The requirements for each are described in the next section.

CELERRA AGENT PREREQUISITES

The Celerra Agent requires login access over the network to the command line of the primary Celerra Control Station. The agent requires either one or two IP addresses or hostnames of the Control Station(s) for each Celerra. If two addresses are supplied, they are entered as a comma-separated list (e.g. cs0, cs1).

If the Celerra has only one Control Station, specify only one IP address for that Control Station to the agent (even if it has multiple interfaces) through the agent configuration in the storability.ini file. If the Celerra has two Control Stations installed and they are configured to share a virtual IP address that is guaranteed always to connect to the current primary (active) control station, specify that single virtual IP address to the agent. Otherwise, supply two comma-separated IP addresses -- in this case, the first IP address must identify the Control Station in slot 0, and the next IP address must identify the Control Station in slot 1. When two addresses are supplied, the agent will dynamically determine which Control Station is the primary control station, and will obtain all configuration information from that Control Station.

CALL HOME CONFIGURATION

The Celerra Agent requires that the /nas/sys/callhome.config file on each Celerra Control Station has been set up properly by EMC support. Specifically, the last line of this text file must contain the Celerra serial number, which begins MLxxxxxx (e.g.

ML123456789). The agent requires a serial number to identify the Celerra uniquely. If this file does not contain the serial number, locate the serial number beginning "ML" on the Celerra cabinet and manually add it to the end of this file using a text editor, such as "vi".

CELERRA FILES

The Celerra Agent currently requires all Celerra-related files to have been installed in the /nas directory on the Control Station(s), which is the default installation directory on a Celerra Control Station. If the /nas directory does not contain the files, create a symbolic link on the Control Station from /nas to wherever the real nas directory is located to meet this requirement.

The agent also requires the following lines to be added at the beginning of the **.bashrc** file in the nasadmin user's home directory on each Control Station. The **NAS_DB environment** variable needs to be set for some commands to work, but the non-interactive login used by the "rsh" and "ssh" methods may not necessarily have set up this variable.

```
NAS_DB=${NAS_DB:-/nas}
export NAS_DB
```

REQUIREMENTS TO USE TELNET PROTOCOL

The Celerra Agent requires telnetd to be enabled on the Celerra Control Station(s). This is normally enabled. Check and verify using the chkconfig --list command, as described below for rshd.

Using the Telnet protocol also requires the username (e.g. nasadmin) and password for login access to the Control Station(s). If security is an issue, be aware that the Username and password are transmitted to the Control Station in clear text over the network.

REQUIREMENTS TO USE RSH PROTOCOL

The Celerra Agent requires an external rsh client program to handle the communications. On Windows, this is normally available in: C:\WINNT\System32\rsh.exe. On UNIX servers, this program is normally located in the directory: /usr/bin/rsh.

The Celerra Agent requires rshd to be enabled on the Celerra Control Station(s). This is normally disabled by default as rshd is an insecure service. To enable rshd:

1. Log in to each Celerra Control Station.
2. Switch user (su) to root.
3. Enable the rshd daemon.

Enabling rshd

The instructions below assume "xinetd" is in use, which is the case on newer model Celerra Control Stations.

1. From the command line, run the command

```
chkconfig --list
```

In the command output, look for the rsh service under xinetd services:

```
xinetd based services:
      linuxconf-web:  off
```

```
rexec:  off
rlogin: off
rsh:    off
```

If rsh is "on", there is no need to change it. If rsh is "off", enable it by doing the following:

2. Switch user ("su") to the root account.

3. Open and then edit the xinetd service definition for rsh:

```
su - root
cd /etc/xinetd.d
vi rsh
```

The file should look something like the following:

```
service shell
{
flags         = REUSE
socket_type   = stream
 protocol      = tcp
  ...
 disabled = yes
  ...
}
```

Change the line containing disabled to

```
disabled      = no
```

Note: The "shell" service has no authentication. However, you can enhance the security of this environment by adding source address filtering on the rsh connection source address. To do so, add a line like the following to this section, where, for example, 10.255.252.150 is the numeric IP address where the agent will run.

Multiple addresses may be specified on a single line, or multiple only_from lines may be added, or /24 may be appended to an IP address to grant access to a subnet. For example, add the entry:

```
service shell
{
 ...
only_from = 10.255.252.150
   ...
}
```

4. When you have completed the changes, save the file.

5. Identify the process ID (PID) of the xinetd process:

```
ps -elf | grep xinetd
```

6. Send that process a USR1 signal to force xinetd to reread its configuration file:

```
kill -USR1 <pid >
```

7. Use the **chkconfig --list** command to verify that rsh is now "on".

8. Verify by running the netstat -a | grep shell to verify that the "shell" port is now being listened on:

```
netstat -a | grep shell
*.shell              *.*                0      0      0      0
LISTEN
```

9. From a separate system, attempt an rsh connection to the Control Station. For example, type:

```
rsh cs0 -l nasadmin date
```

   You will probably receive a "permission denied" message at this point, which is good. If instead you get a timeout, re-check the configuration process.

