Red Hat Enterprise Linux 10

Using IdM Healthcheck to monitor your IdM environment

Performing status and health checks

Last Updated: 2026-01-30

Red Hat Enterprise Linux 10 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

Install and run the IdM Healthcheck tool to help find issues that can impact the performance of your IdM environment.

1.1. HEALTHCHECK IN IDM

The **Healthcheck** command line tool in Identity Management (IdM) helps find issues that can impact the performance of your IdM environment. Using Healthcheck, you can identify an issue in advance so that you can correct it before it becomes critical.

NOTE

You can use Healthcheck without obtaining a Kerberos ticket.

Modules are independent

Healthcheck consists of independent modules which check for:

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

Output formats and destination

You can set the following types of output for Healthcheck to generate by using the **output-type** option:

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

You can specify a file to store the output by using the **--output-file** option.

Results

Each Healthcheck module returns one of the following results:

SUCCESS
: The system is configured as expected.

WARNING
: It is advisable to monitor or evaluate the configuration.

ERROR
: The system is not configured as expected.

CRITICAL

The configuration is not as expected, with a significant potential to impact the functioning of your IdM deployment.

1.2. INSTALLING IDM HEALTHCHECK

You can install the IdM Healthcheck tool to help find issues that can impact the performance of your IdM environment.

Prerequisites

- You are logged in as **root**.

Procedure

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

```
# dnf install ipa-healthcheck
```

Verification

- Perform a basic Healthcheck test:

```
# ipa-healthcheck
```

```
[]
```

The empty square brackets **[]** indicate a fully-functioning IdM installation.

1.3. RUNNING IDM HEALTHCHECK MANUALLY

You can execute Healthcheck tests either manually on the CLI or automatically by using a timer. You can manually run IdM Healthcheck tests from the command line to diagnose and monitor the health of your environment.

Prerequisites

- The Healthcheck tool is installed. See Installing IdM Healthcheck.

Procedure

1. Optional: To display a list of all available Healthcheck tests, enter:

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

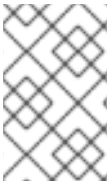
2. To run the Healthcheck utility, enter:

```
# ipa-healthcheck
```

1.4. RUNNING IDM HEALTHCHECK ON A SCHEDULE

You can configure IdM Healthcheck to run on a schedule. This includes configuring the **systemd** timer to run the Healthcheck tool periodically and generate the logs and the **crond** service to ensure log rotation.

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



NOTE

The Healthcheck timer tool is not a real-time tool. It is only meant to be run a few times an hour. If you require real-time monitoring of, for example, services or disk space, use a different tool.

Prerequisites

- You have **root** privileges.

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 you want to be saved:

```
[...]
    rotate 30
}
```

   By default, logs are stored for 30 days before they are overwritten by newer logs.

4. In the same file, configure the path to the file storing the logs.

```
/var/log/ipa/healthcheck/healthcheck.log {
[...]
```

   By default, logs are saved in the **/var/log/ipa/healthcheck/** directory.

5. Save the file.

6. Ensure that the **crond** service is enabled and running:

```
# systemctl enable crond
```

```
# systemctl start crond
```

7. To start generating logs, start the IdM healthcheck service:

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

Verification

1. Navigate to the **/var/log/ipa/healthcheck/** directory.
2. View the contents of the log file to check if it was created correctly.

1.5. LOG ROTATION

Log rotation creates a new log file every day and the files are organized by date. The date is included in the filename.

By using log rotation, you can configure the maximum number of log files to store. If this number is exceeded, the newest file replaces the oldest one. For example, if the maximum rotation number is thirty, the thirty-first log file replaces the first, that is the oldest one.

Log rotation reduces voluminous log files and organizes them. This helps you analyze the logs.

1.6. IDM HEALTHCHECK CONFIGURATION MODIFICATIONS

You can change Identity Management (IdM) 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 log rotation previously and now want to ensure the logs are in a format suitable for automatic analysis, but do not want to set up a new timer.

After you change the settings, all Healthcheck logs will use them, even when you run Healthcheck manually.

