Red Hat Enterprise Linux 9

IdM Healthcheck を使用した IdM 環境の監視

IdM Healthcheck ユーティリティーで Identity Management サーバーのステータスの監視

Last Updated: 2022-07-10

Red Hat Enterprise Linux 9 IdM Healthcheck を使用した IdM 環境の監視

IdM Healthcheck ユーティリティーで Identity Management サーバーのステータスの監視

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.

法律上の通知

概要

本書は、Red Hat Enterprise Linux 9 で Identity Management を効果的に設定、管理、および維持する方法を説明します。

目次

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、弊社の CTO、Chris Wright のメッセージ を参照してください。

RED HAT ドキュメントへのフィードバックの提供

ご意見ご要望をお聞かせください。ドキュメントの改善点はございませんか。

- 特定の部分についての簡単なコメントをお寄せいただく場合は、以下をご確認ください。
  1. ドキュメントの表示が **Multi-page HTML** 形式になっていて、ドキュメントの右上隅に **Feedback** ボタンがあることを確認してください。
  2. マウスカーソルで、コメントを追加する部分を強調表示します。
  3. そのテキストの下に表示される **Add Feedback** ポップアップをクリックします。
  4. 表示される手順に従ってください。
- Bugzilla を介してフィードバックを送信するには、新しいチケットを作成します。
  1. Bugzilla の Web サイトに移動します。
  2. Component で **Documentation** を選択します。
  3. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも記入してください。
  4. **Submit Bug** をクリックします。

第1章 IDM HEALTHCHECK ツールのインストールおよび実行

本章では、IdM Healthcheck ツールと、そのインストールおよび実行方法を説明します。

1.1. IDM の HEALTHCHECK

IdM (Identity Management) の Healthcheck ツールは、IdM 環境の健全性に影響を与える可能性がある問題を見つけるのに役立ちます。

注記

Healthcheck ツールは、Kerberos 認証なしで使用できるコマンドラインツールです。

モジュールは独立しています

Healthcheck は、以下をテストする独立したモジュールで構成されています。

- レプリケーションの問題
- 証明書の有効性
- 認証局インフラストラクチャーの問題
- IdM および Active Directory の信頼の問題
- 正しいファイル許可と所有権設定

2 つの出力形式

ヘルスチェックでは、以下の出力が生成されます。これは、**output-type** オプションを使用して設定できます。

- **JSON**: マシンが判読できる出力 (デフォルト)
- **human**: 人間が判読できる出力

--output-file オプションで別の出力先ファイルを指定できます。

結果

Healthcheck の各モジュールは、次のいずれかの結果を返します。

SUCCESS
: 期待どおりに構成されています。

WARNING
: エラーではありませんが、注目または評価すると良いでしょう。

ERROR
: 期待どおりに構成されていません。

CRITICAL
: 予想どおりに構成されておらず、影響を受ける可能性が高くなっています。

1.2. IDM HEALTHCHECK のインストール

本セクションでは、IdM Healthcheck ツールのインストール方法を説明します。

手順

- **ipa-healthcheck** パッケージをインストールします。

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

検証手順

- **--failures-only** オプションを使用して、**ipa-healthcheck** にエラーのみを報告させます。IdM インストールを完全に使用しても、空の結果 **[]** が返されます。

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

関連情報

- **ipa-healthcheck --help** を使用して、サポートされるすべての引数を表示します。

1.3. IDM HEALTHCHECK の実行

Healthcheck は、ログローテーション を使用して手動で実行することも、自動でも実行できます。

前提条件

- Healthcheck ツールがインストールされている。IdM Healthcheck のインストール を参照してください。

手順

- Healthcheck を手動で実行するには、**ipa-healthcheck** コマンドを実行します。

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

関連情報

すべてのオプションは、man ページの **man ipa-healthcheck** を参照してください。

1.4. ログローテーション

ログローテーションは新しいログファイルを毎日作成し、ファイルが日付別に編成されます。ログファイルは同じディレクトリーに保存されるため、日付に応じて特定のログファイルを選択できます。

