

HP Configure or Repair Agents



Manufacturing Part Number: 381268-002

August 2005, Edition 2

©Copyright 2004-2005 Hewlett-Packard

Table of Contents

Product Overview	3
Procedures	3
Related Topics	3
Legal Notices	3
Warranty	3
Restricted Rights Legend	3
Copyright Notice	4
Trademark Notices	4
Revision History	4
Getting Started	5
Related Procedures	5
Related Topics	5
What's New?	6
Related Topics	6
Overview	7
Related Procedures	7
Related Topics	7
Configure or Repair Agents	7
Related Topics	11
Result Log	11
Related Topics	13
Glossary	14
Index	16

Product Overview

The Configure or Repair Agents feature is an HP Systems Insight Manager feature that enables you to repair credentials for SNMP settings, System Management Homepage or Management HTTP Server trust relationships, setup SSH authentication and create subscriptions to WBEM events on Windows, Linux, and HP-UX systems supported by HP Systems Insight Manager on local or remote systems.

Note:



For systems with Management HTTP Server 4.x and earlier, Configure or Repair Agents adds the Administrator password into the Management HTTP Server store and modifies the SNMP settings but cannot change trust relationship information since Management HTTP Server 4.x and earlier did not deploy trust relationships.

Procedures

- Overview

Related Topics

- Configure or Repair Agents

Legal Notices

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Warranty

A copy of the specific warranty terms applicable to your HP product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

Use of this documentation and any supporting software media supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and backup purposes only. Resale of the programs, in their present form or with alterations, is expressly prohibited.

Copyright Notice

© Copyright 2004 Hewlett-Packard Development Company, L.P.

Trademark Notices

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32- and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95-branded products.

Intel, Celeron, Itanium, Pentium, and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java is a U.S. trademark of Sun Microsystems, Inc.

Linux is a U.S. registered trademark of Linus Torvalds.

Microsoft, Windows, and Windows NT are U.S. registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group.

Revision History

Revision History

Revision Edition 1 November 2004

MPN: 381268-001. The first edition contained Windows information and tasks.

To ensure that you receive newer versions when they become available, subscribe to the appropriate product support service. See your HP sales representative for details.

Getting Started

To start using the Configure or Repair Agents feature, use the following steps as a guideline:

1. Run Discovery from the HP Systems Insight Manager system and identify the systems that need settings repaired. For more information, refer to the HP Systems Insight Manager Online Help System.
2. Using Configure or Repair Agents, deploy the repair task. For more information, refer to "Configure or Repair Agents".

Related Procedures

- [Configure or Repair Agents](#)

Related Topics

- [Product Overview](#)

What's New?

Configure or Repair Agents provides the following enhancements and fixes since the last release:

- Allows repairs and configuration for several aspects of OpenSSH on managed systems
- Enables you to create subscriptions for WBEM events on managed systems
- Support for HP-UX and Linux operating systems

Related Topics

- [Overview](#)

Overview

When HP Systems Insight Manager is unable to communicate with a system or group of systems, you can use the Configure or Repair Agents tool to repair the settings. The Configure or Repair Agents tool enables you to repair SNMP settings and trust relationships that exist between HP Systems Insight Manager and target systems if you have 7.2 agents or later installed. If you have 7.1 agents or earlier installed, you can update Web Agent passwords on target systems.

The Configure or Repair Agents feature adds the security and trap community strings and trust settings to the target systems but it does not replace existing settings. To replace the existing settings on target systems, use the Replicate Agent Settings feature in HP Systems Insight Manager.

Consistent with many other HP Systems Insight Manager tools, the Configure or Repair Agents can be configured to run automatically on a schedule, or you can run it manually.

Note:



The Configure or Repair Agents feature does not support Windows NT 4.0.

Related Procedures

- Configure or Repair Agents

Related Topics

- Product Overview

Configure or Repair Agents

To run Configure or Repair Agents remotely against a system, you must have authorizations to run the Configure or Repair Agents tool.

If a standard practice is to disable or rename the Administrator operating system account, the renamed Administrator account is used by Configure or Repair Agents tool when Windows systems are configured.

You must have full CMS configuration privileges to modify the HP Systems Insight Manager community strings in the node security file. In addition, you must have administrator privileges for Windows systems or root privileges for Linux and HP-UX on the target systems to configure or repair the agent settings.

Note: On a Windows CMS, the Configure or Repair Agents feature enables you to configure remote systems that have the Windows, Linux or HP-UX operating systems. On a Linux or HP-UX CMS, the Configure or Repair Agents feature enables you to configure remote Linux or HP-UX systems. Windows systems can only be configured from a Windows CMS.