NOTE

When running Healthcheck manually, the settings in the configuration file take precedence over the 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

- Running IdM Healthcheck on a schedule

1.7. CONFIGURING HEALTHCHECK TO CHANGE THE OUTPUT LOGS FORMAT

You can configure Healthcheck with a timer already configured. In this example, you re-configure Healthcheck to start producing logs in a human-readable format and to also include successful results instead of only errors.

Prerequisites

- You have **root** privileges.
- You have previously configured Healthcheck to run on a schedule.

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

- Running IdM Healthcheck on a schedule

CHAPTER 2. CHECKING SERVICES BY USING IDM HEALTHCHECK

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

2.1. THE IDM SERVICES HEALTHCHECK TEST

The Healthcheck tool includes a test to check if the Identity Management (IdM) services are running correctly. Start with this Healthcheck test as IdM services that are not running correctly can cause failures in other Healthcheck tests.

The services test is context-specific based on what features are configured. For example, **named** is only checked if the integrated IdM DNS service is configured on the IdM server. Others, for example **smb** or **winbind**, are only checked if an IdM-AD trust is enabled.

The list of IdM services that the test evaluates can look as follows:

- certmonger
- dirsrv
- gssproxy
- httpd
- ipa_custodia
- ipa_otpd
- kadmin
- krb5kdc
- named
- ods_enforcerd
- ipa_dnskeysyncd
- pki_tomcatd
- sssd
- chronyd
- smb
- winbind

You can view this list by running the **ipa-healthcheck --list-sources** command and identifying the **ipahealthcheck.meta.services** section in the output.

2.2. SCREENING IDM SERVICES BY USING HEALTHCHECK

You can run a standalone manual test of services running on the Identity Management (IdM) server by using the Healthcheck tool.

Procedure

- To run the services test, enter:

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

  - The **--source=ipahealthcheck.meta.services** option ensures that IdM Healthcheck only performs the services test.
  - The **--failures-only** option is enabled by default and it ensures that IdM Healthcheck only reports warnings, errors and critical issues.

  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"
  }
}
```

NOTE

Run this test on all IdM servers when trying to discover issues.

Additional resources

- Healthcheck in IdM

CHAPTER 3. CHECKING DISK SPACE BY USING IDM HEALTHCHECK

You can monitor the free disk space on an Identity Management (IdM) server by using the Healthcheck tool.

3.1. DISK SPACE HEALTHCHECK TEST

The Healthcheck tool includes the **FileSystemSpaceCheck** test for checking available disk space.

The test checks the following:

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

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

Insufficient free disk space can cause issues with the following:

- Logging
- Execution
- Backups

You can find the **FileSystemSpaceCheck** test by running the **ipa-healthcheck --list-sources** command and identifying the **ipahealthcheck.system.filesystemspace** section in the output.

3.2. SCREENING DISK SPACE BY USING THE HEALTHCHECK TOOL

You can run a standalone manual test to check available disk space on an Identity Management (IdM) server by using the Healthcheck tool.

Procedure

- To run the disk space test, enter:

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

The **--source=ipahealthcheck.meta.services** option ensures that IdM Healthcheck only performs the disk space test.

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
  }
}
```

This failed test informs you that no space is available in the **/var/lib/dirsrv** directory.

NOTE

Run this test on all IdM servers when trying to discover issues.

Additional resources

- Healthcheck in IdM

CHAPTER 4. VERIFYING PERMISSIONS OF IDM CONFIGURATION FILES BY USING HEALTHCHECK

You can test the ownership and permissions of configuration files on an Identity Management (IdM) server by using the Healthcheck tool.

For general information about the tool, see Healthcheck in IdM.

4.1. FILE PERMISSIONS HEALTHCHECK TESTS

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

If you change the ownership or permissions of these files, the tests return a warning in the **result** section. While this does not necessarily mean that the configuration does not work, it means that the file differs from the default configuration.

You can find the file permissions tests under the **ipahealthcheck.ipa.files** source of the output of the **ipa-healthcheck --list-sources** command.

IPAFileNSSDBCheck

This test checks the 389-ds NSS database and the Certificate Authority (CA) database, if relevant. 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**
- **/etc/resolv.conf**
- **/etc/hosts**
  If PKINIT is enabled, it also tests:
- **/var/lib/ipa/certs/kdc.pem**
- **/var/lib/ipa/private/kdc.key**
  If DNS is configured, it also tests:
- **/etc/named.keytab**
- **/etc/ipa/dnssec/ipa-dnskeysyncd.keytab**

TomcatFileCheck

This test checks certain **tomcat**-specific files:

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

4.2. SCREENING CONFIGURATION FILES BY USING HEALTHCHECK

You can run a standalone manual test to check the ownership and permissions of configuration files on an Identity Management (IdM) server by using the Healthcheck tool.