ローテーションは、ログファイルの最大数が設定されていて、その数を超えると、最新のファイルが最も古いファイルを書き直し、名前を変更することを意味します。たとえば、ローテーションの数が 30 の場合は、31 番目のファイル (最も古いファイル) が新しいファイルにより置き換えられます。

ログローテーションは、膨大なログファイルを減らして整理するため、ログの分析に役立ちます。

1.5. IDM HEALTHCHECK でログローテーションの設定

本セクションでは、以下を使用してログローテーションを設定する方法を説明します。

- **systemd** タイマー
- **crond** サービス

systemd タイマーは、Healthcheck ツールを定期的に実行して、ログを生成します。デフォルト値は毎日午前 4 時に設定されています。

crond サービスは、ログローテーションに使用されます。

デフォルトのログ名は **healthcheck.log** で、ローテーションされるログは **healthcheck.log-YYYYMMDD** 形式を使用します。

前提条件

- root でコマンドを実行できる。

手順

1. **systemd** タイマーを有効にします。

```
# 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. **systemd** タイマーを起動します。

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

3. **/etc/logrotate.d/ipahealthcheck** ファイルを開いて、保存すべきログの数を設定します。
デフォルトでは、ログローテーションは 30 日間設定されます。

4. **/etc/logrotate.d/ipahealthcheck** ファイルで、ログへのパスを設定します。
デフォルトでは、ログは **/var/log/ipa/healthcheck/** ディレクトリーに保存されます。

5. **/etc/logrotate.d/ipahealthcheck** ファイルで、ログ生成の時間を設定します。
デフォルトでは、ログは毎日 午前 4 時に作成されます。

6. ログローテーションを使用するには、**crond** サービスが有効になっており、実行していることを確認します。

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

ログの生成を開始するには、IPA healthcheck サービスを起動します。

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

結果を確認するには、**/var/log/ipa/healthcheck/** に移動して、ログが正しく作成されていることを確認します。

1.6. 関連情報

- IdM Healthcheck の使用例は、『 Identity Management の設定および管理 』の以下の項を参照してください。
  - サービスの確認
  - IdM および AD 信頼設定の確認
  - 証明書の確認
  - システム証明書の確認
  - ディスク領域の確認
  - IdM 設定ファイルの権限の確認
  - レプリケーションの確認
- また、1つのガイドにまとめられた章も確認できます。IdM Healthcheck を使用して IdM 環境を監視することもできます。

第2章 IDM HEALTHCHECK でサービスの確認

本セクションでは、Healthcheck ツールを使用して、Identity Management (IdM) サーバーが使用する監視サービスを説明します。

詳細は「 IdM の Healthcheck 」を参照してください。

2.1. サービスの HEALTHCHECK テスト

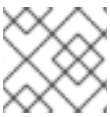
Healthcheck ツールには、IdM サービスが稼働していないかどうかを確認するテストが含まれます。このテストは、実行中ではないサービスが他のテストで不具合を引き起こす可能性があるため、重要です。したがって、全サービスが最初に実行されていることを確認します。次に、その他のテスト結果をすべて確認できます。

すべてのサービステストを表示するには、**--list-sources** オプションを指定して、**ipa-healthcheck** を実行します。

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

ipahealthcheck.meta.services ソースの下に、Healthcheck でテストしたサービスをすべて確認できます。

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



注記

問題を検出するには、すべての IdM サーバーで上記のテストを実行します。

2.2. HEALTHCHECK でサービスのスクリーニング

本セクションでは、Healthcheck ツールを使用して、Identity Management (IdM) サーバーで実行しているサービスのスタンドアロンの手動テストを説明します。

Healthcheck ツールには多くのテストが含まれており、その結果は次の方法で短くすることができます。

- 成功したテストをすべて除外する - **--failures-only**
- サービステストのみを含める - **--source=ipahealthcheck.meta.services**

手順

- サービスに関する警告、エラー、および重大な問題で Healthcheck を実行するには、次のコマンドを実行します。

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

テストに成功すると、空の括弧が表示されます。

