CHAPTER 6

Installing the Agent

An agent is a separate installation component of TES that runs jobs on behalf of the master. Offloading jobs to agents frees the master for intensive scheduling tasks such as production compiles. Agents exist for various platforms. Check with your sales representative for the current list of the types of agents available.

Prerequisites

OS	Version	Chipset	32-bit	64-bit	JVM	Processor	RAM	Disk
Windows	Server 2012	Intel/AMD	X	X	.NET 2.0	Pentium 800MHz	512 MB	100MB Disk (program & data)
Windows	Server 2008 Standard Edition	Intel/AMD	X	X	.NET 2.0	Pentium 800MHz	512 MB	100MB Disk (program & data)
Windows	Server 2008 Enterprise Edition	Intel/AMD	X	X	.NET 2.0	Pentium 800MHz	512 MB	100MB Disk (program & data)
Windows	Server 2003 (Cluster) PS Services Requires	Intel/AMD	X	X	.NET 2.0	Pentium 800MHz	512 MB	100MB Disk (program & data)
HPUX	11.11	PA-RISC	X		HP 1.7.0	100 MHz	512 MB	100MB Disk (program & data)
HPUX	11.23, 11.31	Itanium		X	HP 1.7.0	100 MHz	512 MB	100MB Disk (program & data)
AIX	6.1	PowerPC/RISC	X	X (32-bit emulation mode only)	IBM 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
								(Continued)

OS	Version	Chipset	32-bit	64-bit	JVM	Processor	RAM	Disk
AIX	5.3 TL 5, ~~6~~, 9, 10, 11	PowerPC/RISC	X	X (32-bit emulation mode only)	IBM 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Solaris	9	Sparc	X	X	Sun 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Solaris	10	Sparc	X	X	Sun 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Solaris	10	Opteron		X	Sun 1.5.0			
Linux	Redhat Enterprise Linux AS Release 4 & 5	Intel/AMD	X	X	Sun 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Linux	SUSE Enterprise Server v11	Intel/AMD	X	X	Sun 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Linux	Oracle Enterprise Linux 5.2 (Same as Redhat)	Intel/AMD	X	X	Sun 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Linux	openSUSE 10.2 (i586) - Kernel 2.6.18.8-0.9-default	Intel/AMD	X	X	Sun 1.5.0_14	100 MHz	512 MB	100MB Disk (program & data)
Linux	Cent OS 5.4	Intel/AMD	X	X	Sun 1.5.0	100 MHz	512 MB	100MB Disk (program & data)
Linux	Linux Kernel 269 or above	PowerPC	X	X	IBM Java 1.5	100 MHz	512 MB	100MB Disk (program & data)
zLinux	Suse SLES_ (Suse Linux Enterprise Server) R9 in a 32 bit image. Kernel level is 2.6.5-7.244+	zSeries	X	X	1.4+	100 MHz	512 MB	100MB Disk (program & data)
Tru64	5.1B	Alpha		X	HP 1.4.2_7+	100 MHz	512 MB	100MB Disk (program & data)
VMWare	ESX 3.0, ESXi 3.5, ESXi 4.0							
Microsft Virtual Server	2005							
OVMS	7.3+	Alpha		X	JVM 1.4+			
	8.2+	IA64						
								(Continued)
SCO,NSK, Parallel Virtuoso	Call					Call		
z/OS					JVM 1.4.2+			

Installing the Agent for Windows

Companies often need to provide centralized scheduling and administration of workloads that span multiple machines and multiple locations. TES master/agent architecture provides that capability.

In the basic TES network, the master uses a centralized database, containing all calendar and job scheduling information. One or more agent machines execute the production schedule. One or more client machines provides the TES user interface or console. The only prerequisite for the master/agent relationship is that the machine acting as the master must be on the same TCP/IP network as the machines serving as agents.

Scheduler provides agents for Windows environments and agents for Unix environments. This section discusses the Agent for Windows installation.

Installation Rights	Agent User Rights	Runtime User Rights
Local Administrator Able to access COM objects	Local System or if running under Domain\User must have local administrator rights including: • Logon as a service • Logon as part of the operating system • Replace a process token • Able to access COM objects On machines running Windows 2003 or later: • Bypass traverse checking • Adjust memory quotas for the process	• Logon as a batch job

Installing Agents

To install an agent:

Step 1 Load the installation DVD into your machine's DVD-ROM drive.

Note If you are not running the install from the installation DVD, skip to Step 4.

The Scheduler Installation screen displays.

Step 2 Click the **Tidal Agent for Windows** link.

Step 3 When the dialog box displays asking to save the file, click **Save File**.

Step 4 Double-click the *Agent_windows_TIDAL Agent.msi* file. The Security Warning dialog box displays.

Step 5 Click **Run**. The Status panel displays.

The Welcome panel displays.

Note If any other agents are running on the machine, a dialog box notifies you that the agent(s) must be stopped before the installation can continue.

Step 6 Click **Next**. The Choose Destination Location panel displays.

Step 7 Select the directory where the Scheduler files will reside:

- Click **Change** and select the appropriate file.

  -or-

- Accept the default location at *C:\Program Files*.

Step 8 Click **Next**. The Agent Port Number panel displays.

Step 9 Enter the port number that the agent will listen on. The default port is **5912**.

Step 10 Click **Next**. The Ready to Install the Program panel displays.

Step 11 Click **Install.**

Note Do not click **Cancel** once the installation process begins copying files in the Setup Status screen. Cancelling the installation at this point corrupts the installation program.

You will not be able to install the component without the help of Support. If you decide you do not want to install the component, you must complete the installation and then uninstall.

The Setup Completed panel displays.

Step 12 Click **Finish**.

Verifying the Installation

To verify installation:

Step 1 From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

Step 2 From the Services list, choose **AGENT_1**.

If the Tidal Service Manager displays the message *AGENT_1: Running* at the bottom, then the agent is running and the installation was successful.

Note If you want to edit the service parameters, click the ellipsis button to access the Service Configuration dialog box.

Configuring Agents

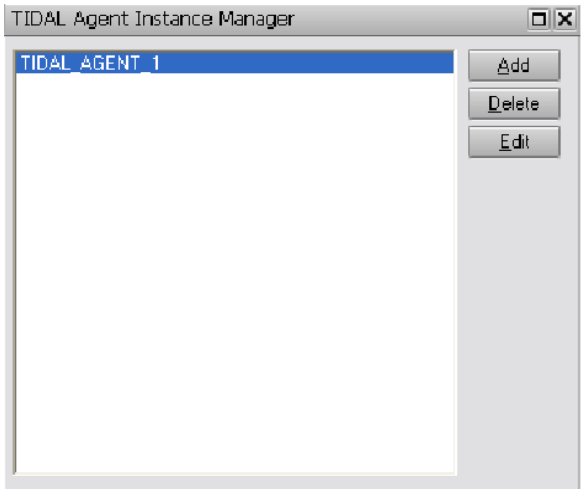
You can add and edit agent instances with the Agent Instance Manager.

Adding Agent Instances

To add an instance:

Step 1 From the Windows Start menu, choose **Programs > TIDAL Software > Agent > Instance Manager** to display the Instance Manager.

Figure 6-1 Tidal Agent Instance Manager



Step 2 Click **Add**. The following dialog box displays.

Figure 6-2 Tidal Agent Instance Manager 2

Step 3 Enter the following:

- Display Name – The name of the agent to add. The name in this text field is automatically generated as a possible candidate for the name of your agent. You can keep the name or change the name.
- Port – Select the port number the agent uses to listen for master connections.

Note Service Name is the name of the agent service. The name in this field is automatically generated and cannot be edited.

Step 4 Click **Save**.

Note To connect to the agent you just added, see "Defining an Agent Connection".

Editing Agent Instances

You can modify the port number and the name of the instance that is displayed but the service name remains the same.

Note The **Edit** button is unavailable as long as the agent is running.

To edit an instance:

Step 1 Stop the agent.

a. From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

b. From the Services list, choose **AGENT_1**.

c. Click **Stop**.

Step 2 Fromthe Windows Start menu, choose **Programs > TIDAL Software > Agent > Instance Manager** to display the Instance Manager.

Step 3 Select the instance.

Step 4 Click **Edit**. The Edit dialog box displays.

Step 5 Make the necessary edits, then click **Save**. The Information dialog box displays.

Step 6 Click **OK**.

Step 7 Re-start the agent.

a. From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

b. From the Services list, choose **AGENT_1**.

c. Click **Start**.

Deleting Agent Instances

Deleting agent instances does not delete the agent. Even if you delete all of the instances you must still uninstall the agent program to remove the agent.

Note The **Delete** button is unavailable as long as the agent is running.

To delete an instance:

Step 1 Stop the agent.

a. From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

b. From the Services list, choose **AGENT_1**.

c. Click **Stop**.

Step 2 Fromthe Windows Start menu, choose **Programs > TIDAL Software > Agent > Instance Manager** to display the Instance Manager.

Step 3 Select the instance.

Step 4 Click **Delete**. A confirmation message displays.

Step 5 Click **Yes**.

Note It is recommended that you do not delete the last agent instance called agent_instance_1. It is better to uninstall the agent program to remove the last agent instance. For instructions on how to uninstall the agent, refer to "Uninstalling Agents".

Note To delete an agent through the client, see "Defining an Agent Connection".

Configuring Agents for Windows

This section is optional.

After installing or adding agents, you can configure some Windows settings through the Services window, as documented below, or through the Tidal Services Manager as discussed in "Verifying the Installation".

To configure an agent for Windows:

Step 1 From the Windows Start menu, choose **Settings > Control Panel**.

Step 2 Double-click **Administrative Tools**.

Step 3 Double-click **Services**.

Step 4 Double-click the agent you just installed.

Step 5 On the **General** tab of the AGENT Properties dialog box, click **Stop** to stop the service.

Step 6 On the **Log On** tab, select **This Account**.