To configure agents remotely:

1. Select a tool from the menu. The **Select Target Systems** page appears.

Note: The **Verify Target Systems** page appears if the targets are selected before selecting a tool.

2. Add targets by first selecting from a group from the dropdown box, the contents of the selected group are displayed and can be selected as targets. Or, to select the group itself check the **Select “group” itself** checkbox.
3. Click **Apply**. The targets appear in the **Verify Target Systems** section.

Note: If the targets selected are not compatible with the tool, the **Tool Launch OK?** column provides a brief explanation for the problem. To remove a target, select the target and then click **Remove Targets**.

4. Select one of the following options:
 - Click **Add Targets** to add more targets to the **Target System List**.
 - To remove a target, select the target and then click **Run Targets**.
 - Click **Next** to specify tool parameters and to schedule the task.
5. Click **Prev** to return to the previous page. The **Enter login credentials** page appears.
6. From the **Enter login credentials** page:
 - a. In the **User name** field, enter the system administrator user name.
 - b. In the **Password** field, enter the system administrator password for the user name previously entered.
 - c. In the **Password (Verify)** field, reenter the system administrator password exactly as it was entered in the **Password** field.
 - d. For Windows managed systems only, in the **Domain** field, enter the Windows domain.

Note: The credentials used in this step must work for all target systems that have been selected. HP recommends using domain **administrator** or **root** credentials.

7. Click **Next**. Click **Prev** to return to the previous page. The **Configure or Repair Settings** page appears.

The following options are available:

- **Configure SNMP.** Select this option to configure SNMP settings.

If this option is selected, the following steps must be considered:

1. Select **Set read community string** and to specify a community string. By default, HP Systems Insight Manager's first community string, that is non-public, appears in the field. If no community string exists in HP Systems Insight Manager, then you must enter one.

Note: If only HP-UX systems with default SNMP installation are being configured at this time, you may deselect this option. HP-UX allows read by default (get-community-name is set to public by default on HP-UX systems).

Note: If this option is selected, the **Read Only** community string is added to the target systems. If the target system is SuSE Linux or Microsoft Windows 2003, the managed nodes do not always allow SNMP communication between themselves and a remote host. This setting is modified to allow the instance of the HP Systems Insight Manager system to communicate SNMP with these target systems.

Note: You can enter a community string up to 255 characters.

Note: Repairing the SNMP settings adds a **Read Write** community string to the target system only if one does not currently exist. This community string is unique for each system, is composed of over thirty characters to include letters and numbers, and is only visible to the user with administrator privileges for that system. This **Read Write** community string is required by the Web Agent to perform certain threshold setting capabilities. This community string is only used locally on the target system and is not used by HP Systems Insight Manager over the network. Linux and HP-UX systems do not need a **Read Write** community string, hence the **Read Write** community is added on Windows systems only.

2. Select **Set traps to refer to this instance of HP Systems Insight Manager** in the target systems' **SNMP Trap Destination List**. This allows the target systems to send SNMP traps to this instance of HP Systems Insight Manager.

- **Trust relationship: Set to "Trust by Certificate"**. Select this option to require systems to use the **Trust by Certificate** trust relationship with the System Management Homepage.

For System Management Homepage on the target systems, this option sets the trust mode to **Trust by Certificate** and copies the HP Systems Insight Manager system certificate to the target system's trusted certificate directory. This enables HP Systems Insight Manager users to connect to the System Management Homepage using the certificate for authentication.

Note: If you experience problems later setting the trust status to Linux, refer to the HP Systems Insight Manager Online Help **Troubleshooting** help file under **Certificate Problems** for assistance.

- **Set administrator password for Insight Management Agents version 7.1 or earlier**. Select this option to repair the administrator password on all Insight Management Agents installed on the target systems as applicable for Windows and Linux systems.

Note: Deselect this option if you have Insight Management Agents 7.2 or later installed.

Note: If the remote system is running HP-UX, this option is not executed on the remote system since it is not applicable on HP-UX systems. If only HP-UX target systems are being configured at this time, you can deselect this option.

If this option is selected, the following steps must be configured:

1. In the **Password** field, enter the new administrator password.

2. In the **Confirm Password** field, re-enter the new administrator password exactly as you entered it previously.

- **Configure secure shell (SSH) access.**

If this option is selected, you must select one of the following options:

- ☐ **Host based authentication for SSH**
- ☐ **Each user has to be authenticated on the managed system**

Note: If the selected systems include Linux or HP-UX systems, and options for Configure SNMP settings, Trust relationships and administrator password for HP Insight Management Agent 7.1 or earlier have been selected, then SSH authentication should be selected now unless already configured earlier.