   Note: When testing, always supply a command to "rsh", such as "date". Without a command, you are actually running rlogin, which connects to a different port than rsh.

When Connecting Via rsh

The Celerra Agent requires a username on the Celerra Control Station (e.g. nasadmin) but does not use a password. This requires that password-less access is set up from the host and username running the agent to each Control Station. To meet this requirement, you create an appropriate .rhosts entry in the Celerra user's home directory (e.g. /home/nasadmin or ~nasadmin).

To create a .rhosts file entry:

1. On the host on which the Celerra Agent will run, log in to the Celerra using the username that will be used for remote access (e.g. "nasadmin").

2. Identify the canonical hostname by which the Celerra Control Station recognizes the system where the agent is running. To do so, type the command:

```
who am I
```

3. The hostname or IP address displayed may be copied and pasted into the .rhosts file. Be aware that very long hostnames will be truncated and you will have to fix that manually. Alternatively, make sure there is an entry in the Control Station's /etc/hosts for the system where the agent is running, and use the exact hostname shown in /etc/hosts.

4. Create an entry in .rhosts containing the canonical hostname followed by the username under which the agent is running. On Windows, this username usually will be "SYSTEM", and on UNIX it will usually be "gsm", although these are configurable. For example:

```
<windowshostname> SYSTEM
<UNIXhostname> gsm
```

5. Add an additional entry allowing access from your interactive login name (this is especially important on Windows since you cannot log on as SYSTEM to test):

```
<agenthostname> Administrator
<UNIXhostname> root
```

6. Run "ls -l .rhosts" to make sure the .rhosts file is owned by the correct Celerra username (e.g. nasadmin) and is only writable by that user. If not, run "chown nasadmin .rhosts" and "chmod 640 .rhosts" to fix the permissions.

7. From the agent system, test running a remote command on the Control Station (e.g. cs0):

```
rsh cs0 -l nasadmin date
```

If the test command fails with a "permission denied" error, the format of the .rhosts file is most likely incorrect. If the command times out, most likely the rshd is not running. Check the Control Station message logs for additional hints.

REQUIREMENTS TO USE SSH PROTOCOL

Using ssh for the Celerra Agent requires that sshd is running on the Celerra Control Station(s). This communication protocol is usually installed and running by default. To verify, run the **chkconfig --list** command and look for a line starting with sshd. This line will normally be listed above the xinetd section.

The Celerra agent also requires an external ssh client program on the system where the agent is installed. See the *Sun StorageTek Business Analytics Support Matrix* for the supported Ssh client software applications.

Additional requirements are described as follows:

- Requires a username for the Celerra Control Station (e.g. nasadmin) but no password.
- Requires the Control Station sshd to accept public key login (this is normally enabled by default).
- Requires password-less public key login access to be set up to this account from the username under which the agent is running (e.g. "SYSTEM" on Windows, or "gsm" on UNIX). The details of setting up such access are version-specific. Specific examples are shown below.
- Protect the private key file from unauthorized users

WINDOWS WITH SSH CLIENT

With any version of SSH for Windows, the main complication when setting up public key access is that the Storability Celerra Agent service normally runs as the local SYSTEM account, which is not a login account. Therefore, setting up public key authentication to work properly and testing is necessary.

One approach can be to run the service as a special local administrator account, with a password that will not change or expire. The service user and stored password can be changed through the services applet. You can then log on as that user to set up the public key credentials and test the connection before running the service.

Frequently, security regulations prohibit setting up such accounts for services. The alternative, setting up public key authentication for the SYSTEM user, is described below.

WINDOWS WITH COMMERCIAL SSH.COM SSH CLIENT VERSION

A configuration example for Windows with Commercial ssh.com Client Version 3.x follows. The example uses the following assumptions (replace as necessary):

- Either you are logged in as the account that the agent will run as, or the agent runs as SYSTEM
- Logged on to Windows as a local administrator
- ssh.com client software is installed and on your PATH
- Control Station hostname is cs0

Run the following commands as local Administrator or a local account in the administrators group.

1. If your current Windows account already has DSA public key / private key identity files, you may want to reuse them instead of replacing. Otherwise, create a DSA public key / private key pair for the current user with the following command:

   C:\>ssh-keygen2 -t dsa -b 1024

   Command output appears similar to the following:

   Generating 1024-bit dsa key pair

   4 .oOOo.oOo.oO

   Key generated.

