Server Automation

Software Version: 10.60

Troubleshooting Guide

Document Release Date: May 24, 2017
Software Release Date: May 24, 2017

Hewlett Packard
Enterprise

Legal Notices

Warranty

Restricted Rights Legend

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: https://softwaresupport.hpe.com/.

This site requires that you register for an HPE Passport and to sign in. To register for an HPE Passport ID, click **Register** on the HPE Software Support site or click **Create an Account** on the HPE Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Support

Visit the HPE Software Support site at: https://softwaresupport.hpe.com.

This website provides contact information and details about the products, services, and support that HPE Software offers.

HPE Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support website to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HPE Support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HPE Passport user and to sign in. Many also require a support contract. To register for an HPE Passport ID, click **Register** on the HPE Support site or click **Create an Account** on the HPE Passport login page.

To find more information about access levels, go to: https://softwaresupport.hpe.com/web/softwaresupport/access-levels.

HPE Software Solutions Now accesses the HPESW Solution and Integration Portal website. This site enables you to explore HPE Product Solutions to meet your business needs, includes a full list of Integrations between HPE Products, as well as a listing of ITIL Processes. The URL for this website is https://softwaresupport.hpe.com/.

Contents

Troubleshoot

This section provides information to troubleshoot issues that may occur while installing, administering, or using SA.

Troubleshoot SA installation

The following section provides information about problems that occur during installation and the resolutions to those problems.

Restarting an interrupted installation

Should the SA Installer encounter a correctable error, the installation stops. Correct the error and retry the installation. To restart an interrupted installation after you have corrected any errors, perform the following tasks:

1. Invoke the SA Installer using the temporary CDF that was created by the interrupted installation; for example:

   ```
   /<distro>/opsware_installer/hpsa_install.sh -c /var/tmp/cdf_ts_temp.xml
   ```

   where `<distro>` is the full path to the media. Use the latest CDF as determined by the time stamp. See How and when CDFs are saved for details.

2. You see a screen similar to the following:

   ```
   Specify Hosts to Install
   ========================

   Currently specified hosts:

   <IP_address> (oracle_sas)
   <IP_address> (word_store)
   <IP_address> (gateway_master, osprov_boot_slice, slice, osprov_media)

   Please select one of the following options:

   1. Add/edit host(s)
   2. Delete host(s)

   Enter the option number or one of the following directives
   (<c>ontinue, <p>revious, <h>elp, <q>uit): c
   ```

where `<IP_address>` is the IP address for the host(s) you specified during the interrupted installation (taken from the CDF).

Press `c` to continue.

3. You see a screen similar to the following:

   ```
   Host Passwords
   ==============

   Parameter 1 of 3
   <IP_address> password []:
   ```

   Enter the root password for each host specified as part of the installation.

   When all passwords have been entered, press Y to continue.

   ```
   All values are entered. Do you wish to continue? (Y/N) [Y]:
   End of interview.
   ```

   At this point, the SA Installer will check the state of any components already installed before the installation was interrupted.

4. Select the Install Type when prompted (must be the same as the Install Type selected for the interrupted installation).

5. You see a screen similar to the following:

   ```
   Host/Component Layout
   =====================

   Installed Components
   Oracle RDBMS for SAS : <IP_address>
   Model Repository, First Core : <IP_address>
   Multimaster Infrastructure Components : <IP_address>
   Software Repository Storage : <IP_address>
   Slice : <IP_address>
   OS Provisioning Media Server : <IP_address>
   OS Provisioning Boot Server, Slice version : <IP_address>
   Software Repository - Content (install once per mesh): <IP_address>

   ------------------------------------------

   Select a component to assign

   1. Slice
   ```

```
Enter the number of the component or one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit): c
```

Press `c` to continue.

6. You see a screen similar to the following:

   ```
   Interview Parameters
   ====================

   Navigation keys:
   Use <ctrl>P to go to the previous parameter.
   Use <ctrl>N to go the next parameter.
   Use <tab> to view help on the current parameter.
   Use <ctrl>C to abort the interview.


   All prompts have values. What would you like to do:

   1. Re-enter values
   2. Continue

   Enter the option number or one of the following directives
   (<c>ontinue, <p>revious, <h>elp, <q>uit): c
   ```

   The SA Installer uses the parameter values specified in the CDF from the interrupted installation. You should not need to change these values. Press `c` to continue.

7. After the Installer completes some preparation, you see a screen similar to the following:

   ```
   Install components
   ==================

   Components to be Installed
   -------------------------
   OS Provisioning Boot Server, Slice version: <IP_address>

   Up-to-date Components (will not install)
   ----------------------------------------
   Oracle RDBMS for SAS : <IP_address>
   Model Repository, First Core : <IP_address>
   Multimaster Infrastructure Components : <IP_address>
   Software Repository Storage : <IP_address>
   Slice : <IP_address>
   ```

```
OS Provisioning Media Server : <IP_address>
Software Repository - Content (install once per mesh): <IP_address>


Enter one of the following directives
(<c>ontinue, <p>revious, <h>elp, <q>uit):
```

Note that the components that had been installed before the installation was interrupted are listed under Up-to-date Components (will not install).

The uninstalled components are listed under Components to be Installed.

Press `c` to continue the installation from the point it was interrupted.

> **Note:** When resuming an interrupted installation, you must not change the hosts or component host assignments you specified during the original installation.

Troubleshoot SA provisioning

Server does not enter maintenance mode

Symptoms

- Server does not show up in SA
- "Wait for HPE SA Agent" fails with a timeout error

What to check for

- Check the server console
- Check that DHCP is working and the server is on the right network
- Check that the SA Agent was able to register

HPE ProLiant Gen8 or newer servers do not enter maintenance mode

Symptoms

- The "Boot" step fails
- The "Wait" step fails after a successful boot step

What to check for

- Check that DHCP is working and the server is on the correct network or that the network information is correct
- Check the error messages from the "Wait" step, they will contain additional information. Failure to download the SA Agent is often a sign that the network is not configured properly
- Consider upgrading "Intelligent Provisioning" on the server and try again
- Consider upgrading the iLO firmware on the server and retry
- Log in to the server's iLO interface of the server and perform an iLO reset

Failure before the OS Install starts

Symptoms

- Failures in "Set Media Source", "Create Stub Partition" or other scripts before the Reboot script

What to check for

- Ensure that the input parameters, such as the media path are correct
- Ensure that the server has a hard disk and that the hard disk is recognized by the service OS
- Ensure that the media server is online and functional
- Ensure that the network and DHCP are configured properly. For example, if the Media Server is specified by host name, check that DNS is configured properly and is working

Failure of the OS Installer

Symptoms

- "Monitoring" or "Run setup" scripts fail
- Other failures before rebooting into the installed OS

What to check for

- Ensure that the media is correct and complete and that it matches the OS, version and architecture of the Build Plan. For example, do not use a Build Plan that installs a 64-bit OS with 32-bit media
- If you customized the installation profile, ensure that it is correct and valid
- Check the server console and/or the output of the Build Plan for more information about the failure
- Check with the OS vendor for more troubleshooting tips

Failure when waiting for the production SA Agent

Symptoms

- The "Wait" step for the production SA Agent fails

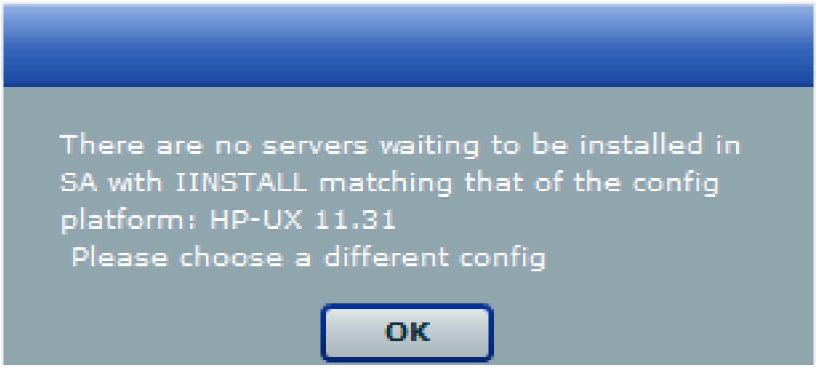
What to check for

- Check the server console to verify that the OS was able to boot. Some installation failures are only detected on first boot. If the OS failed to boot, ensure that the installation profile was correct
- Check that any additional driver that was added during provisioning matches the server
- Check with the OS vendor for more troubleshooting tips. Ensure that the server has correct network drivers and that the server can communicate with the SA Core
- Ensure that a firewall setting is not preventing communication between the SA Agent and SA Core

Troubleshoot HP-UX provisioning

No servers waiting to be installed

If there are no servers waiting at the network boot prompt with the HP-UX version that matches the selected configuration's HP-UX version, the following message is displayed:

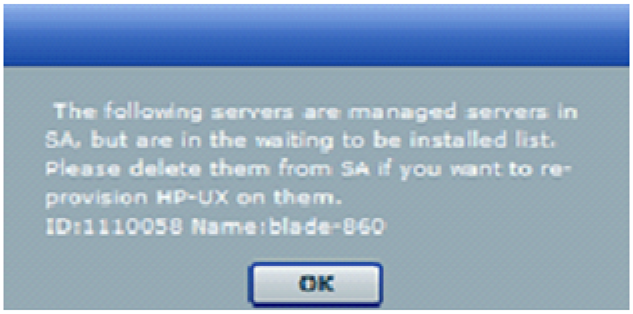


There are no servers waiting to be installed in SA with IINSTALL matching that of the config platform: HP-UX 11.31
Please choose a different config

Ensure that you have the selected correct configuration.

