



Red Hat Enterprise Linux 9

使用 IdM Healthcheck 监控 IdM 环境

执行状态和健康检查

执行状态和健康检查

法律通告

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

ipa-healthcheck 工具可帮助管理员检测 Red Hat Identity Management (IdM)环境中的问题。这包括对 IdM 服务、配置文件权限、复制状态和证书问题的状态检查。

目录

对红帽文档提供反馈	3
第 1 章 安装并运行 IDM HEALTHCHECK 工具	4
1.1. IDM 中的 HEALTHCHECK	4
1.2. 安装 IDM HEALTHCHECK	4
1.3. 运行 IDM HEALTHCHECK	5
1.4. 日志轮转	5
1.5. 使用 IDM HEALTHCHECK 配置日志轮转	5
1.6. 更改 IDM HEALTHCHECK 配置	6
1.7. 配置 HEALTHCHECK 以更改输出日志格式	7
1.8. 其他资源	7
第 2 章 使用 IDM HEALTHCHECK 检查服务	9
2.1. 服务 HEALTHCHECK 测试	9
2.2. 使用 HEALTHCHECK 的扫描服务	9
第 3 章 使用 IDM HEALTHCHECK 检查磁盘空间	11
3.1. 磁盘空间健康检查测试	11
3.2. 使用 HEALTHCHECK 工具扫描磁盘空间	11
第 4 章 使用 HEALTHCHECK 验证 IDM 配置文件的权限	13
4.1. 文件权限 HEALTHCHECK 测试	13
4.2. 使用 HEALTHCHECK 检查配置文件	14
第 5 章 使用 IDM HEALTHCHECK 检查 DNS 记录	15
5.1. DNS 记录健康检查	15
5.2. 使用 HEALTHCHECK 工具屏幕 DNS 记录	15
第 6 章 使用 IDM HEALTHCHECK 验证 KDC WORKER 进程的最佳数量	17
第 7 章 使用 HEALTHCHECK 检查 IDM 复制	19
7.1. 复制健康检查测试	19
7.2. 使用 HEALTHCHECK 检查复制	19
第 8 章 使用 IDM HEALTHCHECK 验证您的 IDM 和 AD 信任配置	21
8.1. IDM 和 AD 信任 HEALTHCHECK 测试	21
8.2. 使用 HEALTHCHECK 工具输出信任	21
第 9 章 使用 IDM HEALTHCHECK 验证系统证书	23
9.1. 系统证书健康检查测试	23
9.2. 使用 HEALTHCHECK 输出系统证书	24
第 10 章 使用 IDM HEALTHCHECK 验证证书	25
10.1. IDM 证书 HEALTHCHECK 测试	25
10.2. 使用 HEALTHCHECK 工具检查证书	26

对红帽文档提供反馈

我们感谢您对我们文档的反馈。让我们了解如何改进它。

通过 Jira 提交反馈（需要帐户）

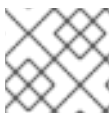
1. 登录到 [Jira](#) 网站。
2. 在顶部导航栏中点 **Create**
3. 在 **Summary** 字段中输入描述性标题。
4. 在 **Description** 字段中输入您的改进建议。包括文档相关部分的链接。
5. 点对话框底部的 **Create**。