   1024-bit dsa, Administrator@winsys1, Fri Dec 05 2003 19:17:21

2. Press RETURN when asked for the passphrase -- the agent must work in batch mode, which is incompatible with a passphrase. Command output similar to the following appears:

   Private key saved to C:/Documents and Settings/Administrator/Application Data/SSH/UserKeys/id_dsa_1024_a

   Public key saved to C:/Documents and Settings/Administrator/Application Data/SSH/UserKeys/id_dsa_1024_a.pub

3. Using ssh2 from the command line, log in to each Celerra Control Station to be managed (using password authentication) in order to populate the local hostkeys database with the appropriate keys. For example:

   ```
   ssh2 -l nasadmin cs0 date
   ( enter password)
   ```

4. If running the agent as SYSTEM, copy the following files from C:\Documents and Settings\Administrator\Application Data\SSH to C:\Documents and Settings\Default User\Application Data\SSH:

   ```
   UserKeys\id_dsa_1024_a
   UserKeys\id_dsa_1024_a.pub
   HostKeys\*.pub  (one public key file for each Celerra Control Station from the step above)
   ```

   Note: The SYSTEM account does not have an SSH application data directory, and simply creating the directory will not cause ssh to use it.

5. If running the agent as SYSTEM, check permissions on the file "C:\Documents and Settings\Default User\Application Data\SSH\UserKeys\id_dsa_1024_a" and verify that it is readable or writable by Administrators and local SYSTEM and no other

users. In addition, check permissions on the UserKeys directory and verify it is only readable or writable by Administrators and local SYSTEM.

6. For each Celerra Control Station, copy the resulting id_dsa_1024_a.pub file (the public key) to the Celerra Control Station. Do not copy the private key file (id_dsa_1024_a), only the public key file. This file does contain line breaks.

7. Log in interactively on the Celerra.

8. Create the .ssh directory in the nasadmin home directory, if it does not already exist. For example:

```
mkdir .ssh
chmod 700 .ssh
```

9. Translate the ssh.com-format public key to the format used by OpenSSH. The recommended way to do this is using OpenSSH "ssh-keygen" on the Celerra Control Station:

```
ssh-keygen -i -f id_dsa_1024_a.pub >> .ssh/authorized_keys
```

   Be especially careful to append >> not overwrite the .ssh/authorized keys file if it already exists. Overwriting the file would interfere with any other users' access to this account using ssh.

10. Verify using the **ls -l** command that the .ssh/authorized_keys file is only writable by the nasadmin user. Correct the permissions if necessary using chmod. For example:

```
chmod 600 .ssh/authorized_keys
```

11. Log out from the Celerra Control Station.

12. Verify that password-less access is now allowed from your current account to the nasadmin account:

```
ssh2 -l nasadmin cs0 date
```

    You should not be prompted for a password, and the date should be displayed. If this works, the agent should work over the ssh protocol also without any additional configuration options.

13. If Step 12 does not work properly, run in verbose mode to see where the problem lies:

```
ssh2 -v -l nasadmin cs0 date
```

    If the keys are set up properly, options may need to be adjusted in either the local ssh_config or the remote Control Station's sshd_config. If any command line ssh options are needed to establish a connection, those command-line options must be provided in the storability.ini file as SSH_CMD_OPTION values.

SOLARIS WITH OPENSSH CLIENT VERSION

A configuration example for OpenSSH Client Version 3.x on Solaris follows. The example uses the following assumptions (replace as necessary):

- Agent runs as gsm with home directory /opt/storability/gsm

- Celerra username is nasadmin
- OpenSSH is installed.
- Control Station hostname is called cs0.

You run the following commands logged in using the gsm user id. For example:

```
su root
su - gsm
```

1. Create a dsa public key / private key pair for the gsm user with the following command. **Note**: Accept the default keyfile location. Press ENTER when asked for the passphrase -- the agent must work in batch mode, which is incompatible with a passphrase.

   ```
   ssh-keygen -t dsa
   ```

   Generating public/private dsa key pair.

2. When prompted to "Enter file in which to save the key (/opt/storability/gsm/.ssh/id_dsa):", accept the default location.

3. When prompted to "Enter passphrase (empty for no passphrase):" press ENTER.

4. When prompted to "Enter same passphrase again:", press ENTER. Command output similar to the following is displayed:

   Your identification has been saved in /opt/storability/gsm/.ssh/id_dsa.

   Your public key has been saved in /opt/storability/gsm/.ssh/id_dsa.pub.

   The key fingerprint is:

   27:0a:c3:58:2d:91:db:0f:c1:df:0b:97:72:49:91:cb gsm@yourhost

5. From the command line, use ssh to log in or run a remote command on each Celerra Control Station to be managed (using password authentication) in order to populate the ssh hostkeys database with the appropriate keys. For example:

   ```
   ssh -l nasadmin cs0 date
   (enter password to log in)
   ```

6. Copy the resulting id_dsa.pub file (the public key) to the Celerra Control Station. Do not copy the private key file (id_dsa), only the public key file. The format of this file is one very long line; using copy-and-paste is not advised. You can copy the file with "scp" or any other file transfer protocol.

7. On the Celerra Control Station, log in as nasadmin and append the file you just copied to the file .ssh/authorized_keys in the nasadmin home directory.

8. If the .ssh directory does not exist, create it, making sure it is only writable by the nasadmin user. For example:

   ```
   mkdir .ssh
   chmod 700 .ssh
   ```

9. If the file .ssh/authorized_keys does not already exist, create it. If it already exists, you must append to this file to avoid interfering with other ssh users' access.

