Hewlett Packard Enterprise

Cloud Service Automation

Health Tool

Software version: 4.60

Document release date: January 2016

Software release date: January 2016

Contents

Overview

The Health Tool is a command line tool for HPE Cloud Service Automation (CSA) that is used to locate a problem within CSA and identify which of its components (such as the database, JBoss server, Cloud Service Management Console, Identity Management component, Marketplace Portal, or LDAP server) may be causing the problem. While the tool is not meant to identify the exact problem, it can be used to identify the area in which additional troubleshooting is needed.

When you run the tool, you will receive immediate feedback on the status (pass/fail) of CSA and its components. If more than the status is needed, you can view a report in a browser or open a text log file to find more details. Once you have located the component which is having problems, you can focus your troubleshooting on that area of CSA and consult with the necessary experts (such as the database administrator) to help solve the problem. For more information about the output from this tool, see the Health Tool Reports section.

Configuration

The Health Tool (`health-tool.jar`) is located in `<csa_home>\Tools\HealthTool\` where `<csa_home>` is the directory in which CSA is installed. In the examples shown in this guide, the Health Tool is run from this directory. If you run the tool from a different directory, you must specify the relative or absolute path to the Health Tool.

Configuration Details

The Health Tool accepts two properties files as input: the configuration properties file (required) and the LDAP configuration properties file (optional). More details about these files can be found below.

Configuration Properties File

The information in the configuration properties file is used to connect to the CSA database, log in to CSA, authenticate REST API calls, and connect to the Identity Management component. The configuration properties file is required to run the Health Tool.

A configuration properties file (`<csa_home>\Tools\HealthTool\config.properties`) is automatically generated during the installation of CSA. The content of this file is based on the database information collected by the installer. This automatically generated file does not contain the CSA login information, REST API authentication information, nor the information to connect to the Identity Management component. You must add these properties in order to complete these tests. You may also want to update the configuration properties file if the information used to communicate with the CSA database differs from what was automatically generated. See “Configuration Properties File Parameters” for more information about these properties.

You can generate a sample configuration properties file using the `-g` option (see “Generating Sample Properties File” for more information). Back up and remove the automatically generated configuration properties file and LDAP configuration properties file (if it exists) before generating the new sample properties file. Or, use the `-o` option with the `-g` option to overwrite the existing properties file.

CAUTION: Using the –o option with the –g option will overwrite both the existing configuration properties and LDAP configuration properties file. Back up both the configuration properties and LDAP configuration properties files before running the Health Tool using these options. If either file exists, you will be prompted to keep or overwrite the existing files.

By default, the configuration properties file must be located in the same folder as the `health-tool.jar` file (`<csa_home>\Tools\HealthTool\`). However, you can specify a different configuration properties file in a different location by using the `-c` or `--config-file` option.

When successfully connected to the database, the Health Tool can report information about the database. When the Health Tool cannot successfully connect to the database, it may still be able to collect and display data about subscriptions, lifecycle transitions, and number of instances.

See “Configuration Properties File Parameters” for more information about the contents of the configuration properties file. See “Sample config.properties Contents” for examples of this file.

LDAP Configuration Properties File

The information in the LDAP configuration properties file is used to connect to the LDAP server. The LDAP configuration properties file is optional and is only required if you want to test your LDAP connection. The LDAP configuration properties file must be located in the same folder as the `health-tool.jar` file (`<csa_home>\Tools\HealthTool\`) and must be named `ldap.config.properties`.

You can generate a sample LDAP configuration properties file using the `-l` or `-g` option (see “Generating Sample Properties File” for more information). Back up and remove the existing LDAP configuration properties file (if it exists) and configuration properties file before generating the new sample LDAP configuration properties file. Or, use the `-o` option with the `-l` or `-g` option to overwrite the existing LDAP configuration properties file.

CAUTION: Using the –o option with the –g option will overwrite both the existing configuration properties and LDAP configuration properties file. Back up both the configuration properties and LDAP configuration properties files before running the Health Tool using these options. If either file exists, you will be prompted to keep or overwrite the existing files.

Using the –o option with the –l option will only overwrite the existing LDAP configuration properties file. Back up the LDAP configuration properties file before running the Health Tool using these options. If the file exists, you will be prompted to keep or overwrite the existing file.

All required properties (Hostname, Port, User Email, Group Membership, Manager Identifier, Manager Identifier Value, User Name Attribute and User Search Filter) must be provided in this file. If you use the sample LDAP configuration properties file, you must provide values for the required properties. See “LDAP Configuration Properties File Parameters” for more information about the contents of this file. See “Sample ldap.config.properties Contents” for examples of this file.

Generating Sample Properties Files

The `health-tool.jar` can be used to generate sample configuration properties and LDAP configuration properties files (`config.properties` and `ldap.config.properties`). The sample files will be generated in the same folder as the `health-tool.jar` file (`<csa_home>\Tools\HealthTool\`)

To generate only the sample LDAP configuration properties file, execute the following at the command prompt:

```
"<csa_jre>\bin\java" -jar health-tool.jar -l
```

where `<csa_jre>` is the directory in which the JRE that is used by CSA is installed.

To generate both the sample configuration properties and LDAP configuration properties files, execute the following at the command prompt:

```
"<csa_jre>\bin\java" -jar health-tool.jar -g
```

> **Note**
> Additional command line options are required if SSL is enabled between the Oracle database and CSA. See “Communicating with the Oracle or MS SQL Database Using SSL” for more information.

If either the `config.properties` or `ldap.config.properties` file exists in the same folder as the `health-tool.jar` file, the Health Tool will display an error message that either or both files exist and exit.

You can either back up and remove the existing `config.properties` and `ldap.config.properties` files before generating the sample properties files or you can overwrite the existing properties files by including the `-o` option. Before running the tool with the `-o` option, back up the existing `config.properties` and `ldap.config.properties` files.

When running the tool with the `-o` option, if either or both files exist, the Health Tool will display an error message that the file(s) exist and prompt you to keep or overwrite the existing file(s). If both files exist and you choose to the keep the

existing files, the tool exits. If both files exist and you choose to overwrite the existing files, the existing files are replaced by new sample files. If only one file exists and you choose to keep the existing file, the existing file is retained and a sample of the other file is generated. If only one file exists and you choose to overwrite the existing file, the existing file is overwritten and a sample of the other file is generated.

To overwrite an existing LDAP configuration properties file with the sample file, execute the following at the command prompt:

```
"<csa_jre>\bin\java" -jar health-tool.jar -l -o
```

When prompted to overwrite the file, enter “yes” (you must enter the full word).

To overwrite both existing configuration properties and LDAP configuration properties files with the sample files, execute the following at the command prompt:

```
"<csa_jre>\bin\java" -jar health-tool.jar -g -o
```

When prompted to overwrite the files, enter “yes” (you must enter the full word).

Configuration Properties File Parameters

This table lists the parameters found in the configuration properties file.

