Red Hat Enterprise Linux 8

使用 IdM Healthcheck 监控 IdM 环境

使用 IdM Healthcheck 实用程序监控身份管理服务器的状态

Last Updated: 2021-12-10

Red Hat Enterprise Linux 8 使用 IdM Healthcheck 监控 IdM 环境

使用 IdM Healthcheck 实用程序监控身份管理服务器的状态

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律通告

摘要

本文档集合提供了如何在 Red Hat Enterprise Linux 8 中有效地配置、管理和维护身份管理的说明。

目录

使开源包含更多

红帽承诺替换我们的代码、文档和网页属性中存在问题的语言。我们从这四个术语开始： master、slave、blacklist 和 whitelist。这些更改将在即将发行的几个发行本中逐渐实施。如需了解更多详细信息，请参阅 CTO Chris Wright 信息。

在身份管理中，计划中的术语变化包括：

- 使用 ***block list*** 替换 *blacklist*
- 使用 ***allow list*** 替换 *whitelist*
- 使用 ***secondary*** 替换 *slave*
- *根据上下文，master* 词语将被替换为更精确的语言：
  - 使用 ***IdM server*** 替换 *IdM master*
  - 使用 ***CA renewal server*** 替换 *CA renewal master*
  - 使用 ***CRL publisher server*** 替换 *CRL master*
  - 使用 ***multi-supplier*** 替换 *multi-master*

对红帽文档提供反馈

我们感谢您对文档提供反馈信息。请让我们了解如何改进文档。要做到这一点：

- 关于特定内容的简单评论：
  1. 请确定您使用 *Multi-page HTML* 格式查看文档。另外，确定 **Feedback** 按钮出现在文档页的右上方。
  2. 用鼠标指针高亮显示您想评论的文本部分。
  3. 点在高亮文本上弹出的 **Add Feedback**。
  4. 按照显示的步骤操作。
- 要提交更复杂的反馈，请创建一个 Bugzilla ticket：
  1. 进入 Bugzilla 网站。
  2. 在 Component 中选择 **Documentation**。
  3. 在 **Description** 中输入您要提供的信息。包括文档相关部分的链接。
  4. 点 **Submit Bug**。

第 1 章 安装并运行 IDM HEALTHCHECK 工具

本章描述了 IdM Healthcheck 工具以及如何安装和运行它。

先决条件

- Healthcheck 工具只在 RHEL 8.1 或更高版本中提供。

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。

1.1.1. 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

1.1.2. 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。

1.1.3. 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

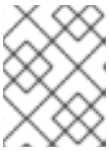
1.2. 安装 IDM HEALTHCHECK

这部分论述了如何安装 IdM Healthcheck 工具。

流程

- 安装 **ipa-healthcheck** 软件包：

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



注意

在 RHEL 8.1 和 8.2 系统中，使用 **dnf install /usr/bin/ipa-healthcheck** 命令替代。

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
[]
```

其它资源

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

1.3. 运行 IDM HEALTHCHECK

Healthcheck 可以手动运行，也可以使用 日志循环 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
```

其它资源

有关所有选项，请查看手册页: **man ipa-healthcheck**。

1.4. 其它资源

- 有关使用 IdM 健康检查的示例，请参阅 配置和管理身份管理 指南中的以下部分。
  - 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

- 您还可以看到整理到一个指南中的章节： 使用 IdM Healthcheck 监控 IdM 环境

第 2 章 收集 IDM 健康检查信息

健康检查已设计为手动命令行工具，可帮助您识别身份管理(IdM)中可能存在的问题。

本章论述了如何根据带有 30 天轮转的 Healthcheck 输出创建日志集合。

先决条件

- Healthcheck 工具仅适用于 RHEL 8.1 或更新版本

2.1. 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。

2.1.1. 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

2.1.2. 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。

2.1.3. 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

2.2. 日志轮转

日志轮转每日创建新的日志文件，并且按日期组织这些文件。由于日志文件保存在同一目录中，因此您可以根据日期选择特定的日志文件。

轮转意味着为最多日志文件数配置一个数字，如果超过这个数字，则最新文件重写并重命名最旧的文件。例如，如果轮转编号为 30，则第三十个日志文件将取代第一个（最旧的）日志文件。