```
[ ]
```

サービスのいずれかが失敗した場合は、以下のような結果になります。

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

関連情報

- **man ipa-healthcheck** を参照してください。

第3章 IDM HEALTHCHECK でディスク領域の確認

本セクションでは、Healthcheck ツールを使用して Identity Management サーバーの空きディスク容量を監視する方法を説明します。

詳細は「 IdM の Healthcheck 」を参照してください。

3.1. ディスク領域のヘルスチェックのテスト

Healthcheck ツールには、利用可能なディスク領域を確認するテストが含まれます。空きディスク容量が十分にないと、以下で問題が発生する可能性があります。

- ロギング
- 実行
- バックアップ

テストでは、以下のパスを確認します。

表3.1 テスト済みのパス

テストで確認されるパス	最小ディスク領域 (MB)
/var/lib/dirsrv/	1024
/var/lib/ipa/backup/	512
/var/log/	1024
var/log/audit/	512
/var/tmp/	512
/tmp/	512

テストの一覧を表示するには、**--list-sources** オプションを指定して、**ipa-healthcheck** を実行します。

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

ファイルシステム容量の確認テストは、**ipahealthcheck.system.filesystemspace** ソースの下にあります。

FileSystemSpaceCheck

このテストでは、次の方法で使用可能なディスク容量を確認します。

- 最低限必要な生の空きバイト。
- パーセント - 空きディスクの最小容量は 20% にハードコーディングされています。

3.2. HEALTHCHECK ツールでディスク領域のスクリーニング

本セクションでは、Healthcheck ツールを使用して、Identity Management (IdM) サーバーで利用可能なディスク容量のスタンドアロンの手動テストを説明します。

Healthcheck には多くのテストが含まれるため、次の方法で結果を絞り込むことができます。

- 成功したテストをすべて除外する - **--failures-only**
- 容量の確認テストのみを含める - **--source=ipahealthcheck.system.filesystemspace**

手順

- ディスク領域に関する警告、エラー、および重大な問題で Healthcheck を実行するには、次のコマンドを実行します。

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

テストに成功すると、空の括弧が表示されます。

```
[]
```

テストに失敗すると、たとえば、以下のような結果が表示されます。

```
{
  "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
  }
}
```

ここでは、**/var/lib/dirsrv** ディレクトリーの容量が不足しているためにテストに失敗したことが通知されます。

関連情報

- **man ipa-healthcheck** を参照してください。

第4章 HEALTHCHECK で IDM 設定ファイルの権限の確認

本セクションでは、Healthcheck ツールを使用して、Identity Management (IdM) 設定ファイルをテストする方法を説明します。

詳細は「 IdM の Healthcheck 」を参照してください。

4.1. ファイルパーミッションの HEALTHCHECK テスト

Healthcheck ツールは、Identity Management (IdM) によりインストールまたは設定される重要なファイルの所有権とパーミッションをテストします。

テストされたファイルの所有権またはパーミッションを変更すると、テストにより **結果** セクションに警告が返ります。必ずしも設定が機能しないことを意味するわけではありませんが、ファイルがデフォルト設定と異なることを意味します。

すべてのテストを表示するには、**--list-sources** オプションを指定して **ipa-healthcheck** を実行します。

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

ファイルパーミッションテストは、**ipahealthcheck.ipa.files** ソースの下にあります。

IPAFileNSSDBCheck

このテストは、389-ds NSS データベースと認証局 (CA) データベースを確認します。389-ds データベースは、**/etc/dirsrv/slapd-<dashed-REALM>** にあり、CA データベースは **/etc/pki/pki-tomcat/alias/** にあります。

IPAFileCheck

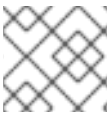
このテストは以下のファイルを確認します。

- **/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**
  PKINIT が有効になっている場合は、以下のファイルを確認します。
- **/var/lib/ipa/certs/kdc.pem**
- **/var/lib/ipa/private/kdc.key**
  DNS が設定されている場合は、以下のファイルを確認します。
- **/etc/named.keytab**
- **/etc/ipa/dnssec/ipa-dnskeysyncd.keytab**

TomcatFileCheck

このテストは、CA が設定されている場合に、いくつかの tomcat 固有のファイルを確認します。

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



注記

問題を確認するには、すべての IdM サーバーで上記のテストを実行します。

4.2. HEALTHCHECK で設定ファイルのスクリーニング

本セクションでは、Healthcheck ツールを使用して、Identity Management (IdM) サーバーの設定ファイルのスタンドアロンの手動テストを説明します。

Healthcheck ツールには、多くのテストが含まれます。結果を絞り込むには、以下を行います。

- 成功したテストをすべて除外する - **--failures-only**
- 所有者テストとパーミッションテストのみを含める - **--source=ipahealthcheck.ipa.files**

手順

1. 警告、エラー、重大な問題のみを表示しながら、IdM 設定ファイルの所有権とパーミッションで Healthcheck テストを実行するには、次のように入力します。

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

テストに成功すると、空の括弧が表示されます。

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

テストに失敗すると、以下の **WARNING** のような結果が表示されます。