Table 1. Configuration Properties File Parameters

Property Name	Description

`jdbc.driverClassName`	The JDBC driver class.
	Examples
	• Oracle
	`jdbc.driverClassName=oracle.jdbc.driver.OracleDriver`
	• MS SQL
	`jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver`
	• PostgreSQL
	`jdbc.driverClassName=org.postgresql.Driver`

`jdbc.dialect`	The classname that allows JDBC to generate optimized SQL for a particular database.
	Examples
	• Oracle
	`jdbc.dialect=org.hibernate.dialect.OracleDialect`
	• MS SQL
	`jdbc.dialect=org.hibernate.dialect.SQLServerDialect`
	• PostgreSQL
	`jdbc.dialect=org.hibernate.dialect.PostgreSQLDialect`

`jdbc.databaseUrl`	The JDBC URL. When specifying an IPv6 address, it must be enclosed in square brackets (see examples below).
	Examples
	• Oracle (SSL not enabled)
	`jdbc.databaseUrl=jdbc:oracle:thin:@//127.0.0.1:1521/XE`
	• Oracle (SSL not enabled, using an IPv6 address):
	`jdbc.databaseUrl=jdbc:oracle:thin:@//[f000:253c::9c10:b4b4]:1521/XE`
	• Oracle (SSL enabled, CSA does not check the database DN)
	`jdbc.databaseUrl=jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS_LIST= (ADDRESS=(PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521))) (CONNECT_DATA =(SERVICE_NAME = ORCL)))`
	where `<host>` is the name of the system on which the Oracle database server is installed.
	• Oracle (SSL enabled, CSA checks the database DN)

Property Name	Description

	`jdbc.databaseUrl=jdbc:oracle:thin:@(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = ORCL))(SECURITY=(SSL_SERVER_CERT_DN= "CN=abc,OU=dbserver,O=xyz,L=Sunnyvale,ST=CA,C=US")))`
	where `<host>` is the name of the system on which the Oracle database server is installed and the values for `SSL_SERVER_CERT_DN` are for the DN of the Oracle database server.
	• MS SQL (SSL not enabled)
	`jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=request`
	• MS SQL (SSL not enabled, using an IPv6 address)
	`jdbc.databaseUrl=jdbc:jtds:sqlserver://[::1]:1433/example;ssl=request`
	• MS SQL (SSL enabled)
	`jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=authenticate`
	• MS SQL (FIPS 140-2 compliant)
	`jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=authenticate`

`jdbc.username`	The database user configured for accessing the CSA database.
`jdbc.password`	The password for the database user. The password should be encrypted (see "Encrypt a Password" in the CSA Configuration Guide for instructions on encrypting passwords). An encrypted password is preceded by ENC without any separating spaces and is enclosed in parentheses. If you have configured CSA to be FIPS 140-2 compliant, encrypt this password after you have configured CSA to be FIPS 140-2 compliant (that is, you should use the updated encryption tools to encrypt the password). **Example** `jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)`
`csa.username`	A user who can access the Cloud Service Management Console. This user is used to test the connection to CSA.
`csa.password`	The password for the CSA user. The password should be encrypted (see "Encrypt a Password" in the CSA Configuration Guide for instructions on encrypting passwords). An encrypted password is preceded by ENC without any separating spaces and is enclosed in parentheses. If you have configured CSA to be FIPS 140-2 compliant, encrypt this password after you have configured CSA to be FIPS 140-2 compliant (that is, you should use the updated encryption tools to encrypt the password). **Example** `csa.password=ENC(ac7fe2d25cf0578a9b45907ee721ab8099)`
`idm.tenantName`	The provider organization identifier of the Cloud Service Management Console whose connection is being tested. This property must be set to **CSA-Provider**.
`idm.transportUser`	A user configured to authenticate REST API calls. This user is used to test the REST API connection and to capture CSA license information.

Property Name	Description
idm.transportPassword	The password for the idm.transportUser. The password should be encrypted (see "Encrypt a Password" in the CSA Configuration Guide for instructions on encrypting passwords). An encrypted password is preceded by ENC without any separating spaces and is enclosed in parentheses. If you have configured CSA to be FIPS 140-2 compliant, encrypt this password after you have configured CSA to be FIPS 140-2 compliant (that is, you should use the updated encryption tools to encrypt the password). **Example** idm.transportPassword=ENC(b5af870d6ce23951af09)
idm.username	A user who can connect to the Identity Management component.
idm.password	The password for the Identity Management component user. The password should be encrypted (see "Encrypt a Password" in the CSA Configuration Guide for instructions on encrypting passwords). An encrypted password is preceded by ENC without any separating spaces and is enclosed in parentheses. If you have configured CSA to be FIPS 140-2 compliant, encrypt this password after you have configured CSA to be FIPS 140-2 compliant (that is, you should use the updated encryption tools to encrypt the password). **Example** idm.password=ENC(79dfa03785cbe407001f7ab310e31)

LDAP Configuration Properties File Parameters

This table lists the parameters found in the LDAP configuration file.

Table 2. LDAP Configuration Properties File Parameters

Property	Name
csa.ldap.hostname	**Required**. The fully-qualified LDAP server domain name (server.domain.com) or IP address. **Example** ldap.xyz.com
csa.ldap.port	**Required**. The port used to connect to the LDAP server. 389 for ldap and 636 for ldaps.
csa.ldap.ssl	Connection Security. If the LDAP server is configured to require ldaps (LDAP over SSL), set this property to true. If the LDAP server does not require ldaps, set this property to false.
csa.ldap.basedn	Base distinguished name. The Base DN is the top level of the LDAP directory that is used as the basis of a search. **Example** DC=cirrus,DC=com
csa.ldap.userid	The fully distinguished name of any user with authentication rights to the LDAP server. If the LDAP server does not require a User ID or password for authentication, this value can be omitted. **Example** CN=csaldap,CN=Users,DC=cirrus,DC=com

Property	Name
csa.ldap.password	Password of the User ID. If the LDAP server does not require a User ID or password for authentication, this value can be omitted. The password should be encrypted (see "Encrypt a Password" in the CSA Configuration Guide for instructions on encrypting passwords). An encrypted password is preceded by ENC without any separating spaces and is enclosed in parentheses. If you have configured CSA to be FIPS 140-2 compliant, encrypt this password after you have configured CSA to be FIPS 140-2 compliant (that is, you should use the updated encryption tools to encrypt the password). **Example** ENC(A0El12PmN6ajnhlInJAnEumDDvCBvQLV)
csa.ldap.useremail	**Required**. Designates the email address of the user to which to send email notifications. Common LDAP attribute names for email include mail and email. If the value for this attribute in the user object in LDAP is empty or not valid, the user for whom the value is empty or not valid does not receive email notifications. **Example** mail
csa.ldap.groupmembership	**Required**. Identifies a user as belonging to the group. Common LDAP attribute names that convey group membership include member and uniqueMember. **Examples** • member • member,uniqueMember
csa.ldap.managerIdentifier	**Required**. Identifies the manager of the user. A common LDAP attribute name for a user's manager is manager. If the value for this attribute in the user object in LDAP is empty or not valid, approval policies that use the User Context Template will fail. **Example** **manager**
csa.ldap.managerIdentifierValue	**Required**. Describes the value of the manager identifier. A common value for the manager identifier in LDAP is the dn (distinguished name) of the manager's user object. If the manager's user object cannot be located based on the values for manager identifier and manager identifier value, approval policies that use the User Context Template will fail. **Example** dn
csa.ldap.userAvatar	LDAP attribute whose value is the URL to a user avatar image that will display for the logged in user in the Marketplace Portal. If no avatar is specified, a default avatar will be used. **Example** avatar
csa.ldap.userNameAttribute	**Required**. The name of the attribute of a user object that contains the username that will be used to log into the Cloud Service Management Console or Marketplace Portal. The value for this field can be determined by looking at one or more user objects in the LDAP directory to determine which attribute consistently contains a unique user name. **Example** sAMAccountName

