Using Avaya HealthCheck Tool

Release 1.0
Issue 1
May 2014

© 2013 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the

authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 7
- Purpose 7
- Intended audience 7
- Related resources 7
  - Documentation 7
- Support 8

Chapter 2: HealthCheck Tool 9
- Overview 9
- Creating a health check report 10
- Searching previously requested reports 11
- Viewing previously requested reports 12

Appendix A: HealthCheck Tool commands 15
- Cajun Data Switch health check 15
- Communication Manager health check 15
- Firewall health check 16
- Media Gateway health check 17
- Platform health check 18
- Port Speed check 20
- Installation Security Screener 21
- Call Management System health check 22
- Messaging health check 23
- Avaya Aura® Application Enablement Services health check 24

Chapter 1: Introduction

Purpose

This document describes Avaya HealthCheck Tool, which is a Web-based tool for diagnosing administration errors in an Avaya system.

Intended audience

This document is intended for Avaya associates, entitled customers, and BusinessPartners who can use HealthCheck Tool to diagnose administration errors in an Avaya system. This tool reduces the time required to diagnose errors in an Avaya system, as compared to the time taken for the manual checking of the same errors.

Related resources

Documentation

Download the following document from the Avaya Support website at support.avaya.com:

Title	Description	Audience
Avaya HealthCheck Tool FAQs	This document contains a list of questions and answers, users commonly ask while using Avaya HealthCheck Tool.	Avaya associates, entitled customers, and BusinessPartners.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: HealthCheck Tool

Overview

Avaya HealthCheck Tool is a Web-based tool that reduces the time required to diagnose errors and faults in an Avaya system. HealthCheck Tool evaluates the settings on your installed Avaya products and reports misconfigurations.

You can connect this tool to an Avaya product to gather configuration data, and compare the data to Avaya recommended settings. The tool then provides a structured report with recommendations on those settings that do not match the Avaya recommended settings.

You can use HealthCheck Tool to diagnose errors in the following Avaya products:

- Avaya Aura® Communication Manager
- Modular Messaging
- Call Management System
- Avaya Intuity Audix®
- Avaya Intuity Audix® LX
- Avaya Aura® Application Enablement Services

You can also use HealthCheck Tool to resolve multiple issues simultaneously for the following solution system settings:

- Communication Manager
- Avaya Aura® Messaging

HealthCheck Tool automatically runs commands and analyzes the resulting information. Depending on the system size, the tool takes 10 to 40 minutes to diagnose an error, while manual checking of the same error takes up to 4 hours.

Creating a health check report

Before you begin

- If you are an Avaya associate, you must have the following:
  - A user ID and password registered with Avaya
  - A Location ID (FL Number), SEID, or Case ID.
- If you are an Avaya customer or a BusinessPartner you must have the following:
  - A single sign-on (SSO) account
  - A Location ID (FL Number).

About this task

Use this task to check your Avaya devices and generate reports to rectify the errors in the devices.

Procedure

1. Log on to support.avaya.com .
2. In the Tools list at the bottom-left corner, click the **All Tools** menu.
3. On the Tools page, click HealthCheck Tool.
4. Click **Create New Health Check Report**.
5. If you are an Avaya associate, enter the Location ID (FL Number) and click **Lookup Now** . You can also enter the SEID and click **Lookup Now**
6. The HealthCheck Tool displays a table with the list of devices that it supports. Select one of the following options:
   - Click **Only the following products (From the Table Below)** to create a report for devices displayed in the table.
   - Click **All products eligible for Health Check reports at this location** to create a report for all the devices that the HealthCheck Tool supports.
   - Type the SEID, SE Code, or the Nick Name and click **Filter**.

   The table displays a list of devices.
7. Click the check box next to the device that you want to select.

   Click the check box in the header row of the table to select all the devices listed in the table.

   Note:

   Currently , users can generate batch reports for maximum 50 devices only.