```
{
  "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"
  }
}
```

関連情報

- **man ipa-healthcheck** を参照してください。

第5章 IDM HEALTHCHECK で DNS レコードの確認

本セクションでは、Identity Management (IdM) の Healthcheck ツールを説明し、DNS レコードの問題を特定します。

5.1. DNS レコード検証テスト

Healthcheck ツールには、自動検出に必要な DNS レコードが解決可能であることを確認するテストが含まれます。

テストの一覧を表示するには、**--list-sources** オプションを指定して、**ipa-healthcheck** を実行します。

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

DNS レコードチェックテストは **ipahealthcheck.ipa.idns** ソースの下にあります。

IPADNSSystemRecordsCheck

このテストは、**/etc/resolv.conf** ファイルで指定された最初のリゾルバーを使用して、**ipa dns-update-system-records --dry-run** コマンドで得られる DNS レコードを確認します。このレコードは IPA サーバーでテストされます。

5.2. HEALTHCHECK ツールを使用した DNS レコードのスクリーニング

本セクションでは、Healthcheck ツールを使用して、Identity Management (IdM) サーバーで DNS レコードのスタンドアロンの手動テストを説明します。

Healthcheck ツールには、多くのテストが含まれます。**--source ipahealthcheck.ipa.idns** オプションを追加して、DNS レコードテストのみを含めることで結果を絞り込むことができます。

前提条件

- Healthcheck テストは root ユーザーで実行する。

手順

- DNS レコードの確認を実行するには、以下を入力します。

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

レコードが解決可能である場合、テストは、結果として **SUCCESS** を返します。

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

たとえば、レコードの数が予想される数と一致しない場合、テストは **WARNING** を返します。