Step 7 Enter the requested information in the User Name/Domain Name and Password fields, then click **OK**.

Step 8 Right-click the agent and choose **Start**.

-or-

On the **General** tab, click **Start** to restart the agent.

Step 9 Close the Services and Administrative Tools dialog boxes.

Step 10 Go to the client and follow the procedure detailed in "Configuring Agents for Windows" to re-connect the agent.

Configuring Agent Parameters

Certain parameters of the Windows agent can be configured for the convenience of users. You modify the parameters of a Windows agent by adding the parameter statements to the command line or optionally (for most parameters) in the *tagent.ini* file. If the default location was used during the agent installation, the agent files are located in *C:\Program Files\TIDAL\Agent\Bin*.

Any parameters specified on the command line will take precedence over anything specified in *tagent.ini*. Some parameters that are needed during start still must be specified on command line (cpuload, msgthreads, rjaport).

The *tagent.ini* file in the *bin* directory works the same as in Unix agents, except the agent(s) definition and ports are not specified there. There is a [config] section and an [<Agent Name>] section. The parameters specified in the [config] section are global and the parameters specified in the [<Agent Name>] section only apply to that agent and will override specifications in the [config] section for the specific agent.

Following is an example of a *tagent.ini* file:

[config]

debug=y

logdays=3

logsize=1024000

encryptonly=y

sslvldcrt=y

vldhstcrt=y this is a synonym for **sslvldcrt**, as host validation also applies to SSH (only works in *tagent.ini*)

[TIDAL_AGENT_1]

debug=high

logdays=5

logsize=2048000

encryptonly=n

vldhstcrt=n

If specified in *tagent.ini,* these parameters do not need to be specified on command line.

Restart the agent after modifying any of the agent's parameters.

Sample and supported parameters list below:

The following agent parameters can be modified:

Debug

y|high

Where:

y (yes) turns on low-level debugging and **high** turns on maximum debug level.

Logdays

n

Where:

n is the number of days to preserve logs. Older logs will be deleted.

Sftpumask

<xxxx>

Where:

xxxx is permissions mask (4 digit octal) for files being created on Unix-type system by SFTP PUT actions. Default is '**0022**'.

Logfilesize

<xxxxxxxxx>

Where:

xxxxxxxxx is the maximum log file size in bytes (1048576 is 1MB). Default is 2048000.

Number of Message Threads

A new startup parameter, **MSGTHREADS=x,** has been added. It can optionally be specified on the startup line. The default number of threads that will handle messages is 5 and this seems optimal for 1-2 CPU machines. If you have more CPUs you may want to increase your thread count.

EncryptOnly Option

The **EncryptOnly** startup parameter option has been added. **EncryptOnly=Y** will cause an Agent to not remain connected to any Master that has turned off message encryption.

The default is **EncryptOnly=N**. It must be set to **Y** (Yes) in order for the more restrictive rules to take effect.

Secure FTP Host Validation

Tidal Enterprise Scheduler Agents v3.0 validates the host defined in FTPS SSL certificate. This is a change in behavior from the current Windows agent. The Host Validation feature can be disabled by specifying a **SSLVLDCRT** parameter on the agent command line. The default is **SSLVLDCRT=Y** (yes). You can turn this off by specifying **SSLVLDCRT=N**. Use Service Manager to edit the Agent startup parameters (add them to the **PATH** field). Use **vldhstcrt** as an optional synonym that is available only in *tagent.ini*.

AGTRESOURCE

AGTRESOURCE=CPU;VMEM enables monitoring CPU and VMEM monitoring with default time (15 seconds)

AGTRESOURCE=CPU,10000 enables monitoring only CPU with default time

AGTRESOURCE=CPU,10000;VMEM,15000 enables

The **AGTRESOURCE** specifications above indicate that (1) CPU utilization and Virtual Memory utilization should be monitored, (2) only CPU utilization should be monitored and change the time interval to 10 seconds (10000 milliseconds) and (3) CPU utilization should be monitored at a time interval of 10 seconds (10000 milliseconds) and that Virtual Memory utilization should be monitored every 15 seconds (15000 milliseconds).

The default time to send the resource value(s) to the Master will be 15 seconds and the minimum allowed will be 5 seconds.

MultiFTPStd

Y|N

Where:

Y is default, Standard FTP, no error if no files are operated on by MGET, MPUT or MDELETE.

N is non-standard FTP completion where the job will complete abnormal if no files are operated on.

FTPTimeout

nnnnnn

Where:
nnnnnn is timeout time in milliseconds. **0** will cause no timeout (infinity).

The Windows default timeout is 2 minutes (120000 milliseconds). This is a signed integer value.

Starting and Stopping Agents

To start or stop an agent:

Step 1 From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

Step 2 From the Services list, choose the name of the agent.

Step 3 Click **Start** to start the agent.

-or-

Click **Stop** to stop the agent.

Checking Agent Status

To check the status of an agent:

Step 1 From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

Step 2 From the Services list, choose the name of the agent.

The status of the agent is displayed at the bottom of the manager.

Configuring Jobs to Run in the Foreground

Since job processes do not normally require user interaction, they usually run in the background on the agent machine. If needed, you can configure your agent's system to run job processes in the foreground. Running processes in the foreground both allows user interaction with the process as it runs and enables more processes to run by providing another desktop. This can be configured to run in two different ways..

Note Changing settings in the Windows registry can have serious consequences on your computer system. Consult with your Windows system administrator before making any changes in the registry.

If you want to be able to interact with the process, you can configure the job to run in a command prompt window.

To configure jobs to run in the foreground:

Step 1 Open the Windows Registry Editor on the agent machine.

a. From the Window Start menu, choose **Run**. The Run dialog box displays.

b. Enter **regedit**.

c. Click **OK**.

Step 2 In the registry tree on the left, select the key at HKEY_LOCAL_MACHINE\SOFTWARE\TIDAL Software\Agent and create the key TIDAL_AGENT_1 (or the name of whichever defined Agent you wish to effect) below Agent.

Note On 64-bit systems, these keys and Strings need to be defined under "Wow6432Node" e.g. HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TIDAL Software\Agent\...

Step 3 Right-click the TIDAL_AGENT_1 key and choose **New > String Value** from the resulting menu.

Step 4 Name the new key that is created on the right pane, JobLaunchMode.

Step 5 Right-click the new JobLaunchMode key and select the Modify option from the context menu to display the Edit String dialog box.

Step 6 In the Value Data field, type one of the following numeric values to configure the appearance of the command prompt window:

0 = Hides the command prompt window and activates another window.

1 = Activates the command prompt window and displays it minimized.

2 = Activates the command prompt window and displays it in its current size and position.

3 = Activates the command prompt window and displays it at maximum size.

4 = Activates the command prompt window and displays it at minimized size.

5 = Displays the command prompt window in its current size and position but the window is not activated.

6 = Displays the command prompt window at its most recent size and position but the window is not activated.

7 = Activates and displays a window at its original size and position. Recommended when displaying the command prompt window for the first time.

If needed, you can repeat this procedure for the other agent instances that are listed in this key.

To revert back to the original configuration, delete the registry key that was added.

If you want the job process to run in the foreground without interacting with the job, you can run it from the default desktop.

Configuring Jobs to Run from the Default Desktop

To run a job from the default desktop:

Step 1 Open the Windows Registry Editor on the agent machine.

a. From the Windows Start menu, choose **Run**. The Run dialog box displays.

b. Enter **regedit**.

c. Click **OK**.

Step 2 In the registry tree on the left, select the key at HKEY_LOCAL_MACHINE\SOFTWARE\TIDAL Software\Agent and create the key TIDAL_AGENT_1 (or the name of whichever defined Agent you wish to effect) below Agent.

Note On 64-bit systems, these keys and Strings need to be defined under "Wow6432Node" e.g. HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TIDAL Software\Agent\...

Step 3 Right-click the TIDAL_AGENT_1 key, then choose **New > String Value** from the resulting menu.

Step 4 Name the new key that is created on the right pane, JobUseDefDesktop.

Step 5 Right-click the new **JobUseDefDesktop** key and choose **Modify** from the context menu to display the Edit String dialog box.

Step 6 In the **Value Data** field, type **1**.

If needed, you can repeat this procedure for the other agent instances that are listed in this key.

To revert back to the original configuration, delete the registry key that was added.

Configuring a Windows Agent to be a Remote Job Adapter Proxy

Designating the Port for HTTPS

To designate the HTTPS port:

Step 1 From the Windows Start menu, choose **All Programs > TIDAL Software > TIDAL Service Manager** to diaplsy the Tidal Service Manager.

Step 2 Click the ellipsis button to display the Service Configuration dialog box.

Step 3 In the Path field, edit the command line of the Agent by entering the following parameter:

RJAPort=PPPPP

Where **PPPPP** (e.g. **50001**) is the port number you want to use for the HTTPS connection from the Adapter.

For example:

"C:\Program Files\TIDAL\Agent\Bin\TidalAgent.exe" AGENT=TIDAL_AGENT_1 PORT=5912 PATH="C:\Program Files\TIDAL\Agent" RJAPort=PPPPP

Step 4 Click **OK**.

Step 5 Allow Service Manager to restart the agent when you save the change.

Note The proxy support will not be available in this Agent if the RJAPort is not specified in the command line. The Agent will not be usable by the Adapter until the RJAPort parameter is specified.

Note After adding the RJAPort parameter, you will need to add another dependency to the Agent service definition called HTTP SSL. You can do this by going into Service Manager and clicking the ellipses (...) for the specific agent, selecting the 'Dependencies' tab, and then selecting 'HTTP SSL' as a new dependency. The Agent will not start automatically at system start-up with-out adding this dependency.(May not be available in Windows 2008 and beyond).

Assigning Certificate to the Port for HTTPS

If your machine already has a valid server certificate, you should only have to perform <Jumps>Step below.