Comments? infodev@avaya.com

8. Click **Submit Selected Devices**.
9. On the Verify Health Check page, verify the Customer and User information populated by the HealthCheck Tool
10. **(Optional)** Type the report name in the **Report Name** field.
11. In case you have changed the password for a product then in the Password Override section, in the **ENTER PASSWORD** field , type the new media gateway password.

    If you leave this field blank, then HealthCheck Tool uses the Avaya default password.
12. Click **Create Report** . The tool displays a message : Request Successful.
13. Click **View Health Check Reports**.
14. The tool displays a table with a list of reports and the details of these reports. Click the **View** link corresponding to the report that you want to view.

Searching previously requested reports

Before you begin

- If you are an Avaya customer or a BusinessPartner, you need the following:
  - A user ID and password registered with Avaya
  - A Case ID
- If you are an Avaya associate, you need the following:
  - A single sign-on (SSO) account
  - A Location ID (FL Number), SEID, or Case ID.

About this task

You can use this task to search for reports generated using HealthCheck Tool in the last 90 days.

Procedure

1. Log on to support.avaya.com.
2. On the Tools list at the bottom-left corner, click the **All Tools** menu.
3. On the Tools page, select HealthCheck Tool.
4. On the HealthCheck Tool page, click **Search Health Check Reports**.
5. You can search for an existing report using one of the following:

- Location ID (FL Number)

  Type the Location ID (FL Number) and click **Search by FL Number**.
- SEID

  Type the SEID and click **Search by SEID**.
- Case ID

  Type the Case ID and click **Search by Case ID**.

Based on the search criteria that you enter, the tool displays a list of reports.

Note:

If you are a customer or a BusinessPartner, you can search for a report using a Case ID only.

6. **(Optional)** In the **Filter** field, type the REQUEST DATE, REPORT ID, SEID, NICKNAME, FL NUMBER, or NAME and click **Filter** to search for a particular report.
7. Click the **View** link for the report that you want to view.

   The HealthCheck Tool displays the report that you selected.

Viewing previously requested reports

Before you begin

- If you are an Avaya entitled customer, get the following:
  - A user ID and password registered with Avaya
  - A Location ID (FL Number) or an SE ID
- If you are an Avaya BusinessPartner or an Avaya associate, get the following:
  - A single sign-on (SSO) account
  - A Location ID (FL Number) or an SE ID

About this task

Use this task to view reports generated using HealthCheck Tool .

Procedure

1. Log on to support.avaya.com .
2. On the Tools list at the bottom-left corner, click the **All Tools** menu.
3. On the Toolspage, select HealthCheck Tool.

4. On the HealthCheck Tool home page, click **View Health Check Reports**.

   The HealthCheck Tool displays a table with the list of reports and the details of these reports.

5. **(Optional)** In the **Filter** field, type the REQUEST DATE, REPORT ID, SEID, NICKNAME, FL NUMBER, or NAME and click **Filter** to search for a particular report.

6. Click the **View** link for the report that you want to view.

Appendix A: HealthCheck Tool commands

HealthCheck Tool uses a different set of commands to perform a health check on different Avaya products.

Cajun Data Switch health check

The Cajun module tests *e-net* to check if the *e-net* is administered in the etc, or host file and then connects to the Cajun and performs the following tests:

Command	Description
`ping`	Communication Manager pings Cajun to check the connectivity.
`port speeds`	Shows port speeds.
`Rmon stat`	Shows packet collisions and errors.
`Uptime`	Displays the system uptime.
`Image version`	Displays the image version.
`Dir`	Displays the directory.
`CAM table`	Displays the Windows IP addresses and the Mac IP addresses.
`Span Tree`	Displays the span tree.
`Span Tree default path`	Displays the span tree default path.

Communication Manager health check

The Communication Manager health check module runs commands in the Communication Manager system and determines errors, if any. This module runs the following commands:

Command	Description
`Status Health`	Checks the health of Communication Manager.

