Red Hat Enterprise Linux 9

Using IdM Healthcheck to monitor your IdM environment

Performing status and health checks

Last Updated: 2024-06-25

Red Hat Enterprise Linux 9 Using IdM Healthcheck to monitor your IdM environment

Performing status and health checks

Legal Notice

Abstract

The ipa-healthcheck utility helps administrators to detect problems in a Red Hat Identity Management (IdM) environment. This includes status checks of IdM services, configuration file permissions, replication statuses, and issues with certificates.

Table of Contents

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

We appreciate your feedback on our documentation. Let us know how we can improve it.

Submitting feedback through Jira (account required)

1. Log in to the Jira website.
2. Click **Create** in the top navigation bar
3. Enter a descriptive title in the **Summary** field.
4. Enter your suggestion for improvement in the **Description** field. Include links to the relevant parts of the documentation.
5. Click **Create** at the bottom of the dialogue.

CHAPTER 1. INSTALLING AND RUNNING THE IDM HEALTHCHECK TOOL

Learn more about the IdM Healthcheck tool and how to install and run it.

1.1. HEALTHCHECK IN IDM

The Healthcheck tool in Identity Management (IdM) helps find issues that may impact the health of your IdM environment.

NOTE

The Healthcheck tool is a command line tool that can be used without Kerberos authentication.

Modules are Independent

Healthcheck consists of independent modules which test for:

- Replication issues
- Certificate validity
- Certificate Authority infrastructure issues
- IdM and Active Directory trust issues
- Correct file permissions and ownership settings

Two output formats

Healthcheck generates the following outputs, which you can set using the **output-type** option:

- **json**: Machine-readable output in JSON format (default)
- **human**: Human-readable output

You can specify a different file destination with the **--output-file** option.

Results

Each Healthcheck module returns one of the following results:

SUCCESS
: configured as expected

WARNING
: not an error, but worth keeping an eye on or evaluating

ERROR
: not configured as expected

CRITICAL
: not configured as expected, with a high possibility for impact

1.2. INSTALLING IDM HEALTHCHECK

Follow this procedure to install the IdM Healthcheck tool.

Procedure

- Install the **ipa-healthcheck** package:

```
[root@server ~]# dnf install ipa-healthcheck
```

Verification steps

- Use the **--failures-only** option to have **ipa-healthcheck** only report errors. A fully-functioning IdM installation returns an empty result of **[]**.

```
[root@server ~]# ipa-healthcheck --failures-only
[]
```

Additional resources

- Use **ipa-healthcheck --help** to see all supported arguments.

1.3. RUNNING IDM HEALTHCHECK

Healthcheck can be run manually or automatically using log rotation

Prerequisites

- The Healthcheck tool must be installed. See Installing IdM Healthcheck.

Procedure

- To run healthcheck manually, enter the **ipa-healthcheck** command.

```
[root@server ~]# ipa-healthcheck
```

Additional resources

For all options, see the man page: **man ipa-healthcheck**.

1.4. LOG ROTATION

Log rotation creates a new log file every day, and the files are organized by date. Since log files are saved in the same directory, you can select a particular log file according to the date.

Rotation means that there is configured a number for max number of log files and if the number is exceeded, the newest file rewrites and renames the oldest one. For example, if the rotation number is 30, the thirty-first log file replaces the first (oldest) one.

Log rotation reduces voluminous log files and organizes them, which can help with analysis of the logs.

1.5. CONFIGURING LOG ROTATION USING THE IDM HEALTHCHECK

Follow this procedure to configure a log rotation with:

- The **systemd** timer
- The **crond** service

The **systemd** timer runs the Healthcheck tool periodically and generates the logs. The default value is set to 4 a.m. every day.

The **crond** service is used for log rotation.

The default log name is **healthcheck.log** and the rotated logs use the **healthcheck.log-YYYYMMDD** format.

Prerequisites

- You must execute commands as root.

Procedure

1. Enable a **systemd** timer:

```
# systemctl enable ipa-healthcheck.timer
Created symlink /etc/systemd/system/multi-user.target.wants/ipa-healthcheck.timer ->
/usr/lib/systemd/system/ipa-healthcheck.timer.
```

2. Start the **systemd** timer:

```
# systemctl start ipa-healthcheck.timer
```

3. Open the **/etc/logrotate.d/ipahealthcheck** file to configure the number of logs which should be saved.
   By default, log rotation is set up for 30 days.