第 1 章 安装并运行 IDM HEALTHCHECK 工具

了解有关 IdM Healthcheck 工具以及如何安装和运行它的更多信息。

1.1. IDM 中的 HEALTHCHECK

身份管理(IdM)中的 Healthcheck 工具可帮助发现可能影响 IdM 环境健康的问题。



注意

Healthcheck 工具是一个命令行工具，可在无需 Kerberos 身份验证的情况下使用。

模块是独立的

Healthcheck由独立模块组成，用于测试：

- 复制问题
- 证书有效期
- 证书颁发机构基础设施问题
- IdM 和 Active Directory 信任问题
- 正确的文件权限和所有权设置

两种输出格式

HealthCheck 生成以下输出，您可以使用 **output-type** 选项来设置：

- **JSON**：JSON 格式的机器可读输出（默认）
- **human**：人类可读的输出

您可以使用 **--output-file** 选项来指定不同的文件目标。

结果

每个 Healthcheck 模块返回以下结果之一：

SUCCESS

配置为预期

WARNING

不是错误，但需要对其进行检查和评估

ERROR

未按预期配置

CRITICAL

未按预期配置，可能会有非常大的影响

1.2. 安装 IDM HEALTHCHECK

按照以下流程安装 IdM Healthcheck 工具。

1.1.1

流程

- 安装 **ipa-healthcheck** 软件包：

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

验证步骤

- 使用 **--failures-only** 选项使 **ipa-healthcheck** 只报告错误。功能齐全的 IdM 安装返回一个空结果 []。

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

其他资源

- 使用 **ipa-healthcheck --help** 查看所有支持的参数。

1.3. 运行 IDM HEALTHCHECK

健康检查可以手工运行或使用[日志轮转](#)自动运行

先决条件

- 必须安装 Healthcheck 工具。请参阅 [安装 IdM Healthcheck](#)。

流程

- 要手动运行healthcheck，请输入 **ipa-healthcheck** 命令。

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

其他资源

有关所有选项，请查看手册页：[man ipa-healthcheck](#)。

1.4. 日志轮转

日志轮转每天创建一个新的日志文件，并按照日期对文件进行组织。由于所有日志文件都保存在同一目录中，您可以根据日期选择特定的日志文件。

轮转意味着，保持的日志文件数量有一个最大的限制，如果超过了这个限制，最新的文件会重写并重命名最旧的文件。例如，如果轮转数量为 30，则第三十一个日志文件会替代第一个（最旧的）日志文件。

日志轮转可以减少日志文件的数量并对它们进行组织，这有助于分析日志。

1.5. 使用 IDM HEALTHCHECK 配置日志轮转

按照以下流程配置日志轮转：

- **systemd** 计时器
- **crond** 服务

systemd 计时器定期运行 Healthcheck 工具并生成日志。默认值设为每天的上午 4 点。

crond 服务用于日志轮转。

默认的日志名是 **healthcheck.log**，轮转的日志使用 **healthcheck.log-YYYYMMDD** 格式。

先决条件

- 您必须以 root 用户身份执行命令。

流程

1. 启用 **systemd** 计时器：

```
# 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. 启动 **systemd** 计时器：

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

3. 打开 **/etc/logrotate.d/ipahealthcheck** 文件，以配置应保存的日志数量。
默认情况下，日志轮转设定为 30 天。

4. 在 **/etc/logrotate.d/ipahealthcheck** 文件中，配置日志的路径。
默认情况下，日志保存在 **/var/log/ipa/healthcheck/** 目录中。

5. 在 **/etc/logrotate.d/ipahealthcheck** 文件中，配置日志生成时间。
默认情况下，日志在每天的上午 4 点创建。

6. 要使用日志轮转，请确保启用了 **crond** 服务并正在运行：

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

要开始生成日志，启动 IPA healthcheck 服务：

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

要验证结果，进入 **/var/log/ipa/healthcheck/** 并检查日志是否已正确创建。

1.6. 更改 IDM HEALTHCHECK 配置

您可以通过在 **/etc/ipahealthcheck/ipahealthcheck.conf** 文件中添加所需的命令行选项来更改 Healthcheck 设置。这很有用，例如，您配置了日志轮转，并希望确保日志采用适合自动分析的格式，但不想设置新的计时器。



注意

此 Healthcheck 功能仅适用于 RHEL 9.1 或更新版本。

在修改后，Healthcheck 创建的所有日志遵循新的设置。这些设置也应用到健康检查的任何手动执行。



注意

手动运行 Healthcheck 时，配置文件中的设置优先于命令行中指定的选项。例如，如果在配置文件中将 **output_type** 设置为 **human**，则在命令行中指定 **json** 不起作用。您用来在配置文件中指定的任何命令行选项都会正常应用。

其他资源

- [使用 IdM Healthcheck 配置日志轮转](#)

1.7. 配置 HEALTHCHECK 以更改输出日志格式

按照以下流程，配置带有已设置了计时器的 Healthcheck。在本例中，您将配置 Healthcheck 以人类可读格式生成日志，并且包含成功结果而不是仅错误。

先决条件

- 您的系统正在运行 RHEL 9.1 或更高版本。
- 您有 **root** 特权。
- 您之前已在计时器中配置了日志轮转。

流程

1. 在文本编辑器中打开 `/etc/ipahealthcheck/ipahealthcheck.conf` 文件。
2. 将选项 **output_type=human** 和 **all=True** 添加到 **[default]** 部分。
3. 保存并关闭该文件。

验证

1. 手动运行 Healthcheck:

```
# ipa-healthcheck
```

2. 进入 `/var/log/ipa/healthcheck/`，检查日志是否采用正确的格式。

其他资源

- [使用 IdM Healthcheck 配置日志轮转](#)

1.8. 其他资源

- 有关使用 IdM Healthcheck 的示例，请参阅[使用 IdM Healthcheck 来监控您的 IdM 环境](#) 指南。
 - [检查服务](#)
 - [验证您的 IdM 和 AD 信任配置](#)
 - [验证证书](#)
 - [验证系统证书](#)

- 检查磁盘空间
- 验证 IdM 配置文件的权限
- 检查复制

第 2 章 使用 IDM HEALTHCHECK 检查服务

您可以使用 Healthcheck 工具监控身份管理(IdM)服务器使用的服务。

详情请查看

[IdM 中的健康检查。](#)

2.1. 服务 HEALTHCHECK 测试

Healthcheck 工具包含一个测试，用于检查任何 IdM 服务是否没有运行。这个测试很重要，因为没有运行的服务可能会导致其他测试中出现失败。因此，检查所有服务是否已首先运行。然后您可以检查所有其他测试结果。

要查看所有服务测试，请使用 `--list-sources` 选项运行 `ipa-healthcheck`:

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

您可以在 `ipahealthcheck.meta.services` 源下查找通过 `Healthcheck.meta.services` 源测试的所有服务：

- certmonger
- dirsrv
- gssproxy
- httpd
- ipa_custodia
- ipa_dnssyncd
- ipa_otpd
- kadmind
- krb5kdc
- named
- pki_tomcatd
- sssd



注意

当尝试检查问题时，在所有 IdM 服务器中运行这些测试。

2.2. 使用 HEALTHCHECK 的扫描服务

按照以下流程，使用 Healthcheck 工具对在身份管理(IdM)服务器上运行的服务运行独立的手动测试。

Healthcheck 工具包括许多测试，其结果可以被缩短：

- 排除所有成功的测试: `--failures-only`

- 仅包含服务测试 : **-- source=ipahealthcheck.meta.services**

流程

- 要运行有关服务的警告、错误和严重级别的问题，请输入：

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

成功测试显示空的括号：

```
[]
```

如果其中一个服务失败，则结果可能会和本例类似：

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

其他资源

- 请参阅 **man ipa-healthcheck**。

第 3 章 使用 IDM HEALTHCHECK 检查磁盘空间

您可以使用 Healthcheck 工具监控身份管理服务器的可用磁盘空间。

详情请参阅 [IdM 中的状况检查](#)。

3.1. 磁盘空间健康检查测试

Healthcheck 工具包括检查可用的磁盘空间的测试。可用磁盘空间不足可能会导致问题：

- 日志
- 执行
- 备份

测试检查以下路径：

表 3.1. 测试的路径

测试检查的路径	最小磁盘空间（以 MB 为单位）
<code>/var/lib/dirsrv/</code>	1024
<code>/var/lib/ipa/backup/</code>	512
<code>/var/log/</code>	1024
<code>var/log/audit/</code>	512
<code>/var/tmp/</code>	512
<code>/tmp/</code>	512

要列出所有测试，请使用 `--list-sources` 选项运行 `ipa-healthcheck`：

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

您可以在 `ipahealthcheck.system.filesystems-space` 源中找到文件系统空间检查测试：

FileSystemSpaceCheck

此测试使用以下方法检查可用的磁盘空间：

- 需要最少的原始可用字节。
- 最小磁盘空间的百分比为 20%。

3.2. 使用 HEALTHCHECK 工具扫描磁盘空间

按照以下流程，使用 Healthcheck 工具在身份管理(IdM)服务器上运行可用磁盘空间的独立的手动测试。

由于 Healthcheck 包括许多测试，因此您可以通过以下方法缩小结果：

- 排除所有成功的测试: **--failures-only**
- 仅包含空间检查测试：**-- source=ipahealthcheck.system.filesystemspace**

流程

- 要运行有关可用空间的警告、错误和严重级别的问题，请输入：

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

成功测试显示空的括号：