日志轮转会减少大量日志文件并组织它们，这有助于分析日志。

2.3. 使用 IDM HEALTHCHECK 配置日志轮转

本节论述了如何使用以下方法配置日志轮转：

- **systemd** 计时器
- **crond** 服务

systemd 定时器定期运行 Healthcheck 工具并生成日志。默认值为每天设为 4 点。

crond 服务用于日志轮转。

默认日志名称为 **healthcheck.log**，轮转的日志使用 **healthcheck.log-YYYMMDD** 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。
默认情况下，日志轮转设置为 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，日志每天凌晨 4 点创建。

6. 要使用日志轮转，请确保 **crond** 服务已启用并在运行：

```
# 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，请转至 **/var/log/ipa/healthcheck/**，并检查日志是否已正确创建。

第 3 章 使用 IDM HEALTHCHECK 检查服务

本节论述了使用 Healthcheck 工具的 Identity Management(IdM)服务器使用的监控服务。

详情请查看 IdM 中的 Healthcheck。

先决条件

- Healthcheck 工具只在 RHEL 8.1 及更新版本中可用

3.1. SERVICES HEALTHCHECK 测试

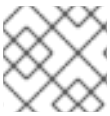
Healthcheck 工具包括一个测试，用于检查是否任何 IdM 服务没有在运行。此测试很重要，因为未运行的服务会在其他测试中造成失败。因此，请先检查所有服务是否都在运行。然后您可以检查所有其他测试结果。

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 源下找到使用 Healthcheck** 测试的所有服务：

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



注意

当尝试发现问题时，在所有 IdM 服务器中运行这些测试。

3.2. 使用 HEALTHCHECK 的服务

本节介绍了使用 Healthcheck 工具在 Identity Management(IdM)服务器中运行的服务的独立手动测试。

Healthcheck 工具包括许多测试，其结果可通过以下方法缩短：

- 排除所有成功测试： **--failures-only**
- 仅包含服务测试：-- **source=ipahealthcheck.meta.services**

流程

- 要使用服务相关的警告、错误和严重问题运行健康检查，请输入：

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

成功测试会显示空括号：