Procedure

- 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
```

A successful test displays empty brackets:

```
[]
```

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"
  }
}
```

NOTE

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

Additional resources

- Healthcheck in IdM

CHAPTER 5. CHECKING DNS RECORDS BY USING IDM HEALTHCHECK

You can identify issues with DNS records in Identity Management (IdM) by using the Healthcheck tool. For general information about the tool, see Healthcheck in IdM.

5.1. DNS RECORDS HEALTHCHECK TEST

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

Specifically, the test checks the DNS records obtained by the **ipa dns-update-system-records --dry-run** command by using the first resolver specified in the **/etc/resolv.conf** file on the IdM server to which you are logged in.

You can find the **IPADNSSystemRecordsCheck** test under the **ipahealthcheck.ipa.idns** source of the output of the **ipa-healthcheck --list-sources** command.

5.2. SCREENING IDM DNS RECORDS BY USING THE HEALTHCHECK TOOL

You can run a standalone manual test to check DNS records on an Identity Management (IdM) server by 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 have **root** privileges.

Procedure

- To run the DNS records test, enter:

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

  - The **--source ipahealthcheck.ipa.idns** option ensures that IdM Healthcheck only performs the DNS records test.
    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

- Healthcheck in IdM

CHAPTER 6. VERIFYING THE OPTIMAL NUMBER OF KDC WORKER PROCESSES BY 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}"
    }
  }
```

CHAPTER 7. CHECKING IDM REPLICATION BY USING HEALTHCHECK

Run Healthcheck tests on your IdM replication topology to identify configuration issues early, preventing data inconsistencies and service disruptions that could affect user authentication and access to domain resources.

You can test Identity Management (IdM) replication by using the Healthcheck tool. For general information about the tool, see Healthcheck in IdM.

7.1. THE IDM REPLICATION AND TOPOLOGY HEALTHCHECK TESTS

Use built-in Healthcheck tests to verify your IdM replication topology meets connectivity and agreement requirements, preventing isolated servers and replication conflicts that could compromise data integrity.

The Identity Management (IdM) Healthcheck tool includes tests of the IdM topology configuration. The tests search for replication conflict issues.

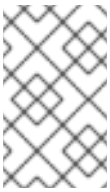
You can find the **IPATopologyDomainCheck** and **ReplicationConflictCheck** tests under the **ipahealthcheck.ipa.topology** and **ipahealthcheck.ds.replication** sources of the output of the **ipa-healthcheck --list-sources** command.

IPATopologyDomainCheck

Tests the following configuration:

- No IdM server is disconnected from the topology.
- The IdM servers do not have more than the recommended number of replication agreements.

If the test succeeds, the test returns the configured domains. Otherwise, specific connection errors are reported.



NOTE

The test runs the **ipa topologysuffix-verify** command for the **domain** suffix. It also runs the command for the **ca** suffix if the IdM Certificate Authority server role is configured on this server.

ReplicationConflictCheck

Searches for entries in LDAP matching **(&(!(objectclass=nstombstone))(nsds5ReplConflict=*))**.

7.2. SCREENING REPLICATION BY USING HEALTHCHECK

Execute focused assessments to identify replication problems before they cause production outages.

You can run a standalone manual test to check the replication and topology configuration of your Identity Management (IdM) server by using the Healthcheck tool.

Prerequisites

- You have **root** privileges.

Procedure

- To run the replication test, enter:

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

The **--source=ipahealthcheck.ds.replication** and **--source=ipahealthcheck.ipa.topology** options ensure that IdM Healthcheck only performs the replication conflict and topology tests.

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.

NOTE

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

Additional resources

- Solving common replication problems

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

You can identify issues with a trust between Identity Management (IdM) and Active Directory (AD) by using the Healthcheck tool.

8.1. IDM AND AD TRUST HEALTHCHECK TESTS

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

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

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

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

IPATrustAgentCheck

This test checks the SSSD configuration if the current host 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 IdM domain.

IPATrustCatalogCheck

This test 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, that is the administrator ID, 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 IdM 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, which is the Domain Admins' RID.

IPATrustPackageCheck

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

8.2. SCREENING THE TRUST WITH THE HEALTHCHECK TOOL

You can run a standalone manual test of an Identity Management (IdM) and Active Directory (AD) trust health check by using the Healthcheck tool.

Procedure

- To run the trust test, enter:

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

The **--source=ipahealthcheck.ipa.trust** option ensures that IdM Healthcheck only performs the trust tests.

A successful test displays empty brackets:

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

NOTE

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

Additional resources

- Healthcheck in IdM

CHAPTER 9. VERIFYING SYSTEM CERTIFICATES BY USING IDM HEALTHCHECK

You can identify issues with system certificates on an Identity Management (IdM) server by using the Healthcheck tool.

9.1. SYSTEM CERTIFICATES HEALTHCHECK TESTS

The Healthcheck tool includes several tests for verifying system, or Dogtag, certificates.

You can find all certificate-related tests under the **ipahealthcheck.dogtag.ca** source in the output of the **ipa-healthcheck --list-sources** command.

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, it also checks:

- **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 following:

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

The test verifies that the **ipa cert-show** command can be executed and that an expected response is returned from the IdM CA - either the certificate itself or a **not found** response.

9.2. SCREENING SYSTEM CERTIFICATES BY USING HEALTHCHECK

You can run a standalone manual test to check system certificates on an Identity Management (IdM) server by using the Healthcheck tool.

Procedure

Procedure

- To run the system certificates test, enter:

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

The **--source=ipahealthcheck.dogtag.ca** option ensures that Healthcheck only performs the certificate tests.

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",
    }
}
```