Property	Name
csa.ldap.userSearchBase	LDAP container that contains the users. This value must be relative to the Base DN. **Example** cn=Users
csa.ldap.userSearchFilter	**Required**. Specifies the general form of the LDAP query used to identify users during login. It must include the pattern {0}, which represents the user name entered by the user when logging in to the Cloud Service Management Console or Marketplace Portal. The filter is generally of the form <attribute>= {0}, with <attribute> typically corresponding to the value entered for User Name Attribute. **Example** sAMAccountName={0}
csa.ldap.searchSubtree	When a user logs in to the Cloud Service Management Console or Marketplace Portal, the LDAP directory is queried to find the user's account. The Search Subtree setting controls the depth of the search under User Search Base. If you want to search for a matching user in the User Search Base and all subtrees under the User Search Base, set this property to yes. If you want to restrict the search for a matching user to only the User Search Base, excluding any subtrees, set this property to no. **Examples** • yes • no

Communicating with the Oracle or MS SQL Database Using SSL

If SSL is enabled between CSA and the Oracle or MS SQL database, additional command line options might be required and the URL property in the database properties file must be configured correctly.

Table 3. Oracle: CSA does not check the database DN and client authentication is enabled

Database Type	Oracle
Configuration Options	• SSL is enabled • CSA does NOT check the database DN • Client authentication is enabled
Command Line Option(s)	-Djavax.net.ssl.keyStore="<certificate_key_file>" -Djavax.net.ssl.keyStorePassword=<certificate_key_file_password> -Djavax.net.ssl.keyStoreType=<certificate_key_file_type> where: • <certificate_key_file> is the same keystore file defined by the certificate-keyfile attribute in the ssl element of the <csa_home>\jboss-as\standalone\configuration\standalone.xml file (for example, <csa_home>\jboss-as\standalone\configuration\.keystore) • <certificate_key_file_password> is the password to the keystore file (for example, changeit) • <certificate_key_file_type> is the keystore type (for example, JKS or PKCS12)
jdbc.databaseURL Value	jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST= (ADDRESS=(PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521))) (CONNECT_DATA =(SERVICE_NAME = ORCL))) where <host> is the name of the system on which the Oracle database server is installed

Table 4. Oracle: CSA does not check the database DN and client authentication is not enabled

Database Type	Oracle
Configuration Options	• SSL is enabled • CSA does NOT check the database DN • Client authentication is NOT enabled
Command Line Option(s)	<none>
jdbc.databaseURL Value	`jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST= (ADDRESS=(PROTOCOL = TCPS)(HOST = <host>)(PORT = 1521))) (CONNECT_DATA =(SERVICE_NAME = ORCL)))` where `<host>` is the name of the system on which the Oracle database server is installed

Table 5. Oracle: CSA checks the database DN and client authentication is enabled

Database Type	Oracle
Configuration Options	• SSL is enabled • CSA checks the database DN • Client authentication is enabled

Command Line Option(s)	`-Doracle.net.ssl_server_dn_match=true`
	`-Djavax.net.ssl.keyStore="<certificate_key_file>"`
	`-Djavax.net.ssl.keyStorePassword=<certificate_key_file_password>`
	`-Djavax.net.ssl.keyStoreType=<certificate_key_file_type>`
	
	where:
	• `<certificate_key_file>` is the same keystore file defined by the certificate-keyfile attribute in the ssl element of the `<csa_home>\jboss-as\standalone\configuration\standalone.xml` file (for example, `<csa_home>\jboss-as\standalone\configuration\.keystore`)
	• `<certificate_key_file_password>` is the password to the keystore file (for example, changeit)
	• `<certificate_key_file_type>` is the keystore type (for example, JKS or PKCS12)

jdbc.databaseURL Value	`jdbc:oracle:thin:@(DESCRIPTION =(ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCPS)(HOST =<host>)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = ORCL))(SECURITY=(SSL_SERVER_CERT_DN= "CN=abc,OU=dbserver,O=xyz,L=Sunnyvale,ST=CA,C=US")))` where: • `<host>` is the name of the system on which the Oracle database server is installed • the values for `SSL_SERVER_CERT_DN` are for the DN of the Oracle database server

Table 6. Oracle: CSA checks the database DN and client authentication is not enabled

Database Type	Oracle
Configuration Options	• SSL is enabled • CSA checks the database DN • Client authentication is NOT enabled
Command Line Option(s)	<none>
jdbc.databaseURL Value	`jdbc:oracle:thin:@(DESCRIPTION =(ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCPS)(HOST =<host>)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = ORCL))(SECURITY=(SSL_SERVER_CERT_DN= "CN=abc,OU=dbserver,O=xyz,L=Sunnyvale,ST=CA,C=US")))` where: • `<host>` is the name of the system on which the Oracle database server is installed and • the values for `SSL_SERVER_CERT_DN` are for the DN of the Oracle database server

Table 7. MS SQL

Database Type	MS SQL
Configuration Options	• SSL is enabled
Command Line Option(s)	<none>
jdbc.databaseURL Value	`jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=authenticate`

Usage

Command Line Options

The command options and sub-options for the Health Tool are shown in the following table.

Option	Option Description
`-h, --help`	Display syntax and usage information.
`-g, --generate`	Generate both a sample LDAP configuration properties file (`ldap.config.properties`) and sample configuration properties file (`config.properties`). A sample configuration properties file is automatically generated when CSA is installed. When used with the `-o` option, both files can be overwritten, if they exist.
`-l,--ldap`	Generate a sample LDAP configuration properties file (`ldap.config.properties`). When used with the `-o` option, an existing file can be overwritten.
`-c,--config-file <config property file>`	**Optional**. The location and name of the configuration properties file. If this option is specified, you must specify the name and location of the configuration properties property file. The location can be an absolute path or a path relative to the location where the Health Tool is run. If the file is located in the same directory from which the Health Tool is run, the path does not need to be specified. If you specify the –c option but do not specify a file location and name or if you do not specify the –c option, the Health Tool will look for a file named `config.properties` that is located in the same directory as the Health Tool (`<csa_home>\Tools\HealthTool\`).
`-j,--jars <Oracle JARs>`	**Required** if you are using an Oracle database. Load the Oracle JDBC JAR files. Note that if more than one jar file is needed, the jar filenames must be separated by a comma (do not include any spaces between the comma and filename). The Oracle JDBC JAR files must be located in the same folder as the `health-tool.jar` file (`<csa_home>\Tools\HealthTool\`). If you are using an MS SQL or PostgreSQL database, you do not need to specify this option.
`-o,--overwrite`	**Optional**. Overwrite the `health_tool.log` (text) and `report.html` report files. If this option is not specified, the current report information is added to the top of the files. When used with the `-g` option, overwrite both the `config.properties` and `ldap.config.properties` files that are located in the same folder as the `health-tool.jar` file (`<csa_home>\Tools\HealthTool\`). When used with the `-l` option, overwrite the `ldap.config.properties` file that is located in the same folder as the `health-tool.jar` file (`<csa_home>\Tools\HealthTool\`).