To create a self-signed host certificate and configure it to a port:

Step 1 Open a DOS prompt (Command Shell).

a. From the Windows Start menu, choose **Run**. The Run dialog box displays.

b. Enter **cmd**.

c. Click **OK**.

Step 2 Enter the following to create and install a self-signed certificate in the certificate store:

```
makecert -r -pe -n "CN=localhost" -eku 1.3.6.1.5.5.7.3.1 -ss my -sr
localMachine -sky exchange
```

Note makecert is available in the SDK if you have Visual Studio 2005 installed (*Microsoft Visual Studio 8\SDK\v2.0\Bin*). There are other ways to get a certificate, Google will give you several options.

Step 3 Start Microsoft Management Console (mmc) and copy the certifcate "local" located in *Personal* > *Certificates* into *Trusted Root Certification Authorities* > *Certificates*.

Step 4 At the DOS prompt (Command shell) run:

Note The port used to connect from the master to the proxy agent via HTTPS (the RJAPORT) requires that it be configured to use SSL.

For pre-2008 systems:

httpcfg.exe set ssl -i 0.0.0.0:PPPPP -c "Root" -h XXXXX

where **0.0.0.0:PPPPP** is the IP and port. This is for **https://localhost:PPPPP**, where **XXXX** is the Thumbprint value of the local certificate. To obtain the thrumbprint of a certificate, open the certificate and click the **Details** tab. Copy the thumbprint and delete all blanks (spaces) between numbers in 'Thumbprint'

Note It is critical that the name after '-c' in the httpcfg set matches the store that the certificate is in, Root is recommended (see below).

Store Names:

- AddressBook -The X.509 certificate store for other users.
- AuthRoot - The X.509 certificate store for third-party certificate authorities (CAs).
- CertificateAuthority - The X.509 certificate store for intermediate certificate authorities (CAs).
- Disallowed - The X.509 certificate store for revoked certificates.
- My - The X.509 certificate store for personal certificates.
- Root - The X.509 certificate store for trusted root certificate authorities (CAs).
- TrustedPeople - The X.509 certificate store for directly trusted people and resources.
- TrustedPublisher - The X.509 certificate store for directly trusted publishers.

For post-2008 systems:

netsh http add sslcert ipport=0.0.0.0:PPPPP certhash=XXXX appid={YYYYYY}

where **ipport=0.0.0.0:PPPPP** (e.g. **0.0.0.0:50001**) is IP and port, this is for **https://localhost:PPPPP**.

`certhash= XXXX` is the Thumbprint value of the local certificate. To obtain the thrumbprint of a certificate, open the certificate and select the Details tab. Copy the thumbprint and delete all blanks (spaces) between numbers in 'Thumbprint'.

`appid={YYYYYY}` is a GUID identifying the owning application.

Step 5 Click **OK**.

Uninstalling Agents

To uninstall the agent, you must use the **Add/Remove Programs** utility in the Windows Control Panel.

To uninstall an agent:

Step 1 Close the TES client to begin the uninstallation process.

Step 2 From the Windows Start menu, choose **Settings>Control Panel**, then double-click **Add or Remove Programs**.

Step 3 Scroll down the list of programs installed on the machine to the Scheduler program.

Step 4 Click the Scheduler program to highlight it.

Step 5 Click **Remove** to start the uninstallation process.

Step 6 When prompted to confirm that you want to uninstall the program, click **OK**.

Step 7 Click **Finish** to end the uninstallation process.

Step 8 Reboot the machine to save the changes to the registry.

Note Occasionally, an empty folder may be left in the Start menu after uninstalling Scheduler components. If this occurs, go to the Programs directory and manually delete the empty folder. The installation log file must also be manually deleted.

Installing the Agent for Unix

Companies often need to provide centralized scheduling and administration of workloads that span multiple machines and multiple locations. TES master/agent architecture provides that capability.

In the basic TES network, the master uses a centralized database, containing all calendar and job scheduling information. One or more agent machines execute the production schedule. One or more client machines provides the TES user interface or console. The only prerequisite for the master/agent relationship is that the machine acting as the master must be on the same TCP/IP network as the machines serving as agents.

TES provides agents for Windows environments and agents for Unix environments. This chapter discusses the Agent for Unix installation.

Installing the Agent for Unix from the Command Line

Before installing the Tidal Agent for Unix, backup your files and gather the following information:

- Name of the user who will own the agent
- Port number for the agent
- Directory path for the Java Virtual Machine (JVM)

To install the agent from the command line:

Step 1 Insert the installation DVD-ROM into the machine you want to install the agent on.

Step 2 Login as root.

Step 3 Copy the *install.sh* and *install.tar* files from the directory on the DVD-ROM (**<DVD-ROM>\agent\unix\cmdline**) to your temp directory..

Note Do not unpack the install.tar file. The file will automatically unpack during the installation process

Step 4 Change the permissions on the *install.sh* file in the directory to make the file executable:

chmod 554 install.sh install.tar

Step 5 Begin the installation by entering:

./install.sh

An introduction screen displays as the installation program begins.

Step 6 Type **Y** to continue the installation and press **Enter**. The Select the Owner screen displays.

The top of the screen shows the users defined on the machine you are installing on. In some cases, you may want to select a user who is not defined on the local machine but is defined as a NIS user allowing the user to install over the network.

Step 7 Enter the name of the user to own the agent.

Note Carefully consider which user to run the agent as. It may be desireable to create a user specifically for this purpose.

Step 8 Press **Enter**. The Select the Location screen displays.

Step 9 Type **Y**, then press **Enter.**

Note Carefully consider which user to run the agent as. It may be desireable to create a user specifically for this purpose.

The Agent Configuration Menu screen displays.

Step 10 Type **1** to select the Add Instance option, then press **Enter.** The Select the Location for the Agent Files screen displays.

Step 11 Enter the information you gathered before beginning installation:

- Name to call the agent
- Number of the port the agent should use
- Directory path for the Java binary files (JVM)

Step 12 Press **Enter**. A confirmation summary screen displays the information that you entered.

Step 13 If the information is correct, press **Enter**.

-or-

If the information is not correct, type **n**. You are prompted again for the name, port number, and directory path for the agent.

Configuring Agents

You can configure Unix agents (add and delete agent instances) using the **Agent Configuration Menu**.

To display this menu:

Step 1 Log on as agent owner on the agent machine.

Step 2 Go to the *bin* directory by entering:

cd /opt/TIDAL/Agent/bin

Step 3 Type in the following:

./tagent config

The **Agent Configuration Menu** displays.

Adding Agent Instances

To add an instance:

Step 1 In the Agent Configuration Menu enter **1 a**nd press **Enter**.

Step 2 Enter the name of the agent, its port number and the directory path to the Java binaries and then press **Enter**.

Step 3 Enter **Y** and press **Enter**. An agent instance is added.

Step 4 Start the agent by entering:

./tagent <agent name> start

Viewing the Status of Agent Instances

View the status of an agent by entering in the *bin* directory:

./tagent <agent name> status

Once you have entered that command a status screen displays.

Deleting Agent Instances

To delete an instance:

Step 1 Stop the agent.

Step 2 In the Agent Configuration Menu enter **3** and press **Enter**. The Select Agent Instance to Delete panel displays.

Step 3 Type the number of the instance to delete.

Step 4 Press **Enter** to delete the instance.

Configuring Agent Parameters

Certain parameters of the Unix agent can be configured for the convenience of users. You modify the parameters of an agent by changing the parameter values in the *tagent.ini* file. The *tagent.ini* file is located in the Unix agent directory. If the default location was used during the agent installation, the agent files are located at */opt/TIDAL/Agent/bin*. Following is an example of a *tagent.ini* file:

```
# ========================================
# Agent Configuration Information
# ========================================
[config]
agents=sun02,sun11,aix02,test
degbug=yes
ovb=tidaldebug
java=/usr/bin/
#sslvldcrt=n
sshvldhst=/home/secure/prd2_id_rsa.pub
sslvldhst=/home/secure/vvm1.pem


[test]
port=5915
java=/usr/j2rel.4.2_06/bin
minmem=32
maxmem=64
logdays=5
```

```
[sun02]
port=5915
java=/usr/j2rel.4.2_06/bin
sslvldcrt=n

[sun11]
port=5915
encryptonly=y

[aix02]
port=5915
java=/usr/java5_64/bin
sslvldcrt=/home/secure/host.crt
ulimitold=y
~
~
~
~
~
“tagent.samp” 34 lines, 592 characters
```

Restart the agent after modifying any of the agent's parameters.

The following agent parameters can be modified:

Debug

y

Where:

y (yes) turns on low-level debugging of startup activity of agent.

Ovb

tidaldebug

Where this statement turns on the maximum level of debug logging of agent activity.

Logdays

n

Where:

n is the number of days to preserve logs. Older logs will be deleted.

Sftpumask

<xxxx>

Where:

xxxx is permissions mask (4 digit octal) for files being created on Unix-type system by SFTP PUT actions. Default is **0022**.

profile=y

The profile parameter is used to have the agent permanently override the For Unix, source user's profile option on the Options tab of the Job Definition dialog box.

Specifying the **y** value means that all jobs that run on this agent will source the specified runtime user profile. In effect, a y forces For Unix, source user's profile to be set for all jobs.

Leaving the parameter value blank (the default value) or specifying a n value means that only jobs with the For Unix, source user's profile option selected will source the user's profile.

homedir=y

The `homedir` parameter specifies the agent's home directory.

A `y` value means that the starting path will be the runtime user's home directory instead of the agent's home directory.

Leaving the parameter value blank (the default value) or specifying a **`n`** value means that the home directory remains the directory where the agent is installed..

Note This parameter will override the working directory setting in the master for all jobs to the user's home directory.

minmem and maxmem

The `minmem` and `maxmem` parameters control how many MB of memory should be allocated to the agent processes. These memory parameters can be adjusted as individual needs warrant. Your system may need more or less than the default memory allotments.