```
[]
```

例如，无法显示失败的测试：

```
{
  "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
  }
}
```

失败测试告知您 **/var/lib/dirsrv** 目录已空间不足。

其他资源

- 请参阅 **man ipa-healthcheck**。

第 4 章 使用 HEALTHCHECK 验证 IDM 配置文件的权限

了解如何使用 Healthcheck 工具测试身份管理(IdM)配置文件。

详情请查看

[IdM 中的健康检查。](#)

4.1. 文件权限 HEALTHCHECK 测试

Healthcheck 工具测试由 Identity Management(IdM)安装和配置的一些重要文件的所有权和权限。

如果您更改了任何测试的文件的所有权或权限，则测试会在 **result** 部分中返回一个警告。这不意味着配置无法正常工作，它意味着该文件与默认配置不同。

要查看所有测试，请使用 **--list-sources** 选项运行 **ipa-healthcheck**:

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

您可以在 **ipahealthcheck.ipa.files** 源中找到文件权限测试：

IPAFileNSSDBCheck

此测试会检查 389-ds NSS 数据库和证书颁发机构(CA)数据库。389-ds 数据库位于 **/etc/dirsrv/slapd-~~<dashed-REALM>~~**，CA 数据库位于 **/etc/pki/pki-tomcat/alias/** 中。

IPAFileCheck

此测试会检查以下文件：

- **/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**
如果启用了 PKINIT：
- **/var/lib/ipa/certs/kdc.pem**
- **/var/lib/ipa/private/kdc.key**
如果配置了 DNS:
- **/etc/named.keytab**
- **/etc/ipa/dnssec/ipa-dnskeysyncd.keytab**

TomcatFileCheck

如果配置了 CA，这个测试会检查一些特定于 tomcat 的文件：

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



注意

当尝试查找问题时，在所有 IdM 服务器中运行这些测试。

4.2. 使用 HEALTHCHECK 检查配置文件

按照以下流程，使用 Healthcheck 工具对身份管理(IdM)服务器配置文件运行独立的手动测试。

Healthcheck 工具包括多个测试。可以通过以下方法缩小结果：

- 排除所有成功的测试: `--failures-only`
- 仅包含所有权和权限测试：`-- source=ipahealthcheck.ipa.files`

流程

1. 要在 IdM 配置文件所有权和权限上运行 Healthcheck 测试，同时只显示警告、错误和严重问题，请输入：

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

成功测试显示空的括号：

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

失败测试显示类似如下的 **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"
  }
}
```

其他资源

- 请参阅 `man ipa-healthcheck`。

第 5 章 使用 IDM HEALTHCHECK 检查 DNS 记录

您可以使用 Healthcheck 工具识别身份管理(IdM)中 DNS 记录的问题。

5.1. DNS 记录健康检查

Healthcheck 工具包含一个测试，用于检查自动发现所需的 DNS 记录是否可以解析。

要列出所有测试，请使用 `--list-sources` 选项运行 `ipa-healthcheck`:

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

您可以在 `ipahealthcheck.ipa.idns` 源中找到 DNS 记录检查测试。

IPADNSSystemRecordsCheck

此测试使用 `/etc/resolv.conf` 文件中指定的第一个解析器检查 `ipa dns-update-system-records --dry-run` 命令的 DNS 记录。记录在 IPA 服务器上测试。

5.2. 使用 HEALTHCHECK 工具屏幕 DNS 记录

按照以下流程，使用 Healthcheck 工具在身份管理(IdM)服务器中运行 DNS 记录的独立的手动测试。

Healthcheck 工具包括多个测试。通过添加 `--source ipahealthcheck.ipa.idns` 选项，可以仅包含 DNS 记录测试来缩小结果。

先决条件

- 您必须以 `root` 用户身份执行 Healthcheck 测试。

流程

- 要运行 DNS 记录检查，请输入：

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

如果可解析记录，则测试会返回 **SUCCESS**：

```
{
  "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."
  }
}
```

当测试会返回 **WARNING** 时，测试会返回 WARNING，例如，记录数与预期数目不匹配：

```
{
  "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
}
```

其他资源

- 请参阅 `man ipa-healthcheck`。

第 6 章 使用 IDM HEALTHCHECK 验证 KDC WORKER 进程的最佳数量

您可以使用身份管理(IdM)中的 Healthcheck 工具来验证 Kerberos 密钥分发中心(KDC)是否已配置为使用 **krb5kdc** worker 进程的最佳数量，它应该等于主机上的 CPU 核数。