To list the supported options, invoke the Health Tool from the command line as follows:

```
java.exe -jar health-tool.jar -h

usage: java -jar health-tool.jar

-h,--help                          Print this help.
-g,--generate                      Create database and LDAP connection property files.
-j,--jars                          Additional JAR files to load (JDBC driver).
-c,--config-file                   Path to database 'config.properties' file.
-o,--overwrite                     Overwrite reports
                                    (or configuration files when using the -g option).
-l,--ldap                          Create LDAP connection properties file.
```

Health Tool Reports

The Health Tool generates three different reports which provide different levels of information. When you run the Health Tool, the following reports in the following formats are generated:

- Online display – general status for each section (described below) is displayed in the window from which the tool was run
- HTML report – status and response times for each test and more detailed information about the database, JBoss server, and CSA data are captured in a table in an HTML file (`<csa_home>\Tools\HealthTool\report.html`)
- Text log file – general status for each section (described below), response times, and information about the database, JBoss server, and CSA data are captured in a text file (`<csa_home>\Tools\HealthTool\health_log.txt`)

Each report generated by the Health Tool is separated into the following sections:

- Database
- JBoss server
- CSA service
- Identity Management component
- Marketplace portal
- LDAP server
- CSA data

Online Display

When you run the Health Tool, data is displayed on the screen that includes the general status (passed/failed) of the following:

- Database connection
- JBoss server connection
- CSA service
- Identity Management component connection
- Marketplace portal service
- LDAP server connection
- CSA data checks

An example of the online display output is shown below.

```
------------------------------------------------------------
Start Health Tool at 4/13/15 11:55 AM
 Note: It is required to run this tool using the same Java as CSA is using.

------------------------------------------------------------
Check CSA database connection … passed

------------------------------------------------------------
Check connection to JBoss …
 passed

------------------------------------------------------------
Check CSA is running … passed

------------------------------------------------------------
Check IDM is running … passed

------------------------------------------------------------
Check MPP is running … passed

------------------------------------------------------------
Check connection to LDAP … passed

------------------------------------------------------------
CSA Data Checks … passed

------------------------------------------------------------
End Health Tool at 4/13/15 11:55 AM
'report.html' report was created.
Check files report.html and health_tool.log for detailed results.
```

HTML Report

When you run the Health Tool, data is captured in an html file named `report.html` (and is located in the same directory as the Health Tool). The Health Tool report file contains the following displayed in a table:

- Status (passed/failed) for each test
- Response times for each test (where applicable)
- Log messages for failed connections
- Database: number of records in csa_person table
- Database: type and version
- Database: driver and version
- JBoss: JMX connection
- JBoss: MBean server connection
- JBoss: server system resource usage
- JBoss: server memory usage
- CSA: Cloud Service Management Console login
- CSA data: number of active subscriptions
- CSA data: number of transitions
- CSA data: number of completed instances
- CSA data: Process return code

- CSA data: Process state
- CSA data: number of pending subscriptions
- CSA data: REST API connection and CSA licensing
- CSA data: all uncommented properties in csa.properties

If the connection fails to the database, JBoss server, or CSA server, the related information will not be available in the Health Tool report file. For example, if the database connection fails, the number of records in csa_person table, database type and version, and database driver and version are not available and not reported in the Health Tool report file. Also, if the database connections fails, the subscription, lifecycle transition, and instance information is not available and is not reported in the Health Tool report file.

If the connection using the REST API fails, the CSA licensing information is not available and is not reported in the Health Tool report file.

If the Health Tool cannot get information for one of the CSA data items (for example, the REST API connection fails), the global CSA data check status is failed.

An example of the Health Tool report file is shown below.

Health Tool Report

Tue Apr 13 11:55:50 PDT 2015

Check	Result	Message	Duration	Log
Ping database	**PASSED**	Database connection passed	50 milliseconds	
Table 'csa_person' rows count	**PASSED**	Database table 'csa_person' has 1 records.	0 milliseconds	
CSA database check	**PASSED**	Connection to CSA database passed.		
Get database info	**PASSED**	Connected to database: PostgreSQL 9.3.6	4 milliseconds	
Get database driver info	**PASSED**	Connected to database: PostgreSQL Native Driver PostgreSQL 9.0 JDBC4 (build 801)	0 milliseconds	
JMX connection check	**PASSED**	Connection to JBoss JMX passed.	346 milliseconds	
MBean Server connection check	**PASSED**	Connection to JBoss MBean Server	898 milliseconds	
MBean Server connection check	**PASSED**	JBoss MBean Server data load	0 milliseconds	Operating System --- LoadAverage: 0.23 FreePhysicalMemory: 192 MB processCpuTime: 351120000000 committedVirtualMemorySize: 7996 MB freeSwapSpaceSize: 30498 MB totalPhysicalMemorySize: 15999 MB totalSwapSpaceSize: 30516 MB Memory - Heap Memory Usage --- commited : 1989 MB init : 2048 MB max : 1989 MB used : 549 MB percentage : 27 % Memory - Non Heap Memory Usage --- commited : 328 MB init : 2 MB max : 0 MB used : 310 MB
CSA running check	**PASSED**	CSA Service is running		
Login to CSA	**PASSED**	CSA login passed	407 milliseconds	
IDM running check	**PASSED**	Connection to IDM passed	230 milliseconds	
MPP running check	**PASSED**	MPP Service is running		
CSA LDAP check	**PASSED**	LDAP connection passed	72 milliseconds	
CSA data: Subscriptions	**PASSED**	ACTIVE: 25	10 milliseconds	
CSA data: Lifecycle Transitions	**PASSED**		2 milliseconds	
CSA data: Instances	**PASSED**	COMPLETED: 25	2 milliseconds	
CSA data: Process return code	**PASSED**	No NULL data found in 'CSA_PROCESS_INSTANCE.PROCESS_RETURN_CODE_ID'.	2 milliseconds	
CSA data: Process state	**PASSED**	No NULL data found in 'CSA_PROCESS_INSTANCE.PROCESS_INSTANCE_STATE_ID'.	2 milliseconds	
CSA data: Pending Subscriptions	**PASSED**	There are no Pending Subscriptions.	2 milliseconds	