Command	Description
`List ipserver-interface`	Checks to make sure that the IPSI is in service and the CPEG values are *0*.
`List sys link`	Checks the system links.
`Status Synch`	Checks the system synchronization.
`Display alarms`	Displays alarms.
`Status CDR-link`	Displays status links.
`Status ess port-networks`	Checks to determine if the port networks are up.
`Status media-processor all`	Checks for alarms in all media processors.
`Status clan-all`	Checks to determine if the control LANs (CLANs) are up.
`Display disabled tests`	Displays a list of all the disabled tests.
`List disabled MO's`	Displays a list of the disabled maintenance objects.
`list survivable-processor`	Displays a list of the local survivable processor and Enterprise Survivable Processors.
`List suspend-alm-orig`	Checks whether the maintenance objects is suspended or not.
`display ip-interface`	Displays information about the IP interface.

Firewall health check

The firewall health check ensures that the Communication Manager firewall, at a basic level, is configured correctly. This health check runs the following commands:

Command	Description
`/sbin/service iptables status`	Checks service IP table entries.
`ls -l /opt/ws/iptables`	Checks IP tables in the opt/ws directory.
`grep update_activate /var/log/ecs/update.log`	Checks updates.

Media Gateway health check

HealthCheck Tool runs on the primary server that has Media Gateways connected to the system. The tool connects to the Media Gateway by using either telnet or SSH depending on whichever connection method works. HealthCheck Tool connects to the product and performs the following:

Command	Description
`swversion`	Collects the system version. This data is important in the later steps to determine what actions to take and what commands to run to gather information.
`list media`	Connects to Communication Manager and displays a list of Media Gateways. The tool does not work if Media Gateways are unavailable.
`IP addresses`	Gathers all the IP addresses of the media gateways and puts the addresses in a table for use at a later stage.
`LSP IP addresses`	Gathers the LSP IP addresses and puts the addresses in a table for use at a later stage.
`PROCR IP`	Gathers the processor IP (PROCR IP) and treats PROCR IP as a C-LAN, if the system is an S8500 version 3.1 and higher, or a S8300 standalone.
`C-LAN IP addresses`	Gathers all C-LAN IP addresses and puts the addresses in a table for use at a later stage.
`Display system-parameters ip-options`	Retrieves the value of the H.248 link loss delay timer.
`Ping`	If HealthCheck Tool can ping the gateway, the tool attempts to use telnet to connect to the gateway. If HealthCheck Tool cannot ping the gateway, the customer might have blocked ICMP on the network.
`show voltages`	Reports any status that is not *ok*.
`show faults`	Reports any fault condition.
`show mg list`	Verifies that the synchronization source is set up correctly, such as for an MG-DS1/E1 media module, the tool checks to see if the media module is set up as the primary synchronization source, and incase of two sources, the tool checks to see if one is the primary and the other is the secondary source.
`show MGC`	Checks to ensure the following for the media gateways:

Command	Description
	• The gateways are registered • The link status is working. • The IP addresses are C-LANs or PROCR IP. The C-LANs or PROCR IP is dependent on the release and the system type. • The last IP is an LSP, which is turned on. Compares this LSP to the LSP IP addresses gathered earlier. A customer might choose to not to use the IP address. The last IP address might be a C-LAN.
`show recovery or show mgp recovery`	Displays the media gateway recovery timer. You can find out the time before the media gateway attempts to re-register back to the main server depending on the gateway. The value of the primary search must be one less than the value in the **`Display system-parameters ip-options`** command. The value transition point must be equal to the number of C-LANs or PROCR IPs, or both depending on the version and the system type. The tool takes into account the version and the system type when calculating these values.
`list node-n`	Displays the list of node information.
`list ip-interface clan`	Displays the list of C-LAN specific information.
`show sync timing`	Displays how the synchronization timing is set up.
`Show system`	Displays media gateway information.

Platform health check

This module runs the following series of commands on the Linux platform:

Command	Description
`swversion`	Displays the output.
`statapp`	Reports any applications that are not active. On single server systems, the command does not report any faults if the *dupmgr* or *arbiter* is not running.
`Server`	Checks if the server hardware and process are functioning on single server systems.