```
[]
```

如果其中一个服务失败，则结果可能类似以下示例：

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

其它资源

- 要查看详细参考，请在命令行中输入 **man ipa-healthcheck**。

第 4 章 使用 IDM 健康检查验证您的 IDM 和 AD 信任配置

本节帮助您了解并使用身份管理(IdM)中的 Healthcheck 工具来识别 IdM 和 Active Directory 信任的问题。

详情请查看 第 2.1 节 “IdM 中的 Healthcheck”。

先决条件

- Healthcheck 工具仅适用于 RHEL 8.1 或更新版本

4.1. IDM 和 AD 信任健康检查测试

Healthcheck 工具包括多个测试，用于测试您的身份管理(IdM)和 Active Directory(AD)信任状态。

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** 源下找到所有测试：

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/sssd/sssd.conf** 中的每个域，其中 **id_provider=ipa** 确保 **ipa_server_mode** 为 **True**。

IPATrustDomainsCheck

此测试通过将 **sssctl domain-list 中的域列表与 ipa trust- find** 中的域列表进行比较，检查信任域是否与 SSSD 域匹配。

IPATrustCatalogCheck

此测试解析为 AD 用户 **Administrator@REALM**。这将填充 **sssctl domain-status** 输出中的 AD Global 目录和 AD 域控制器值。
对于每个信任域，查找 SID + 500（管理员） ID 的用户，然后检查 **sssctl domain-status <domain> --active-server** 的输出以确保域处于活跃状态。

IPAsidgenpluginCheck

此测试会验证 IPA 389-ds 实例中是否启用了 **sidgen** 插件。该测试还验证 **cn=plugins,cn=config 中的 IPA SIDGEN 和 ipa-sidgen-task** 插件是否包含 then **sslapd-pluginEnabled** 选项。

IPATrustAgentMemberCheck

此测试将验证当前主机是否为 **cn=adtrust 代理,cn=sysaccounts,cn=etc,SUFFIX** 的成员。

IPATrustControllerPrincipalCheck

此测试将验证当前主机是否为 **cn=adtrust 代理,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 ADTRUST 服务。

IPATrustControllerConfCheck

此测试验证 **net conf** 列表输出中是否为 passdb 后端启用了 **ldapi**。

IPATrustControllerGroupSIDCheck

此测试将验证 admin 组的 SID 是否以 512(Domain Admins RID)结束。

IPATrustPackageCheck

如果没有启用信任控制器和 AD 信任，这个测试会验证是否安装了 **trust-ad** 软件包。

注意

当尝试找到问题时，在所有 IdM 服务器中运行这些测试。

4.2. 使用 HEALTHCHECK 工具建立信任

本节论述了使用 Healthcheck 工具对 Identity Management(IdM)和 Active Directory(AD)信任健康检查的独立手动测试。

因此，Healthcheck 工具包含许多测试，您可以通过以下方式缩短结果：

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

流程

- 要运行带有信任中的警告、错误和严重问题的健康检查，请输入：

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

成功测试会显示空括号：

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

其它资源

- 要查看详细参考，请在命令行中输入 **man ipa-healthcheck**。

第 5 章 使用 IDM HEALTHCHECK 验证证书

本节帮助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。

详情请查看 IdM 中的 Healthcheck。

先决条件

- Healthcheck 工具只在 RHEL 8.1 及更新版本中可用。

5.1. IDM 证书健康检查测试

Healthcheck 工具包括多个测试，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。

此测试套件检查过期、验证、信任和其他问题。对于相同的根本问题，可能会抛出多个错误。

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** 源下找到所有测试：

IPACertmongerExpirationCheck

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

如果出现警告，证书很快就会过期。默认情况下，此测试在证书过期前 28 天或少于 28 天内适用。

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

注意

Certmonger 加载和维护自己的证书过期视图。此检查不会验证磁盘中的证书。

IPACertfileExpirationCheck

此测试检查证书文件或 NSS 数据库是否无法打开。此测试还会检查过期情况。因此，请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

此测试会检查磁盘中的证书。如果证书丢失、不可读取等单独错误，也可以引发单独的错误。

IPACertNSSTrust

此测试比较存储在 NSS 数据库中的证书的信任。对于 NSS 数据库中的预期跟踪证书，会将信任与预期值进行比较，并在不匹配时引发错误。

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。与 **NSSChain** 验证相当的 OpenSSL 命令是我们执行的 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 LDAP in **uid=ipara,ou=People,o=ipaca** 中的等效记录进行比较。

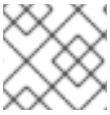
IPACertRevocation

此测试使用 certmonger 验证证书是否已被撤销。因此，测试只能查找与 certmonger 维护的证书连接的问题。

IPACertmongerCA

此测试将验证证书授权机构(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，它通过 IdM 发布证书，它作为主机或用户主体进行身份验证，用于主机或服务证书。

还有一个 **dogtag-ipa-ca-renew-agent** 和 **dogtag-ipa-ca-renew-agent-reuse** （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。

5.2. 使用 HEALTHCHECK 工具验证证书

本节论述了使用 Healthcheck 工具对 Identity Management(IdM)证书健康检查的独立手动测试。

因此，Healthcheck 工具包括了许多测试，您可以使用以下方法缩短结果：

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

先决条件

- 健康检查测试必须以 root 用户身份执行。

流程

- 要使用证书的警告、错误和严重问题运行健康检查，请输入：

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

成功测试会显示空括号：