CSA REST Check	**PASSED**	https://localhost:8444/csa/api/license/	108 milliseconds	
CSA REST: License	**PASSED**	https://localhost:8444/csa/api/license/	108 milliseconds	Total OS Instance Limit : 0 Active OS Instance Count : 2 daysRemaining : 90 licenseType : INSTANT_ON activeOSInstancesLimit : 0 expiresOn : Mon Jun15 23:59:59 PDT 2015 productName : HP CSA
CSA Properties	**PASSED**			csa.provider.msvc.rest.protocol : http com.hp.csa.service.process.ProcessExecutorDelegate.EXTERNAL_POOL_SIZE : 2 com.hp.ccue.consumption.disallowedExtensions : exe,bat,com,cmd csa.productPerspective : enterprise com.hp.csa.PEM.PARAM_PROCESS_INSTANCE_ID : CSA_PROCESS_ID com.hp.csa.LifecycleExecutor.THREAD_POOL_SIZE : 2 com.hp.csa.TimeoutChecker.THREAD_WAKEUP_TIME : 300000 csa.consumer.legalNoticeUrl : http://www8.hp.com/us/en/privacy/privacy.html csa.provider.msvc.port : 9000 csaAuditEnabled : true com.hp.csa.ProcessExecutor.THREAD_WAKEUP_TIME : 5000 csaTruststorePassword : ***** com.hp.csa.service.process.ProcessExecutorDelegate.INTERNAL_POOL_SIZE : 2 securityCodarIntegrationUserPassword : ***** csa.ldapReadOnly : false securityEncryptedSigningKey : ***** csa.group.numberOfApprovers : 10 com.hp.csa.OosMonitor.THREAD_WAKEUP_TIME : 60000 com.hp.csa.service.process.OosMonitorDelegate.MONITOR_POOL_SIZE : 2 com.hp.csa.oo.OOClient.SOCKET_TIMEOUT : 60000 com.hp.csa.service.ssl.insecure : true securityCatalogAggregationTransportUserPassword : ***** csa.topology.cloudOsSpecEnabled : false com.hp.csa.plugin.cloudos.util.TokenCache.TIMEOUT : 300000 TopologyDesignProvisioning.TIMEOUT : 7200 serviceRequestProcessorScheduler.period : 5000 com.hp.csa.ApprovalDecisionMaker.THREAD_WAKEUP_TIME : 1 csa.provider.rest.protocol : https embedded.oo.root.dir : C:/Program Files/Hewlett-Packard/CSA/emb_oo com.hp.csa.service.process.ProcessExecutorDelegate.MONITOR_POOL_SIZE : 2 csa.subscriber.portal.url : {protocol}://{host}:8089/org/{orgName} integrationAccountUserList : admin,csaReportingUser,ooInboundUser,cdaInboundUser,csaTransportUser,csaCatalogAggregationTransportUser com.hp.csa.UserGroupExecutor.THREAD_WAKEUP_TIME : 20 csa.provider.es.name : csa.maxFileUploadSize : 50 com.hp.csa.UserGroupExecutor.UserGroupDeletionBatchSize : 250 csa.additionalSupportedExtensionsForImport : jboss.shutdown.log.location : C:/Program Files/Hewlett-Packard/CSA/jboss-as/bin/shutdown.log securityIdmTransportUserPassword : ***** OrchestratedTopologyDesignProvisioning.ProviderSelection.Enabled : true serviceRequestProcessorScheduler.maxInstancesToProcess : 100 csa.consumer.endDatePeriod : 12 DynamicPropertyFetch.READ_TIMEOUT : 30000 csa.security.enable : false securityCsaReportingUserPassword : ***** csa.orgName.identifier : CSA-Provider securityTransportPassword : ***** csa.provider.hostname : localhost csa.consumer.featuredCategory : APPLICATION_SERVERS securityOoInboundUserPassword : ***** OOS_PASSWORD : ***** csaTruststore : C:/Program Files/Hewlett-Packard/CSA/openjre/lib/security/cacerts rest.restrict.fields : createdBy,updatedBy,createdOn,updatedOn,objectId,isCriticalSystemObject,description,iconUrl,disabled,categoryType com.hp.csa.PEM.PARAM_CONTEXT_ID : CSA_CONTEXT_ID csa.provider.msvc.hostname : localhost csa.consumer.termsOfUseUrl : http://www8.hp.com/us/en/privacy/terms-of-use.html com.hp.csa.ProcessExecutor.THREAD_POOL_CORE_SIZE : 2 OOS_URL : https://localhost:8445 enableHPSSO : true rest.excludedoc : false loggerEnabled : false csa.topology.expressDesignEnabled : false OOS_USERNAME : admin xAuthToken : X-Auth-Token com.hp.csa.LifecycleExecutor.THREAD_WAKEUP_TIME : 5000 com.hp.csa.service.process.ProcessExecutorDelegate.CALLBACK_POOL_SIZE : 2 deploymentMode : single com.hp.csa.UserGroupExecutor.CACHE_EXPIRATION_TIME : 30 csa.provider.port : 8444 defaultDaysToExtendExpirationDate : 1 rest.restrict : false DynamicPropertyFetch.RESPONSE_SIZE : 50000 securityAdminPassword : ***** securityCdaInboundUserPassword : ***** csa.topology.calloutsEnabled : false securityTransportUserName : csaTransportUser com.hp.csa.import.BUILD_ARTIFACT_RELATIONSHIP : true csa.provider.es.exists : no com.hp.csa.aosMonitor.THREAD_WAKEUP_TIME : 20000

Text Log File

When you run the Health Tool, data is captured in a text file named `health_tool.log` (and is located in the same directory as the Health Tool). The Health Tool log file contains the following:

- General status (the same information that is displayed online)
- Log messages for failed connections
- Database: connection response time
- Database: number of records in csa_person table
- Database: type and version
- Database: driver and version
- JBoss: JMX connection
- JBoss: MBean server connection
- JBoss: server system resource usage
- JBoss: server memory usage
- CSA: Cloud Service Management Console login
- CSA: login response time
- Identity Management component: connection response time
- LDAP: connection response time
- CSA data: subscriptions status
- CSA data: lifecycle transitions status
- CSA data: instances status
- CSA data: Process return code status
- CSA data: Process state status
- CSA data: Pending subscriptions status
- CSA data: REST API connection and CSA licensing
- CSA data: all uncommented properties in csa.properties

If the connection fails to the database, JBoss server, or CSA server, the related information will not be available in the Health Tool log file. For example, if the database connection fails, the number of records in csa_person table, database type and version, and database driver and version are not available and not reported in the Health Tool log file. Also, if the database connections fails, the subscription, lifecycle transition, and instance information is not available and is not reported in the Health Tool log file.

If the connection using the REST API fails, the CSA licensing information is not available and is not reported in the Health Tool log file.

If the Health Tool cannot get information for one of the CSA data items (for example, the REST API connection fails), the global CSA data check status is failed.