4. In the **/etc/logrotate.d/ipahealthcheck** file, configure the path to the logs.
   By default, logs are saved in the **/var/log/ipa/healthcheck/** directory.

5. In the **/etc/logrotate.d/ipahealthcheck** file, configure the time for log generation.
   By default, a log is created daily at 4 a.m.

6. To use log rotation, ensure that the **crond** service is enabled and running:

```
# systemctl enable crond
# systemctl start crond
```

To start with generating logs, start the IPA healthcheck service:

```
# systemctl start ipa-healthcheck
```

To verify the result, go to **/var/log/ipa/healthcheck/** and check if logs are created correctly.

1.6. CHANGING IDM HEALTHCHECK CONFIGURATION

You can change Healthcheck settings by adding the desired command line options to the **/etc/ipahealthcheck/ipahealthcheck.conf** file. This can be useful when, for example, you configured a log rotation and want to ensure the logs are in a format suitable for automatic analysis, but do not want to set up a new timer.

NOTE

This Healthcheck feature is only available on RHEL 9.1 and newer.

After the modification, all logs that Healthcheck creates follow the new settings. These settings also apply to any manual execution of Healthcheck.

NOTE

When running Healthcheck manually, settings in the configuration file take precedence over options specified in the command line. For example, if **output_type** is set to **human** in the configuration file, specifying **json** on the command line has no effect. Any command line options you use that are not specified in the configuration file are applied normally.

Additional resources

- Configuring log rotation using the IdM Healthcheck

1.7. CONFIGURING HEALTHCHECK TO CHANGE THE OUTPUT LOGS FORMAT

Follow this procedure to configure Healthcheck with a timer already set up. In this example, you configure Healthcheck to produce logs in a human-readable format and to also include successful results instead of only errors.

Prerequisites

- Your system is running RHEL 9.1 or later.
- You have **root** privileges.
- You have previously configured log rotation on a timer.

Procedure

1. Open the **/etc/ipahealthcheck/ipahealthcheck.conf** file in a text editor.
2. Add options **output_type=human** and **all=True** to the **[default]** section.
3. Save and close the file.

Verification

1. Run Healthcheck manually:

```
# ipa-healthcheck
```

2. Go to **/var/log/ipa/healthcheck/** and check that the logs are in the correct format.

Additional resources

- Configuring log rotation using the IdM Healthcheck

1.8. ADDITIONAL RESOURCES

- See the following sections of the Using IdM Healthcheck to monitor your IdM environment guide for examples of using IdM Healthcheck.
  - Checking services
  - Verifying your IdM and AD trust configuration
  - Verifying certificates
  - Verifying system certificates
  - Checking disk space
  - Verifying permissions of IdM configuration files
  - Checking replication

CHAPTER 2. CHECKING SERVICES USING IDM HEALTHCHECK

You can monitor services used by the Identity Management (IdM) server using the Healthcheck tool.

For details, see

Healthcheck in IdM.

2.1. SERVICES HEALTHCHECK TEST

The Healthcheck tool includes a test to check if any IdM services is not running. This test is important because services which are not running can cause failures in other tests. Therefore, check that all services are running first. You can then check all other test results.

To see all services tests, run **ipa-healthcheck** with the **--list-sources** option:

```
# ipa-healthcheck --list-sources
```

You can find all services tested with Healthcheck under the **ipahealthcheck.meta.services** source:

- certmonger
- dirsrv
- gssproxy
- httpd
- ipa_custodia
- ipa_dnskeysyncd
- ipa_otpd
- kadmin
- krb5kdc
- named
- pki_tomcatd
- sssd

NOTE

Run these tests on all IdM servers when trying to discover issues.

2.2. SCREENING SERVICES USING HEALTHCHECK

Follow this procedure to run a standalone manual test of services running on the Identity Management (IdM) server using the Healthcheck tool.