```
[]
```

失败的测试会显示以下输出：

```
{
```

```
  "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]"
  }
}
```

在打开 NSS 数据库时，这个 **IPACertfileExpirationCheck** 测试失败。

其它资源

- 要查看详细参考，请在命令行中输入 **man ipa-healthcheck**。

第 6 章 使用 IDM HEALTHCHECK 验证系统证书

本节论述了 Identity Management(IdM)中的 Healthcheck 工具来识别系统证书的问题。

详情请查看 IdM 中的 Healthcheck。

先决条件

- Healthcheck 工具仅在 RHEL 8.1 或更新版本中可用。

6.1. 系统证书健康检查测试

Healthcheck 工具包括一些用于验证系统(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** 源下找到所有测试：

DogtagCertsConfigCheck

此测试将其 NSS 数据库中的 CA（证书授权机构）证书与存储在 **CS.cfg** 中的相同值进行比较。如果不匹配，CA 无法启动。
具体来说，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**
- 针对 **ca .sslserver.cert 的 server-Cert cert-pki-ca**

如果安装了 Key Recovery Authority(KRA)：

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

DogtagCertsConnectivityCheck

此测试验证连接性。这个测试等同于检查的 **ipa cert-show 1** 命令：

- Apache 中的 PKI 代理配置
- IdM 能够找到 CA
- RA 代理客户端证书
- CA 回复请求的正确性

请注意，测试会使用 serial #1 检查证书，因为您要验证是否 **可以执行证书** 并返回 CA 中的预期结果（证书或未找到）。

注意

当尝试找到问题时，在所有 IdM 服务器中运行这些测试。

6.2. 使用 HEALTHCHECK 强制系统证书

本节论述了使用 Healthcheck 工具对 Identity Management(IdM)证书的独立手动测试。

由于 Healthcheck 工具包含许多测试，因此您可以通过仅包含 DogTag 测试来缩小结果范围：**--source=ipahealthcheck.dogtag.ca**

流程

- 要运行限制为 DogTag 证书的 Healthcheck，请输入：

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

测试成功示例：

```
{
  "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"
    }
}
```

测试失败的示例：

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

其它资源

- 要查看详细参考，请在命令行中输入 **man ipa-healthcheck**。

第 7 章 使用 IDM HEALTHCHECK 检查磁盘空间

本节论述了如何使用 Healthcheck 工具监控身份管理服务器的可用磁盘空间。

详情请查看 IdM 中的 Healthcheck。

先决条件

- Healthcheck 工具仅适用于 RHEL 8.1 及更新的版本。

7.1. 磁盘空间健康检查测试

Healthcheck 工具包括用于检查可用磁盘空间的测试。可用磁盘空间不足可能会导致以下问题：

- 日志
- 执行
- Backups

测试检查以下路径：

表 7.1. 测试的路径

测试检查的路径	以 MB 为单位的最小磁盘空间
/var/lib/dirsrv/	1024
/var/lib/ipa/backup/	512
/var/log/	1024
var/log/audit/	512
/var/tmp/	512
/tmp/	512

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

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

文件系统空间检查测试放在 **ipahealthcheck.system.filesystemspace** 源下：

FileSystemSpaceCheck

此测试以以下方式检查可用磁盘空间：

- 需要最少的原始可用字节数。
- 最小可用磁盘空间百分比为 20%。

7.2. 使用 HEALTHCHECK 工具强制磁盘空间

本节论述了使用 Healthcheck 工具在身份管理(IdM)服务器上独立手动测试可用磁盘空间。

因为健康检查包括许多测试，因此您可以通过以下方式缩小结果范围：

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

流程

- 要使用可用磁盘空间的警告、错误和严重问题运行健康检查，请输入：

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

成功测试会显示空括号：

```
[]
```

例如，测试失败可显示：

```
{
  "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
  }
}
```

失败的测试会通知您 **/var/lib/dirsrv** 目录已用尽空间。

其它资源

- 要查看详细参考，请在命令行中输入 **man ipa-healthcheck**。

第 8 章 使用 HEALTHCHECK 验证 IDM 配置文件的权限

本节论述了如何使用 Healthcheck 工具测试身份管理(IdM)配置文件。

详情请查看 IdM 中的 Healthcheck。

先决条件

- Healthcheck 工具仅在 RHEL 8.1 或更新的系统中可用。

8.1. 文件权限健康检查测试

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文件的所有权或权限，测试会在 results **部分中** 返回警告。虽然这不一定意味着配置不起作用，但这意味着 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
```

文件权限测试放在 **ipahealthcheck.ipa.files** 源下：

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>** 中，CA 数据库位于 **/etc/pki/pki-tomcat/alias/** 中。

IPAFileCheck

此测试检查以下文件：

- **/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，则此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