The `minmem` parameter specifies that at least the amount of RAM specified should be available. The default value is 16 MB of RAM.

The `maxmem` parameter specifies that no more than the amount of RAM specified should be available for the agent processes. The default value is 48 MB of RAM.

For example, to set the minimum memory to 32 MB and the maximum memory to 64 MB, specify:

minmem=32

maxmem=64

fp=path of environment file

The `fp` parameter specifies a particular environment file to be used by an agent instance. To associate an environment file to an agent, enter the pathname of the environment file using the following format, **`fp=/folder/file`**.

Each agent instance can be assigned its own environment file and its associated environment variables with their various values. Each variable specified in the environment file should follow a **`variable=value`** format as in the following examples:

TZ=CST
SchedulerT=1
PATH=/usr/sbin

Jobstopwait=n seconds

The Jobkillwait parameter specifies the time interval between sending a SIGTSTP warning that a Unix job is about to be put on hold and actually sending the SIGSTOP signal to pause the job.

The default value is 1 second before pausing the job but the number of seconds between the warning and the actual pausing of the job can be modified from this parameter.

Jobkillwait=n seconds

The Jobkillwait parameter specifies the time interval between sending a SIGTERM warning that a Unix job is about to be aborted/cancelled and actually sending the SIGKILL signal to abort/cancel the job.

The default value is 5 seconds before cancelling the job but the number of seconds between the warning and the actual cancelling of the job can be modified from this parameter.

EncryptOnly Option

The EncryptOnly startup parameter option has been added. EncryptOnly=Y will cause an Agent to not remain connected to any Master that has turned off message encryption.

The default is EncryptOnly=N. It must be set to **Y** (Yes) in order for the more restrictive rules to take effect.

Secure FTP Host Validation

Tidal Enterprise Scheduler Agents v3.0 validates the host defined in FTPS SSL certificate. This is a change in behavior from the current Windows agent. The Host Validation feature can be disabled by specifying a SSLVLDCRT parameter on the agent command line. The default is **SSLVLDCRT=Y** (yes). You can turn this off by specifying SSLVLDCRT=N. Use Service Manager to edit the Agent startup parameters (add them to the PATH field).

SSLVLDHST

<location of file containing host certification key file>

For FTPS Host validation, the location of the file containing the public host certificates (generally self-signed), if not authenticated through a Certificate Authority.

The certificates in the file must be of the OpenSSL PEM format and be bracketed as follows:

```
-----BEGIN CERTIFICATE-----
... first certificate ...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... second certificate ...
-----END CERTIFICATE-----
```

SSHVLDHST

<location of SSH host key file>

For SFTP Host validation, the location of the file containing the public Keys for the servers that SFTP connections will be established with.

Provides a list of hosts and their associated public keys in the given file. The format of the file is similar to that used in OpenSSH. Each line contains the name of a host followed by its IP address (separated by a comma), the type of key it has, and its key (in base-64 printable form). For example:

```
jackspc,192.168.1.1 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIE...
```

cpuload

The cpuload parameter controls whether the Agent sends system load information back to the master. The default is 'no'. The information is only needed if you are using the Balanced option on an Agent list. When 'yes' is specified, the load information will be collected and sent back to the master at one minute intervals.

AGTRESOURCE

AGTRESOURCE=CPU;VMEM enables monitoring CPU and VMEM monitoring with default time (15 seconds)

AGTRESOURCE=CPU,10000 enables monitoring only CPU with default time

AGTRESOURCE=CPU,10000;VMEM,15000 enables

The AGTRESOURCE specifications above indicate that (1) CPU utilization and Virtual Memory utilization should be monitored, (2) only CPU utilization should be monitored and change the time interval to 10 seconds (10000 milliseconds) and (3) CPU utilization should be monitored at a time interval of 10 seconds (10000 milliseconds) and that Virtual Memory utilization should be monitored every 15 seconds (15000 milliseconds).

The default time to send the resource value(s) to the Master will be 15 seconds and the minimum allowed will be 5 seconds.

Starting and Stopping Agents

You can start or stop an agent by entering on the command line:

./tagent <agent name> start

-or-

./tagent <agent name> stop

Note You should stop all Unix agents before rebooting the Unix system. It is recommended to add the agent stop command to a Unix system shutdown script to be used when restarting a Unix system.

Note When issuing the tagent start command, verify that you are logged on as the user intended to run the agent.

Preventing Unauthorized Users from Using an Agent

The Unix agent can be configured to allow only specific users to run jobs on that agent. A list of users can be created to exclude or allow users access to the agent. If an unauthorized user tries to run a job on an agent that he is excluded from, the job will end with an "Error Occurred" status.

To exclude users from an agent

Step 1 Login as the owner of the agent.

Step 2 Create a file called *Users.cfg* in the agent's root directory, e.g., **/opt/TIDAL/Agent/<name of agent>**.

Note The file name, *Users.cfg*, is case sensitive, so only the first letter should be capitalized and the rest of the name should be lower-case.

Step 3 Change the *Users.cfg* file permissions to limit access to just the agent owner, by entering:

chmod 700 Users.cfg

Step 4 In the *Users.cfg* file, enter:

EXCLUDE

Step 5 List those users that will be prohibited from accessing the agent.

Each user must be on a separate line.

Following is an example of a *Users.cfg* file:

EXCLUDE
JDegnan
MCarpent
TESUser

If the list of users to exclude is long, enter **INCLUDE** instead of **EXCLUDE**. Then you can list the users to give access to the agent if this is easier.

Step 6 To ensure that the changes take effect, stop and restart the agent.

-or-

Disconnect and reconnect the client connection to the agent.

Note While this procedure prevents unauthorized users from running system commands on an agent they are excluded from, FTP jobs can still be run from the agent because an user does not login to an agent to FTP.

Uninstalling Agents

The Agent for Unix is uninstalled from the command line.

Uninstalling Using the Command Line

The uninstallation procedure will not be successful if the agent is running. Stop the agent before removing the TES Agent for Unix.

To uninstall:

Step 1 Check the status of the agent to verify that it is not running by entering:

./tagent <agent name> status

Step 2 If the status check shows the agent is not running, proceed to the next step.

-or-

If the status check shows the agent is running, stop the agent by entering:

./tagent <agent name> stop

Step 3 Once the agent is stopped, return to the location where you installed the Unix agent. By default, this location is the */opt* directory.

Step 4 At the command prompt, enter:

cd /opt

Step 5 Have your Unix administrator remove the agent directory and its contents

Connections and Agent Procedures

Defining an Agent Connection

To define a connection between the agent and the master :

Step 1 From the Navigator pane of the TES client, choose **Administration > Connections**.

-or-

Click the **Connections** button on the TES toolbar.

The Connections pane displays.

Step 2 Double-click the agent name.

-or-

Right-click in the Connections pane and choose **Add Connection > Agent for Windows** or **Add Connection > Agent for Unix** from the resulting menu.

The Connection Definition dialog box displays.

Step 3 Enter a name for the agent you installed.

Note This name does not have to match the machine name or instance name.

Step 4 On the General tab, configure:

- Job Limit – The maximum number of jobs you want to run concurrently on this agent. It is recommended that you do not run more than 80 jobs at once.
- Default Runtime User – The default runtime user that will appear when creating a new job on this agent.

Step 5 Select the Enabled option.

Step 6 Select the Connection tab.

Step 7 In the Machine Name field, enter the name or IP address of the machine that the agent is installed on. This name must be a valid DNS name.

Step 8 In the Master-to-Agent Communication Port field, enter the agent's listener port number specified when installing the agent.

Step 9 If you want to enter a description of this agent, select the Description tab and enter a description; otherwise, click **OK** to save the connection.

Deleting an Agent Connection

To delete an agent connection:

Step 1 From the Connections pane, select the agent to delete.

Step 2 Click the **Delete** button on the TES toolbar or press the **Delete** key on your keyboard.

Note You cannot delete an agent connection unless you are connected to the master. You can delete an agent connection that is currently in use, however, jobs that were to run on that agent will be disabled. Those jobs will not run again until you assign them to a valid new agent.

Enabling or Disabling Agents

You can disable an agent if you do not want it to run jobs. If a job is about to be submitted to run on a disabled agent, its status changes to *Agent Disabled*.

To enable/disable an agent:

Step 1 From the Navigator pane, choose **Administration > Connections** to display the Connections pane.

Step 2 Double-click the agent.

-or-

Select the agent and click the **Edit** button on the TES toolbar.

Step 3 In the agent's Connection Definition dialog box:

- To enable the agent, select the Enabled option.
- To disable the agent, clear the Enabled option.

Note You can also enable or disable agents using the context menu in the Connections pane.

Step 4 Click **OK**.

Changing an Agent's Job Limit

You can change an agent's job limit to specify the number of jobs that can run on it concurrently. You can also control the number of jobs running concurrently using queues.

To change an agents job limit:

Step 1 From the Navigator pane, choose **Administration > Connections** to display the Connections pane with the licensed computers.

Step 2 Double-click the agent to edit or select the agent and click the **Edit** button on the TES toolbar to display the agent's connection definition.

Step 3 Select the General tab if it is not showing.

Step 4 In the Job Limit field on the General tab, change the job limit to the desired value.

Step 5 Click **OK**

Changing the Name of the Computer Displayed in TES

To change the name of the computer:

Step 1 From the Connections pane, double-click the licensed computer to edit or select the computer and click the **Edit** button. The licensed computer's Connection Definition displays.

Step 2 In the Name field, change the computer's name. This name is used when referring to the computer on TES panes and dialog boxes.

Step 3 Click **OK**.

Changing the Machine Hostname of the Computer

To change the hostname of the computer:

Step 1 From the Connections pane, double-click the licensed computer to edit, or select the computer and click the **Edit** button to display the licensed computer's Connection Definition dialog box.

Step 2 Select the Connection tab.