Warning: Do not overwrite an existing authorized_keys file or you will interfere with other ssh users' access to the account. For example:

```
cat id_dsa >> .ssh/authorized_keys
```

10. Verify with **ls -l** that the .ssh/authorized_keys file is only writable by the nasadmin user. Correct the permissions if necessary using **chmod**. For example:

```
chmod 600 .ssh/authorized_keys
```

11. Log out from the Celerra, and verify that password-less access is now allowed from the gsm account to the nasadmin account:

```
ssh -l nasadmin cs0 date
```

You should not be prompted for a password, and the date should be displayed. If this works, the agent should work over the ssh protocol also without any additional configuration options.

12. If Step 11 does not work properly, run ssh in verbose mode to see where the problem lies:

```
ssh -v -l nasadmin cs0 date
```

Some other useful checks are described as follows:

- Double-check the permissions on the authorized_keys file. The OpenSSH sshd requires that only the owner has write access to this file, or it will not grant access.

- If the keys are set up properly, options may need to be adjusted in either the local ssh_config or the remote Control Station's sshd_config. If any command-line ssh options are needed to establish a connection, those command-line options must be provided in the storability.ini file as SSH_CMD_OPTION values. See sample options in the following section.

ADVANCED STORABILITY.INI OPTIONS FOR SSH SUPPORT

Any option that could normally be passed by the -o switch on the ssh or ssh2 command line may be passed through the storability.ini as an SSH_CMD_OPTION value. The following are particularly useful:

- SSH_CMD_OPTION = BatchMode=yes

  For most versions of SSH, this will avoid interactive questions that could interfere with operation as a service.

- SSH_CMD_OPTION = StrictHostKeyChecking=no

  This option prevents changes in the remote system's host key from preventing ssh login, which will cause the agent connection to fail. It is usually safe to skip host key checking on a trusted internal network. Because the agent only uses public key authentication, this option can also be helpful when running the agent as SYSTEM on Windows.

- SSH_CMD_OPTION = VerboseMode=yes

  For ssh.com's version of ssh, this option turns on verbose messages which can help you to troubleshoot. The verbose messages may, for example, indicate that ssh is looking for the key file(s) in a different directory than expected. For this option to be effective, the agent must also be in debug mode, so the messages returned from ssh will be logged to Message.log.

- SSH_CMD_OPTION = LogLevel=VERBOSE

  For OpenSSH, turns on verbose messages for troubleshooting. Can be set to DEBUG for greater verbosity. For this to be effective, the agent must also be in debug mode, so the messages returned from ssh will be logged to Message.log

- SSH_CMD_OPTION = IdentityFile=pathname

  This option specifies a non-default identity file to use for public key authentication. For OpenSSH, this should be the full pathname to the private key file you want to use for the connection. For commercial SSH this is the name of a file that contains the location of the private key file you want to use for this connection, in the format:

  ```
  idkey   directory/filename
  ```

  Note that commercial SSH looks for this file in the default directory location for the current user. Commercial SSH 3.2.3 will only accept a full pathname in a UNIX format beginning with a /. For example:

  /Documents and Settings/SYSTEM/SSH/Identity

  which will be interpreted as a pathname on the same drive as the agent is installed.

INSTALLING THE CELERRA AGENT - WINDOWS

The following section describes how to install and configure the Celerra Agent on a Windows platform.

1. Insert the Sun StorageTek Business Analytics Windows Local Manager Installation 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. Check the **Celerra Agent** checkbox on the screen that lists agents for installation.