Note: SSH can be configured only if the OpenSSH service is running on the managed systems. OpenSSH can be installed on Windows systems, by running the **Install Open SSH** tool under **Deploy->Deploy Drivers->Firmware and Agents->Install Open SSH**.

- **Create subscriptions for WBEM events.**

Note: This option is only applicable to Linux and HP-UX systems. If this option is selected, the target system is configured to send WBEM indications or events to HP Systems Insight Manager.

Note: Subscriptions for WBEM events can be created only if WBEM event providers are installed and running on the managed systems.

8. Click **Run Now**. Click **Prev** to return to the previous page. The **Task Results** page appears.

Note: Click **Schedule** to run this task at a later time.

Note: The Configure or Repair Agents tool can be used to update multiple target systems, each of which might potentially have different results. The `hprepair.log` is used to display the information on the stdout tab. The log results indicate whether the repair attempt was successful.

Note: Repair of SNMP settings, Trust relationships and administrator password for Insight Management Agents 7.1 or earlier on Linux systems is executed by a separate task, which can be viewed in the tasks log menu selection. Repair of SNMP settings, Trust relationships on HP-UX systems is executed by a separate task, which can be viewed in the tasks log menu selection. If Linux and HP-UX systems are selected, there are two Task IDs, one for Linux and one for HP-UX systems.

The **Task Results** page displays the following information:

- **Status.** This field displays the details for each target system within a task instance.
- **Exit Code.** This field represents the success or failure of an executable program. If the return value is zero or positive, the executable ran successfully. If a negative value is returned, the executable failed.

- **Target Name.** This field displays the name/IP address of the target.
- **The stdout Tab.** This tab displays the output text information.
- **The Stderr Tab.** This tab displays information if the executable experienced an error.
- **Files Copied Tab.** This tab displays what files are in the process of being copied or have been copied to the target system.
- **View Printable Report.** Reports can be printed for the currently selected target system or for all target systems associated with the task instance.

To print a report:

1. Click **View Printable Report**.

An **Options Message** box appears, asking if you want to generate a report containing only the currently selected target system or all systems associated with the task instance.

2. Select which report to print.
3. Click **OK** to print the report, or click **Cancel** to return to the **View Task Results** page.

9. If Management HTTP Server is installed on target systems, the login credentials are updated in the Management HTTP Server password file.

Related Topics

- Overview

Result Log

Possible log results:

- **Normal**
 - Successfully updated the administrator password (for Insight Management Agents version 7.1 or earlier).
 - Successfully created a unique SNMP READ-WRITE community string needed by the HP Web Agent.
 - Successfully changed SNMP setting to accept SNMP requests from this instance of HP Systems Insight Manager.
 - Successfully added this instance of HP Systems Insight Manager to the SNMP trap destination list.
 - Successfully added this instance of HP Systems Insight Manager to trusted certificate list for Insight Management Agents 7.1 or earlier.
 - Successfully updated the SNMP READ-ONLY community string.

- Successfully added this instance of HP Systems Insight Manager to the trusted certificate list for System Management Homepage 2.0 or later.
- Successfully restarted the Insight Management Agents. All successful changes will be effective.
- Successfully updated the permissions for the target server's SSH folders and files.
- Successfully added user to the target server's SSH passwd file in order to enable user authorization based SSH.
- Successfully added user to the target server's SSH passwd file in order to enable host authorization based SSH.
- Successfully removed duplicate entries in passwd file.
- Successfully modified SSH target server's password file to allow the renamed Administrator account name.
- Successfully HPSIM TDEF files for a renamed Administrator account name.
- Indication subscription successfully created.
- Successfully configured SSH for host based authentication.
- Successfully configured SSH for user based authentication.

● **Minor**

- SNMP is not installed on this system, so no SNMP settings were altered. To install SNMP, go to Control Panel and add the Windows component of Simple NetWork Management Protocol.
- SNMP READ-ONLY community string not updated because it already exists with different rights.
- Unable to create an SNMP READ-WRITE community string needed by the HP Web Agent.
- Unable to create a unique ID for a SNMP READ-WRITE community string needed by the HP Web Agent.
- Array Configuration Utility is running. Not all changes will be effective. Manually restart the target server when convenient.
- No settings were changed. There are no management applications utilizing the System Management Homepage present on this system.
- Failed to create indication subscription.
- Error: Identification launch exception.

● **Major**

- The operating system on the target is not supported.