The overall status of a test (passed/failed) is displayed in each section (typically at the end of the section).

An example of the Health Tool log file is shown below.

```
_____________________________________________________________
Start Health Tool at 4/13/15 11:55 AM

-------------------------------------------------------------
Check CSA database connection ...
Database connection passed in 50 milliseconds
Database table 'csa_person' has 1 records.
Connected to database: PostgreSQL 9.3.6
Connected to database: PostgreSQL Native Driver PostgreSQL 9.0 JDBC4 (build 801)
passed

-------------------------------------------------------------
Check connection to JBoss ...
Connection to JBoss JMX passed.
Connection to JBoss MBean Server
JBoss MBean Server data load
Operating System
-----------------------------------------------------
                LoadAverage: 0.23
                FreePhysicalMemory: 192 MB
                processCpuTime: 351120000000
                committedVirtualMemorySize: 7996 MB
                freeSwapSpaceSize: 30498 MB
                totalPhysicalMemorySize: 15999 MB
                totalSwapSpaceSize: 30516 MB

Memory - Heap Memory Usage
-----------------------------------------------------
                committed  : 1989 MB
                init       : 2048 MB
                max        : 1989 MB
                used       : 549 MB
                percentage : 27 %

Memory - Non Heap Memory Usage
-----------------------------------------------------
                committed  : 328 MB
                init       : 2 MB
                max        : 0 MB
                used       : 310 MB
                percentage : -32572404800 %

passed

-------------------------------------------------------------
Check CSA is running ...
passed

CSA  login  passed in 407 milliseconds.

-------------------------------------------------------------
Check IDM is running ...
Connection to IDM passed in 230 milliseconds.
passed

-------------------------------------------------------------
Check MPP is running ...
passed

-------------------------------------------------------------
```

```
Check connection to LDAP ...
LDAP connection passed in 72 milliseconds
passed

------------------------------------------------------------
CSA Data Checks ...
------------------------------------------------------
CSA data: Subscriptions

Result: passed
------------------------------------------------------
CSA data: Lifecycle Transitions

Result: passed
------------------------------------------------------
CSA data: Instances

Result: passed
------------------------------------------------------
CSA data: Process return code

Result: passed
------------------------------------------------------
CSA data: Process state

Result: passed
------------------------------------------------------
CSA data: Pending Subscriptions

Result: passed
CSA REST call to 'license/'
{
  "activeOSInstanceCount" : 2,
  "totalOSInstanceLimit" : 0,
  "members" : [ {
    "licenseKey" : "ABCD 1234 H0PA CHf3 U4B5 H72F Y9J9 K7PL BP9H MZ9U D0AU 2C9M G1TG L762 KYW2 HWVA
WPNH MCFY TM3Q DBEV X6YR PW9D B9TS XFXC LK4U R46A V888 RCKY 5SCT JC4P 4QNJ 9GEJ\"InstantOn for 90
days with 1 capacity\"",
    "licenseType" : "INSTANT_ON",
    "daysRemaining" : 90,
    "expiresOn" : 1234567899000,
    "activeOSInstancesLimit" : 0,
    "productName" : "CSA"
  } ]
}

CSA Properties:
csa.provider.msvc.rest.protocol : http
com.hp.csa.service.process.ProcessExecutorDelegate.EXTERNAL_POOL_SIZE : 2
com.hp.ccue.consumption.disallowedExtensions : exe,bat,com,cmd
csa.productPerspective : enterprise
com.hp.csa.PEM.PARAM_PROCESS_INSTANCE_ID : CSA_PROCESS_ID
com.hp.csa.LifecycleExecutor.THREAD_POOL_SIZE : 2
com.hp.csa.TimeoutChecker.THREAD_WAKEUP_TIME : 300000
csa.consumer.legalNoticeUrl : http://www8.hp.com/us/en/privacy/privacy.html
csa.provider.msvc.port : 9000
csaAuditEnabled : true
com.hp.csa.ProcessExecutor.THREAD_WAKEUP_TIME : 5000
csaTruststorePassword : *****
com.hp.csa.service.process.ProcessExecutorDelegate.INTERNAL_POOL_SIZE : 2
```

```
securityCodarIntegrationUserPassword : *****
csa.ldapReadOnly : false
securityEncryptedSigningKey : *****
csa.group.numberOfApprovers : 10
com.hp.csa.OosMonitor.THREAD_WAKEUP_TIME : 60000
com.hp.csa.service.process.OosMonitorDelegate.MONITOR_POOL_SIZE : 2
com.hp.csa.oo.OOClient.SOCKET_TIMEOUT : 60000
com.hp.csa.service.ssl.insecure : true
securityCatalogAggregationTransportUserPassword : *****
csa.topology.cloudOsSpecEnabled : false
com.hp.csa.plugin.cloudos.util.TokenCache.TIMEOUT : 300000
TopologyDesignProvisioning.TIMEOUT : 7200
serviceRequestProcessorScheduler.period : 5000
com.hp.csa.ApprovalDecisionMaker.THREAD_WAKEUP_TIME : 1
csa.provider.rest.protocol : https
embedded.oo.root.dir : "C:/Program Files/Hewlett-Packard/CSA/emb_oo"
com.hp.csa.service.process.ProcessExecutorDelegate.MONITOR_POOL_SIZE : 2
csa.subscriber.portal.url : {protocol}://{host}:8089/org/{orgName}
integrationAccountUserList : admin,csaReportingUser,ooInboundUser,cdaInboundUser,
csaTransportUser,csaCatalogAggregationTransportUser
com.hp.csa.UserGroupExecutor.THREAD_WAKEUP_TIME : 20
csa.provider.es.name :
csa.maxFileUploadSize : 50
com.hp.csa.UserGroupExecutor.UserGroupDeletionBatchSize : 250
csa.additionalSupportedExtensionsForImport :
jboss.shutdown.log.location : C:/Program Files/Hewlett-Packard/CSA/jboss-as/bin/shutdown.log
securityIdmTransportUserPassword : *****
OrchestratedTopologyDesignProvisioning.ProviderSelection.Enabled : true
serviceRequestProcessorScheduler.maxInstancesToProcess : 100
csa.consumer.endDatePeriod : 12
DynamicPropertyFetch.READ_TIMEOUT : 30000
csa.security.enable : false
securityCsaReportingUserPassword : *****
csa.orgName.identifier : CSA-Provider
securityTransportPassword : *****
csa.provider.hostname : localhost
csa.consumer.featuredCategory : APPLICATION_SERVERS
securityOoInboundUserPassword : *****
OOS_PASSWORD : *****
csaTruststore : C:/Program Files/Hewlett-Packard/CSA/openjre/lib/security/cacerts
rest.restrict.fields : createdBy,updatedBy,createdOn,updatedOn,objectId,
isCriticalSystemObject,description,iconUrl,disabled,categoryType
com.hp.csa.PEM.PARAM_CONTEXT_ID : CSA_CONTEXT_ID
csa.provider.msvc.hostname : localhost
csa.consumer.termsOfUseUrl : http://www8.hp.com/us/en/privacy/terms-of-use.html
com.hp.csa.ProcessExecutor.THREAD_POOL_CORE_SIZE : 2
OOS_URL : https://localhost:8445
enableHPSSO : true
rest.excludedoc : false
loggerEnabled : false
csa.topology.expressDesignEnabled : false
OOS_USERNAME : admin
xAuthToken : X-Auth-Token
com.hp.csa.LifecycleExecutor.THREAD_WAKEUP_TIME : 5000
com.hp.csa.service.process.ProcessExecutorDelegate.CALLBACK_POOL_SIZE : 2
deploymentMode : single
com.hp.csa.UserGroupExecutor.CACHE_EXPIRATION_TIME : 30
csa.provider.port : 8444
defaultDaysToExtendExpirationDate : 1
rest.restrict : false
```

```
DynamicPropertyFetch.RESPONSE_SIZE : 50000
securityAdminPassword : *****
securityCdaInboundUserPassword : *****
csa.topology.calloutsEnabled : false
securityTransportUserName : csaTransportUser
com.hp.csa.import.BUILD_ARTIFACT_RELATIONSHIP : true
csa.provider.es.exists : no
com.hp.csa.aosMonitor.THREAD_WAKEUP_TIME : 20000
passed

_____________________________________________________________
End Health Tool at 4/13/15 11:55 AM
```