Step 3 In the Machine Name field, update the computer's name.

This name can be found in the DNS section of the TCP/IP protocol of your network configuration. See your System Administrator for more information.

Cluster Configuration

Configuring a Cluster to Run the Windows Agent

The Agent for Windows can run in a Windows cluster environment. A cluster environment is defined as multiple machines working together as one system. The cluster environment provides a level of redundancy so that if one of the machines in the cluster fails, another machine is available to replace the failed component.

The following instructions describe how to configure a two node cluster environment to run the Windows agent offered by Scheduler.

Prerequisites

Before installing the Tidal Agent for Windows on the nodes of a cluster, you must first complete and/or verify the following on each node:

- Verify that the systems on each node are identical
- Verify that the agent machines in each node meet the hardware and software requirements specified in the Installing the Agent for Windows chapter of the Installation and Configuration Guide for Scheduler.
- Verify that the user installing the Windows agent has the specified user rights including access to the registry on each machine.
- Verify that the cluster group has the following resouce types:
  - Network name
  - IP address
  - Physical disk

Configuring the Agents for a Cluster

During configuration, you should complete a step on a machine and then go around to the other machines in the cluster and do the same step. When that step has been performed on each machine in the cluster, return to the first machine and do the next step and then again do that step on the other machines in the cluster, and return to the first machine and do the next step, etc.

An agent instance must exist on every node in the cluster before it can be configured to run as a cluster. This means that if you add a third agent instance to a machine, before you configure that instance, go to all of the other machines in the cluster and add a third instance.

To configure the agents:

Step 1 Verify that the cluster works correctly.

Check that the cluster software is installed and configured correctly by forcing a failure on a server. Be sure that a failover to another server occurs as intended and that control can be returned to the server that failed. Your Windows Cluster Administrator should help you with this.

Step 2 Install the Agent for Windows on the first cluster node.

Be sure to install the agent to a non-clustered physical disk on the local machine using the default directory path during installation.

Caution You must install the agent on the same disk drive letter on each cluster node. For example, if you install the agent on the C drive of one node, the agent must be installed on the C drive of the other nodes also.

Step 3 Stop the agent if it is running.

Note If an agent instance is configured as part of a cluster, you will not be able to stop the agent. You must stop the agent service.

Step 4 An agent instance must exist on every node in the cluster before it can be configured to run as a cluster. If you are adding an agent instance, add the agent instance to a machine. See "Installing the Agent for Windows". Go to each of the other nodes in the cluster and add that same instance.

Once each of the nodes on the cluster have the same agent instance on it, you can edit the agent instance to configure it for the cluster.

Step 5 From the Windows Start menu, choose **Programs > TIDAL Software > Agent > Instance Manager** to display the Agent Instance Manager.

Step 6 Select the first agent instance and click the **Edit** button to display the Agent Instance Manager's configuration screen.

If this agent instance is on a node that is configured for a cluster with an existing agent service, the Run on a cluster group option is available. If the node is not part of a cluster than this option is unavailable. You cannot proceed any further without verifying with your Windows Cluster Administrator that the node is correctly configured as a member of the cluster.

Step 7 Select the Run on a cluster group option to expand the screen to display the cluster configuration fields.

Step 8 In the Cluster Group field, select which cluster group that this agent instance belongs to.

Step 9 In the Physical Disk field, select the disk that the agent instance resides on. All the disks that were created on all of the cluster groups are listed. Be sure to select a disk that exists on the cluster group you selected.

Step 10 In the Work Directory field, enter the pathname to the work directory that was created for the cluster group.

Note This Work Directory must be on a shared disk that moves with the active node on a fail-over.

Step 11 In the Cluster Nodes field, select which node this agent instance is on. When the fields are completed, click the **Save** button.

Step 12 Go to each node and repeat this procedure for each agent instance.

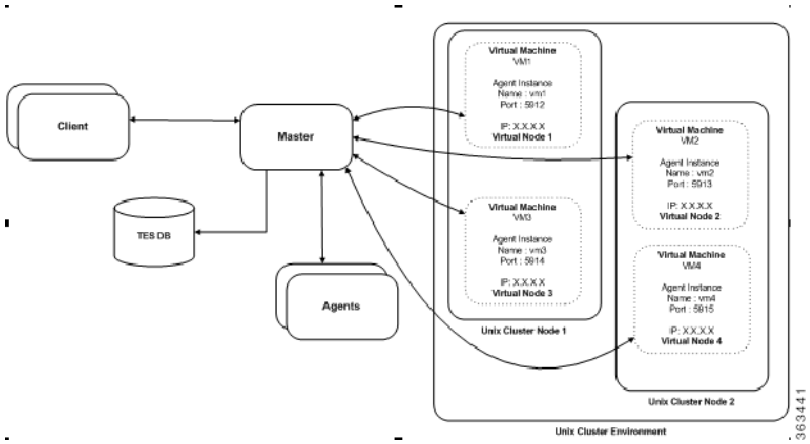
Step 13 When each agent instance on each node is configured properly, start each clustered agent instance from its active node using Scheduler's Service Control Manager. Starting the agent instance in the Service Control Manager automatically starts the agent resource in the Windows Cluster Administrator.

Configuring a Cluster to Run the Unix Agent

The Agent for Unix can run in a Unix cluster environment.

The following diagram illustrates how Enterprise Scheduler is configured in an environment with Unix cluster

Figure 6-3 Unix Cluster Environment



The Master component connects to agent instances associated to a virtual machine using the virtual machine name and IP address and the port number. This allows the Scheduler master to maintain the agent connection when the cluster management software moves the virtual machine to another participating node.

Prerequisites

To configure the Tidal Agent for Unix on a cluster to follow the virtual machine, the following prerequisites must be met:

- The SAN/NFS Agent installation location must be mounted at the same mount point on all of the cluster nodes.
- Java Virtual Machine (JVM) prerequisites must be installed on all of the nodes. These prerequisites for the JVM include installing all OS patches, maintaining kernel parameters, etc.
- The same JVM must be installed on each of the physical nodes (and, whenever possible, the JVM should be installed in the same directory location on each of the nodes.)
- The Agent owner account must be accessible from all of the nodes.
- The minimum requirements for the Scheduler agent must be met on each of the individual nodes.
- The installation and configuration of Tidal Agents for Unix in a cluster can be broken down into the following four steps:
  - Installing Agent files on the SAN/NFS mount location.
  - Configuring agent instances (only one instance per virtual machine).
  - Configuring the cluster Virtual Machine.
  - Configuring Scheduler to connect to the agent instances on a virtual machine.

Installing Agent on the SAN/NFS Location

To install the agent on the SAN/NFS location:

Step 1 FTP the agent installation files to one of the participating nodes in the cluster.

Step 2 Login as root to the same physical node where the agent installation files were copied.

Step 3 Change to the directory where the agent installation files were copied.

Step 4 Follow the normal Agent installation procedure that is described in the "Installing the Agent for Windows" with the following exceptions:

- When entering a location for the agent files, select the SAN/NFS location (visible to all the nodes).
- Ensure that the Agent owner is a NIS user or if the agent owner is a local user on all of the participating nodes than the Agent owner must have the same UID and GID.
- At the end of the installation procedure, do not configure any agent instances.

Configuring Agent Instances

To configure agent instances:

Step 1 Identify each of the Virtual Machines that require an agent instance associated with it.

Step 2 Login to a cluster node as the agent owner.

Step 3 Change to the agent *bin* directory and run the t**agent –config** command to begin the agent configuration.

Step 4 Select the Add Instance option and add one instance for each of the virtual machines.

- It is a best practice to give each agent instance the same name as the virtual machine hostname to help identify which instance is associated to which virtual machine.
- The port number for each agent instance must be unique.

The Agent Instance configuration file will look similar to the following example that shows a configuration file for a cluster with four virtual machines:

Agent Instance configuration file

[/opt/TiDAL/Agent/bin/tagent.ini]

```
# ================================================================
# Agent Configuration Information
# ================================================================

[config]
agents=vm1,vm2,vm3,vm4

[vm1]
port=5912

[vm2]
port=5913
```

[vm3]

port=5914

[vm4]

port=5915

Configuring Cluster Virtual Machine

This step varies from one cluster solution to another but basically all cluster solutions require the following three operations to enable the agent instance to be associated to the virtual machine.

- Start the Agent instance
- Monitor the Health of the Agent instance
- Stop the Agent instance

Start a Agent instance

To start an agent instance, issue the following command:

su <agent owner> -c "<agent install location>/bin/tagent <agent instance name> start"

Replace the text in brackets < > with the name of your agent owner and agent instance and the directory pathname to the agent files.

Monitor the Health of the Agent Instance

Check the status of the agent with the **`tagent <agent>`** status command as illustrated in the sample script below:

#!/bin/sh

cd /agentdir/bin/

./tagent $1 status | grep "Down"

if [$? -eq 0]

then

echo "Agent $1 is down"

exit 1

fi

exit 0

Stopping the Agent Instance

Stop an agent instance with the following command:

<agent install location>/bin/tagent <agent instance name> stop

Replace the text in brackets < > with the name of your agent instance and the directory pathname to the agent files.