Servers waiting to be installed are managed servers

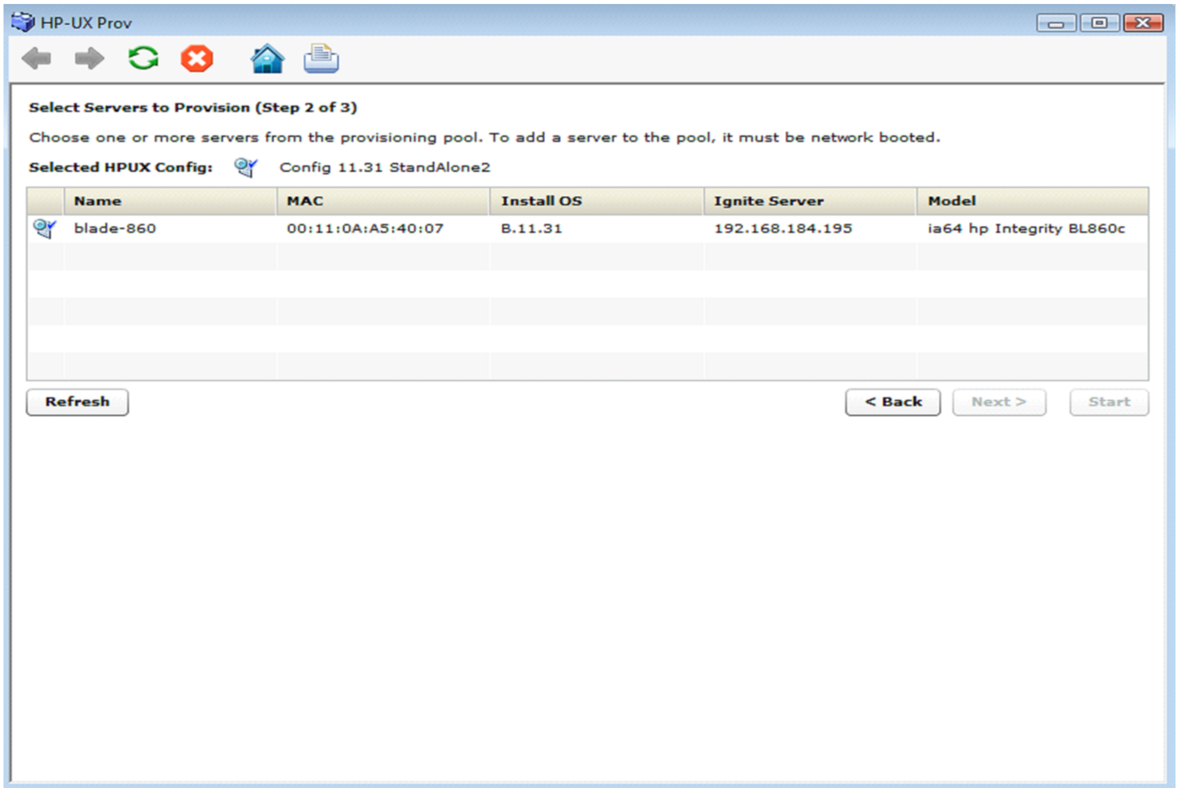
If there are servers waiting for network installation but they are already managed by SA, the following warning message is displayed.



The following servers are managed servers in SA, but are in the waiting to be installed list. Please delete them from SA if you want to re-provision HP-UX on them.
ID:1110058 Name:blade-860

This warning message indicates that the listed servers are waiting for installation but are not candidates for reprovisioning because they are listed as Managed Servers in SA. To continue reprovisioning these servers, you must manually delete them from the SA managed server list.

For more information about deactivating and deleting a server from the SA managed servers list, see the SA User Guide.



Select Servers to Provision (Step 2 of 3)

Choose one or more servers from the provisioning pool. To add a server to the pool, it must be network booted.

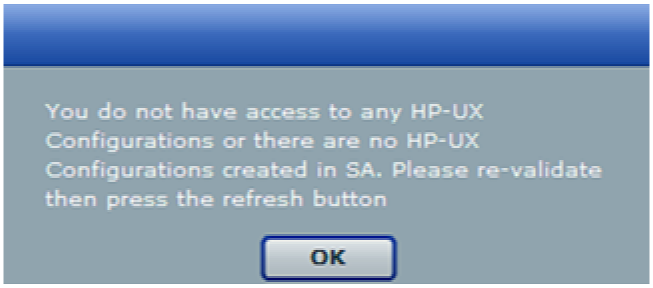
Selected HPUX Config: Config 11.31 StandAlone2

Name	MAC	Install OS	Ignite Server	Model
blade-860	00:11:0A:A5:40:07	B.11.31	192.168.184.195	ia64 hp Integrity BL860c

Once a server is deleted, it is not listed under the SA managed server list. Click **Refresh** in the HP-UX Provisioning APX window and the server should be listed under the unprovisioned server pool. Select the server and continue provisioning it.

Configurations unavailable or permissions not granted

This message appears when you do not have enough permission granted to list the configurations or there are no configurations found.



You do not have access to any HP-UX Configurations or there are no HP-UX Configurations created in SA. Please re-validate then press the refresh button

Contact your SA Administrator to obtain permission or create required configurations using the Custom Configuration Editor APX.

Incorrect target listing

In certain error scenarios, you may see stale data in the APX client's menu such as clients that are not currently waiting to be network installed or clients with an incorrect hostname.

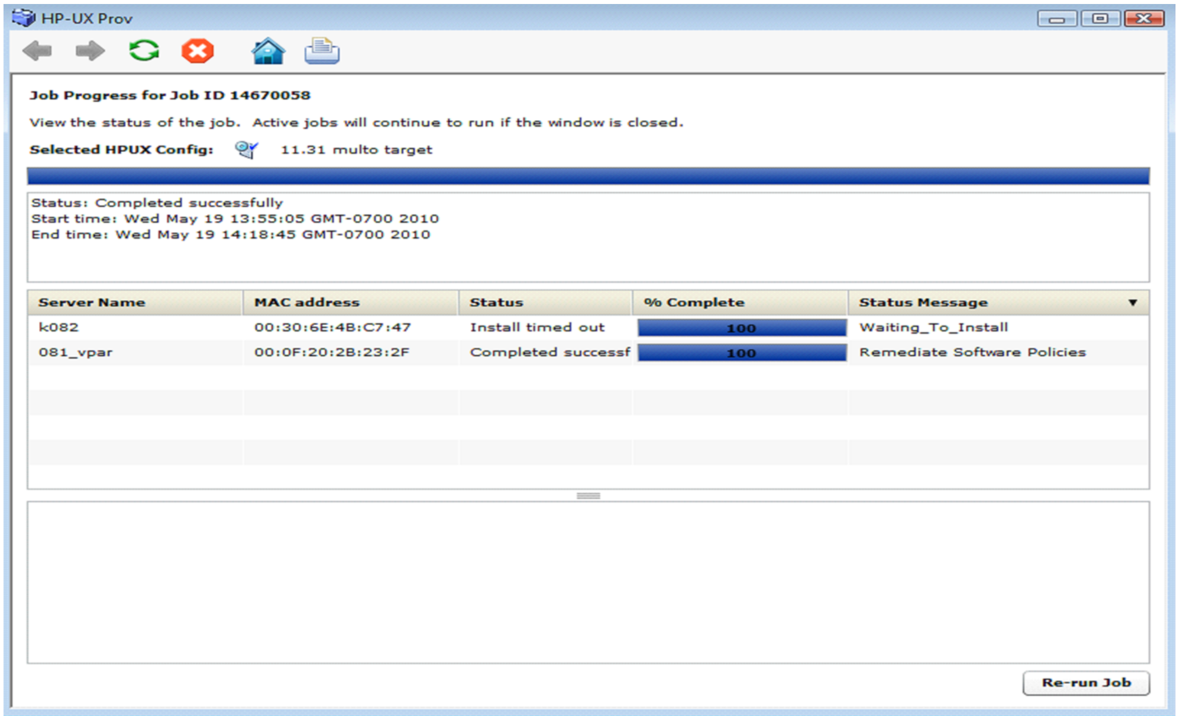
- A client that is not currently waiting to be network installed is displayed in the APX clients list.
  If the target server is reset while waiting to be network installed, the Ignite-UX cannot detect the change and does not update the client's status.

  Retry the installation or delete the directories for the target under `/var/opt/ignite/clients/`. There are two directories for each client, one of the form `<mac address>` (for example, `0x00306EF37245`) and the other a symbolic link to the directory. Delete both directories.

- A client is listed in the APX with an incorrect hostname.
  This can happen when you modify DHCP to provide a different hostname after having previously provisioned the client. Ignite UX reuses the directories in `/var/opt/ignite/clients/` it set up for a client (when it finds a client based on the MAC address), so the APX reuses that information. You can delete the two directories for the client under `/var/opt/ignite/clients` and retry the installation.

Installation timed out error

An installation timed out error occurs when the provisioning job is not initiated on the target server. This could be due to a network issue, the golden image not being available, or for other reasons.



Job Progress for Job ID 14670058

View the status of the job. Active jobs will continue to run if the window is closed.

Selected HPUX Config: 11.31 multo target

```
Status: Completed successfully
Start time: Wed May 19 13:55:05 GMT-0700 2010
End time: Wed May 19 14:18:45 GMT-0700 2010
```

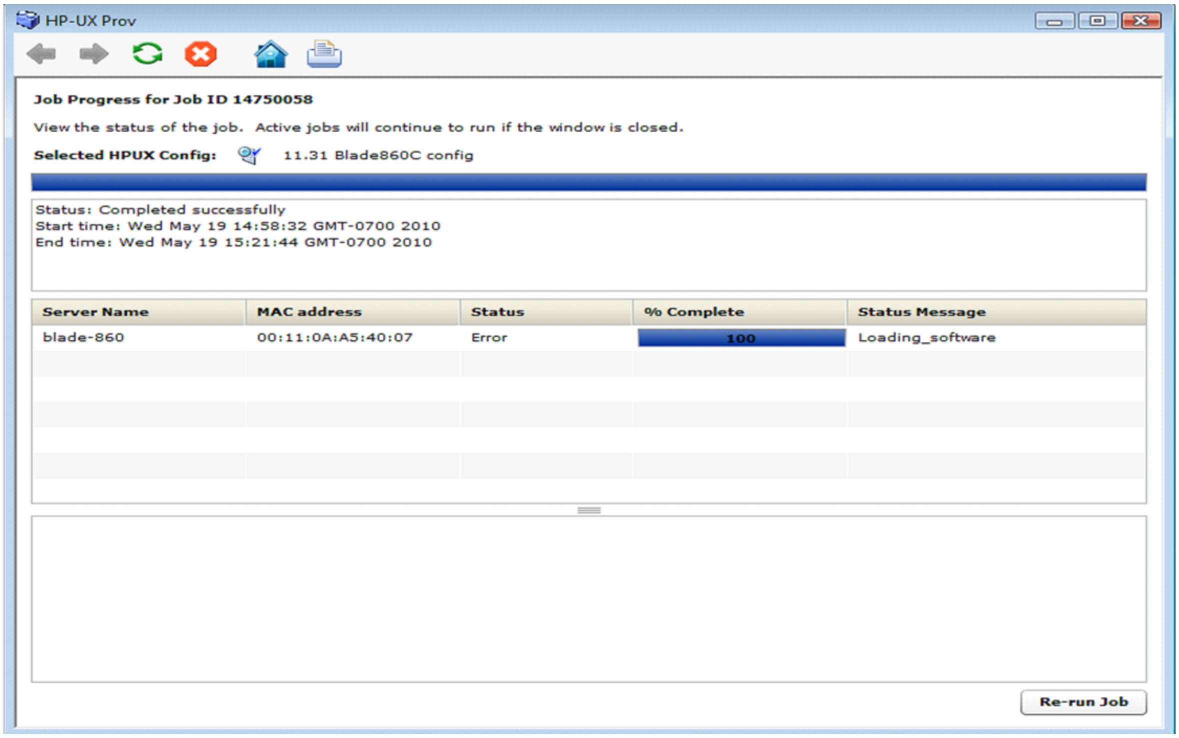
Server Name	MAC address	Status	% Complete	Status Message
k082	00:30:6E:4B:C7:47	Install timed out	100	Waiting_To_Install
081_vpar	00:0F:20:2B:23:2F	Completed successf	100	Remediate Software Policies

Ensure that the network connection and Ignite images are accessible and run the APX again to initiate provisioning.