Interpreting the Health Tool Reports

Use the Health Tool reports to locate a problem within CSA and identify which of its components may be causing the problem. The tool is not meant to identify the exact problem. It is used to identify the area in which additional troubleshooting is needed.

Duration will vary based on your environment. There is no single magic number or range of numbers that can be used as a comparison. Duration is provided to help locate where there may be performance or other issues. For example, if the duration for all connection checks is long, there may be a network issue. If only the duration for one connection check is long, the connection to that component should be checked.

When available, log file content related to the check is reported.

The following table explains what each check is doing and basic troubleshooting if the check fails.

Check	Description
Ping database	Checks connectivity to the CSA database. If this check fails, verify that the information in the `config.properties` file is correct.
Table 'csa_person' rows count	Checks that data can be accessed in the CSA database. If connectivity to the CSA database fails, this information is not reported.
CSA database check	Checks connectivity to the CSA database. If this check fails, verify that the information in the `config.properties` file is correct.
Get database info	Displays the database type and version. Verify that you are using a supported version of the database. Refer to the Cloud Service Automation System and Software Support Matrix for more information about supported versions.
Get database driver info	Displays the JDBC drivers used by CSA to connect to the database. Use this information to verify that you are using drivers that are compatible with the database.
JMX connection check	Checks connectivity to the JBoss JMX server. If this check fails, start the JBoss JMX server.
MBean Server connection check	Checks connectivity to the JBoss MBean server. If this check fails, start the JBoss MBean server.
MBean Server connection check	Displays JBoss MBean server data load. If connectivity to the JBoss MBean server fails, this information is not reported.
CSA running check	Checks if the CSA service is running. If this check fails, start the CSA service.
Log in to CSA	Checks if the given user can log in to the Cloud Service Management Console. If this check fails, verify that the CSA credentials (`csa.username` and `csa.password`) in the `config.properties` file are valid and that the user has permissions to log in to the Cloud Service Management Console.
IdM running check	Checks connectivity to the Identity Management component. If this check fails, verify that the Identity Management component credentials (`idm.username` and `idm.password`) are valid and that the user has permissions to connect to the Identity Management component.
MPP running	Checks if the Marketplace Portal service is running. If this check fails, start the Marketplace

Check	Description
check	Portal service.
CSA LDAP check	Checks connectivity to the LDAP server. If this check fails, verify the information in the `ldap.config.properties` file is correct.
CSA data: Subscriptions	Displays the number of active subscriptions. The value can be used to determine if this is the root cause of performance issues.
CSA data: Lifecycle Transitions	Displays the number of lifecycle transitions. The value can be used to determine if this is the root cause of performance issues.
CSA data: Instances	Displays the number of operating system instances (OSIs) being used in current, active subscriptions. The value can be used to determine if this is the root cause of performance issues.
CSA data: Process return code	Checks the value of CSA_PROCESS_INSTANCE.PROCESS_RETURN_CODE_ID. The value can be used to determine if this is the root cause of performance issues.
CSA data: process state	Checks the value of CSA_PROCESS_INSTANCE.PROCESS_INSTANCE_STATE_ID. The value can be used to determine if this is the root cause of performance issues.
CSA data: Pending Subscriptions	Displays the number of pending subscriptions. The value can be used to determine if this is the root cause of performance issues.
CSA REST Check	Checks the connection to CSA using the REST API. If this check fails, verify that the CSA credentials (`idm.transportUser` and `idm.transportPassword`) in the `config.properties` file are valid and that the user has permissions to connect to CSA using the REST API.
CSA REST: License	Displays the CSA license information. If connectivity to CSA using the REST API fails, this information is not reported.
CSA REST Check	Checks the connection to CSA using the REST API. If this check fails, verify that the CSA credentials (`idm.transportUser` and `idm.transportPassword`) in the `config.properties` file are valid and that the user has permissions to connect to CSA using the REST API.
CSA REST: License	Displays the CSA license information. If connectivity to CSA using the REST API fails, this information is not reported.
CSA Properties	Displays all uncommented properties in the `<csa_home>\jboss-as\standalone\deployments\csa.war\WEB-INF\classes\csa.properties` file. If this check fails, verify that you are logged into the CSA system as a user who has access to the `csa.properties` file and that the file exists.

Example Usage

Note: Additional command line options are required if SSL is enabled between the Oracle database and CSA. See Communicating with the Oracle or MS SQL Database Using SSL.

Examples for Oracle (SSL is not Enabled)

- Display the Health Tool help:

```
"<csa_jre>\bin\java" -jar health-tool.jar -h
```

- Generate sample configuration properties and LDAP configuration properties files:

```
"<csa_jre>\bin\java" -jar health-tool.jar -g
```

- Generate sample LDAP configuration properties file:

```
"<csa_jre>\bin\java" -jar health-tool.jar -l
```

- Run the health tool, overwriting existing logs and reports:

  ```
  "<csa_jre>\bin\java" -jar health-tool.jar –o -j ojdbc6.jar
  ```

Examples for MS SQL and PostgreSQL

- Display the LDAP Configuration Tool help:

  ```
  "<csa_jre>\bin\java" -jar health-tool.jar –h
  ```

- Generate sample configuration properties and LDAP configuration properties files:

  ```
  "<csa_jre>\bin\java" -jar health-tool.jar –g
  ```

- Generate sample LDAP configuration properties file:

  ```
  "<csa_jre>\bin\java" -jar health-tool.jar –l
  ```

- Run the health tool, overwriting existing logs and reports:

  ```
  "<csa_jre>\bin\java" -jar health-tool.jar -o
  ```

Sample config.properties Contents

The following are examples of the properties that can be configured in the `config.properties` file. There are examples for each type of database (Oracle, MS SQL, and PostgreSQL), CSA, and the Identity Management component.