6. Review the settings and click **Next>**.

7. If prompted, specify whether (yes/no) to install the new version of the Configuration Tool.

8. When the Configuration Tool is automatically launched, select **File** -> **Edit** -> **Smart Agent Configuration**.

9. Click the **Celerra Agent** tab.

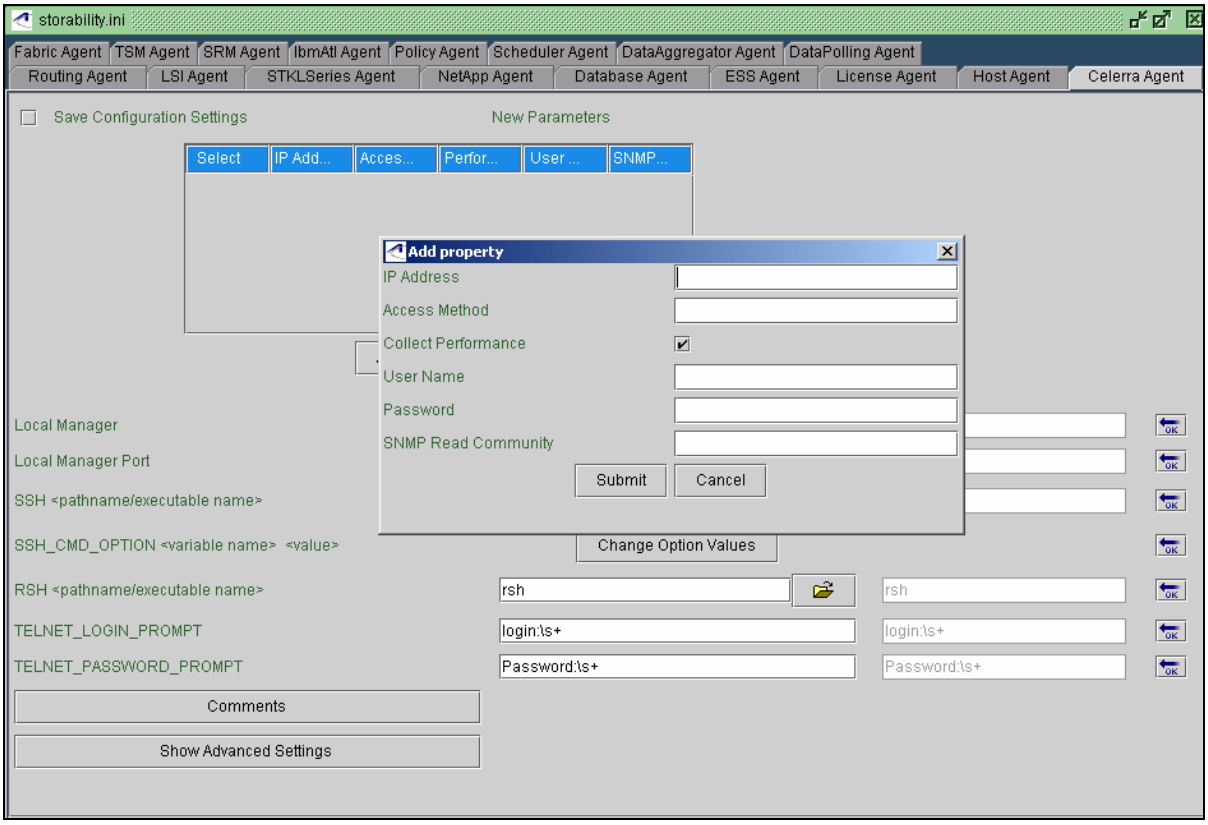


Figure 4 - Celerra Agent Configuration Window

10. Click **Add** and the **Add Property** dialog box appears. For each Celerra, enter the following information and then click **Submit**:

    - **IP Address** - Enter one or two addresses or hostnames of the Control Station(s) for this Celerra. If two addresses are specified, separate the addresses by a comma. The first address must be for the Control Station in Slot 0, and the second address is for the Control Station in Slot 1.

    - **Access Method** – Specify the communication protocol to log in to the Control Station(s); the communication protocol is ssh, rsh, or telnet.

    - **Collect Performance** – Uncheck the box, as this release does not support performance collection.

    - **Username** – Enter the User Name used to log in to the Control Station (e.g., nasadmin).

    - **Password** - Is required only for telnet. For rsh, this field is ignored and should be left empty. For ssh, it is interpreted as a non-default identity key file pathname, or may be left empty to use the default identity key file.

    - **SNMP Read Community** - This field is currently unused and may be set to "public" or "snmp".

11. If using ssh as the communications protocol, click the **folder** icon next to the SSH <pathname/executable name> heading to locate and then set the fully qualified path name and ssh executable program name (e.g., C:\Program Files\SSH Communications Security\SSH Secure Shell\ssh2.exe).

12. If using ssh communications protocol, click the **Change Options Values** tab and the Enter SSH Command Option dialog box appears. Enter ssh -o style command-line options that may be necessary to customize this connection. Multiple SSH_CMD_OPTION entries may be specified, one per line. See the earlier section on "Advanced storability.ini Options for SSH Support" for details.

13. Click **Submit** after you have finished entering the options.

14. If using rsh as the communications protocol, click the **Folder** icon next to the RSH <pathname/executable name> heading to locate and then set the fully qualified path name and rsh executable program name (e.g., C:\WINNT\System32\rsh.exe).

15. If using telnet as the communications protocol, specify the command terminator (e.g., login:\s+) to support sending a user name to log in using non-interactive mode.

16. If using telnet as the communications protocol, specify the command terminator (e.g., Password:\s+) to support sending a password using non-interactive mode.

17. In the **Local Manager** field, specify the network resolvable host name or IP address of the Local Manager with which the Celerra Agent is to register if auto registration is enabled.

18. In the **Local Manager Port** field, specify the TCP port number the Local Manager uses for agent auto registration. The default port is 17146.

19. Click **Show Advanced Settings** and review/modify the following configuration variables:

    - **Enable Auto Registration** - Accept that auto registration is enabled (true) or set to false to disable auto registration.

    - **CONFIG_CACHE_REFRESH_INTERVAL**– Specify the frequency the agent queries the Celerra Control Station(s) to refresh its data in seconds. This sets an approximate maximum age for the data that will be returned by the agent. The default value is 1200 seconds.