您可以在 **ipahealthcheck.ipa.kdc** 源中找到正确的 KDC worker 进程数量的测试。由于 Healthcheck 工具包括许多测试，因此您可以通过添加 **--source ipahealthcheck.ipa.kdc** 选项，通过只包括 KDC worker 测试来缩小结果范围。

先决条件

- KDC worker 进程 Healthcheck 工具仅适用于 RHEL 8.7 或更新版本。
- 您必须以 **root** 用户身份执行 Healthcheck 测试。

流程

- 要运行对 KDC worker 进程的检查，请输入：

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

如果 KDC worker 进程的数量与 CPU 核数匹配，则测试会返回 **SUCCESS**：

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

如果 worker 进程数量与 CPU 核数不匹配，则测试会返回 **WARNING**。在以下示例中，带有 2 个核的主机被配置为只有一个 KDC worker 进程：

```
{
  "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}"
  }
}
```

如果没有配置的 worker，则测试也会输出 **WARNING**。在以下示例中，`/etc/sysconfig/krb5kdc` 配置文件中缺少 **KRB5KDC_ARGS** 变量：

```
{
  "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}"
  }
}
```

其他资源

- `man ipa-healthcheck`

第 7 章 使用 HEALTHCHECK 检查 IDM 复制

您可以使用 Healthcheck 工具测试身份管理(IdM)复制。

详情请参阅 [IdM 中的 Healthcheck](#)。

7.1. 复制健康检查测试

Healthcheck 工具测试身份管理(IdM)拓扑配置，并搜索复制冲突问题。

要列出所有测试，请使用 `--list-sources` 选项运行 `ipa-healthcheck`：

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

拓扑测试放置在 `ipahealthcheck.ipa.topology` 和 `ipahealthcheck.ds.replication` 源下：

IPATopologyDomainCheck

此测试验证：

- 无论拓扑是否没有断开连接，所有服务器之间都有复制路径。
- 如果服务器没有超过推荐的复制协议数。
如果测试失败，测试返回错误，如连接错误或复制协议太多。

如果测试成功，则测试会返回配置的域。



注意

测试为域和 ca 后缀（假设在这个服务器上配置了证书颁发机构）运行 `ipa topologysuffix-verify` 命令。

ReplicationConflictCheck

测试搜索 LDAP 中与 `(&!(objectclass=nstombstone))(nsds5ReplConflict=*)` 匹配的项。



注意

当尝试检查问题时，在所有 IdM 服务器中运行这些测试。

有关解决 LDAP 复制冲突的更多信息，请参阅 [解决常见复制问题](#)。

7.2. 使用 HEALTHCHECK 检查复制

按照以下流程，使用 Healthcheck 工具对身份管理(IdM)复制拓扑和配置运行独立的手动测试。

Healthcheck 工具包括许多测试，您可以对结果进行简化：

- 复制冲突测试：`--source=ipahealthcheck.ds.replication`
- 正确拓扑测试：`--source=ipahealthcheck.ipa.topology`