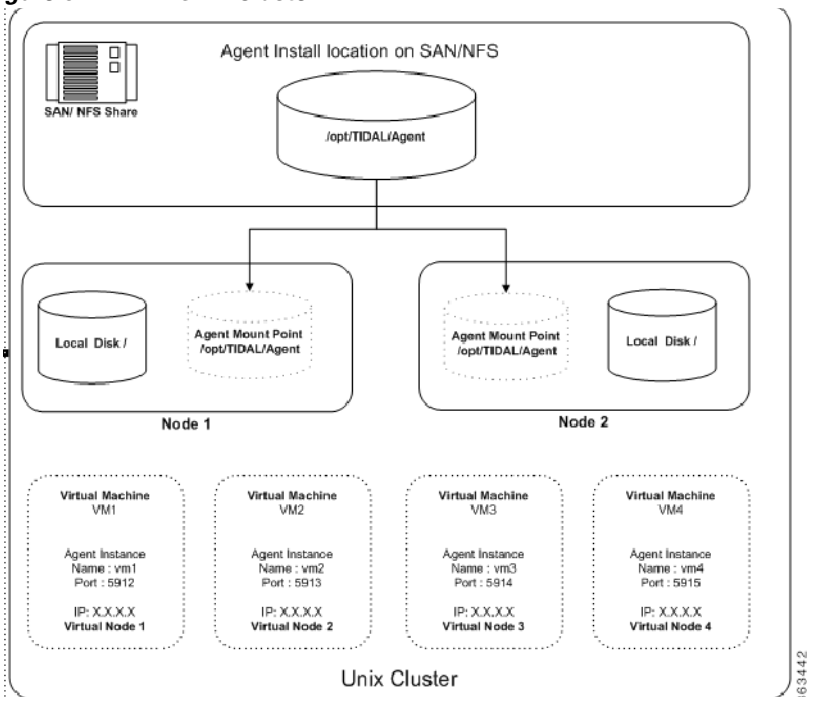
Configure Scheduler to Connect to Agent Instances on a Virtual Machine

Configuring the connection to the Agent instances in the Scheduler client is the same procedure as configuring other agent connections with the following exceptions:

- Use the virtual machine hostname/IP address instead of the physical node hostname.
- Use the agent instance port number for the agent instance that is associated with the virtual machine.

The following diagram illustrates an agent installed on a two node cluster with four virtual machines.

Figure 6-4 Unix Cluster



Agent/Master Secure Connection

In order to provide strict control over which Tidal Enterprise Schedulers (Enterprise Scheduler) Masters can connect to a specific agent, a *Masters.cfg* file has been implemented at the Agent. By specifying the Master 'alias', the Master 'alias' and a specific 'local' TCP/IP address or the Master 'alias', the specific 'local' TCP/IP address and a 'global' TCP/IP address you can uniquely identify the specific Enterprise Scheduler Masters that a Enterprise Scheduler Agent will create connections to.

The *Masters.cfg* file must be created in the Agents local directory. This directory is in the install path of the Agent and has the name of the Agent as it was specified when the Agent was defined. For example, by default, this would be something like:

- For Unix (Linux, z/OS)

  `/opt/TIDAL/Agent/TidalAgent1`

- For Windows

  `C:\Program Files\TIDAL\Agent\TIDAL_AGENT_1`

- For OVMS

  `sys$sysdevice:[tidal.agent.tidalagent1]`

This file should have limited access using native system access control definitions.

Agent Connect Protocol

The following describes the normal connection sequence for an Agent to Master connection to be established.

The Master connects to the Agent well-known port (default 5912, configurable). The Master sends a registration message to the Agent specifying the Masters IP address and listening port (and some other configuration information). This connection is then terminated.

For each Master that has registered as above, the Agent will attempt to connect using the information from the registration. This will happen each time the connection is lost for any reason.

The Agent will attempt to connect to the IP and port provided by the Master in the registration message. If this fails, the Agent will attempt to connect to the IP obtained from the network as the source IP (may be firewall IP) and the port provided in the registration message.

When the connection is made, the Agent will generate an encryption key based on a random seed. This encryption key and other configuration information about the Agent will be sent to the Master. The encryption key is 'wrapped' by a method that the Master knows how to 'unwrap' in order to get the raw key. This key is used to encrypt the body of all future messages (encryption is a configurable option that is on by default).

Masters.cfg

The *Masters.cfg* file contains the following structure:

Optional INCLUDE or EXCLUDE statement on first line. If specified, these one word entries must be on the first line. INCLUDE is the default if nothing is specified.

- INCLUDE - only the specified Masters with optionally specified IP addresses will be connected to by the Agent.
- EXCLUDE - the specified Masters will be specifically excluded from being connected to by the Agent.

Master entries of the form:

- MasterAlias

  The MasterAlias typically has the form 'ES_<hostname of master>_1' and is case-insensitive. If specified alone on the line, then only the MasterAlias will be verified that it matches what was presented by the Master in its registration message.

- MasterAlias:IPaddress1

  For connections that are 'local', i.e. their Master host machine IP addresses are directly accessible by the Agent, then only IPaddress1 needs to be specified. This address will be verified against the IP address presented by the Master in its registration message and the IP address obtained from the network as the origination of the connection that provided the registration message.

- MasterAlias:IPaddress1;IPaddress2

  For connections that must traverse a firewall, then IPaddress2 must be specified. IPaddress2 will be the externally known address of the firewall. The externally known address of the firewall is what will be obtained by the Agent when it retrieves the IP address of the origination of the connection through which the registration message was delivered .

For situations where a Master could have multiple IPs, Failover scenarios, or disaster recovery situations, the same MasterAlias can be specified with different IPaddress parameters.

Following is an example of a *Masters.cfg* file:

INCLUDE

hou-testvm-531:192.168.48.111;172.19.25.125

hou-testvm-531:192.168.55.211;172.19.25.125

zostest:192.168.95.92

zostest:192.168.42.92

catest

Troubleshooting

Verifying the Version of the Agent

When consulting with Technical Services about a problem with an agent, one of the most basic pieces of information they need is which version of the agent is being used.

To verify the version of the agent:

Step 1 From the Navigator pane of the client, choose **Administration > Connections** to display the Connections pane.

Step 2 In the various connections listed in the pane, locate the agent with the problem.

Step 3 Look in the Version column of that agent to see the version of the agent being used.

Diagnostics

Unix Agent

The first line of every Unix agent shell script must adhere to standard Unix scripting guidelines and refer to a shell; for example, **#!/bin/sh**. For more information, refer to your Unix system documentation or consult your System Administrator.

When the Agent for Unix generates errors and doesn't operate properly, you need to contact Technical Services to help you resolve the technical issues. However, Technical Services requires specific information on how the Agent for Unix is operating before they can track down the source of the problem. Before contacting Technical Services about an agent issue, you should turn on diagnostic logging to collect information about the way the agent is functioning. This is the first step that Technical Services will have you do, if you have not done it before contacting them.

To turn on diagnostic logging:

Step 1 On the agent machine type the following command to stop the agent:

./tagent <agent name> stop

Step 2 Go to the */bin* directory and locate the *tagent.ini* file for the desired agent.

Step 3 Inside the *tagent.ini* file, under the port setting, type the following:

ovb=Tidaldebug

Step 4 Save the file and its changes.

Step 5 Start the agent:

./tagent <agent name> start

Ideally, you want to reproduce the situation that caused the issue so the diagnostics can log what occurred in the system at that time. As soon as the problem reoccurs, contact Technical Services.

Step 6 Once the problem repeats itself and the diagnostic information is recorded, turn off the agent diagnostics by commenting out the debugging parameter:

#ovb=Tidaldebug

Step 7 Go to the *Log* directory to get the diagnostic file to send to Technical Services:

cd <agent directory>/<agent name>/logs

Each agent instance has its own directory. The diagnostic files are named <*FTP*>.*log*, <*agent name*>.*log* and <*master server*>.*log*.

Restarting the agent does not override the recorded information. Though only a small amount of information is normally recorded without the debug parameter, the file will continue to grow in size. You should delete or rename the file after you finish debugging the agent.

Note Whenever diagnostic logging is being used, you must carefully monitor the amount of disk and database space being consumed. Diagnostic logging can generate large amounts of data and affect system performance.

Windows Agent

To run diagnostics for the Windows agent:

Step 1 Login to the agent console as an authorized user.

Step 2 Using Service Manager, select the Agent that you wish to use diagnose.

Step 3 Add the following string to the end of the **Path:** field.

Debug=high

Step 4 Click **OK** at bottom of panel and respond yes to the "Would you like to restart the service?" pop-up.

To stop diagnostics, close the agent application window and restart the agent from the Service Control Manager.

Working With Agents

You can start and stop agents in your network at any time. A yellow agent status light at the bottom of the client screen indicates that you need to restart your agent(s).

Note Before starting or stopping the agent, check the agent's status using the Tidal Service Manager.

Checking Agent Status

The following steps are for Windows Agents only.

To check the agent status:

Step 1 On the agent machine, click the Windows **Start** button and then select **Programs > Tidal Software > Tidal Service Manager** to display the Tidal Service Manager.

Step 2 In the **Service** drop-down list, select the agent you wish to check so that it displays in the Service field.

Step 3 At the bottom of the Tidal Service Manager, the status of the selected service displays.

Note The Agent for Unix does not use the Tidal Service Manager so the command line is used to start, stop and check the status of the agent. Use the following commands:
To start: **./tagent <agent name> start**
To stop: **./tagent <agent name> stop**
To check agent status: **./tagent <agent name> status**

Starting the Agent

The following steps are for Java-based Agents only (**tagent** command).

To start the agent:

Step 1 From the Windows Start menu, choose **Programs > Tidal Software > Tidal Service Manager** to display the Tidal Service Manager.

Step 2 From the Service list, choose the correct agent if it is not displayedand click the **Start** button. The light will turn green when the agent starts.

Note The Agent for Unix does not use the Tidal Service Manager so the command line is used to start, stop and check the status of the agent. Use the following commands:
To start: **./tagent <agent name> start**
To stop: **./tagent <agent name> stop**
To check agent status: **./tagent <agent name> status**

Stopping the Agent

The following steps are for Windows Agents only (Service Manager).

To stop the agent:

Step 1 From the Windows Start menu, choose **Programs > Tidal Software > Tidal Service Manager** to display the Tidal Service Manager.

Step 2 From the Service list, choose the correct agent if it is not displayedand click the **Stop** button. The light will turn red when the agent stops.

DataMover Job Support

Note DataMover jobs are only supported on Unix/Linux agents.