Loading software error

A loading software error can occur due to:

- Network issues
- Corresponding archive missing or not accessible
- Incorrect setup of golden images



Job Progress for Job ID 14750058

View the status of the job. Active jobs will continue to run if the window is closed.

Selected HPUX Config: 11.31 Blade860C config

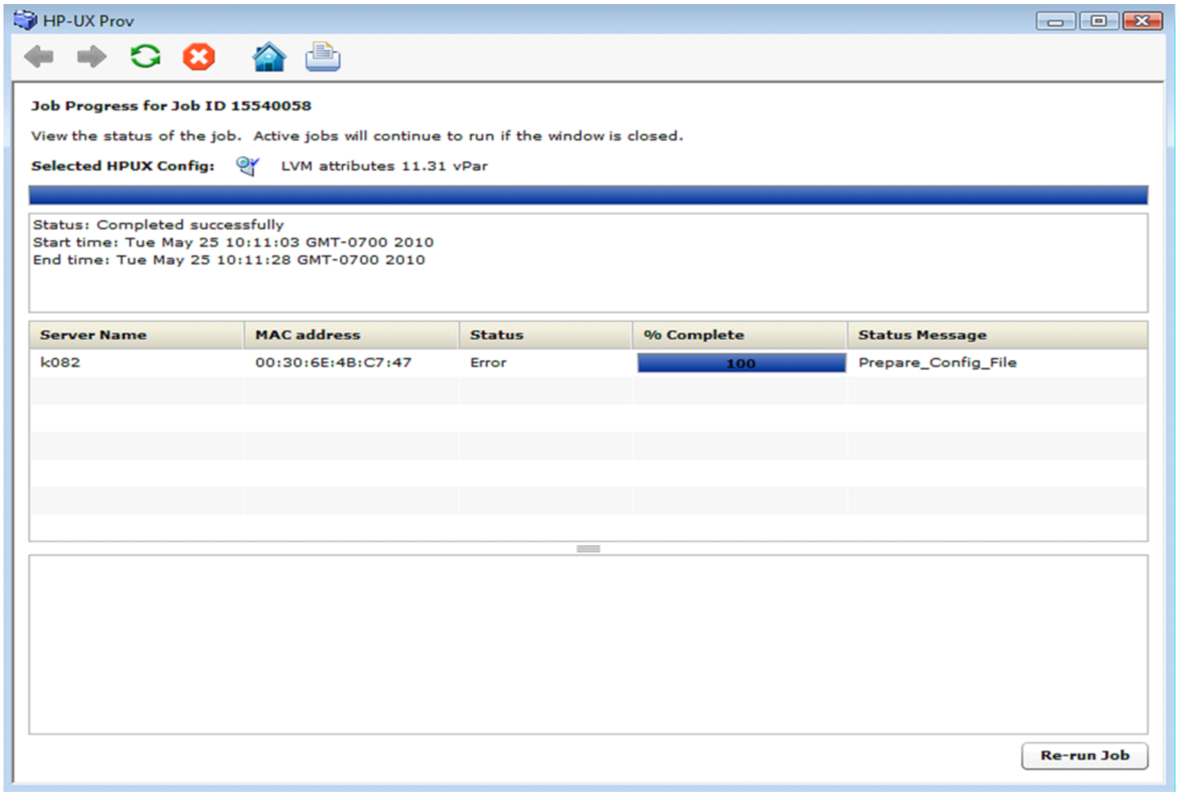
```
Status: Completed successfully
Start time: Wed May 19 14:58:32 GMT-0700 2010
End time: Wed May 19 15:21:44 GMT-0700 2010
```

Server Name	MAC address	Status	% Complete	Status Message
blade-860	00:11:0A:A5:40:07	Error	100	Loading_software

To resolve this, ensure that the Ignite-specific configuration file, Index file, and archives are correctly set up and pointing to correct locations. Also ensure that the network connection between the target and the Ignite server is accessible.

Prepare config file error

The provisioning job fails to initiate on the server when any syntax errors are found in the custom attributes specified in the configuration or when the custom attributes are not compatible.



Job Progress for Job ID 15540058

View the status of the job. Active jobs will continue to run if the window is closed.

Selected HPUX Config: LVM attributes 11.31 vPar

```
Status: Completed successfully
Start time: Tue May 25 10:11:03 GMT-0700 2010
End time: Tue May 25 10:11:28 GMT-0700 2010
```

Server Name	MAC address	Status	% Complete	Status Message
k082	00:30:6E:4B:C7:47	Error	100	Prepare_Config_File

You may need to reboot the system and bring it back to the network boot prompt, then create a new configuration with corrected custom attributes. Ensure that the specified syntax is correct and compatible.

Agent fails to start

If, after successful job completion, the SA Agent fails to start on a newly provisioned target, the golden image you used may already have an Agent installed.

For example, as part of the standard provisioning process, after HP-UX is installed on the server, a post-install script that installs an Agent runs on the server. Because the Agent was previously installed with the golden image, the Agent may not start.

Troubleshoot SA-uCMDB integration

Running the SA-uCMDB connector on a second core

In some cases, a particular core in a multi-master SA Mesh needs to be deactivated and it becomes necessary to run the SA-uCMDB Connector from a different core in that mesh. Sometimes this is also needed if network performance from another core to the uCMDB server is preferred. In those scenarios, the following steps are necessary:

To run the connector on a second core:

1. Stop the SA-uCMDB Connector on the first core and remove its affinity to it.
   /etc/init.d/opsware-sas stop telldaemon
   ```
   /opt/opsware/tell/bin/tell --release
   ```
2. On the second core, enable the SA-uCMDB Connector by running the **enable** command. The syntax of the **enable** command varies depending on your environment. See The enable command in this document for an explanation of the enable command syntax and options.
3. Take responsibility of the SA-uCMDB integration, and then start the SA-uCMDB Connector.
   ```
   /opt/opsware/tell/bin/tell --take
   /etc/init.d/opsware-sas start telldaemon
   ```

To enable additional logging:

1. Start the SA-uCMDB Connector. Normal log files are stored in the /var/log/opsware/tell directory. Default file names include the following:
   tell.0.log (normal startup log)
   ucmdb_failure.*.log (uCMDB failures seen during synchronization)
   LOAD_STATS.*.log (number of processed data)
2. To request additional logging details, specify the requested information in the `/etc/opt/opsware/tell/logging.properties` file as shown in the following table.

/etc/opt/opsware/tell/logging.properties fields

Field	Description
`java.util.logging.FileHandler.limit`	Specifies the maximum number of bytes to write to

/etc/opt/opsware/tell/logging.properties fields, continued

Field	Description
	any one file. Default value is 10000000.
`java.util.logging.FileHandler.count`	Specifies the number of files to use. Default value is 10.
`java.util.logging.FileHandler.append`	Specifies append mode, defaults to true.
`java.util.logging.FileHandler.pattern`	Specifies the pattern for naming the output file where the log file can be found. Defaults to **/var/log/opsware/tell/tell.%g.log**

> **Caution:** Use caution when modifying the file limit. Large numbers might impact performance.

On-demand synchronization

Upon SA restart, the SA-uCMDB Connector normally continues synchronizing SA data to uCMDB from where it ended before the restart. The connector also runs a full sync, periodically. However, in some cases, such as when there are networking or server issues that prevent the updates from reaching the uCMDB server, you may need to trigger the full sync on demand.

To trigger the synchronization on demand:

1. Stop the SA-uCMDB Connector.
2. Restart the SA-uCMDB Connector with the following option:
   ```
   /opt/opsware/tell/bin/tell --startfresh
   ```

Viewing log files

The SA-uCMDB Connector generates the following text log files. You can view these log files in a text editor to get more information.

- /var/log/opsware/tell/tell.0.log is the main log file for information, warnings and errors encountered by the SA-uCMDB Connector.
- /var/log/opsware/tell/LOAD_STATS.0.log contains the status and statistics of the initial data load, and approximate times to complete the initial data load.
- /var/log/opsware/tell/ucmdb_failure.0.log contains uCMDB errors, primarily reconciliation errors if the SA data is incomplete, for example, if the required uCMDB keys are missing. This could happen

if a server did not have a serial number or an IP address, for example. This log file contains the uCMDB exception, the reason why it failed and a trace of the CIs that caused the exception.

SA-uCMDB connector daemon

The SA-uCMDB Connector runs the daemon /etc/opt/opsware/startup/telldaemon on your SA core server. Make sure this process is running on your SA core server.

If it is not running, start it as described in New syntax in the enable command.

If it is running, check the status as described in Displaying the status of the SA-uCMDB connector.