The Healthcheck tool includes many tests, whose results can be shortened with:

- Excluding all successful test: **--failures-only**
- Including only services tests: **--source=ipahealthcheck.meta.services**

Procedure

- To run Healthcheck with warnings, errors and critical issues regarding services, enter:

```
# ipa-healthcheck --source=ipahealthcheck.meta.services --failures-only
```

A successful test displays empty brackets:

```
[ ]
```

If one of the services fails, the result can looks similarly to this example:

```
{
  "source": "ipahealthcheck.meta.services",
  "check": "httpd",
  "result": "ERROR",
  "kw": {
    "status": false,
    "msg": "httpd: not running"
  }
}
```

Additional resources

- See **man ipa-healthcheck**.

CHAPTER 3. CHECKING DISK SPACE USING IDM HEALTHCHECK

You can monitor the Identity Management server's free disk space using the Healthcheck tool.

For details, see Healthcheck in IdM.

3.1. DISK SPACE HEALTHCHECK TEST

The Healthcheck tool includes a test for checking available disk space. Insufficient free disk space can cause issues with:

- Logging
- Execution
- Backups

The test checks the following paths:

Table 3.1. Tested paths

Paths checked by the test	Minimal disk space in MB
/var/lib/dirsrv/	1024
/var/lib/ipa/backup/	512
/var/log/	1024
var/log/audit/	512
/var/tmp/	512
/tmp/	512

To list all tests, run the **ipa-healthcheck** with the **--list-sources** option:

```
# ipa-healthcheck --list-sources
```

You can find the file system space check test under the **ipahealthcheck.system.filesystemspace** source:

FileSystemSpaceCheck

This test checks available disk space in the following ways:

- The minimum raw free bytes needed.
- The percentage – the minimum free disk space is hardcoded to 20%.

3.2. SCREENING DISK SPACE USING THE HEALTHCHECK TOOL

Follow this procedure to run a standalone manual test of available disk space on an Identity Management (IdM) server using the Healthcheck tool.

Since Healthcheck includes many tests, you can narrow the results by:

- Excluding all successful test: **--failures-only**
- Including only space check tests: **--source=ipahealthcheck.system.filesystemspace**

Procedure

- To run Healthcheck with warnings, errors and critical issues regarding available disk space, enter:

```
# ipa-healthcheck --source=ipahealthcheck.system.filesystemspace --failures-only
```

A successful test displays empty brackets:

```
[]
```

As an example, a failed test can display:

```
{
  "source": "ipahealthcheck.system.filesystemspace",
  "check": "FileSystemSpaceCheck",
  "result": "ERROR",
  "kw": {
    "msg": "/var/lib/dirsrv: free space under threshold: 0 MiB < 1024 MiB",
    "store": "/var/lib/dirsrv",
    "free_space": 0,
    "threshold": 1024
  }
}
```

The failed test informs you that the **/var/lib/dirsrv** directory has run out of space.

Additional resources

- See **man ipa-healthcheck**.

CHAPTER 4. VERIFYING PERMISSIONS OF IDM CONFIGURATION FILES USING HEALTHCHECK

Learn more about how to test Identity Management (IdM) configuration files using the Healthcheck tool.

For details, see

Healthcheck in IdM.

4.1. FILE PERMISSIONS HEALTHCHECK TESTS

The Healthcheck tool tests ownership and permissions of some important files installed or configured by Identity Management (IdM).

If you change the ownership or permissions of any tested file, the test returns a warning in the **result** section. While it does not necessarily mean that the configuration will not work, it means that the file differs from the default configuration.

To see all tests, run the **ipa-healthcheck** with the **--list-sources** option:

```
# ipa-healthcheck --list-sources
```

You can find the file permissions test under the **ipahealthcheck.ipa.files** source:

IPAFileNSSDBCheck

This test checks the 389-ds NSS database and the Certificate Authority (CA) database. The 389-ds database is located in **/etc/dirsrv/slapd-<dashed-REALM>** and the CA database is located in **/etc/pki/pki-tomcat/alias/**.