当尝试找到问题时，在所有 IdM 服务器中运行这些测试。

8.2. 使用 HEALTHCHECK 处理配置文件

本节论述了使用 Healthcheck 工具对身份管理(IdM)服务器配置文件的独立手动测试。

Healthcheck 工具包含许多测试。可以通过以下方法缩小结果：

- 排除所有成功测试： **--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中运行 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
```

成功测试会显示空括号：

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

失败的测试显示结果 **类似如下** ：

```
{
  "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"
  }
}
```

其它资源

- 要查看详细参考材料，请在命令行中打开 **man ipa-healthcheck**。

第 9 章 使用 HEALTHCHECK 检查 IDM 复制

本节论述了如何使用 Healthcheck 工具测试身份管理(IdM)复制。

详情请查看 IdM 中的 Healthcheck。

先决条件

- Healthcheck 工具仅在 RHEL 8.1 或更新版本中可用。

9.1. 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
```

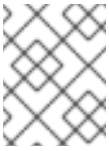
拓扑测试放置在 **ipahealthcheck.ipa.topology** 和 **ipahealthcheck.ds.replication 源** 下：

IPATopologyDomainCheck

此测试会验证：

- 拓扑是否未断开连接，所有服务器之间是否存在复制路径。
- 如果服务器的复制协议数量不超过推荐的数量。
  如果测试失败，测试会返回错误，如连接错误或太多复制协议。

  如果测试成功，则测试会返回配置的域。



注意

该测试为域和 ca 后缀运行 **ipa topologysuffix-verify** 命令（假设在此服务器上配置了证书颁发机构）。

ReplicationConflictCheck

测试在 LDAP 匹配中搜索条目 **（&（!(objectclass=nstombstone)）(nsds5ReplConflict=*)。**

注意

当尝试检查问题时，在所有 IdM 服务器中运行这些测试。

9.2. 使用 HEALTHCHECK 进行复制

本节论述了使用 Healthcheck 工具对身份管理(IdM)复制拓扑和配置的独立手动测试。

因此，Healthcheck 工具包括了许多测试，您可以使用以下方法缩短结果：

- 复制冲突测试：-- **source=ipahealthcheck.ds.replication**
- 正确的拓扑测试： **--source=ipahealthcheck.ipa.topology**

先决条件

先决条件

- 健康检查测试必须以 root 用户身份执行。

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
```

可能会有四种不同的结果：

- SUCCESS SAS- SAS 测试成功通过。

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

- 预告：测试通过，但可能存在问题。
- ERROR SAS- SAS 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 SAS- SAS 测试失败，它会影响 IdM 服务器功能。

其它资源

- 要查看详细参考，请在命令行中打开 **man ipa-healthcheck**。

第 10 章 使用 IDM HEALTHCHECK 检查 DNS 记录

本节论述了 Identity Management(IdM)中的 Healthcheck 工具来识别 DNS 记录的问题。

详情请查看 IdM 中的 Healthcheck。

先决条件

- DNS 记录 Healthcheck 工具仅在 RHEL 8.2 或更新版本中可用。

10.1. DNS 记录健康检查测试

Healthcheck 工具包括一个测试，用于检查自动发现所需的预期 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
```

DNS 记录检查测试放在 **ipahealthcheck.ipa.idns** 源下。

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** 命令中的 DNS 记录。记录在 IPA 服务器上测试。

10.2. 使用 HEALTHCHECK 工具识别 DNS 记录

本节论述了使用 Healthcheck 工具在身份管理(IdM)服务器上独立手动测试 DNS 记录。

Healthcheck 工具包含许多测试。通过添加 **--source ipahealthcheck.ipa.idns** 选项，可以只包含 DNS 记录测试来缩小结果范围。

先决条件

- 健康检查测试必须以 root 用户身份执行。

流程

- 要运行 DNS 记录检查，请输入：

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

如果记录可以解析，测试会返回 **SUCCESS**，从而返回：

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

例如，当记录数量与预期数目不匹配时，测试将返回 **WARNING** ：

```
{
    "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
    }
}
```

其它资源

- 要查看详细参考，请在命令行中输入 **man ipa-healthcheck**。