Example– SA-uCMDB Connector Mapping File

```
<DB-UCMBD-HIGHLEVEL-MAPPING>

    <!-- generates installed_software.xml -->

    <Model-Definition model-name='sa' enable='true'>

        <CI ucmdb-ci-type-name='server_automation_system' enable='true' base-
class='server_automation_system'>

            <Attribute source='SA/Description' target-attr='description'
enable='true'/>

            <Attribute source='SA/Name'  target-attr='name' enable='true'/>

            <Attribute-Default target-attr='version' target-attr-value='9.14'
enable='true'/>

        </CI>

    </Model-Definition>

    <!-- generates node.xml -->

    <Model-Definition model-name='hosts' enable='true'>

        <CI ucmdb-ci-type-name='server_automation_system' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='ip_address' enable='true' base-class='node'>

            <Attribute source='IpAddress/PrimaryIpName' target-attr='name'
enable='true'/>

            <Attribute source='IpAddress/RoutingDomain' target-attr='routing_
domain' enable='true'/>

        </CI>

        <CI ucmdb-ci-type-name='node' enable='true' base-class='node'>
```

```
            <Attribute source='Node/Name' target-attr='name' enable='true'/>

            <Attribute source='Node/Description' target-attr='description'
enable='true'/>

            <Attribute source='Node/BiosAssetTag' target-attr='bios_asset_tag'
enable='true'/>

            <Attribute source='Node/BiosSerialNumber' target-attr='serial_number'
enable='true'/>

            <Attribute source='Node/BiosUuid' target-attr='bios_uuid'
enable='true'/>

            <Attribute source='Node/DefaultGatewayIpAddress' target-attr='default_
gateway_ip_address' enable='true'/>

            <Attribute source='Node/NetBiosName' target-attr='net_bios_name'
enable='true'/>

            <Attribute source='Node/NodeModel' target-attr='node_model'
enable='true'/>

            <Attribute source='Node/MemorySize' target-attr='memory_size'
enable='true'/>

            <Attribute source='Node/OsDescription' target-attr='os_description'
enable='true'/>

            <Attribute source='Node/OsFamily' target-attr='os_family'
enable='true'/>

            <Attribute source='Node/TenantOwner' target-attr='TenantOwner'
enable='true'/>

            <Attribute source='Node/Facility' target-attr='facility'
enable='false'/>

            <Attribute source='Node/VirtualizationTypeId' target-
attr='virtualization_type_id' enable='false'/>

            <Attribute source='IpAddress/ManagementIpName' target-attr='ip_address'
enable='false'/>

            <CI-Filter enable='true'><![CDATA[(DEVICES.OPSW_LIFECYCLE =
'MANAGED')]]></CI-Filter>

        </CI>

        <Relation ucmdb-relation-type-name='containment' ucmdb-relation-from-ci-
type-name='node' ucmdb-relation-to-ci-type-name='ip_address' enable='true' ucmdb-
relation-id-link='true'/>

        <Relation ucmdb-relation-type-name='aggregation' ucmdb-relation-from-ci-
type-name='server_automation_system' ucmdb-relation-to-ci-type-name='node'
enable='true' ucmdb-relation-id-link='false'/>
```

```
    </Model-Definition>
    <!-- generates installed_software.xml -->
    <Model-Definition model-name='software' enable='true'>
        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>
        <CI ucmdb-ci-type-name='installed_software' enable='true' base-
class='installed_software'>
            <Attribute source='InstalledSoftware/DmlProductName' target-attr='dml_
product_name' enable='true'/>
            <Attribute source='InstalledSoftware/Name'  target-attr='name'
enable='true'/>
            <Attribute source='InstalledSoftware/Version' target-attr='version'
enable='true'/>
            <Attribute source='InstalledSoftware/Vendor' target-attr='vendor'
enable='true'/>
        </CI>
        <Relation ucmdb-relation-type-name='composition' ucmdb-relation-from-ci-
type-name='node' ucmdb-relation-to-ci-type-name='installed_software' ucmdb-
relation-id-link='true' enable='true'/>
    </Model-Definition>
    <!-- generates policy.xml -->
    <Model-Definition model-name='compliance' enable='true'>
        <CI ucmdb-ci-type-name='server_automation_system' reference-ci='true'
enable='true'/>
        <CI ucmdb-ci-type-name='policy' base-class='policy' enable='true'>
            <Attribute source='Policy/Name' target-attr='name' enable='true'/>
            <Attribute source='Policy/Description' target-attr='description'
enable='true'/>
            <Attribute-Default target-attr='policy_defined_by' target-attr-
value='SA' enable='true'/>
            <Attribute-Default target-attr='policy_category' target-attr-
value='audit' enable='true'/>
        </CI>
        <Relation ucmdb-relation-type-name='aggregation' ucmdb-relation-from-ci-
type-name='server_automation_system' ucmdb-relation-to-ci-type-name='policy'
enable='true' ucmdb-relation-id-link='false'/>
```

```
     </Model-Definition>

    <!-- generates hypervisor.xml -->

    <Model-Definition model-name='hypervisor' enable='true'>

        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='hypervisor' base-class='hypervisor' enable='true'>

            <Attribute source='Hypervisor/Name' target-attr='name' enable='true'/>

            <Attribute source='Hypervisor/Description' target-attr='description'
enable='true'/>

            <Attribute source='Hypervisor/ProductName' target-attr='product_name'
enable='true'/>

        </CI>

        <Relation ucmdb-relation-type-name='composition' ucmdb-relation-from-ci-
type-name='node' ucmdb-relation-to-ci-type-name='hypervisor' ucmdb-relation-id-
link='true' enable='true'/>

    </Model-Definition>

    <!-- generates hypervisorRelation.xml -->

    <Model-Definition model-name='vmrelations' enable='true'>

        <CI ucmdb-ci-type-name='hypervisor' base-class='hypervisor' reference-
ci='true' enable='true'/>

        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>

        <Relation ucmdb-relation-type-name='execution_environment' ucmdb-relation-
from-ci-type-name='hypervisor' ucmdb-relation-to-ci-type-name='node' ucmdb-
relation-id-link='false' enable='true'/>

    </Model-Definition>

    <!-- generates policyResult.xml -->

    <Model-Definition model-name='compliance_status' enable='true'>

        <CI ucmdb-ci-type-name='policy' base-class='policy' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='node' base-class='node' reference-ci='true'
enable='true'/>

        <CI ucmdb-ci-type-name='policy_result' base-class='policy_result'
enable='true'>

            <Attribute source='PolicyResult/Name' target-attr='name'
enable='true'/>
```

```
            <Attribute source='PolicyResult/ComplianceStatus' target-attr='compliance_status' enable='true'/>

            <Attribute source='PolicyResult/PolicyResultDateTime' target-attr='policy_result_date_time' enable='true'/>

            <Attribute source='PolicyResult/RulesCompliant' target-attr='rules_compliant' enable='true'/>

            <Attribute source='PolicyResult/RulesNonCompliant' target-attr='rules_non_compliant' enable='true'/>

            <Attribute source='PolicyResult/ComplianceLevel' target-attr='compliance_level' enable='true'/>

        </CI>

        <Relation ucmdb-relation-type-name='composition' ucmdb-relation-from-ci-type-name='policy' ucmdb-relation-to-ci-type-name='policy_result' ucmdb-relation-id-link='false' enable='true'/>

        <Relation ucmdb-relation-type-name='aggregation' ucmdb-relation-from-ci-type-name='node' ucmdb-relation-to-ci-type-name='policy_result' ucmdb-relation-id-link='true' enable='true'/>

    </Model-Definition>

</DB-UCMBD-HIGHLEVEL-MAPPING>
```

Troubleshoot SA-OO integration

SA-OO connection error

If SA cannot connect to OO, administrators can:

- Check that the settings in the Edit Flow Integration Settings window fields are correct. See Use cases: SA-OO flows for more information.)
- Examine the following log file for error messages on the Command Engine server:

  ```
  /var/log/opsware/waybot/waybot.err
  ```

  The error messages do not appear in the SA Client.
- Check that the OO URL, user name, and password are correct.
- Make sure the specified OO user has correct permissions to run the flow.

To check a flow status, see the Flow Integration Panel. For more information on this panel, see Use cases: SA-OO flows.

If you are a user and you see this error, check with your administrator.

Flow run error

This section describes errors you might encounter when you run a flow as a user.

Incorrect inputs

When you try to run a flow, you might receive one of the following error:

- `SA will not pass the selected Device(s) to this flow.`
- `SA-OO Integration Configuration Error: Flow Integration Settings are incorrect. Please verify that the flow Integration URL, username, and password are correct.`

Typically, these errors are displayed when one or more of the following occurred:

- You (as a user) selected the wrong flow to run.
- The OO server is not responding. Ask your administrator for help.
- The inputs an administrator entered in the Edit Flow Integration Settings window are incorrect. Ask your administrator to check the information in the Edit Flow Integrations Settings window. See Use cases: SA-OO flows for more information.
- The flow author must modify the flow definition to use the naming conventions.

Troubleshoot SA-NA integration

To test whether SA is communicating with NA, check the following conditions:

- You can log in to NA with your SA credentials. This verifies that NA can communicate with SA.
- The SA credentials specified in the NA Administrative Settings under External Authentication Type are set to SA. This ensures that NA can look up server MAC addresses.
- The NA Topology Gathering Diagnostic has run successfully. To verify this condition, search for tasks and check their results. This ensures that NA has gathered MAC addresses and tried to look them up in SA.

Troubleshoot Global Shell error messages

The Global Shell feature provides the file system error messages that are described in the following table.

Global Shell errors

Error	Description	Action
Input/output error	Your session has exceeded the time-out limit or the Agent is not running.	Start a new session or check the status of the Agent.
Operation not permitted.	No password was found.	Verify that you have a valid password.
Permission denied.	You are not allowed to view a directory. This does not mean that the directory does not exist on a given server. See the SA Administration Guide for more information.	Verify that you have `readFileSystem` permissions.
RFS Specific error	You do not have permissions on the managed server. For example, this error will occur if you are trying to perform an operation on a managed server and you do not belong to the Administrators group that has the required permissions assigned to it.	You must have a set of permissions to perform operations on managed servers. To obtain these permissions, contact your SA administrator. See the SA Administration Guide for more information.

Troubleshoot Solaris patch installation

Changing the Solaris patch install mode

When you remediate a Solaris patch that has the Install Mode (under Install Parameters in the Properties view) set to Single User Mode, the server will be rebooted into single user-mode before installing the patch. If the remediation fails for some reason (such as when there is a network outage or a hardware failure), the system will remain in single-user mode.

To return the system to multi-user mode:

1. Log in to the Solaris server console.
2. Depending on the Solaris version, change to the directory by entering one of the following commands:

   ```
   cd /etc/rcS.d/    # On Solaris 5.10
   cd /etc/rc1.d    # On Solaris 5.6 - 5.9
   ```

3. Enter the following command.

   ```
   ./S99zOpswPatching exit_single_user_mode
   ```

4. Reboot the server by entering the following command or another method. This will reboot the server into multi-user mode.

   ```
   shutdown -y -g 0 -i 6
   ```

If you do not have access to a server console on your Solaris server, use the SA Global Shell (OGSH) rosh utility:

1. Using an SA user who has the OGFS permission “Log in to Server”, open an OGSH session. For example, you could enter an ssh command such as:

   ```
   ssh -p 2222 <user-name>@<ogfs-host>
   ```

2. Navigate to your Solaris server using a command such as:

   ```
   cd /opsw/Server/@/<server name>/files/root
   ```

3. Launch the rosh utility.

4. Depending on the Solaris version, change to the directory by entering one of the following commands:

   ```
   cd /etc/rcS.d/    # On Solaris 5.10
   cd /etc/rc1.d    # On Solaris 5.6 - 5.9
   ```

5. Enter the following command:

   ```
   ./S99zOpswPatching exit_single_user_mode
   ```

6. Reboot the server entering the following command or another method. This will reboot the server into multi-user mode.

   ```
   shutdown -y -g 0 -i 6
   ```

When you reboot the server, your rosh process will be terminated. Make sure the server is configured to auto-reboot.