    - **PERF_SAMPLE_INTERVAL** - Since performance is disabled, this value is currently ignored.

    - **PERF_AVERAGE_INTERVAL** – Since performance is disabled, this value is currently ignored.

    - **ARRAY_STATUS_CHECK_INTERVAL -** Specify the frequency with which the agent will check and rebuild its list of accessible or responding control stations. The default value is 3600 seconds.

    - **CMD_EXECUTION_TIMEOUT –** Specify the amount of time to wait for the remote Celerra commands to finish. The default value is 900 seconds.

    - **MAX_EXECUTION_THREADS –** Specify the maximum number of Celerras we will process at any given time. The default value is four (4).

20. With "Save Configuration Settings" turned on (check mark), select **File->Save** and then confirm changes to the storability.ini file.

21. Select **File->Exit** to close the Configuration Tool.
22. Use the Windows **Services** panel to start the agent before you verify agent functionality.

INSTALLING THE CELERRA AGENT - SOLARIS

1. Mount the Sun StorageTek Business Analytics Solaris Local Manager Installation CD on the Solaris server. For example:

```
mount -F hsfs -o ro /dev/dsk/c0t6d0s0 /mnt
```

2. Change directory to the UNIX directory for the Solaris operating system.

3. Run the pkgadd command. The main package installation menu is displayed.

```
pkgadd -d .
```

```
The following packages are available:
 1  GSMacsls      Storability GSM STK/ACSLS Library Agent
                  (sparc) prod-4.0.36-qa
 2  GSMbase       Storability GSM base
                  (sparc) prod-4.0.36-qa
 3  GSMclarii     Storability GSM Clariion Agent
                  (sparc) prod-4.0.36-qa
 4  GSMclra       Storability GSM EMC Celerra Agent
                  (sparc) prod-4.0.36-qa
 5  GSMcpq        Storability GSM Compaq StorageWorks Agent
                  (sparc) prod-4.0.36-qa
 6  GSMcpqeva     Storability GSM Compaq EVA Agent
                  (sparc) prod-4.0.36-qa
 7  GSMdb         Storability GSM Database Agent
                  (sparc) prod-4.0.36-qa
 8  GSMess        Storability GSM ESS Array Agent
                  (sparc) prod-4.0.36-qa
 9  GSMhds        Storability GSM Hitachi Agent
                  (sparc) prod-4.0.36-qa
10  GSMhicmd      Storability GSM HiCommand Array Agent
                  (sparc) prod-4.0.36-qa
```

Figure 5 - Select Celerra Agent Package

4. Type the package selection number (Option 4) for the Celerra Agent (GSMclra) and press **Enter** to select installing this agent.

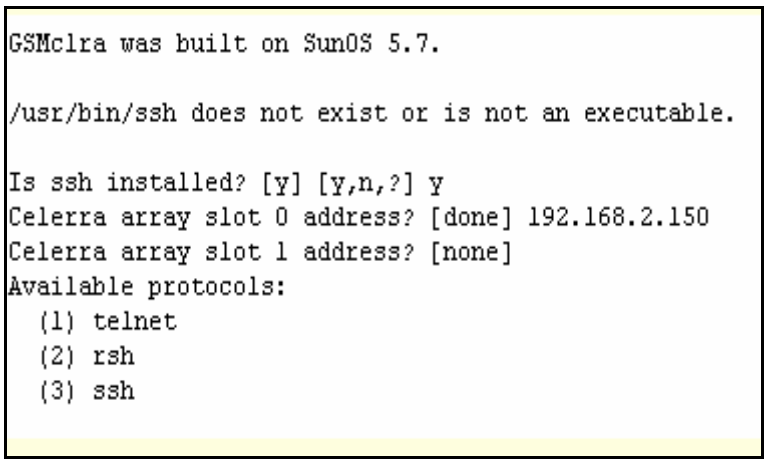


Figure 6 - Celerra Agent Package Install

5. Specify (y/n) whether SSH is installed and press Enter.

6. Type the IP address for the Control Station in Slot 0 and press Enter.

7. Type the IP address for the Control Station in Slot 1 (if installed) and press **Enter**. If there are redundant control stations, the agent will automatically determine which Control Station is primary and which is the Standby.

8. Specify the available protocol that the agent will use and **Enter** press.

9. Specify the username or press Enter to specify the default user name, nasadmin.

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

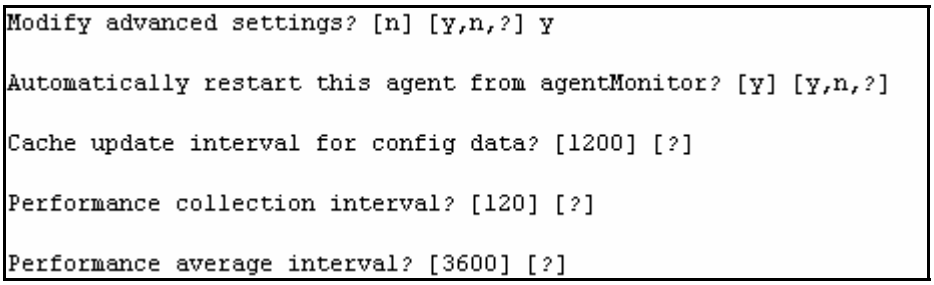


Figure 7 - Celerra Agent Advanced Settings

11. Specify whether (y/n) to have the Agent Monitor restart the agent if it is detected as not running.

12. Specify the frequency that the agent cached configuration data is refreshed. The default value is 1200 seconds.

13. Specify how often performance data is collected. This value is not currently used as the collection of performance data is not supported.