Oracle (SSL not enabled)

```
jdbc.driverClassName=oracle.jdbc.driver.OracleDriver
jdbc.databaseUrl=jdbc:oracle:thin:@//127.0.0.1:1521/XE
jdbc.username=csadbuser
jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)
jdbc.dialect=org.hibernate.dialect.OracleDialect
```

MS SQL (SSL not enabled)

```
jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver
jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=request
jdbc.username=csadbuser
jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)
jdbc.dialect=org.hibernate.dialect.SQLServerDialect
```

MS SQL (SSL enabled)

```
jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver
jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=authenticate
jdbc.username=csadbuser
jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)
jdbc.dialect=org.hibernate.dialect.SQLServerDialect
```

MS SQL (FIPS 140-2 compliant)

```
jdbc.driverClassName=net.sourceforge.jtds.jdbc.Driver
jdbc.databaseUrl=jdbc:jtds:sqlserver://127.0.0.1:1433/example;ssl=authenticate
jdbc.username=csadbuser
jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)
jdbc.dialect=org.hibernate.dialect.SQLServerDialect
```

PostgreSQL

```
jdbc.driverClassName=org.postgresql.Driver
jdbc.databaseUrl=jdbc:postgresql://127.0.0.1:5432/csadb
jdbc.username=csadbuser
jdbc.password=ENC(fc5e38d38a5703285441e7fe7010b0)
jdbc.dialect=org.hibernate.dialect.PostgreSQLDialect
```

CSA

```
# CSA credentials
csa.username=admin
csa.password=ENC(aJx51YfoPjzN3Dt8FWyugg==)
```

Identity Management Component

```
# IDM credentials
idm.tenantName=CSA-Provider
idm.transportUser=idmTransportUser
idm.transportPassword=ENC(5BMf3m8nKYyJqnTgNj4FT/KqUyVIJ5ovEKtpmgUGDRA=)
idm.username=admin
idm.password=ENC(aJx51YfoPjzN3Dt8FWyugg==)
```

Sample ldap.config.properties Contents

```
csa.ldap.hostname=172.16.200.50
csa.ldap.port=389
csa.ldap.ssl=false
csa.ldap.basedn=DC=cirrus,DC=com
csa.ldap.userid=CN=csaldap,CN=Users,DC=cirrus,DC=com
csa.ldap.password=ENC(A0El12PmN6ajnhlInJAnEumDDvCBvQLV)
csa.ldap.useremail=mail
csa.ldap.groupmembership=member
csa.ldap.managerIdentifier=manager
csa.ldap.managerIdentifierValue=dn
csa.ldap.userAvatar=avatar
csa.ldap.userNameAttribute=sAMAccountName
csa.ldap.userSearchBase=
csa.ldap.userSearchFilter=sAMAccountName={0}
csa.ldap.searchSubtree=n
```

Generated Sample LDAP Configuration Properties File

```
# A sample config properties file for an LDAP configuration in CSA.

# The fully-qualified LDAP server domain name (server.domain.com) or IP address. Example:
ldap.xyz.com
csa.ldap.hostname=

# The port used to connect to the LDAP server. 389 for ldap and 636 for ldaps.
csa.ldap.port=

# Connection Security. If the LDAP server is configured to require ldaps (LDAP over SSL), set this
attribute to true.
csa.ldap.ssl=false

# Base distinguished name. The Base DN is the top level of the LDAP directory that is used as the
basis of a search.
csa.ldap.basedn=dc=example,dc=com

# The fully distinguished name of any user with authentication rights to the LDAP server. If the
LDAP server does not require a User ID or password for authentication, this value can be omitted.
csa.ldap.userid=

# Password of the User ID. If the LDAP server does not require a User ID or password for
authentication, this value can be omitted.
csa.ldap.password=


# Required. This LDAP attribute designates the email address of the user to which to send email
notifications. Common LDAP attribute names for email include mail, email,
# and userPrincipalName. If the value for this attribute in the user object in LDAP is empty or not
valid, the user for whom the value is empty or not valid does not receive email
# notifications.
csa.ldap.useremail=mail

# Required. This attribute type identifies a user as belonging to the group. Common LDAP attribute
names that convey group membership include member and uniqueMember.
csa.ldap.groupmembership=member

# Required. This attribute type identifies the manager of the user. A common LDAP attribute name
for a user's manager is manager. If the value for this
# attribute in the user object in LDAP is empty or not valid, approval policies that use the User
Context Template will fail.
csa.ldap.managerIdentifier=manager

# Required. This attribute type describes the value of the manager identifier.
# A common value for the manager identifier in LDAP is the dn (distinguished name) of the manager's
user object.
# If the manager's user object cannot be located based on the values for manager identifier and
manager identifier value, approval policies that use the User Context Template will fail.
csa.ldap.managerIdentifierValue=dn

# LDAP attribute whose value is the URL to a user avatar image that will display for the logged in
user in the Marketplace Portal. If no avatar is specified, a default avatar will be used.
csa.ldap.userAvatar=avatar

# The name of the attribute of a user object that contains the username that will be used to log
into the Cloud Service Management Console or Marketplace Portal.
# The value for this field can be determined by looking at one or more user objects in the LDAP
directory to determine which attribute consistently contains a unique user name.
```

```
# Often, you will want a User Name Attribute whose value in a use object is an email address.
#csa.ldap.userNameAttribute=sAMAccountName

# The LDAP container that contains users. This value must be relative to the Base DN. If users are
not located in a common directory under the Base DN, leave this field blank. Example:ou=People
csa.ldap.userSearchBase=cn=Users

# Specifies the general form of the LDAP query used to identify users during login.
# It must include the pattern {0}, which represents the user name entered by the user when logging
in to the Cloud Service Management Console or Marketplace Portal. The filter is generally of the
form <attribute>= 0}, with <attribute> typically corresponding to the value entered for User Name
Attribute. Example: uid={0}
csa.ldap.userSearchFilter= AMAccountName={0}

# When a user logs in to the Cloud Service Management Console or Marketplace Portal, the LDAP
directory is queried to find the user's account.
# The Search Subtree setting controls the depth of the search under User Search Base.
# If you want to search for a matching user in the User Search Base and all subtrees under the User
Search Base, set the value of this attribute to y (yes).
# If you want to restrict the search for a matching user to only the User Search Base, excluding
any subtrees, set the value of this attribute to n (no).
csa.ldap.searchSubtree=n
```

Send documentation feedback

If you have comments about this document, you can send them to clouddocs@hpe.com.

Legal notices

Warranty

The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted rights legend

Confidential computer software. Valid license from Hewlett Packard Enterprise 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.

Copyright notice

Trademark notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

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 the following URL and sign-in or register: https://softwaresupport.hp.com.

Select Manuals from the Dashboard menu to view all available documentation. Use the search and filter functions to find documentation, whitepapers, and other information sources.

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

Support

Visit the Hewlett Packard Enterprise Software Support Online web site at https://softwaresupport.hp.com.