If a patch requires single-user mode and fails to install for some other reason, such as a dependent patch is not installed, the Solaris host will be rebooted to single-user mode, the patch installation will be attempted, and the host will be rebooted to multi-user mode. These two reboots occur even if the path installation fails.

Channel-specific sections

Here is an example of a channel specific section. In this case, it enables the Oracle Enterprise Linux 5 Update 6 Patch channel, creating a policy composed of all the packages in that channel. Note that this section is enabled by default as long as the ‘channels’ option is not specified in the [main] section. If the ‘channels’ option is specified in the [main] section, then it must be explicitly enabled via the "enabled" option. Also, channel_path is defined here only as we don't wish to create channel policies for top-level channels

```
[ol5_u6_x86_64_patch]

; enabled=1

# You may wish to import all versions of each packages in the channel. By

# default, only the latest version of each package is imported. Note that

# when importing all versions, it is recommended that packages_only=1 also be

# used since it is not useful to have a policy with more than one version of

# each package.

; which_packages=all
```

```
# You may wish to download the packages for this channel only and then
# create the policies manually. Also useful in combination with
# which_packages=all:
; packages_only=1
# To locate a child channel's packages next to the corresponding policy in
# the library, use a path such as the following:
; package_path=/ULN/Channels/$channel_name Packages
```

Mounting the staging directory in single-user mode

When one item in a remediation process requires a server to restart in single-user mode it can prohibit the rest of the items from being processed if the item is stored in an atypical directory that is not available in single-user mode.

Single-user mode will need to mount the staging directory upon startup. The default staging directory is `/var/opt/opsware/agent`. If the next item is not in the default directory, then the remediation process will not be able to find it and the job will fail.

To resolve this, the managed server just needs to mount the staging directory where the items are stored prior to running the remediation. The simplest way to do this is to write a server script with mount instructions and add it to an existing Solaris start-up script.

For example:

```
echo "mount<stage_dir>">>/etc/rcS.d/S99mount_stage
```

where '`<stage_dir>`' is the directory where the item is stored and '`/etc/rcS.d/S99mount_stage`' is the start-up script on a Solaris managed server.

Troubleshoot server communication tests

This section describes the server communication tests in detail. For an overview, see Running server communication tests.

The server communication test performs the following diagnostic tests to determine if a server is reachable:

- "Command Engine to Agent (AGT) test" on the next page: Determines if the SA Command Engine can communicate with the agent. The Command Engine is the Server Automation core component that enables distributed programs to run across many servers. The Command Engine handles the storage and versioning of scripts into the SA Model Repository. SA stores scripts in the Model Repository.
- "Crypto Match (CRP) test" on page 38: Checks that the SSL encryption files that the agent uses are valid.
- "Agent to Command Engine (CE) test" on page 40: Verifies that the agent can connect to the Command Engine and retrieve a command for execution.
- "Agent to Data Access Engine (DAE) test" on page 46: Checks whether or not the agent can connect to the Data Access Engine and retrieve its device record. The Data Access Engine provides an XML-RPC interface to the Model Repository that simplifies interaction with various clients such as the SA Client, system data collection, and monitoring agents on servers.
- "Agent to Software Repository (SWR) test" on page 51: Determines if the agent can establish an SSL connection to the Software Repository. SA stores software in the Software Repository, including software packages for operating systems, applications, databases, customer code and software configuration information.
- "Machine ID Match (MID) test" on page 57: Checks that the Machine ID (MID) on the server matches the MID registered in the Model Repository.

When the test run finishes, it returns results that show either success or failure for each test run on each server. For each failed test, the nature of failure is listed by error type in the error details column of the Communication Test window. In some cases, the failure of one test might prevent other tests from being executed.

See Running server communication tests for information about how to run a Communication Test.

Command Engine to Agent (AGT) test

The Command Engine to Agent (AGT) communications test system checks that the Command Engine can initiate an SSL connection to the Agent and execute an XML/RPC request.

The thirteen possible results are:

- "AGT – OK" below
- "AGT – Untested" below
- "AGT – Unexpected error" on the next page
- "AGT – Connection refused" on the next page
- "AGT – Connection time-out" on page 35
- "AGT – Server never registered" on page 35
- "AGT – Realm is unreachable" on page 36
- "AGT — Tunnel setup error" on page 36
- "AGT — Gateway denied access" on page 37
- "AGT — Internal Gateway error" on page 37
- "AGT — Gateway could not connect to server" on page 37
- "AGT — Gateway time-out" on page 37

AGT – OK

No troubleshooting necessary.

AGT – Untested

This result is returned when a functional area cannot be tested because of a previous failure that prevents further testing. For example, if the Command Engine cannot contact the Agent, then no other tests are possible.

What can I do if a test is not run during an AGT test?

First resolve all tests that failed, and then run the Communication Test again.

AGT – Unexpected error

This result indicates that the test encountered an unexpected error.

What can I do if I get an unexpected error?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Hewlett Packard Enterprise Customer Support.

AGT – Connection refused

This result indicates that the Command Engine is receiving a TCP reset packet when it attempts to connect to the Agent on port 1002. The likely cause is that the Agent is not running. A firewall might also be blocking the connection.

What can I do if the connection is refused during an AGT test?

Log into the server and confirm that the Agent is running. See "Verifying that a Server Agent is running" on page 59.

If the Agent is not running, restart the Agent. See "Restarting a Server Agent" on page 60.

From the managed server, use netstat to confirm that a socket is in listen mode on port 1002. If not, stop and restart the Agent.

From the server itself, use SSH to connect to the IP address of the server where the Agent is installed and port (1002) that the Agent is listening on. If this does not succeed, stop and restart the Agent.

Verify that the Management IP address that Server Automation is using to reach the server is the correct address. See "Checking management IP of a managed server" on page 61 for more information. If the IP addresses do not match, stop and restart the Agent, then rerun the test.

If the previous steps are performed and the test still fails, the problem is likely caused by either a software-based firewall on the server itself or an external firewall blocking the connection.

AGT – Connection time-out

This result indicates that the Command Engine is not receiving any reply packets when it attempts to initiate a TCP connection to the Agent on port 1002. The likely cause is that the server is not running, or that the IP address that Server Automation is using to reach the Agent is incorrect. (A firewall might also be blocking the connection.) To check the IP address that Server Automation is using to reach the Agent, see "Checking management IP of a managed server" on page 61.

What can I do if the connection times out during an AGT test?

Follow the same steps used to resolve this issue specified in "What can I do if the connection is refused during an AGT test?" on the previous page.

AGT – Request time-out

This result indicates that the Command Engine is able to successfully complete a TCP connection to the Agent on port 1002, but no response is received from the Agent in response to the XML-RPC request. The likely cause is that the Agent is hung.

What can I do if the request times out during an AGT test?

Log into the server and restart the Agent. See "Restarting a Server Agent" on page 60 for detailed information.

Check to see whether or not some other process is consistently utilizing an excessive amount of the CPU on the server where the Agent is installed. Also check to see if the system is performing slowly due to a lack of available memory and/or excessive file IO. In any of these cases, the system might be performing too slowly to permit the Agent to respond to the test in a timely manner.

AGT – Server never registered

This test indicates that the server being tested has neither been registered with the Command Engine, nor can it communicate with the Command Engine. The cause of this could be any number of reasons similar to those in the "Agent to Command Engine (CE) test" on page 40 test. It is also possible (but unlikely) that the Agent was installed but never started.

What can I do if the server has not been registered with the Command Engine during an AGT test?

To troubleshoot this error, use the following procedures:

1. Ensure that the Agent is running. For these instructions, see "Verifying that a Server Agent is running" on page 59.
2. Ensure that the Agent can contact the Command Engine.
3. If the Agent is in a Satellite facility, ensure that its Gateways are properly configured and that it is properly configured to use those Gateways. See "Checking network gateway configuration" on page 61 for more information.
4. If the Agent is not in a Satellite:
5. Ensure the host name “way” (no quotes) resolves to its valid IP address. See "Resolving the host name" on page 62 for more information.
6. Verify that a connection can be established to port 1018 of way.

One (or more) of the above checks will fail. To solve that failure, refer to the corresponding error code in "Agent to Command Engine (CE) test" on page 40, or to the realm connectivity and configuration test.

AGT – Realm is unreachable

The Satellite realm where the managed server is located is unreachable. This means that a path of tunnels between the Gateways in the SA core and the realm of the managed server cannot be established.

What can I do if the realm is unreachable during an AGT test?

This error could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration. Contact Hewlett Packard Enterprise Customer Support for assistance in troubleshooting the Gateway network.

AGT — Tunnel setup error

The Command Engine could not establish a connection through any of its defined Gateways. This could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration.

What can I do if I get a Tunnel Setup error during an AGT test?

Contact your SA administrator.

AGT — Gateway denied access

The Gateway is working but refused to proxy the connection on behalf of the Agent. This error most likely means that the Gateway is misconfigured such that the Gateway will not allow the Command Engine access to the Agent.

What can I do if the gateway is denied access during an AGT test?

Contact your SA administrator.

AGT — Internal Gateway error

Due to an internal error, the Gateway was unable to proxy the connection. This typically occurs when the Gateway is overloaded.

What can I do if there is an internal gateway error during an AGT test?

Contact your SA administrator.

AGT — Gateway could not connect to server

The Gateway could not establish a connection to the Agent. This might be because the Agent is not running, or because a firewall might be blocking the connection.

What can I do if the gateway couldn’t connect to the server during an AGT test?

If you suspect the Agent is not running, see "Verifying that a Server Agent is running" on page 59. To make sure that the Gateway can establish a connection to the IP address of the server where the Agent is installed, try to ping the IP address of the server where the Agent is installed.

AGT — Gateway time-out

The Gateways on the two ends of a tunnel could not communicate with each other, most likely due to a network connectivity problem.

What can I do if the gateway times out during an AGT test?

Ensure that network connectivity is available between the Gateways in the path between the realm of the managed server and the SA core.

Crypto Match (CRP) test

This test checks that the X509 certificates that the Agent uses are valid.

The five possible results are:

- "CRP – OK" below
- "CRP – Untested" below
- "CRP – Unexpected error" below
- "CRP – Agent certificate mismatch" on the next page
- "CRP – SSL negotiation failure" on the next page

CRP – OK

No troubleshooting necessary.

CRP – Untested

This result is returned when a functional area cannot be tested because of a previous failure that prevents further testing. For example, if the Agent cannot be reached, then no other tests are possible.

What can I do if a test is not run during a CRP test?

First resolve all tests that failed, and then run the Communication Test again.

CRP – Unexpected error

This result indicates that the test encountered an unexpected error.