14. Performance average interval is also not currently used.

15. Specify how often the agent checks the status of the array. The default value is 3600 seconds.

16. Specify the command execution timeout; the default value is 120 seconds.

17. For Enable agent auto registration, press Enter to accept that it is enabled (default), or type n and press Enter to disable agent auto registration.

18. Specify the IP address or network resolvable host name of the Local Manager to be contacted for agent auto registration.

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

20. Specify whether (y/n) to start all the agents on the server after the installation has completed.

21. If prompted, example any file conflicts and specify whether (y/n) to proceed with the installation.

22. The installation will complete and return you to the main package installation menu.

23. Enter the number for any other package you wish to install, or type **Ctrl-D** and enter **q** to quit.

VERIFYING NAS AGENT

Use the GSM Agent Diagnostic Tool (GSMDiag**)** to verify the NAS Agent functionality. GSMdiag is installed as part of the 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 the Storability NAS Agent has started 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 17136 (Celerra Agent) or 17150 (NetApp Agent) or select the respective 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 NAS Agent.

    e. Select the **gsa_nas_config** object and verify that data is returned.

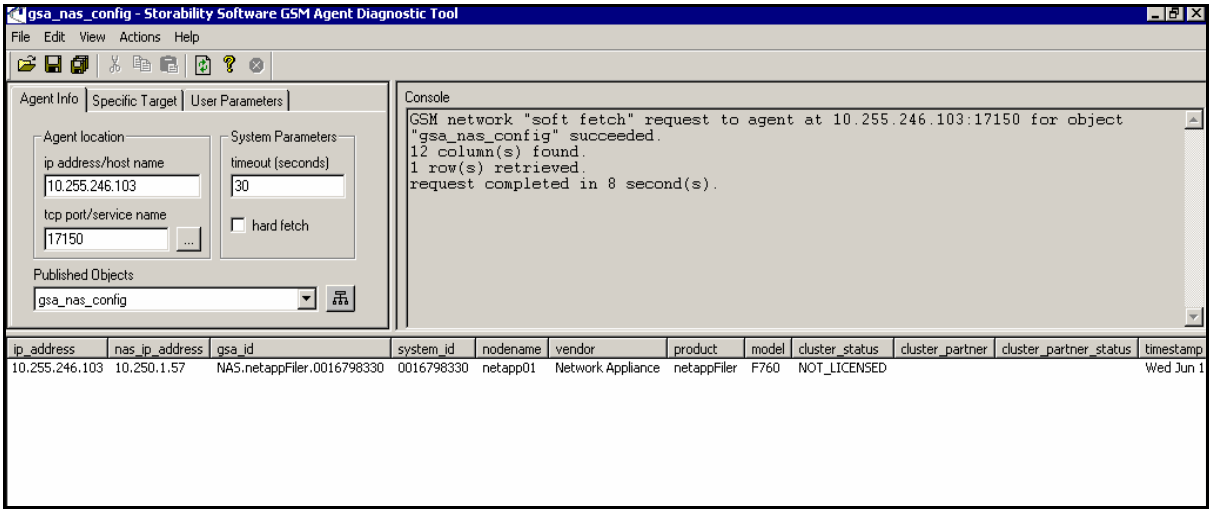


Figure 8 – Sample NAS Configuration Object

f. Verify all other objects published by the agent.

2. To verify the NAS 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.

   b. Set the port to 17146 (or select the Storability Routing 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 Routing Agent.

   d. Select the **gsa_agent_register** table.

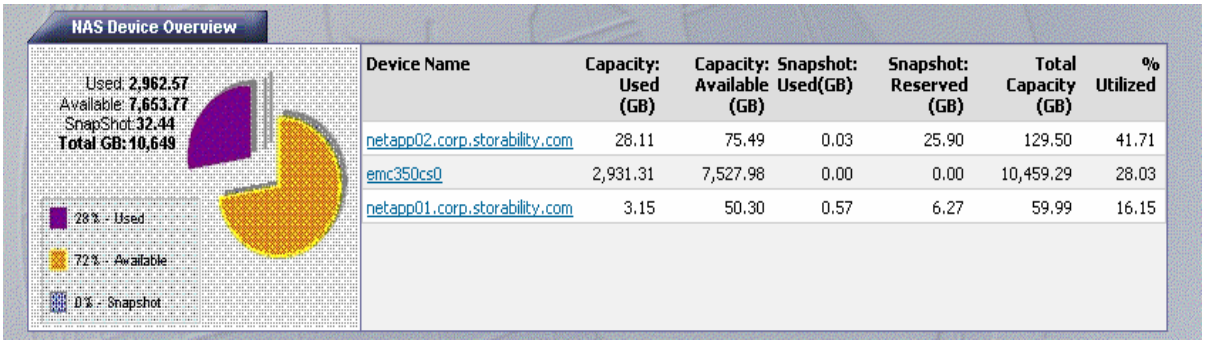
   e. Verify this collected object reports the NAS Agent in the "active_peer" field by IP address and port number of 17136 (Celerra Agent) or 17150 (NetApp Agent).