- The HP repair tool will not run unless the supplied credentials are for an OS administrator. Provide correct OS administrator credentials for this target and run the Configure or Repair Agents tool again.
- No input data was supplied to the HP Repair tool.
- Insufficient memory to run HP Repair tool on target system. Stop unnecessary services on the target and run the Configure or Repair Agents tool again.
- SNMP READ-ONLY community string not updated.
- Failed to change SNMP setting to accept SNMP requests from this instance of HP Systems Insight Manager.
- Unable to add this instance of HP Systems Insight Manager to the SNMP trap destination list.
- Unable to restart the Insight Management Agents (version 7.1 or earlier). Not all changes will be effective. Manually restart the target server when convenient.
- HP Systems Insight Manager was unable to connect to the target. Retry with administrator credentials for this target.
- SSH is not installed on the target server. In order to install SSH, use a web browser to browse to HP Systems Insight Manager, select Deploy from the menu, select Install OpenSSH, and follow instructions.
- SSH could not be fixed on the target server because the user has not logged in. Log in to the target server and then run this tool again for that target.
- Unsuccessful running mxagentconfig on HP Systems Insight Manager. SSH is not properly configured for the target server. Use SSH white paper for SSH in HP Systems Insight Manager from hp.com to further troubleshoot.
- Error while retrieving OS name.
- Error: Windows repair tool execution exception.
- Error when trying to establish SSH connection, to determine operating system name.
- Error: HP-UX SSA tool launch exception.
- Error: Linux SSA tool launch exception.
- Error: Writing SNMP read string.

Related Topics

- Configure or Repair Agents
- Overview

Glossary

central management server (CMS)	A system in the management domain that executes the HP Systems Insight Manager software. All central operations within HP Systems Insight Manager are initiated from this system.
Configure or Repair Agents	The Configure or Repair Agents feature is an HP Systems Insight Manager plug-in feature that enables you to repair credentials for SNMP settings and trust relationships that exist between HP Systems Insight Manager and target systems. You can also update Web Agent passwords on target systems that have 7.1 agents or earlier installed.
discovery	A feature within a management application that finds and identifies network objects. In HP management applications, discovery finds and identifies all the HP systems within a specified network range.
HP Systems Insight Manager	<p>System management software that is capable of managing a wide variety of systems, including HP systems, clusters, desktops, workstations, and portables.</p> <p>HP Systems Insight Manager combines the strengths of HP Insight Manager 7, HP Tootools, and HP Servicecontrol Manager to deliver a single tool for managing HP ProLiant, Integrity, and HP 9000 systems running Windows, Linux, and HP-UX. The core HP Systems Insight Manager software delivers the essential capabilities required to manage all HP server platforms. HP Systems Insight Manager can also be extended to deliver unparalleled breadth of system management with plug-ins for HP storage, power, client, and printer products. Plug-ins for rapid deployment, performance management, and workload management enable systems administrators to pick the value added software required to deliver complete lifecycle management of their hardware assets.</p>
Management HTTP Server	An integrated piece of software used by the HP suite of HP Web-enabled System Management Software to communicate over HTTP and HTTPS. It provides a uniform set of functionality and security to HP Web-enabled System Management Software. This version is available in the ProLiant or Support Pack 7.10 or earlier.
Simple Network Management Protocol (SNMP)	One of the management protocols supported by HP Systems Insight Manager. Traditional management protocol used extensively by networking systems and most servers. MIB-2 is the standard information available consistently across all vendors.
standard output (stdout)	The default place to which a program writes its output. The default is the terminal display.
system	Nodes on the network that communicate through TCP/IP or IPX. To manage a system, some type of management protocol (for example, SNMP, DMI, or WBEM) must be present on the system.

	Examples of systems include servers, workstations, desktops, portables, routers, switches, hubs, and gateways.
System Management Homepage	A Web-based application that provides a consolidated interface for single system management. By aggregating the data from HP Web-based agents and management utilities, the System Management Homepage provides a common, easy-to-use interface for displaying hardware fault and status monitoring, performance data, system thresholds, diagnostics, and software version control for an individual server. This version is available in the ProLiant or Integrity Support Pack 7.20 or later.
user	A network user with a valid login on the CMS that has been added to HP Systems Insight Manager.

Index

C

configuring, 3, 5–7
copyright, 3

G

getting started, 5

H

HP Configure or Repair Agents, 3, 5–7, 11

L

legal notices, 3
log
 Configure or Repair Agents results, 11

M

managing, 6

O

overview, 3

R

release history, 3
repairing, 5–7

S

setting up, 6

T

trademarks, 3

U

updating, 7

W

warranty, 3
What's New?, 6