IPAFileCheck

This test checks the following files:

- **/var/lib/ipa/ra-agent.{key|pem}**
- **/var/lib/ipa/certs/httpd.pem**
- **/var/lib/ipa/private/httpd.key**
- **/etc/httpd/alias/ipasession.key**
- **/etc/dirsrv/ds.keytab**
- **/etc/ipa/ca.crt**
- **/etc/ipa/custodia/server.keys**
  If PKINIT is enabled:
- **/var/lib/ipa/certs/kdc.pem**
- **/var/lib/ipa/private/kdc.key**
  If DNS is configured:
- **/etc/named.keytab**

- **/etc/ipa/dnssec/ipa-dnskeysyncd.keytab**

TomcatFileCheck

This test checks some tomcat-specific files if a CA is configured:

- **/etc/pki/pki-tomcat/password.conf**
- **/var/lib/pki/pki-tomcat/conf/ca/CS.cfg**
- **/etc/pki/pki-tomcat/server.xml**

NOTE

Run these tests on all IdM servers when trying to find issues.

4.2. SCREENING CONFIGURATION FILES USING HEALTHCHECK

Follow this procedure to run a standalone manual test of an Identity Management (IdM) server's configuration files using the Healthcheck tool.

The Healthcheck tool includes many tests. Results can be narrowed down by:

- Excluding all successful test: **--failures-only**
- Including only ownership and permissions tests: **--source=ipahealthcheck.ipa.files**

Procedure

1. To run Healthcheck tests on IdM configuration file ownership and permissions, while displaying only warnings, errors and critical issues, enter:

```
# ipa-healthcheck --source=ipahealthcheck.ipa.files --failures-only
```

A successful test displays empty brackets:

```
# ipa-healthcheck --source=ipahealthcheck.ipa.files --failures-only
[]
```

Failed tests display results similar to the following **WARNING**:

```
{
  "source": "ipahealthcheck.ipa.files",
  "check": "IPAFileNSSDBCheck",
  "result": "WARNING",
  "kw": {
    "key": "_etc_dirsrv_slapd-EXAMPLE-TEST_pkcs11.txt_mode",
    "path": "/etc/dirsrv/slapd-EXAMPLE-TEST/pkcs11.txt",
    "type": "mode",
    "expected": "0640",
    "got": "0666",
    "msg": "Permissions of /etc/dirsrv/slapd-EXAMPLE-TEST/pkcs11.txt are 0666 and should be 0640"
  }
}
```

Additional resources

- See **man ipa-healthcheck**.

CHAPTER 5. CHECKING DNS RECORDS USING IDM HEALTHCHECK

You can identify issues with DNS records in Identity Management (IdM) using the Healthcheck tool.

5.1. DNS RECORDS HEALTHCHECK TEST

The Healthcheck tool includes a test for checking that the expected DNS records required for autodiscovery are resolvable.

To list all tests, run the **ipa-healthcheck** with the **--list-sources** option:

```
# ipa-healthcheck --list-sources
```

You can find the DNS records check test under the **ipahealthcheck.ipa.idns** source.

IPADNSSystemRecordsCheck

This test checks the DNS records from the **ipa dns-update-system-records --dry-run** command using the first resolver specified in the **/etc/resolv.conf** file. The records are tested on the IPA server.

5.2. SCREENING DNS RECORDS USING THE HEALTHCHECK TOOL

Follow this procedure to run a standalone manual test of DNS records on an Identity Management (IdM) server using the Healthcheck tool.

The Healthcheck tool includes many tests. Results can be narrowed down by including only the DNS records tests by adding the **--source ipahealthcheck.ipa.idns** option.

Prerequisites

- You must perform Healthcheck tests as the **root** user.

Procedure

- To run the DNS records check, enter:

  ```
  # ipa-healthcheck --source ipahealthcheck.ipa.idns
  ```

  If the record is resolvable, the test returns **SUCCESS** as a result:

  ```
  {
    "source": "ipahealthcheck.ipa.idns",
    "check": "IPADNSSystemRecordsCheck",
    "result": "SUCCESS",
    "uuid": "eb7a3b68-f6b2-4631-af01-798cac0eb018",
    "when": "20200415143339Z",
    "duration": "0.210471",
    "kw": {
      "key": "_ldap._tcp.idm.example.com.:server1.idm.example.com."
    }
  }
  ```

The test returns a **WARNING** when, for example, the number of records does not match the expected number:


```
{
    "source": "ipahealthcheck.ipa.idns",
    "check": "IPADNSSystemRecordsCheck",
    "result": "WARNING",
    "uuid": "972b7782-1616-48e0-bd5c-49a80c257895",
    "when": "20200409100614Z",
    "duration": "0.203049",
    "kw": {
      "msg": "Got {count} ipa-ca A records, expected {expected}",
      "count": 2,
      "expected": 1
    }
}
```


Additional resources

- See **man ipa-healthcheck**.