Command	Description
	Checks the following on duplicated server systems: • Server hardware and process are working. • Duplication link is working. • Standby refreshed is *yes*. • Standby shadowing is *on*. • Standby busied is *on*.
statuslicense -v	Checks to ensure that the license is `ok`.
uptime	Reports uptime.
pingall -a	Reports any failed pings.
serialnumber	Checks whether a reference IPSI is identified in the system.
almcall	Checks whether the alarm call out number is set to default.
productid	Reports error if set as default value.
almdisplay -v	Displays all alarms.
almenable	Checks whether alarming is enabled or disabled.
corevector -l	Checks whether the system has taken the core dumps.
setsoh hw	Checks whether SOH is *ready*.
backup -t	Checks for recent failed backups.
ls -l /etc/cron.d	Checks whether the *Web backup* is in the file.
/usr/sbin/ntpq -p	Shows the NTP table for the server.
cat /etc/ppp/ipaddrs	Checks for duplicate or default PPP IP address.
service dhcpd status	Checks whether DHCP is on the stop mode.
netstat -nr	Displays network connections for both incoming and outgoing networks.
cat /proc/mdd	Checks the status, the memory size and the type of duplication card.
restartcause	Displays the number and the type of restarts.

Command	Description
`cat /etc/group | grep avaya`	Checks whether the login *Avaya* is used.
`ls -l /etc/cron.d/webbackup*`	Checks whether backups are scheduled.

Port Speed check

HealthCheck Toolchecks the duplex and the speed settings of the following on Communication Manager version 2.x and later:

- IPSI
- C-LAN
- IPMEDPRO
- MEDPRO
- VAL Boards
- Server ports
- Cajun ports

Autonegotiation best practices

Note:

These best practices apply only to new installations.

Equipment manufactured after 2000 supports the auto-negotiation standard, and you need not lock the server or TN boards at 100/Full. However, Avaya does not change the existing server or TN Board autonegotiation configurations on upgrades or additions. Avaya leaves these configurations locked at 100/Full.

In an ideal situation, both the server and TN Board from Avaya are at 100/Full. The Ethernet switch port of the customers that correlates with the server or TN Board is also locked at 100/Full.

- Ensure that both the devices match at 100/Full otherwise the customer experiences issues when one end is auto and the other end is locked down at 100/Full.
- Making changes to the current settings is a billable activity. Besides the general command changes, the new settings require data gathering and coordination with the IT staff of the customer.
- For a new installation, revert back to 100/Full based on the customer network configuration.
- For new upgrades, ensure that remote engineers check the boards to see whether the boards are still locked at 100/Full for IPSI, C-LAN, MedPro, Crossfire, and VAL.

Comments? infodev@avaya.com

Autonegotiation on S8730 or S8800 Software Duplex pair

Communication Manager Software Duplication Links must run at 1GB/Full-duplex with a crossover cable between the eth0 port of the two servers.

When autonegotiation is enabled, the statuses are as follows:

- If the link status is at 100/Full or 1000/Full, the system does not display any message.
- If the link status is lesser than 100/Full, then the system displays the following message: `An auto-negotiated Ethernet link should negotiate to 100M/Full-duplex (or 1G/Full-duplex for gig links). Verify that both ends of this link are set to auto-negotiate and that they are negotiating properly to the highest common speed/duplex. If the link is not negotiating properly, lock down both ends of the link to the desired speed/duplex.`
- If link status is unknown or unchecked, then the system displays the following message: `An auto-negotiated Ethernet link should negotiate to 100M/Full-duplex (or 1G/Full-duplex for gig links). Verify that both ends of this link are set to auto-negotiate and that they are negotiating properly to the highest common speed/duplex. If the link is not negotiating properly, lock down both ends of the link to the desired speed/duplex.`

When autonegotiation is disabled, the statuses are as follows:

- If the setting is at 100/Full, then the system does not display any message.
- If the setting is at 1000/Full, then the system displays the following message: `The best practice for gig links is to let them auto-negotiate to 1000/Full, but some vendors do provide the option to lock down the interface to 1000/Full. As with all Ethernet links, verify that both ends of the gig link are configured identically and will need to match.`
- If setting is lesser than 100/Full, then the system displays the following message: `This link has been locked down to a setting below 100M/Full-duplex, which is acceptable but not typical. Verify that both ends of the link are configured identically.`

Installation Security Screener

Installation Security Screener of HealthCheck Tool checks configuration faults that lead to unauthorized use of the voice network. The tool runs the following commands:

Command	Description
`display system-parameters security`	Checks for **Login Violation Notification Enabled**, **login threshold**, **Barrier code threshold**, and **Time Interval** .

Command	Description
`list vdn`	Checks whether the default class of restriction is used.
`display remote-access`	Checks whether remote access is disabled.
`display feature-access-codes`	Checks whether defaults are used in the following areas: **Data origination code**, **Data privacy access code** and **Facility test calls**.
`display system-parameters features`	Checks the trunk-to-trunk transfer.
`List Logins`	Checks for default logins.

Call Management System health check

You can use HealthCheck Toolto tests Call Management System (CMS). The commands this module runs are as follows:

Command	Description
`./active_alarms`	Checks active alarms.
`uptime`	Checks the system uptime.
`sar`	Displays the system activity report.
`sar 2 10`	Displays the system activity report in real time.
`lpstat –o | wc –l`	Displays the print job status queue.
`df –k`	Displays the disk space.
`ifconfig –a`	Displays the network card status.
`passwd -sa |egrep "root| root2|informix|cmssvc| cms"`	Performs the password aging check.
`su – cms`	Performs the CMS default password check.
`su – root`	Performs the CMS root default password check.
`Send test alarm`	Runs a series of commands that tests whether CMS can call out alarm.
`cat /usr/elog/elog.0* | egrep –i "unexpected unix`	Checks for unexpected restarts.
`netstat –i`	Displays the network collision status.

Comments? infodev@avaya.com

Command	Description
pkginfo -x cms	Performs the CMS base load verification.
cat /usr/elog/elog |egrep -i "timetable"	Checks the CMS time table status.
cat /cms/maint/backup/back.log|egrep -i "failed|finished"	Checks the CMS full maintenance backup status.
cat /cms/install/logdir/backup.log|egrep -i "failed|finished"	Checks the CMS ADM backup status.

Messaging health check

You can run a health check on Avaya Intuity Audix® , Avaya Intuity Audix® LX, and Modular Messaging using HealthCheck Tool. The module runs the following commands:

Command	Description
chassis_type	Displays the chassis type.
vihexec	Displays the hard disk drive type and other related components.
vs_status	Checks the status of the voice system.
ss	Displays the system software process.
uptime	Checks the uptime of the system.
pkgdisp	Displays the packages that are on the system.
displog -l act	Displays active alarms.
disp	Displays all cards.
dfspace	Checks that the disk space is not greater then 80%.
displog -l res -d	Displays alarm history in the *mm/dd/yy* format, where the date can be maximum 30 days before the date of the check. The command is only applicable to the alarm history of the last 30 days.
displog -l admin -a MT -e BKRST001 -d	Displays backup information for *mm/dd/yy*, where the date is any date in the last 2 weeks prior to the date of the check. This command is

Command	Description
	applicable only when backup happens during the previous health checks.

Avaya Aura® Application Enablement Services health check

You can run a health check on Application Enablement Services using HealthCheck Tool. This module runs the following commands:

Command	Description
`Swversion -a`	Checks the system version.
`uptime`	Checks the system uptime.
`df`	Checks the disk usage.
`free`	Checks the memory usage.
`ethtool`	Checks the NIC settings.
`ifconfig`	Displays the interface configuration.
`netconfig`	Displays the NIC settings and the default gateway.
`Server reboots`	Checks the time of the last restart.
`/route`	Displays a list of routes.
`Cat /etc/hosts`	Displays a list of the connected devices and the IP addresses of these devices.