NOTE

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

Additional resources

- Healthcheck in IdM

CHAPTER 10. VERIFYING CERTIFICATES BY USING IDM HEALTHCHECK

You can identify issues with certificates maintained by the **certmonger** utility on an Identity Management (IdM) server by using the Healthcheck tool.

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 certificate expiration, validation, trust, and other configuration. Healthcheck can report multiple errors for the same underlying issue.

You can find these certificate tests under the **ipahealthcheck.ipa.certs** source in the output of the **ipa-healthcheck --list-sources** command.

IPACertmongerExpirationCheck

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

If a warning appears, the certificate expires soon. By default, a warning appears if the test is run 28 days or fewer before certificate expiration.

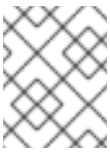
You can configure the number of days in the **/etc/ipahealthcheck/ipahealthcheck.conf** file. After opening the file, change the **cert_expiration_days** option located in the **default** section.

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 have correct access rights configured. 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 or unreadable, Healthcheck returns an error.

IPACertNSSTrust

This test analyzes the trust for certificates stored in the NSS databases. For the expected tracked certificates in the NSS databases, Healthcheck compares the trust to an expected value and raises an error on a non-match.

IPANSSChainValidation

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

IPAOpenSSLChainValidation

This test validates the certificate chain of the OpenSSL certificates. Specifically, Healthcheck executes the following OpenSSL command:

```
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 verifies that certificates that are maintained by **certmonger** have not been revoked.

IPACertmongerCA

This test verifies the **certmonger** Certificate Authority (CA) configuration. IdM cannot issue certificates without a CA.
Certmonger maintains a set of CA helpers. A CA named **IPA** issues certificates for hosts or services through IdM, authenticating as a host or user principal.

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

10.2. SCREENING CERTIFICATES BY USING THE HEALTHCHECK TOOL

You can run a standalone manual test to check certificates on an Identity Management (IdM) server by using the Healthcheck tool.

Prerequisites

- You have **root** privileges.

Procedure

- To run the certificates test, enter:

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

  - The **--source=ipahealthcheck.ipa.certs** option ensures that IdM Healthcheck only performs the **certmonger** certificate tests.
    A successful test displays empty brackets:

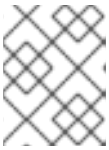
```
[]
```

    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.



NOTE

Run this suite of Healthcheck tests on all IdM servers when trying to check for issues.

Additional resources

- Healthcheck in IdM