CHAPTER 6. VERIFYING THE OPTIMAL NUMBER OF KDC WORKER PROCESSES USING IDM HEALTHCHECK

You can use the Healthcheck tool in Identity Management (IdM) to verify that the Kerberos Key Distribution Center (KDC) is configured to use the optimal number of **krb5kdc** worker processes, which should be equal to the number of CPU cores on the host.

You can find the test for the correct number of KDC worker processes under the **ipahealthcheck.ipa.kdc** source. As the Healthcheck tool includes many tests, you can narrow down the results by including only the KDC worker tests by adding the **--source ipahealthcheck.ipa.kdc** option.

Prerequisites

- The KDC worker process Healthcheck tool is only available on RHEL 8.7 or newer.
- You must perform Healthcheck tests as the **root** user.

Procedure

- To run the check for KDC worker processes, enter:

```
# ipa-healthcheck --source ipahealthcheck.ipa.kdc
```

If the number of KDC worker processes matches the number of CPU cores, the test returns **SUCCESS** as a result:

```
{
 "source": "ipahealthcheck.ipa.kdc",
 "check": "KDCWorkersCheck",
 "result": "SUCCESS",
 "uuid": "68f6e20a-0aa9-427d-8fdc-fbb8196d56cd",
 "when": "20230105162211Z",
 "duration": "0.000157",
 "kw": {
   "key": "workers"
 }
}
```

The test returns a **WARNING** if the number of worker processes does not match the number of CPU cores. In the following example, a host with 2 cores is configured to have only one KDC worker process:

```
{
    "source": "ipahealthcheck.ipa.kdc",
    "check": "KDCWorkersCheck",
    "result": "WARNING",
    "uuid": "972b7782-1616-48e0-bd5c-49a80c257895",
    "when": "20230105122236Z",
    "duration": "0.203049",
    "kw": {
      "key": 'workers',
      "cpus": 2,
      "workers": 1,
      "expected": "The number of CPUs {cpus} does not match the number of workers
```

```
{workers} in {sysconfig}"
    }
}
```

The test also outputs a **WARNING** if there are no configured workers. In the following example, the **KRB5KDC_ARGS** variable is missing from the **/etc/sysconfig/krb5kdc** configuration file:

```
  {
    "source": "ipahealthcheck.ipa.kdc",
    "check": "KDCWorkersCheck",
    "result": "WARNING",
    "uuid": "5d63ea86-67b9-4638-a41e-b71f4
56efed7",
    "when": "20230105162526Z",
    "duration": "0.000135",
    "kw": {
      "key": "workers",
      "sysconfig": "/etc/sysconfig/krb5kdc",
      "msg": "KRB5KDC_ARGS is not set in {sysconfig}"
    }
  }
```

Additional resources

- **man ipa-healthcheck**

CHAPTER 7. CHECKING IDM REPLICATION USING HEALTHCHECK

You can test Identity Management (IdM) replication using the Healthcheck tool.

For details, see Healthcheck in IdM.

7.1. REPLICATION HEALTHCHECK TESTS

The Healthcheck tool tests the Identity Management (IdM) topology configuration and searches for replication conflict issues.

To list all tests, run the **ipa-healthcheck** with the **--list-sources** option:

```
# ipa-healthcheck --list-sources
```

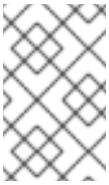
The topology tests are placed under the **ipahealthcheck.ipa.topology** and **ipahealthcheck.ds.replication** sources:

IPATopologyDomainCheck

This test verifies:

- Whether topology is not disconnected and there are replication paths between all servers.
- If servers do not have more than the recommended number of replication agreements. If the test fails, the test returns errors, such as connection errors or too many replication agreements.

  If the test succeeds, the test returns the configured domains.



NOTE

The test runs the **ipa topologysuffix-verify** command for both the domain and ca suffixes (assuming the Certificate Authority is configured on this server).

ReplicationConflictCheck

The test searches for entries in LDAP matching **(&(!(objectclass=nstombstone))(nsds5ReplConflict=*))**.