What can I do if I get an unexpected error during a CRP test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Hewlett Packard Enterprise Customer Support.

CRP – Agent certificate mismatch

This result indicates that the certificate that the Agent is using (`agent.p12`) does not match the certificate that is registered with Server Automation for that Agent. Also, a server hosting a Slice Component bundle with the wrong time zone specified could cause a large number of servers with a CRP error during a communications test.

What can I do if I get a certificate CN mismatch during a CRP test?

If the mismatch is determined to be due to a time zone mismatch, synchronize the time zone specifications for the servers. If the error is due to a certificate mismatch, use the Recert Agent Custom Extension to issue a new certificate to the Agent.

CRP – SSL negotiation failure

This result indicates that the Agent is not accepting SSL connections from the SA core. (The SA core is the entire collection of servers and services that provide Server Automation services.) The likely cause of this error is that one or more files in the Agent crypto directory are missing or are invalid.

What can I do if I get an SSL negotiation failure during an CRP test?

Run the Server Recert custom extension in the “set allow recert flag only” mode on the server, and then Run the Server Agent Installer with the “-c” switch.

Reinstalling the Agent with the “-c” option (“c” stands for “clean”) removes all certs on the server and also removes the MID file, which forces the Agent to retrieve a new MID from the Data Access Engine.

See Running server communication tests for more information about how to install a Server Agent using the “-c” switch.

After you reinstall the Agent, run the test again to check if the Agent is now reachable.

Agent to Command Engine (CE) test

This test checks that the Agent can connect to the Command Engine and retrieve a command for execution.

The sixteen possible results are:

- "CE – OK" below
- "CE – Untested" on the next page
- "CE – Unexpected error" on the next page
- "CE – Connection refused" on the next page
- "CE – Connection time-out" on page 42
- "CE – DNS does not resolve" on page 42
- "CE – Old Agent version" on page 42
- "CE – Realm is unreachable" on page 43
- "CE – No Gateway defined" on page 43
- "CE – Tunnel setup error" on page 43
- "CE – Gateway denied access" on page 44
- "CE – Gateway name resolution error" on page 44
- "CE – Internal Gateway error" on page 44
- "CE – Gateway could not connect to server" on page 45
- "CE – Gateway time-out" on page 45
- "CE – No callback from Agent" on page 45

CE – OK

No troubleshooting necessary.

CE – Untested

This result is returned when a functional area cannot be tested because of a previous failure that prevents further testing. For example, if the Agent cannot reach the Command Engine, then no other tests are possible.

What can I do if a test is not run during a CE test?

First resolve all tests that failed, and then run the Communication Test again.

CE – Unexpected error

This result indicates that the test encountered an unexpected condition.

What can I do if I get an unexpected error during a CE test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Hewlett Packard Enterprise Customer Support.

CE – Connection refused

This result indicates that the Agent is receiving a TCP reset packet when attempting to connect to the Command Engine on port 1018. The likely cause is that the Agent is connecting to the wrong IP address. In other words, the Agent does not know the correct IP address of the Command Engine. It is also possible that a firewall might be blocking the connection.

What can I do if the connection is refused during a CE test?

Check that the name “way” resolves to its correct IP address. For instructions on how to do this, see "Resolving the host name" on page 62.

Check to make sure there isn't a firewall refusing the connection to this IP address.

CE – Connection time-out

This result indicates that the Agent is not receiving any reply packets when it attempts to initiate a TCP connection to the Command Engine on port 1018. The likely cause is that the Agent is connecting to the “wrong” IP address. In other words, the Agent doesn’t know the correct IP address of the Command Engine. A firewall might also be blocking the connection.

What can I do if the connection times out during a CE test?

Follow the same steps specified in "What can I do if the connection is refused during a CE test? " on the previous page

CE – DNS does not resolve

This result indicates that the Agent cannot resolve the host name “way” to a valid IP address. In other words, the Agent does not know the correct IP address of the Command Engine.

What can I do if the command engine name does not resolve during a CE test?

Log into the server and confirm that the host name “way” can resolve. If not, check the DNS configuration of the server to make sure that the host name “way” is configured to its correct IP address. See "Resolving the host name" on page 62 for more information.

CE – Old Agent version

This result indicates that the Agent was unable to contact the Command Engine, but the test was unable to determine the exact cause because the Agent is out of date.

What can I do if the agent is out of date during a CE test?

If this error occurs, it will likely be for one of two reasons: either the host name of the Command Engine (“way”) did not resolve, or the connection was refused.

If you believe that the host name of the Command Engine (“way”) did not resolve, then "CE – DNS does not resolve" above.

If you determine that the connection was refused, "CE – Connection refused" on the previous page.

Alternatively, you can upgrade the Agent to the latest version (contact Hewlett Packard Enterprise Customer Support) and re-run the test. See Running server communication tests for more information about how to install an agent.

CE – Realm is unreachable

The Satellite realm where the managed server is located is unreachable. This error means that a path of tunnels between the Gateways in the SA core and the realm of the managed server cannot be established.

What can I do if the realm is unreachable during a CE test?

This error could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration. Contact your SA administrator for assistance in troubleshooting the Gateway network.

CE – No Gateway defined

The managed server is in a Satellite realm, but its Agent is not properly configured to use a Gateway. Agents located in satellites must use a Gateway to contact the core.

What can I do if no gateway is defined during a CE test?

To troubleshoot this error, try the following:

Create or open the opswgw.args file on the managed server. The opswgw.args file is located on the managed server at:

UNIX/Linux: /etc/opt/opsware/agent

Windows: %SystemDrive%\Program Files\Common Files\Opsware\etc\agent

Make sure that this file contains a single line as shown:

```
opswgw.gw_list: <gw_ip_address>:<gw_port>,<gw_up_address>:<gw_port>
```

CE – Tunnel setup error

The Command Engine could not establish a connection through any of its defined Gateways. This could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration.

What can I do if a tunnel setup occurs error during a CE test?

Contact your SA administrator.

CE – Gateway denied access

The Gateway is working, but refused to proxy the connection on behalf of the Agent. This error most likely means that the Gateway is misconfigured such that the Gateway will not allow the Agent to access the Command Engine.

What can I do if the gateway is denied access during a CE test?

Contact your SA administrator.

CE – Gateway name resolution error

The server running the Gateway in the SA core was unable to resolve the host name “way”. It must be able to do this in order to proxy connections on behalf of managed servers in Satellite realms.

What can I do if a name resolution error cccurs on the gateway during a CE test?

Log into the server where the core Gateway is located and use a command such as ping or host to confirm that the host name “way” can be resolved (for example: “host way”).

If you cannot connect, contact your SA administrator so that you can check the DNS configuration of the core Gateway server.

CE – Internal Gateway error

Due to an internal error, the Gateway was unable to proxy the connection. This typically occurs when the Gateway is overloaded.

What can I do if an internal gateway error occurs during a CE test?

Contact your SA administrator.

CE – Gateway could not connect to server

The Gateway could not establish a connection to the Command Engine. The situation might be because the Command Engine is not running, or because the Gateway is resolving the Command Engine host name (“way”) to the wrong IP address. It is also possible that a firewall might be blocking the connection.

What can I do if the gateway can’t connect to server during a CE test?

Check that the name “way” resolves to the correct IP address and that the Gateway can establish a connection to port 1018 at that IP. See "Resolving the host name" on page 62 and "Verifying that a port is open on a managed server" on page 60 for more information.

CE – Gateway time-out

The Gateways on the two ends of a tunnel could not communicate with each other, most likely due to a network connectivity problem.

What can I do if the gateway times out during a CE test?

Ensure that network connectivity is available between the Gateways in the path between the realm of the managed server and the SA core.

CE – No callback from Agent

The Command Engine was able to contact the Agent, but the Agent did not call back to retrieve its command. However, the Agent reports that it can connect to a Command Engine.

What can I do if there is no callback from Agent?

Ensure network connectivity between the agent and the nearest agent gateway. For example, make sure no firewalls are preventing access. The default port for the agent gateway is 3001. For more information on gateway monitoring, see the SA 10.60 Administration Guide. For information on configuring the agent gateway, see the SA 10.60 Install Guide.

Agent to Data Access Engine (DAE) test

This test checks that the Agent can retrieve its device record from Data Access Engine. The fifteen possible results are:

- "DAE – OK" below
- "DAE – Untested" on the next page
- "DAE – Unexpected error" on the next page
- "DAE – Connection refused" on the next page
- "DAE – Connection time-out" on page 48
- "DAE – DNS does not resolve" on page 48
- "DAE – Old Agent version" on page 48
- "DAE – Old Agent version" on page 48
- "DAE – Realm is unreachable" on page 49
- "DAE – No Gateway defined" on page 49
- "DAE – Tunnel setup error" on page 50
- "DAE – Gateway denied access" on page 50
- "DAE – Gateway name resolution error " on page 50
- "DAE – Internal Gateway error" on page 50
- "DAE – Gateway could not connect to server" on page 51
- "DAE – Gateway time-out" on page 51

DAE – OK

No troubleshooting necessary.

DAE – Untested

This result is returned when a functional area cannot be tested, because of a previous failure that prevents further testing. For example, if the Agent cannot reach the Data Access Engine then no other tests are possible.

What can I do if a test is not run during a DAE test?

First resolve all tests that failed, and then run the Communication Test again.

DAE – Unexpected error

This result indicates that the test encountered an unexpected condition.

What can I do if I get an unexpected error during a DAE test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Hewlett Packard Enterprise Customer Support.

DAE – Connection refused

This result indicates that the Agent is receiving a TCP reset packet when attempting to connect to the Data Access Engine on port 1004. The likely cause is that the Agent is connecting to the wrong IP address. A firewall might also be blocking the connection.

What can I do if the connection is refused during a DAE test?

Check that the name “spin” resolves to its correct IP address. See "Resolving the host name" on page 62 for more information.

Check to make sure that a firewall is not refusing the connection to this IP address.

DAE – Connection time-out

This result indicates that the Agent is not receiving any reply packets when it attempts to initiate a TCP connection to the Data Access Engine on port 1004. The likely cause is that the Agent is connecting to the wrong IP address. In other words, the Agent does not know the correct IP address of the Command Engine. A firewall might also be blocking the connection.

What can I do if the connection times out during a DAE test?

Follow the steps specified in "What can I do if the connection is refused during a DAE test?" on the previous page

DAE – DNS does not resolve

This result indicates that the Agent cannot resolve the host name “spin” to a valid IP address. In other words, the Agent does not know the correct IP address of the Data Access Engine.

What can I do if the data access engine name does not resolve during a DAE test?

Log into the server and confirm that the host name “spin” can be resolved. If not, check the DNS configuration of the server to make sure that the host name “spin” is configured to its correct IP address. See "Resolving the host name" on page 62 for more information.