先决条件

- 您必须以 **root** 用户身份执行 Healthcheck 测试。

流程

- 要运行 Healthcheck 复制冲突和拓扑检查，请输入：

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

可能有四个不同的结果：

- SUCCESS – 测试成功通过。

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

- WARNING – 测试通过但可能会有问题。
- ERROR – 测试失败。

```
{  
  "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 – 测试失败，它会影响 IdM 服务器的功能。

其他资源

- 请参阅 **man ipa-healthcheck**。

第 8 章 使用 IDM HEALTHCHECK 验证您的 IDM 和 AD 信任配置

了解如何使用 Healthcheck 工具识别 IdM 和身份管理(IdM)中活动目录信任的问题。

8.1. IDM 和 AD 信任 HEALTHCHECK 测试

Healthcheck 工具包括几个测试用来测试您的身份管理(IdM)和 Active Directory(AD)信任的状态的测试。

要查看所有信任测试，请使用 `--list-sources` 选项运行 `ipa-healthcheck`:

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

您可以在 `ipahealthcheck.ipa.trust` 源中找到所有测试：

IPATrustAgentCheck

当机器配置为信任代理时，这个测试会检查 SSSD 配置。对于 `/etc/sss/sss.conf` 中的每个域，其中 `id_provider=ipa` 可确保 `ipa_server_mode` 为 `True`。

IPATrustDomainsCheck

此测试通过对比 `ssctl domain-list` 中的域列表和 `ipa trust-find` 的域列表（不包括 IPA 域），来检查信任域是否匹配 SSSD 域。

IPATrustCatalogCheck

此测试解析一个 AD 用户 `Administrator@REALM`。这会在 `ssctl domain-status` 输出中生成 AD Global catalog 和 AD Domain Controller 值。

对于每个信任域，查找 SID + 500（管理员）的 id 用户，然后检查 `ssctl domain-status <domain> --active-server` 的输出，以确保域处于活动状态。

IPAsidgenpluginCheck

此测试会验证 `sidgen` 插件是否在 IPA 389-ds 实例中启用。该测试还验证 `cn=plugins,cn=config` 中的 `IPA SIDGEN` 和 `ipa-sidgen-task` 插件是否包含 `nsslapd-pluginEnabled` 选项。

IPATrustAgentMemberCheck

此测试会验证当前主机是 `cn=adtrust agents,cn=sysaccounts,cn=etc,SUFFIX` 的成员。

IPATrustControllerPrincipalCheck

此测试会验证当前主机是 `cn=adtrust agents,cn=sysaccounts,cn=etc,SUFFIX` 的成员。

IPATrustControllerServiceCheck

此测试会验证当前主机是否在 `ipactl` 中启动了 ADTRUST 服务。

IPATrustControllerConfCheck

此测试会验证在 `net conf` 列表中是否为 `passdb` 后端启用 `ldapi`。

IPATrustControllerGroupSIDCheck

此测试会验证 `admins` 组的 SID 是否以 512 结尾(Domain Admins RID)。

IPATrustPackageCheck

此测试会验证是否没有启用信任控制器和 AD 信任，是否安装了 `trust-ad` 软件包。



注意

当尝试查找问题时，在所有 IdM 服务器中运行这些测试。

8.2. 使用 HEALTHCHECK 工具输出信任

按照以下流程，使用 Healthcheck 工具对身份管理(IdM)和活动目录(AD)信任健康检查运行独立的手动测试。

Healthcheck 工具包括多个测试，因此您可以缩短结果：

- 排除所有成功的测试: **--failures-only**
- 仅包含信任测试：**-- source=ipahealthcheck.ipa.trust**

流程

- 要运行有关信任的警告、错误和严重级别的问题，请输入：

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

成功测试显示空的括号：

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

其他资源

- 请参阅 **man ipa-healthcheck**。

第 9 章 使用 IDM HEALTHCHECK 验证系统证书

了解如何使用 Healthcheck 工具识别身份管理(IdM)中系统证书的问题。

详情请查看

[IdM 中的健康检查。](#)

9.1. 系统证书健康检查测试

Healthcheck 工具包括多个用于验证系统(DogTag)证书的测试。

要查看所有测试，请使用 `--list-sources` 选项运行 `ipa-healthcheck`:

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

您可以在 `ipahealthcheck.dogtag.ca` 源中找到所有测试：

DogtagCertsConfigCheck

此测试会将其 NSS 数据库中的 CA(Certificate Authority)证书与 `CS.cfg` 中存储的相同值进行比较。如果不匹配，CA 无法启动。

特别是，它会检查：

- `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` 与 `ca.sslserver.cert`

如果安装了密钥恢复授权(KRA)：

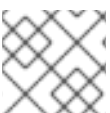
- `transportCert cert-pki-kra` against `ca.connector.KRA.transportCert`

DogtagCertsConnectivityCheck

此测试会验证连接。此测试等同于 `ipa cert-show 1` 命令，它检查：

- Apache 中的 PKI 代理配置
- IdM 可以找到 CA
- RA 代理客户端证书
- CA 回复请求的更正

请注意，测试会检查带有串行 #1 的证书，因为您想要验证证书是否可以被执行，并从 CA 返回预期的结果（证书或未找到证书）。



注意

当尝试查找问题时，在所有 IdM 服务器中运行这些测试。

9.2. 使用 HEALTHCHECK 输出系统证书

按照以下流程，使用 Healthcheck 工具运行身份管理(IdM)证书的独立的手动测试。

由于 Healthcheck 工具包括许多测试，您可以通过只包括 DogTag 测试：`--source=ipahealthcheck.dogtag.ca` 来缩小结果范围

流程

- 要运行 Healthcheck 限制为 DogTag 证书，请输入：

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

成功测试示例：