NOTE

Run these tests on all IdM servers when trying to check for issues.

For more information on resolving LDAP replication conflicts, see Solving common replication problems.

7.2. SCREENING REPLICATION USING HEALTHCHECK

Follow this procedure to run a standalone manual test of an Identity Management (IdM) replication topology and configuration using the Healthcheck tool.

The Healthcheck tool includes many tests, therefore, you can shorten the results with:

- Replication conflict test: **--source=ipahealthcheck.ds.replication**
- Correct topology test: **--source=ipahealthcheck.ipa.topology**

Prerequisites

- You must perform Healthcheck tests as the **root** user.

Procedure

- To run Healthcheck replication conflict and topology checks, enter:

```
# ipa-healthcheck --source=ipahealthcheck.ds.replication --
source=ipahealthcheck.ipa.topology
```

Four different results are possible:

- SUCCESS – the test passed successfully.

```
{
  "source": "ipahealthcheck.ipa.topology",
  "check": "IPATopologyDomainCheck",
  "result": "SUCCESS",
  "kw": {
    "suffix": "domain"
  }
}
```

- WARNING – the test passed but there might be a problem.
- ERROR – the test failed.

```
{
  "source": "ipahealthcheck.ipa.topology",
  "check": "IPATopologyDomainCheck",
  "result": "ERROR",
  "uuid": d6ce3332-92da-423d-9818-e79f49ed321f
  "when": 20191007115449Z
  "duration": 0.005943
  "kw": {
    "msg": "topologysuffix-verify domain failed, server2 is not connected
(server2_139664377356472 in MainThread)"
  }
}
```

- CRITICAL – the test failed and it affects the IdM server functionality.

Additional resources

- See **man ipa-healthcheck**.

CHAPTER 8. VERIFYING YOUR IDM AND AD TRUST CONFIGURATION USING IDM HEALTHCHECK

Learn more about identifying issues with IdM and an Active Directory trust in Identity Management (IdM) by using the Healthcheck tool.

8.1. IDM AND AD TRUST HEALTHCHECK TESTS

The Healthcheck tool includes several tests for testing the status of your Identity Management (IdM) and Active Directory (AD) trust.

To see all trust tests, run **ipa-healthcheck** with the **--list-sources** option:

```
# ipa-healthcheck --list-sources
```

You can find all tests under the **ipahealthcheck.ipa.trust** source:

IPATrustAgentCheck

This test checks the SSSD configuration when the machine is configured as a trust agent. For each domain in **/etc/sssd/sssd.conf** where **id_provider=ipa** ensure that **ipa_server_mode** is **True**.

IPATrustDomainsCheck

This test checks if the trust domains match SSSD domains by comparing the list of domains in **sssctl domain-list** with the list of domains from **ipa trust-find** excluding the IPA domain.

IPATrustCatalogCheck

This test resolves resolves an AD user, **Administrator@REALM**. This populates the AD Global catalog and AD Domain Controller values in **sssctl domain-status** output.
For each trust domain look up the user with the id of the SID + 500 (the administrator) and then check the output of **sssctl domain-status <domain> --active-server** to ensure that the domain is active.

IPAsidgenpluginCheck

This test verifies that the **sidgen** plugin is enabled in the IPA 389-ds instance. The test also verifies that the **IPA SIDGEN** and **ipa-sidgen-task** plugins in **cn=plugins,cn=config** include the **nsslapd-pluginEnabled** option.

IPATrustAgentMemberCheck

This test verifies that the current host is a member of **cn=adtrust agents,cn=sysaccounts,cn=etc,SUFFIX**.

IPATrustControllerPrincipalCheck

This test verifies that the current host is a member of **cn=adtrust agents,cn=sysaccounts,cn=etc,SUFFIX**.

IPATrustControllerServiceCheck

This test verifies that the current host starts the ADTRUST service in ipactl.

IPATrustControllerConfCheck

This test verifies that **ldapi** is enabled for the passdb backend in the output of **net conf** list.

IPATrustControllerGroupSIDCheck

This test verifies that the admins group's SID ends with 512 (Domain Admins RID).

IPATrustPackageCheck

This test verifies that the **trust-ad** package is installed if the trust controller and AD trust are not enabled.