By default, when the 3.1.0.02+ agent is installed, it can run with Java 1.4.x as previous agents, but it will not support Amazon S3 (AS3) or Hadoop DFS (HFS) DataMover operations. DataMover jobs sent to the default agent will fail with a 'wrong agent' indication.

In order to utilize AS3 or HFS DataMover functionality, you must be running the appropriate level of Java and you must copy the associated support files into the Agent/ lib directory. AS3 functionality requires Java 1.5 as a minimum and HFS functionality requires Java 1.6 as a minimum.

There are new subdirectories on the DVD image under the Agent/unix directory. There is a new DataMover directory with three subdirectories - AS3, HFS-A (Apache Hadoop) and HFS-C (Cloudera Hadoop) that contain the associated files to support the DataMover functionality, if the associated support is needed.

AS3 Functionality

The TAgent.AS35 file in the installed *Agent/lib* directory is the *TAgent.jar* file that is compiled with Java 1.5 and contains the AS3 interface support.It will replace the existing *TAgent.jar* file in the installed *Agent/lib* directory. Rename the existing *TAgent.jar file* (not using the .jar extension), if desired, and then copy or rename the *TAgent.AS35* file to *TAgent.jar.* The *tagent.ini* file for this installation of the agent must point to a Java 1.5 (or higher) or the default Java must be 1.5 (or higher).

Copy all files from the above referenced AS3 subdirectory into the *Agent/lib* directory.

AS3 Usage Notes

The total volume of data and number of objects you can store are unlimited. Individual Amazon S3 objects can range in size from 1 byte to 5 terabytes. The largest object that can be uploaded in a single PUT is 5 gigabytes. For objects larger than 100 megabytes, customers should consider using the Multipart Upload capability.

When using Multipart upload, each part must be at least 5 MB in size, except the last part. So, in the list of files provided on the dialog box, each must be at least 5MB other than the last file in the list.

HFS Functionality

The *TAgent.HFS6* file in the installed *Agent/lib* directory is the *TAgent.jar* file compiled with Java 1.6 and contains the Hadoop Distributed File System interface support. It will replace the existing *TAgent.jar* file in the installed *Agent/lib* directory. Rename the existing *TAgent.jar* file (not using the .jar extension), if desired, and then copy or rename the *TAgent.HFS6* file to *TAgent.jar.* The *tagent.ini* file entry for this installation of the agent must point to a Java 1.6 (or higher) or the default Java must be 1.6 (or higher). You can also run AS3 DataMover jobs with this *TAgent.jar*, but you must copy all the files from the AS3 subdirectory into the *Agent/lib* directory also in order to run AS3 jobs.

Apache Hadoop

HFS-A subdirectory contains jars related to apache.

It contains multiple sub directories - 1.1, and 1.1.2, each representing the corresponding version of Apache, that is, Apache 1.1, and Apache 1.1.2.

Copy all files from the above referenced *HFS-A* subdirectory into the *Agent/lib* directory.

Cloudera Hadoop

HFS-C subdirectory contains jars related to Cloudera.It contains subdirectories supporting CDH3 and CDH 4 versions.Copy all files from the above referenced *HFS-C* subdirectory into the *Agent/lib* directory.

MapR Hadoop

In order to use DataMover for MapR Hadoop, the MapR Client must be installed on the machine running the TES agent. The TES agent supports MapR Client versions 1.2.9 and 2.0.0. It is the user's responsibility to ensure that the MapR Client is installed properly and is communicating with the MapR Cluster. The following Web page contains information on how to set up the MapR Client:

http://www.mapr.com/doc/display/MapR/Setting+Up+the+Client

There are no files to be copied for MapR Hadoop. However, updates to the *tagent.ini* file are required. See "HFS Usage Notes" for details.

HFS Usage Notes

Agent Ini File

Kerberos Configuration

If the Agent is going to access any Hadoop file system that is secured by Kerberos, then the Kerberos Realm and Kerberos KDC Name must be specified in the Agent's *tagent.ini* file. The new parameters are **`KerberosRealm`** and **`KerberosKDC`**. Like other *tagent.ini* parameters, these values can be specified at a global (all) agent level and/or on a per agent basis. Unless both of these parameters are defined, the agent will not attempt Kerberos authentication even if the Hadoop Data Mover Job has checked the **Use Kerberos Authentication** check box.

MapR Configuration

When using MapR Hadoop on a 64-bit machine, add the following line to your *tagent.ini* file (assuming the MapR Client is installed in the default location):

jvmpara=-Djava.library.path=/opt/mapr/hadoop/hadoop-0.20.2/lib/native/Linux-amd64-64

When using MapR Hadoop on a 32-bit machine, add the following line to your *tagent.ini* file (assuming the MapR Client is installed in the default location):

jvmpara=-Djava.library.path=/opt/mapr/hadoop/hadoop-0.20.2/lib/native/Linux-i386-32

To use MapR Hadoop, you must also specify the location of the MapR Hadoop jar files. Use the *MapRClasspath* parameter to specify the full path to the required MapR Hadoop jar file directory.

Add the following line to your tagent.ini file (assuming the MapR Client is installed in the default location):

maprclasspath=/opt/mapr/hadoop/hadoop-0.20.2/lib/*

User Configuration File

With this release of the Agent, there is a new user configuration file, *TdlUser.cfg*, that specifies parameters for the runtime user associated with a job. It is located in the agent's root directory, for example, /opt/TIDAL/Agent/<name of agent>.

The user configuration file has the following layout:

parameter=value

parameter=value

[user-1]

parameter=value

parameter=value

.

.[user-2]

parameter=value

parameter=value

A parameter value is specified in a parameter/value line which has the form parameter=value. Default configuration parameters to be applied to all users are specified before the first user specific parameter values. This is referred to as the “default section”. To specify parameter values and/or to override a default parameter value for a particular user, add a section for that user. A user section starts with a "user section" line that contains the user name enclosed in brackets (“[", “]”) followed by a number of parameter/value lines. All parameter/value lines following a user section line up until the next user section line (or end of the file) are applied to that specific user. Parameter values specified in a user section override parameter values that are specified in the default section. Lines that start with the "#" character are ignored.

The new user configuration parameters are KerberosPrincipal and KeyTabFilePath. These parameters specify the Principal and KeyTab file for the Agent to use when performing Kerberos authentication.

Tidal Agent for z/OS

The Tidal z/OS agent component of the z/OS adapter provides the following services to a master:

- Submits JCL (JES2)
- Executes USS (OMVS) scripts and programs
- Executes system (console) commands
- Tracks current state and status of Scheduler submitted jobs
- Monitors file dependencies (HFS and exist/non-exist for datasets)
- Transfers job output to the master

This agent is implemented using Tidal Java agent technology and is stored along with configuration and logging files in the hierarchical file system (HFS) of USS. The z/OS agent uses IBM’s implementation of TCP/IP to communicate with the Scheduler master.

z/OS Agent Requirements

The following is a list of minimum hardware and software requirements for using the z/OS agent:

	Requirement
Hardware	S/390 or compatible architecture
	Approximately 4MB of available disk space. At least 40MB for production (logs, working files, etc.) is recommended.
	Network connectivity between the Scheduler agent and Scheduler master machines

	Requirement
Software	OS/390 V2R10 with JES2 and z/OS Unix system services
	Workload Manager must be running in **goal** mode to use the workload balancing and job control (stop and resume) features
	TCP/IP network protocol
	The Scheduler master system must be able to ping the Scheduler agent system, and the Scheduler agent system must be able to ping the Scheduler master system
	z/OS UNIX system services
	JVM 1.4.2+ (recommended) (To download the JVM file (PTF) with its instructions, visit IBM's website at: www.ibm.com/servers/eserver/zseries/software/java

Note The z/OS agent cannot work properly unless all software prerequisites are installed and configured properly.

Prerequisites for Installation

There will be two user IDs involved in installing and running the agent. The first user ID that is needed to install the agent must have the following capabilities:

- Utilize OMVS environment
- UID 0 authority
- APF authority (BPX.FILEATTR.* facility read access in RACF or equivalent)

The userid that is created or chosen to own and run the Agent must have the following capabilities:

- OMVS segment
- BPX.DAEMON facility read access (in RACF or equivalent)
- OPERCMDS authority (RACF or equivalent) at a minimum, requires:
  - Submit jobs
  - Display job status
  - Cancel jobs
  - Suspend jobs
  - Restart jobs
  - Monitor jobs

Note Both, the installer and the owner of the agent, need an assigned GID.
The user installing the agent requires the Superuser UID of 0.
The owner of the agent, however, should not have the UID of 0 (superuser) associated with it.
The user name associated with the agent owner's UID should not be more than six characters long.

The z/OS agent requires APF authorization to issue JES2 and MVS operator commands to control and monitor an MVS job's execution. These authorization rights for the agent must include:

- submitting jobs
- displaying job status
- canceling jobs
- suspending jobs
- restarting jobs that execute in a known address space
- monitoring jobs

Create a USS Directory

Before installing the z/OS agent on a z/OS system, you must create a directory in the USS HFS that conforms to the following:

- It is recommended that you use the directory **/TIDAL/Agent** when installing the agent. The agent installation will create multiple subdirectories under that directory.
- The volume dedicated to the z/OS agent should be at least 20 MB in size but may need to be larger depending on the number of jobs running and the volume of their output.
- The owner of the z/OS agent product files must have **READ** and **EXECUTE** access rights to the directory under which they were installed; otherwise, the installation will fail.

Note Both, the installer and the owner of the agent, need an assigned GID.
The user installing the agent requires the Superuser UID of 0.
The owner of the agent, however, should not have the UID of 0 (superuser) associated with it.
The user name associated with the agent owner's UID should not be more than six characters long.