DAE – Old Agent version

This result indicates that the Agent was unable to contact the Data Access Engine, and the test is unable to determine the exact cause, because the Agent is out of date.

What can I do if the agent is out of date during an DAE test?

If this error occurs, it will likely be for one of two reasons: either the host name of the Data Access Engine (“spin”) did not resolve, or the connection was refused.

If you believe that the host name of the Data Access Engine (“way”) did not resolve, then see "DAE – DNS does not resolve" above.

If you determine that the connection was refused, see "What can I do if I get an unexpected error during a DAE test? " on the previous page.

Alternatively, you can upgrade the Agent to the latest version (contact Hewlett Packard Enterprise Customer Support) and re-run the test. See Running server communication tests for information about how to install an agent.

DAE – Realm is unreachable

The Satellite realm where the managed server is located is unreachable. This error means that a path of tunnels between the gateways in the SA core and the realm of the managed server cannot be established.

What can I do if the realm is unreachable during a DAE test?

This error could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration. Contact your SA administrator for assistance in troubleshooting the Gateway network

DAE – No Gateway defined

The managed server is in a Satellite realm, but its Agent is not properly configured to use a Gateway. Agents located in satellites must use a Gateway to contact the core.

What can I do if no gateway is defined during a DAE test?

To troubleshoot this error, try the following:

Create or open the opswgw.args file on the managed server. The opswgw.args file is located on the managed server at:

- **UNIX/Linux**: /etc/opt/opsware/agent
- **Windows**: %SystemDrive%\Program Files\Common Files\Opsware\etc\agent

Make sure this file contains a single line as shown:

```
opswgw.gw_list: <gw_ip_address>:<gw_port>,<gw_up_address>:<gw_port>
```

DAE – Tunnel setup error

The Data Access Engine could not establish a connection through any of its defined Gateways. This could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration.

What can I do if a tunnel setup error occurs during a DAE test?

Contact your SA administrator.

DAE – Gateway denied access

The Gateway is working, but refused to proxy the connection on behalf of the Agent. This error most likely means that the Gateway is misconfigured such that the Gateway will not allow the Agent to access the Data Access Engine.

What can I do if the gateway is denied access during a DAE test?

Contact your SA administrator.

DAE – Gateway name resolution error

The server running the Gateway in the SA core was unable to resolve the host name “spin”. It must be able to do this in order to proxy connections on behalf of managed servers in Satellite realms.

What can I do if there is a name resolution error on the gateway during a DAE test?

Log into the server where the core Gateway is located and use a command such as ping or host to confirm that the host name “spin” can be resolved (for example: “host spin”).

If you cannot connect, contact your SA administrator so that you can check the DNS configuration of the core Gateway server.

DAE – Internal Gateway error

Due to an internal error, the Gateway was unable to proxy the connection. This typically occurs when the Gateway is overloaded.

What can I do if an internal gateway error occurs during a DAE test?

Contact your SA administrator.

DAE – Gateway could not connect to server

The Gateway could not establish a connection to the Data Access Engine. This might be because the Data Access Engine is not running, or because the Gateway is resolving the Data Access Engine host name (“spin”) to the wrong IP address. It is also possible that a firewall might be blocking the connection.

What can I do if the gateway can’t connect to server during a DAE test?

Check that the name “spin” resolves to the correct IP address and that the Gateway can establish a connection to port 1018 at that IP. See "Resolving the host name" on page 62 and "Verifying that a port is open on a managed server" on page 60 for more information.

DAE – Gateway time-out

The Gateways on the two ends of a tunnel could not communicate with each other, most likely due to a network connectivity problem.

What can I do if the gateway times out during a DAE test?

Ensure that network connectivity is available between the Gateways in the path between the managed server's realm and the SA core.

Agent to Software Repository (SWR) test

This test checks that the Agent can establish an SSL connection to the Software Repository.

There 16 possible results are:

- "SWR – OK" on the next page
- "SWR – Untested" on the next page
- "SWR – Unexpected error" on the next page
- "SWR – Connection refused" on page 53

- "SWR – Connection time-out" on the next page
- "SWR – DNS does not resolve" on the next page
- "SWR – Old Agent version" on page 54
- "SWR - Server identification error" on page 54
- "SWR – Realm is unreachable" on page 55
- "SWR – No Gateway defined" on page 55
- "SWR – Tunnel setup error" on page 56
- "SWR – Gateway denied access" on page 56
- "SWR – Gateway name resolution error" on page 56
- "SWR – Internal Gateway error" on page 56
- "SWR – Gateway could not connect to server" on page 57
- "SWR – Gateway time-out" on page 57

SWR – OK

No troubleshooting necessary.

SWR – Untested

This result is returned when a functional area cannot be tested because of a previous failure that prevents further testing. For example, if the Agent cannot reach the Software Repository, then no other tests are possible.

What can I do if a test is not run during a SWR test?

First resolve all tests that failed, and then run the Communication Test again.

SWR – Unexpected error

This result indicates that the test encountered an unexpected condition.

What can I do if I get an unexpected error during a SWR test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Hewlett Packard Enterprise Customer Support.

SWR – Connection refused

This result indicates that the Agent is receiving a TCP reset packet when attempting to connect to the Software Repository on port 1003. The likely cause is that the Agent is trying to connect to the wrong IP address. A firewall might also be blocking the connection.

What can I do if the connection is refused during an SWR test?

Check that the name “theword” resolves to the correct IP address. For this information, see "Resolving the host name" on page 62.

Check to make sure that a firewall isn’t refusing the connection to this IP address.

SWR – Connection time-out

This result indicates that the Agent is receiving a TCP reset packet when attempting to connect to the Software Repository on port 1003. The likely cause is that the Agent is connecting to the wrong IP address. In other words, the Agent does not know the correct IP address of the Software Repository. A firewall might also be blocking the connection.

What can I do if the connection times out during an SWR test?

Follow the same steps specified in "What can I do if the connection is refused during an SWR test? " above.

SWR – DNS does not resolve

This result indicates that the Agent cannot resolve the host name “theword” to a valid IP address. In other words, the Agent does not know the correct IP address of the Software Repository.

What can I do if the software repository name (“theword”) does not resolve during an SWR test?

Log into the server and confirm that the host name “theword” can be resolved. If not, contact your SA administrator so that you can check the DNS configuration of the server.

SWR – Old Agent version

This result indicates that the Agent was unable to contact the Software Repository, and the test is unable to determine the exact cause because the Agent is out of date.

What can I do if the agent is out of date during an SWR test?

If this error occurs, it will likely be for one of two reasons: either the host name of the Software Repository (“theword”) did not resolve, or the connection was refused.

If you think that the host name of the Software Repository (“theword”) did not resolve, then see "SWR – DNS does not resolve" on the previous page.

If you determine that the connection was refused, see "SWR – Connection refused" on the previous page.

Alternatively, you can upgrade the Agent to the latest version (contact Hewlett Packard Enterprise Customer Support) and re-run the test. See Server Agent Management for information how to install a server agent.

SWR - Server identification error

Whenever an Agent makes a request of the Software Repository, the identity of the server is validated to confirm that the server should be allowed access to the information requested. This error indicates that the Software Repository was unable to identify the server being tested, or incorrectly identified that server.

What can I do if I get a server identification error?

The Software Repository identifies servers based on the incoming IP address of the request. To troubleshoot this error, try the following:

Check the Network Settings tab for the server in the SA Client to see if Network Address Translation (NAT) is in use. If it is, make sure that NAT is statically configured, and that only one server is using the NAT address. If multiple servers are using the same IP address, you will need to reconfigure the NAT device.

If the Agent is installed on a cluster, check that each node in the cluster has a unique IP address at which it can be reached. You might have to add static routes to the server to ensure that connections made from that server to the SA core use the unique IP. If NAT is not in use, you can alternately mark the correct interface as the "primary" interface through the Network node under the Inventory panel in server browser, via SA Client.

The server's IP address might have changed recently. If this is the case, stop and restart the Agent. For instructions on how to stop and start an Agent, see "Restarting a Server Agent" on page 60.

SWR – Realm is unreachable

The Satellite realm where the managed server is located is unreachable. This error means that a path of tunnels between the gateways in the SA core and the realm of the managed server cannot be established.

What can I do if the realm is unreachable during a SWR test?

This error could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration. Contact your SA administrator for assistance in troubleshooting the Gateway network.

SWR – No Gateway defined

The managed server is in a Satellite realm, but its Agent is not properly configured to use a Gateway. Agents located in satellites must use a Gateway to contact the core.

What can I do if no gateway is defined during a SWR test?

To troubleshoot this error, try the following:

Create or open the opswgw.args file on the managed server. The opswgw.args file is located on the managed server at:

- **UNIX/Linux**: /etc/opt/opsware/agent
- **Windows**: %SystemDrive%\Program Files\Common Files\Opsware\etc\agent

Make sure that this file contains a single line as shown:

```
opswgw.gw_list: <gw_ip_address>:<gw_port>,<gw_up_address>:<gw_port>
```

SWR – Tunnel setup error

The Data Access Engine could not establish a connection through any of its defined Gateways. This could be due to a network problem, a malfunctioning or failed Gateway, or a Gateway misconfiguration.

What can I do if a tunnel setup error occurs during a SWR test?

Contact your SA administrator.

SWR – Gateway denied access

The Gateway is working but refused to proxy the connection on behalf of the Agent. This error most likely means that the Gateway is misconfigured such that the Gateway will not allow the Agent to access the Software Repository.

What can I do if the gateway is denied access during a SWR test?

Contact your SA administrator.

SWR – Gateway name resolution error

The server running the Gateway in the SA core was unable to resolve the host name “theword”. It must be able to do this in order to proxy connections on behalf of managed servers in Satellite realms.

What can I do if a name resolution error occurs on the gateway during a SWR test?

Log into the server where the core Gateway is located and use a command such as ping or host to confirm that the host name “theword” can be resolved (for example: “host theword”).

If you cannot connect, contact your SA administrator so that you can check the DNS configuration of the core Gateway server.

SWR – Internal Gateway error

Due to an internal error, the Gateway was unable to proxy the connection. This typically occurs when the Gateway is overloaded.

What can I do if an internal gateway error occurs during a SWR test?

Contact your SA administrator.

SWR – Gateway could not connect to server

The Gateway couldn't establish a connection to the Software Repository. This error might be because the Software Repository is not running, or because the Gateway is resolving the Software Repository host name (“theword”) to the wrong IP address. It is also possible that a firewall might be blocking the connection.

What can I do if the gateway can’t connect to server during a SWR test?

Check that the name “theword” resolves to the correct IP address and that the Gateway can establish a connection to port 1018 at that IP address. For more information, see "Resolving the host name" on page 62 and "Verifying that a port is open on a managed server" on page 60.