VERIFYING MANAGEMENT CONSOLE FUNCTIONALITY

The following procedure describes how the administrator verifies the NAS 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 **Data Polling Schedule** 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.**
3. Use the **Collect Now** button to collect the **NAS** (collection type) **Filesystem** (Collection Metric) data using a polling schedule that includes all sites.
4. Use the **Collect Now** button to collect the **NAS** (collection type) **Configuration** (Collection Metric) data using a polling schedule that includes all sites.
5. Use the **Collect Now** button to collect the **NAS** (collection type) **Logical VM** (Collection Metric) data using a polling schedule that includes all sites.
6. Close the **Data Polling Schedule** window.

7. Refresh the browser (e.g., pressing F5) and the **NAS Device Overview** pane should display information on the NAS device.



Device Name	Capacity: Used (GB)	Capacity: Available (GB)	Snapshot: Used(GB)	Snapshot: Reserved (GB)	Total Capacity (GB)	% Utilized
netapp02.corp.storability.com	28.11	75.49	0.03	25.90	129.50	41.71
emc350cs0	2,931.31	7,527.98	0.00	0.00	10,459.29	28.03
netapp01.corp.storability.com	3.15	50.30	0.57	6.27	59.99	16.15

Figure 9 - NAS Device Overview

8. Click the **Device Name** link and the Detailed NAS Configuration (tabular) report is displayed.
9. After you generate the tabular reports (e.g., Components), close the browser session with the Management Console as the above steps complete verifying the Management Console functionality.

NAS 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.
2. Use the **Agent Diagnostic Tool** to save the output for all the tables if escalating a problem to Sun Technical Support.
   a. Run the GSM Agent Diagnostic Tool (gsmdiag.exe).
   b. Enter the **IP Address** or **Hostname** of the server where the agent is installed and set the port by selecting the NAS 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 NAS Agent. If unsuccessful, verify the Ethernet connectivity to the server running the Storability NAS Agent and that the Storability NAS Agent is running.
   d. Select the **alerts** 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**.

3. **Review the Message Log** – Review/collect the agent's 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 <NAS Agent> Agent folder.

- Can enable debug level logging by appending **LOG_SEVERITY=Debug** to the NAS Agent section of the storability.ini file (if Sun Technical Support 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 your support representative requests it).

4. **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.
5. **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 NAS Agent and registration information.
6. **Confirm Polling Schedules** – Using the Management Console's **Data Polling Schedule** menu, review/modify the existing Polling Schedules for the Collection Type of NAS for all sites.
7. **Review Aggregator Message Log** – Open the Aggregator's Message Log in a text editor and validate that the NAS 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 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.

8. **Check the assurent database** – The assurent database is the data repository for your Business Analytics application. Use any MS SQL Query interface, such as osql, to verify rows have been inserted into the NAS-related tables, such as the **gsa_nas_config** table.
9. **Verify Management Console Functionality** – As a final step in the agent troubleshooting procedure, minimally verify that the **NAS Device Overview** pane on the home page is now populated with data.

Upgrade NAS Agent

To upgrade a NAS Agent, you perform the following tasks:

1. Uninstall the currently installed NAS Agent.
2. Upgrade by installing the current version of the NAS Agent.

Uninstall NAS Agent - InstallShield

1. Select **Start->Program Files->Storability->Uninstall->Uninstall Local Manager**
   Or:
   Start->Program Files->Storability->Uninstall->Uninstall <NAS Agent Name>. The Storability **Uninstall** dialog appears.
2. Click the checkbox for the appropriate NAS Agent.
3. Click **Next>**. The **Question** dialog appears.
4. Click **Yes** to confirm the uninstallation of the agent. An uninstalling agent splash box appears as each selected agent is uninstalled.
5. When the InstallShield Wizard Complete dialog box appears, click **Finish**.

Uninstall NAS Agent – Solaris

1. Type:

   ```
   pkgrm GSM<NAS_Agent_Name>
   ```

2. At the "do you want to remove this package" prompt, enter **y** and press **Enter**.

3. At the "do you want to continue the removal of the package?" prompt, type **y** and press **Enter**. The "Removal of GSM<NAS Agent Name> agent was successful" message should appear to indicate the package was removed successfully.