NOTE

Run these tests on all IdM servers when trying to find an issue.

8.2. SCREENING THE TRUST WITH THE HEALTHCHECK TOOL

Follow this procedure to run a standalone manual test of an Identity Management (IdM) and Active Directory (AD) trust health check using the Healthcheck tool.

The Healthcheck tool includes many tests, therefore, you can shorten the results by:

- Excluding all successful test: **--failures-only**
- Including only trust tests: **--source=ipahealthcheck.ipa.trust**

Procedure

- To run Healthcheck with warnings, errors and critical issues in the trust, enter:

```
# ipa-healthcheck --source=ipahealthcheck.ipa.trust --failures-only
```

Successful test displays empty brackets:

```
# ipa-healthcheck --source=ipahealthcheck.ipa.trust --failures-only
[]
```

Additional resources

- See **man ipa-healthcheck**.

CHAPTER 9. VERIFYING SYSTEM CERTIFICATES USING IDM HEALTHCHECK

Learn more about identifying issues with system certificates in Identity Management (IdM) by using the Healthcheck tool.

For details, see

Healthcheck in IdM.

9.1. SYSTEM CERTIFICATES HEALTHCHECK TESTS

The Healthcheck tool includes several tests for verifying system (DogTag) certificates.

To see all tests, run the **ipa-healthcheck** with the **--list-sources** option:

```
# ipa-healthcheck --list-sources
```

You can find all tests under the **ipahealthcheck.dogtag.ca** source:

DogtagCertsConfigCheck

This test compares the CA (Certificate Authority) certificates in its NSS database to the same values stored in **CS.cfg**. If they do not match, the CA fails to start.
Specifically, it checks:

- **auditSigningCert cert-pki-ca** against **ca.audit_signing.cert**
- **ocspSigningCert cert-pki-ca** against **ca.ocsp_signing.cert**
- **caSigningCert cert-pki-ca** against **ca.signing.cert**
- **subsystemCert cert-pki-ca** against **ca.subsystem.cert**
- **Server-Cert cert-pki-ca** against **ca.sslserver.cert**

If Key Recovery Authority (KRA) is installed:

- **transportCert cert-pki-kra** against **ca.connector.KRA.transportCert**

DogtagCertsConnectivityCheck

This test verifies connectivity. This test is equivalent to the **ipa cert-show 1** command which checks:

- The PKI proxy configuration in Apache
- IdM being able to find a CA
- The RA agent client certificate
- Correctness of CA replies to requests

Note that the test checks a certificate with serial #1 because you want to verify that a **cert-show** can be executed and get back an expected result from CA (either the certificate or a not found).

NOTE

Run these tests on all IdM servers when trying to find an issue.

9.2. SCREENING SYSTEM CERTIFICATES USING HEALTHCHECK

Follow this procedure to run a standalone manual test of Identity Management (IdM) certificates using the Healthcheck tool.

Since, the Healthcheck tool includes many tests, you can narrow the results by including only DogTag tests: **--source=ipahealthcheck.dogtag.ca**

Procedure

- To run Healthcheck restricted to DogTag certificates, enter:

```
# ipa-healthcheck --source=ipahealthcheck.dogtag.ca
```

An example of a successful test:

```
{
  "source: ipahealthcheck.dogtag.ca",
  "check: DogtagCertsConfigCheck",
  "result: SUCCESS",
  "uuid: 9b366200-9ec8-4bd9-bb5e-9a280c803a9c",
  "when: 20191008135826Z",
  "duration: 0.252280",
  "kw:" {
    "key": "Server-Cert cert-pki-ca",
    "configfile":  "/var/lib/pki/pki-tomcat/conf/ca/CS.cfg"
    }
}
```

An example of a failed test:

```
{
  "source: ipahealthcheck.dogtag.ca",
  "check: DogtagCertsConfigCheck",
  "result: CRITICAL",
  "uuid: 59d66200-1447-4b3b-be01-89810c803a98",
  "when: 20191008135912Z",
  "duration: 0.002022",
  "kw:" {
    "exception": "NSDB /etc/pki/pki-tomcat/alias not initialized",
    }
}
```

Additional resources

- See **man ipa-healthcheck**.