```
{
  "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"
  }
}
```

一个失败的测试示例：

```
{
  "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",
  }
}
```

其他资源

- 请参阅 `man ipa-healthcheck`。

第 10 章 使用 IDM HEALTHCHECK 验证证书

了解更多有关理解和使用身份管理(IdM)中的 Healthcheck 工具，以识别由 **certmonger** 维护的 IPA 证书的问题。

详情请参阅 [IdM 中的 Healthcheck](#)。

10.1. IDM 证书 HEALTHCHECK 测试

Healthcheck 工具包括几个测试，用于验证 Identity Management(IdM)中由 certmonger 维护的证书状态。有关 certmonger 的详情，请参阅[使用 certmonger 为服务获取 IdM 证书](#)。

这个测试套件会检查过期、验证、信任和其他问题。可能会为相同的底层问题抛出多个错误。

要查看所有证书测试，请使用 **--list-sources** 选项运行 **ipa-healthcheck**:

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

您可以在 **ipahealthcheck.ipa.certs** 源中找到所有测试：

IPACertmongerExpirationCheck

此测试会检查 **certmonger** 中的过期时间。
如果报告错误，代表证书已过期。

如果显示警告，代表证书将很快过期。默认情况下，这个测试会在证书过期前的 28 天或更短的天数内应用。

您可以在 **/etc/ipahealthcheck/ipahealthcheck.conf** 文件中配置天数。打开文件后，更改 default 部分中的 **cert_expiration_days** 选项。

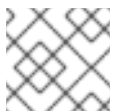


注意

certmonger 加载并维护其证书过期视图。此检查不会验证磁盘上的证书。

IPACertfileExpirationCheck

此测试会检查是否无法打开证书文件或 NSS 数据库。此测试还会检查过期时间。因此，仔细阅读错误或警告输出中的 **msg** 属性。消息指定了问题。



注意

此测试会检查磁盘上的证书。如果缺少证书且不可读取，也会引发单独的错误。

IPACertNSSTrust

此测试会比较 NSS 数据库中存储的证书的信任。对于 NSS 数据库中的预期跟踪证书，信任与预期值进行比较，导致在非匹配时引发错误。

IPANSSChainValidation

此测试会验证 NSS 证书的证书链。测试执行：**certutil -V -u V -e -d [dbdir] -n [nickname]**

IPAOpenSSLChainValidation

此测试会验证 OpenSSL 证书的证书链。为了可以与这里的 **NSSChain** 验证比较，执行 OpenSSL 命令：

-

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

IPARAAgent

此测试将磁盘上的证书与 `uid=ipara,ou=People,o=ipaca` 中的 LDAP 中的等效记录进行比较。

IPACertRevocation

此测试使用 `certmonger` 验证证书没有被撤销。因此，测试只能查找与由 `certmonger` 维护的证书连接的问题。

IPACertmongerCA

此测试会验证 `certmonger` 证书颁发机构(CA)配置。IdM 无法在没有 CA 的情况下发布证书。`certmonger` 维护一组 CA 帮助程序。在 IdM 中，有一个名为 IPA 的 CA，它会在主机或服务证书中以主机或用户主体身份通过 IdM 发出证书。

另外，还有 `dogtag-ipa-ca-renew-agent` 和 `dogtag-ipa-ca-renew-agent-reuse`，它们续订 CA 子系统证书。



注意

当尝试检查问题时，在所有 IdM 服务器中运行这些测试。

10.2. 使用 HEALTHCHECK 工具检查证书

按照以下流程，使用 Healthcheck 工具运行身份管理(IdM)证书健康检查的独立的手动测试。

Healthcheck 工具包括许多测试，您可以对结果进行简化：

- 排除所有成功的测试: `--failures-only`
- 仅包含证书测试: `--source=ipahealthcheck.ipa.certs`

先决条件

- 您必须以 `root` 用户身份执行 Healthcheck 测试。

流程

- 要运行带有警告的 Healthcheck，有关证书的错误和严重问题，请输入：

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

成功测试显示空的括号：

```
[]
```

失败测试显示以下输出：

```
{
  "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]"  
}  
}
```

这个 `IPACertfileExpirationCheck` 测试在打开 NSS 数据库时失败。

其他资源

- 请参阅 `man ipa-healthcheck`。