Verify that Workload Manager is in Goal Mode (optional)

To verify that Workload Manager is in Goal mode:

Step 1 To display the current mode, enter the following from the system console:

```
D WLM,SYSTEMS
```

Step 2 If the agent system is not running in goal mode, you can modify the mode from the console by entering the following command:

```
F WLM,MODE=GOAL
```

Step 3 If you want your system to automatically run Workload Manager in goal mode, remove the **IPS=xx** parameter from the IEASYSxx member in PARMLIB.

During IPL, the absence of this parameter causes Workload Manager to run in goal mode.

Step 4 If Workload Manager on your system runs in compatibility mode and you do not want your system to run in goal mode, the workload balancing feature and the stop/resume job control feature are not available. If you want to use the agent workload balancing feature and the stop and resume job control feature, Workload Manager must be running in goal mode.

Installing the z/OS Agent

To install the z/OS agent, perform the following steps:

Step 1 From the **z/OS Agent** folder on the Scheduler DVD-ROM, copy or FTP (binary mode) the installation files, *install.sh* and *install.tar*, to the temp directory you created for the installation in the HFS.

Step 2 Change to the directory where you FTPed the installation files.

Step 3 Log on to TSO or ISPF.

When you log on, be sure to allocate at least two MB of memory (SIZE=2048000) for your session. This amount of memory is required during installation and is needed anytime the agent is started.

Step 4 Invoke the USS shell from TSO (do not use **rlogin**).

You must be a user with Superuser authority (UID=0) and change to the directory you created for the agent or the directory where the agent is already installed.

For example:

```
READY
OMVS
IBM
Licensed Material - Property of IBM
5647-A01 (C) Copyright IBM Corp. 1993, 2000
(C) Copyright Mortice Kern Systems, Inc., 1985, 1996.
(C) Copyright Software Development Group, University of
Waterloo, 1989.
All Rights Reserved.
U.S. Government users - RESTRICTED RIGHTS - Use,
Duplication, or Disclosure restricted by GSA-ADP schedule
contract with IBM Corp.
IBM is a registered trademark of the IBM Corp.
=> cd /opt/<temp directory>
```

Step 5 Change mode on *install.sh* so it can be executed.

```
chmod 755 install.*
```

Step 6 Run the installation script by entering:

```
./install.sh
```

After starting the installation script, you may have to wait a few moments. Do *not* press **ENTER**.

Step 7 You will see a banner and a message about making a current backup before installing new software. If you have not backed up your files before beginning the installation, quit the installation by typing **n** and back up your files. To proceed with the installation, type **y.**

Note Throughout this installation, default responses to prompts are shown in brackets.

Step 8 Enter the name of the user who will own the agent files (agent owner).

Step 9 Enter the directory location where the files should be installed. It is recommended that default location (**/TIDAL/Agent**) be used. Entering **y** will begin installing the agent files.

Information on the files being installed is displayed. Once the files are installed, the **Agent Configuration Menu** is displayed with options for adding, editing and deleting agent instances.

Note You must add at least one agent instance and configure it.

Step 10 After selecting the option to add an agent instance (1), you must enter a name for the agent, a port number and the directory path to the Java binaries directory.

Step 11 It is recommended to use the default port number, **5912**, if possible. If you have used the default locations when installing, you can just press the **ENTER** button.

Step 12 Once you confirm the selections, you are returned to the **Agent Configuration Menu**. Quit the **Agent Configuration Menu** by typing **Q** and pressing **ENTER**.

Non-Stop Kernel (NSK) Agent

The Non-Stop Kernel (NSK) system has two user environments, Guardian and Open System Services (OSS) that run on the base operating system called **NonStop**. The Tidal Agent for NSK uses Java Virtual Machine (JVM) and runs in the OSS user environment.

Like all Tidal agents, the following four services of the NSK agent are available to the master for scheduling processes and monitoring files.

- Jobs (OSS environment and Guardian environment using the **gtacl** command)
- File state monitoring
- FTP and SFTP Jobs
- File monitoring

Prerequisites for Installation

The following requirements must be met prior to installation and operation of the agent for NSK:

- NSK S-series or NSK Itanium machine
- Java Virtual Machine (JVM) 1.4.2_7+
- Agent machines require a minimum of:
  - 512 MB of RAM
  - 100 MB of disk space for the product and its log files
- A license file for the agent should be available to apply after installation.
- A *super.super* user alias to install the agent and another user alias to own and control the agent. This agent owner must have right to access the JVM.

Installing the NSK Agent

Before installing the Tidal Agent for NSK, backup your files and gather the following information:

- Name of the user alias who will own the agent
- Port number for the agent
- Directory path for the Java Virtual Machine (JVM)

To install the agent from the command line:

Step 1 If you have not already done so, backup your files before beginning the installation procedure.

Step 2 Insert the installation DVD-ROM into the machine you want to install the agent on.

Step 3 Login as *system.system* user alias.

Step 4 Copy the *install.com* and *install.tar* files from the directory on the DVD-ROM (**<DVD-ROM>\agent\NSK\command**) to your **Temp** directory.

Step 5 Change the permissions on the *install.sh* file in the directory to make the file executable.

```
chmod 755 install.sh install.tar
```

Step 6 To begin the installation, type the following and press ENTER to display the initial screen:

```
./install.sh
```

Step 7 To continue the installation, type **y** and press **ENTER**.

Note You can exit the installation program at any time by pressing **CTRL+C**.

Step 8 Type the user alias who will own the agent and press **ENTER**.

Step 9 Enter the user's password and press **ENTER**.

Note Do not unpack the *install.tar* file. This file will automatically unpack during the installation process.

A directory recommendation for the agent files displays.:

Type the name of the directory where you want to install the agent files and press **ENTER**.

It is recommended that you use the default directory path.

The default directory is displayed inside of brackets. If you wish to install into the default directory, press **ENTER** without typing anything.

Step 10 Type y and press **ENTER**.

Step 11 Review the information that you have entered.

If the information is correct, begin installing the agent files by typing **y** at the command prompt and pressing **ENTER**.

The **Agent Configuration** menu displays.

Step 12 Enter **1** to add an instance and press **ENTER**.

Step 13 Enter the name to call the agent and press **ENTER**.

Step 14 Enter the number of the port the agent will use and press **ENTER**.

Step 15 Enter the Java binaries (JVM) directory path and press **ENTER**.

To use the default directory path, do not type a directory path and press **ENTER**.

Step 16 Enter **y** to accept the selections.

If the information is not correct, type **n**. You are prompted again for the name, port number and directory path for the agent.

Tidal Agent for OVMS

Installation Prerequisites

The following requirements must be met prior to installation and operation of the agent for OVMS:

- OVMS Alpha 7.2.2 with JVM 1.4.1OVMS Alpha 7.3.2 with JVM 1.4.2(Be sure the user has the rights to access the JVM.)
- Agent machines for the OVMS agent require a minimum of:
  - 1 Gig of RAM on the agent machine dedicated to the OVMS agent
  - 100 MB of disk space dedicated to the OVMS agent and its log files
- A user needs the following privileges to run jobs on the OVMS agent:
  - NETMBX
  - TMPMBX
- A user needs the following additional privileges to manage the agent:
  - CMKRNL
  - GRPPRV
  - IMPERSONATE NETMBX
  - SYSPRV
  - TMPMBX
- A license file for the agent should be available to apply after installation.
- A root user account to install the agent with an OVMS user account to own and control the agent. (Be sure the user has the rights to access the JVM.)

Installing the Agent

Before installing the Tidal Agent for OVMS, backup your files and gather the following information:

- Name of the user who will own the agent
- Port number for the agent
- Directory path for the Java Virtual Machine (JVM)

To install the agent from the command line:

Step 1 If you have not already done so, backup your files before beginning the installation procedure.

Step 2 Login as system or the account that the account will run as.

Step 3 Copy the *install.com* and *pduct.bck* files to your system. The two files require different formats when they are FTPed.

- Send the *install.com* file in ASCII format
- Send the *pduct.bck* file in binary format.

Step 4 After downloading the *pduct.bck* file at the OVMS machine, set the Logical Record Length by applying the following command:

```
set file/attrib=(lrl:32256) pduct.bck
```

Step 5 To begin the installation, type the following and press ENTER to display the initial screen:

```
$ @install
```

Step 6 To begin the installation process, type **2** and press **Enter**.

Note You can exit the installation program at any time by pressing CTRL + c

If the installation program cannot find the Java Runtime Engine (JRE), the installation will not proceed and the following message is displayed:

```
"Java Run Time not found. Please install Java Run Time first."
```

Step 7 Type the name of the disk of your system where you want to install the agent files and press **Enter**. The default disk is displayed inside of brackets. If you wish to install into the default disk, press **Enter** without typing anything; however, if your system does not have a disk with this name than the installation process will stop.

Step 8 Type the name of the directory where you want to install the agent files and press **Enter**. The default directory is displayed inside of brackets. If you wish to install into the default directory, press **Enter** without typing anything.

The installation procedure will create the OVMS agent files in the designated location.

Step 9 Type the name of the user who will own the agent and press **Enter**.

Step 10 The installation program will prompt for the version of Java being used. If your system is using OVMS alpha version 7.2.2 you need to use JVM 1.4.1. If your system uses OVMS alpha version 7.3, you need to use JVM 1.4.2. Type the JVM version you are using and press **Enter**.

Once the JVM is determined, the installation program starts creating the agent files.

Step 11 Type a name for the agent.

Step 12 Type the number of the port that the OVMS agent should use and press **Enter**. The default port number is **5912**.

The installation of the OVMS files is complete.

Step 13 Run the following command in the directory where the agent was installed:

```
$ @AGENT_SYM.COM
```

Step 14 Verify that the OVMS agent is correctly installed by running the agent in debug mode.

Note The agent can only be started and stopped from its *.bin* directory. Be sure that you are in the *.bin* directory when starting and stopping the agent.

Step 15 Type the following, replacing the brackets and the text between them with the name of the agent, and press ENTER.

```
$ tagent <name of OVMS agent> debug
```