CHAPTER 10. VERIFYING CERTIFICATES USING IDM HEALTHCHECK

Learn more about understanding and using the Healthcheck tool in Identity management (IdM) to identify issues with IPA certificates maintained by **certmonger**.

For details, see Healthcheck in IdM.

10.1. IDM CERTIFICATES HEALTHCHECK TESTS

The Healthcheck tool includes several tests for verifying the status of certificates maintained by certmonger in Identity Management (IdM). For details about certmonger, see Obtaining an IdM certificate for a service using certmonger.

This suite of tests checks expiration, validation, trust and other issues. Multiple errors may be thrown for the same underlying issue.

To see all certificate tests, run the **ipa-healthcheck** with the **--list-sources** option:

```
# ipa-healthcheck --list-sources
```

You can find all tests under the **ipahealthcheck.ipa.certs** source:

IPACertmongerExpirationCheck

This test checks expirations in **certmonger**.
If an error is reported, the certificate has expired.

If a warning appears, the certificate will expire soon. By default, this test applies within 28 days or fewer days before certificate expiration.

You can configure the number of days in the **/etc/ipahealthcheck/ipahealthcheck.conf** file. After opening the file, change the **cert_expiration_days** option located in the default section.

NOTE

Certmonger loads and maintains its own view of the certificate expiration. This check does not validate the on-disk certificate.

IPACertfileExpirationCheck

This test checks if the certificate file or NSS database cannot be opened. This test also checks expiration. Therefore, carefully read the **msg** attribute in the error or warning output. The message specifies the problem.

NOTE

This test checks the on-disk certificate. If a certificate is missing, unreadable, etc a separate error can also be raised.

IPACertNSSTrust

This test compares the trust for certificates stored in NSS databases. For the expected tracked certificates in NSS databases the trust is compared to an expected value and an error raised on a non-match.

IPANSSChainValidation

This test validates the certificate chain of the NSS certificates. The test executes: **certutil -V -u V -e -d [dbdir] -n [nickname]**

IPAOpenSSLChainValidation

This test validates the certificate chain of the OpenSSL certificates. To be comparable to the **NSSChain** validation here is the OpenSSL command we execute:

```
openssl verify -verbose -show_chain -CAfile /etc/ipa/ca.crt [cert file]
```

IPARAAgent

This test compares the certificate on disk with the equivalent record in LDAP in **uid=ipara,ou=People,o=ipaca**.

IPACertRevocation

This test uses certmonger to verify that certificates have not been revoked. Therefore, the test can find issues connected with certificates maintained by certmonger only.

IPACertmongerCA

This test verifies the certmonger Certificate Authority (CA) configuration. IdM cannot issue certificates without CA.
Certmonger maintains a set of CA helpers. In IdM, there is a CA named IPA which issues certificates through IdM, authenticating as a host or user principal, for host or service certs.

There are also **dogtag-ipa-ca-renew-agent** and **dogtag-ipa-ca-renew-agent-reuse** which renew the CA subsystem certificates.

NOTE

Run these tests on all IdM servers when trying to check for issues.

10.2. SCREENING CERTIFICATES USING THE HEALTHCHECK TOOL

Follow this procedure to run a standalone manual test of an Identity Management (IdM) certificate health check using the Healthcheck tool.

The Healthcheck tool includes many tests, therefore, you can shorten the results with:

- Excluding all successful test: **--failures-only**
- Including only certificate tests: **--source=ipahealthcheck.ipa.certs**

Prerequisites

- You must perform Healthcheck tests as the **root** user.

Procedure

- To run Healthcheck with warnings, errors and critical issues regarding certificates, enter:

```
# ipa-healthcheck --source=ipahealthcheck.ipa.certs --failures-only
```

Successful test displays empty brackets:

```
[]
```

Failed test shows you the following output:

```
{
  "source": "ipahealthcheck.ipa.certs",
  "check": "IPACertfileExpirationCheck",
  "result": "ERROR",
  "kw": {
    "key": 1234,
    "dbdir": "/path/to/nssdb",
    "error": [error],
    "msg": "Unable to open NSS database '/path/to/nssdb': [error]"
  }
}
```

This **IPACertfileExpirationCheck** test failed on opening the NSS database.

Additional resources

- See **man ipa-healthcheck**.