SWR – Gateway time-out

The Gateways on the two ends of a tunnel could not communicate with each other, most likely due to a network connectivity problem.

What can I do if the gateway times out during a SWR test?

Ensure that network connectivity is available between the Gateways in the path between the realm of the managed server and the SA core.

Machine ID Match (MID) test

This test checks whether the MID that the Agent reported matches that recorded in the Model Repository (SA data repository).

You can receive four possible errors from the Machine ID (MID) Communication Test:

- "MID – OK" on the next page
- "MID – Untested" on the next page

- "MID – Unexpected error" below
- "MID – MID mismatch" below

MID – OK

No troubleshooting necessary.

MID – Untested

This result is returned when a functional area cannot be tested, because of a previous failure that prevents further testing. For example, if the Agent cannot reach the Model Repository, then no other tests are possible.

What can I do if a test is not run during an MID test?

First resolve all tests that failed, and then run the Communication Test again.

MID – Unexpected error

This result indicates that the test encountered an unexpected condition.

What can I do if I get an unexpected error during an MID test?

First resolve all tests that failed, and then run the Communication Test again. If the unexpected error recurs, check to see if any additional details in the error message indicate the problem. If the error cannot be resolved, contact Hewlett Packard Enterprise Customer Support.

MID – MID mismatch

This result indicates that the MID that the Agent reported does not match the recorded MID in the Model Repository for that Agent. The likely cause is that the Command Engine is running the test against the wrong Agent.

What can I do if the MID is mismatched during an MID test?

To troubleshoot this error:

Check the Network Settings tab for the server in the SA Client to see if NAT is in use for this server. If it is, make sure that static, 1-to-1 NAT is being used. Server Automation requires that all managed servers be reachable on a distinct, consistent IP address, so configurations that assign addresses dynamically or use port-based translation are not supported.

If the Agent is installed on a cluster, check that each node in the cluster has a unique IP address at which it can be reached. You might have to add static routes to the server to ensure that connections made from that server to the SA core use the unique IP. If NAT is not in use, you can alternately mark the correct interface as the “primary” interface from the Network node under the Inventory panel in server browser, via SA Client.

The IP address might have changed recently. If this is the case, stop and restart the Agent. For these instructions, see "Restarting a Server Agent" on the next page.

Common troubleshooting tasks

The following list of troubleshooting tasks are common to more than one Communication Test error:

- "Verifying that a Server Agent is running" below
- "Verifying that a port is open on a managed server" on the next page
- "Restarting a Server Agent" on the next page
- "Checking management IP of a managed server" on page 61
- "Checking network gateway configuration" on page 61
- "Resolving the host name" on page 62

Verifying that a Server Agent is running

To verify that a Server Agent is running on a server:

1. On Solaris, HP-UX, or AIX, enter this command:

   ```
   /usr/ucb/ps auxwww | grep opsware
   ```

   You should get this result if the Agent is running:

   ```
   /opt/opsware/agent/bin/python /opt/opsware/agent/pylibs/shadowbot/daemonbot.pyc
   ```

```
--conf /etc/opt/opsware/agent/agent.args
```

2. On Linux, enter this command:
   ```
   ps auxwww | grep opsware
   ```
   You should get the same result as the preceding step.
3. On Windows, from the Administrative Tools | Services, check to make sure that the `opswareagent` service is running.

Verifying that a port is open on a managed server

For some errors, you will need to verify that the port is open on the server where the Agent is installed. To do this:

1. Check if the port is open.
2. On Solaris, HP-UX, AIX, or Linux enter:
   ```
   netstat -an | grep 1002 | grep LISTEN
   ```

   If the port is open on the box, you should get back the following:
   ```
   *.1002    *.*    0 0 24576 0 LISTEN
   ```
3. On Windows, at the command prompt enter:
   ```
   netstat -an | find "1002" | find "LISTEN"
   ```

   If the port is open on the box, you should get back the following result:
   ```
   TCP 0.0.0.0:1002 0.0.0.0:0 LISTENING
   ```
4. Confirm that the port is actually open. To do this, from the computer where the Agent is installed, connect to port 1002 by using both localhost and the external IP address of the server. Performing the connection will help you confirm that a connection refused message is being caused by the lack of an open port on the managed server rather than a problem with networking hardware between the core and the managed server.

Restarting a Server Agent

To restart a Server Agent, log onto the managed server and enter the following commands:

UNIX

- for Systemd agents: `systemctl restart opsware-agent.service`
- for agents on other startup systems: `/etc/init.d/opsware-agent restart`

HP-UX

```
/sbin/init.d/opsware-agent restart
```

AIX

```
/etc/rc.d/init.d/opsware-agent restart
```

Windows

- `net stop opswareagent`
- `net start opswareagent`

Checking management IP of a managed server

To check the Management IP of a managed server:

1. To view the management IP of the managed server, log into the SA Client.
2. From the Navigation panel, click **Devices** > **All Managed Servers**.
3. From the A**ll Managed Servers** list, open the server for which you want to check the Management IP.
4. Select the Inventory panel and then Network node.
5. Check to make sure that the Management IP address matches the IP address of the managed server.

Checking network gateway configuration

To check the network Gateway configuration:

1. On Solaris, enter this command to check routing table:
   ```
   netstat -rn
   ```

   Your results should look like this:
   ```
   default 192.168.8.1 UG 1 5904
   ```

where `192.168.8.1` is the IP of the Gateway.

2. On Linux, enter this command to check routing table:

   ```
   route -n
   ```

   Your results should look like this:

   ```
   0.0.0.0 192.168.8.1 0.0.0.0 UG 0 0 0 eth0
   ```

   where `192.168.8.1` is the IP of the Gateway.

3. On Windows, enter this command to check routing table:

   ```
   route print
   ```

   Your results should look something like this:

   ```
   0.0.0.0 0.0.0.0 192.168.8.1 192.168.8.120 20
   ```

   where `192.168.8.1` is the IP of the Gateway.

4. In each case, you should also ping 192.168.8.1 (IP) to confirm that you can actually reach the Gateway.

Resolving the host name

All managed servers (those with agents) must be able to resolve unqualified Server Automation service names for the following components:

- spin (Data Access Engine)
- way (Command Engine)
- theword (Software Repository)

If you need to ensure that one of these host names resolves correctly, contact your SA administrator to find out what qualified host name or IP address these service names should resolve to.

1. Try to ping the host. For example, execute the following command if you wanted to resolve the host name, way:

   ```
   ping way
   ```

2. If the host name cannot resolve, you will get the following errors:

   Linux/Solaris/AIX/HP-UX:

   ```
   ping: unknown host way
   ```

Windows:

```
Ping request could not find host way. Please check the name and try again.
```

3. If the host name can resolve, you might get back various permutations of these types of messages (OS independent):

   ```
   way is alive
   ```

   or

   ```
   pinging way (ip) with 32 bytes of data
   ```

Troubleshoot SAV

To help keep track of the state of a business application at any given time, the application administrator continually clicks **Refresh Snapshot** on the SAV toolbar in order to create new snapshots. Each snapshot can be saved to the SA Client Library or to a local system, which can be used later to compare previous snapshots of the business application with a current state to find any important differences and troubleshoot errors.

For example, if at some point his business application malfunctions and stops working, the administrator can open his saved the business application, select the Compare feature, and visualize the differences between snapshots that compare the current state of the business application with the last known good state. Comparing snapshots can show numerous thing, such as if specific devices are not communicating with other devices. For example, he can drill into the network map and see that an interface is missing from his VMware ESX hypervisor from the same diagram and select Open Remote Terminal to remedy to problem.

For more information on snapshots, see Comparing snapshots.

SAV scan error messages

SAV indicates when an error occurred on a managed server by displaying the following server icons when you move your mouse pointer over the icon:

- **Server Error Icon**: There was an error in gathering information from the server when SAV scanned it (see "Server error messages in SAV" on the next page for possible causes of the error).
- **Server Unreachable Error Icon** : The SA core was not able to communicate with the SA Agent installed on the server.
- **Server Unknown** : SAV is unable to scan the server at all, possibly because the server is no longer in the core and under SA management.

It shows these icons before the server name in the Devices tree, Network Map, Virtualization Map, and Server Map. You can move your cursor over the server name to display the detailed error message.

Scan failures and scan time-outs typically occur when the SA managed server is very busy, or when network traffic is very heavy or running over a low bandwidth connection. If these types of errors occur too frequently, please contact your SA administrator for assistance.

Server scan errors

Server error messages in SAV

Error	Description	Action
Not Enough Disk Space	A selected managed server does not have enough disk space to perform a scan.	Free up disk space.
Remediation Failed	The Runtime State Server Module failed to remediate on the selected server.	Select the server from the Devices Tree, and then in the property pane. Click the Remediation job number link and the job window from the SA Client opens. Or, select the server, right-click, and select **Open Device Explorer** to troubleshoot the error.
Scan Timed Out	The scan process has exceeded the time-out limit.	See Scan time-out preference.
Server Access Denied	By using the OGFS, you are unable to access the server's file system as root (on a UNIX server) or as LocalSystem (on a Windows server).	Contact your SA administrator for the required permissions.
Server Capture Failed	The remote capture of data or the transfer of data back to the SA core failed.	Review the log file that is in /tmp/.sitemap/<number> for details in your global shell session.
Server ID Invalid	The server's directory was not found in the OGFS, which means that SA does not know the server exists.	
Server Scan Agent Failed	The driver used to collect data could not be correctly copied to the managed server. This could be caused by a checksum mismatch.	Contact HPE Support and provide the log file.
Server Unreachable	The managed server is unreachable by SA. This could be caused if the SA core cannot communicate with the server's agent.	Try again later. If this condition persists, contact your HPE administrator.
Unknown Scan Error	An unknown error occurred during the scanning process.	Try again later. If this condition persists, contact your HPE administrator.

Server error messages in SAV, continued

Error	Description	Action
Unsupported Agent for Scan	The SAV does not support the Server Agent version running on a selected managed server.	SA Agent 7.0 or higher is required.
Unsupported OS for Scan	The SAV does not support the operating system running on a selected managed server.	See Supported operating systems.

Network device scan errors

The table below describes network device scan errors and recommended actions.

Network device scan error messages in SAV

Error	Description	Action
NA Scan Timed Out	The time needed to gather NA data exceeded the timeout	Scan fewer devices or wait until the NA server can handle this request.
NA Scan Failed	Gathering NA data failed.	Save this snapshot to a Business Application and contact your SA administrator.

Send documentation feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Troubleshooting Guide (Server Automation 10.60)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to hpe_sa_docs@hpe.com.

We appreciate your feedback!