```
{
    "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
    }
}
```

関連情報

- **man ipa-healthcheck** を参照してください。

第6章 HEALTHCHECK で IDM レプリケーションの確認

本セクションでは、Healthcheck ツールを使用して Identity Management (IdM) レプリケーションをテストする方法を説明します。

詳細は「 IdM の Healthcheck 」を参照してください。

6.1. レプリケーションの HEALTHCHECK テスト

Healthcheck ツールは、Identity Management (IdM) トポロジーの設定をテストして、レプリケーションの競合問題を検索します。

テストの一覧を表示するには、**--list-sources** オプションを指定して、**ipa-healthcheck** を実行します。

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

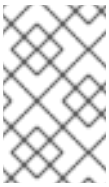
トポロジーのテストは、**ipahealthcheck.ipa.topology** ソースおよび **ipahealthcheck.ds.replication** ソースの下にあります。

IPATopologyDomainCheck

このテストでは、以下が検証されます。

- トポロジーが切断されておらず、すべてのサーバー間にレプリケーションパスがあるかどうか。
- サーバーに推奨される数以上のレプリカ合意がない場合。
  テストに失敗すると、テストは、接続エラーや、レプリカ合意が多すぎるなど、エラーを返します。

  テストに成功すると、テストにより設定済みのドメインが返されます。



注記

テストは、ドメインおよび ca サフィックスの両方で **ipa topologysuffix-verify** コマンドを実行します (認証局がこのサーバーに設定されていることを前提とします)。

ReplicationConflictCheck

テストにより、**(&(!(objectclass=nstombstone))(nsds5ReplConflict=*))** に一致する LDAP エントリーを検索します。

注記

問題を確認するには、すべての IdM サーバーで上記のテストを実行します。

6.2. HEALTHCHECK でレプリケーションのスクリーニング

本セクションでは、Healthcheck ツールを使用して、Identity Management (IdM) レプリケーショントポロジーおよび設定に対するスタンドアロンの手動テストを説明します。

Healthcheck ツールには多くのテストが含まれるため、以下の方法で結果を短くすることができます。

- レプリケーションの競合テスト - **--source=ipahealthcheck.ds.replication**
- 正確なトポロジーテスト - **--source=ipahealthcheck.ipa.topology**

前提条件

- Healthcheck テストは root ユーザーで実行する。

手順

- Healthcheck のレプリケーションの競合とトポロジーの確認を実行するには、次のコマンドを実行します。

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

以下のような 4 つの結果が取得できます。

- SUCCESS - テストが成功

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

- WARNING - テストには合格したが、問題の可能性あり
- ERROR - テストが失敗

```
{
  "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 - テストが失敗し、IdM サーバー機能に影響が及ぶ

関連情報

- **man ipa-healthcheck** を参照してください。

第7章 IDM HEALTHCHECK を使用した IDM および AD 信頼設定の検証

本セクションでは、Identity Management (IdM) の Healthcheck ツールを理解および使用して、IdM と Active Directory 信頼に関する問題を特定する方法を説明します。

7.1. IDM および AD 信頼の HEALTHCHECK のテスト

Healthcheck ツールには、Identity Management (IdM) および Active Directory (AD) 信頼のステータスをテストするためのテストが複数含まれています。

すべての信頼テストを表示するには、**--list-sources** オプションを指定して **ipa-healthcheck** を実行します。

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

ipahealthcheck.ipa.trust ソースでテストをすべて見つけることができます。

IPATrustAgentCheck

このテストは、マシンが信頼エージェントとして設定されている場合に、SSSD 設定を確認します。**/etc/sssd/sssd.conf** 内の各ドメインで、**id_provider=ipa** は、**ipa_server_mode** が **True** であることを確認します。

IPATrustDomainsCheck

このテストでは、**sssctl domain-list** のドメインの一覧を、IPA ドメインを除く **ipa trust-find** のドメインの一覧と比較して、信頼ドメインが SSSD ドメインと一致するかどうかを確認します。

IPATrustCatalogCheck

このテストでは、AD ユーザー **Administrator@REALM** を解決します。これにより、**sssctl domain-status** の出力に、AD Global カタログと AD Domain Controller の値が追加されます。各信頼ドメインに対して、SID + 500 (管理者) の ID でユーザーを検索し、**sssctl domain-status <domain> --active-server** の出力を確認して、ドメインがアクティブであることを確認します。

IPAsidgenpluginCheck

このテストは、IPA 389-ds インスタンスで **sidgen** プラグインが有効になっていることを確認します。このテストでは、**cn=plugins,cn=config** の **IPA SIDGEN** プラグインおよび **ipa-sidgen-task** プラグインに、**nsslapd-pluginEnabled** オプションが含まれていることを検証しています。

IPATrustAgentMemberCheck

このテストでは、現在のホストが **cn=adtrust agents,cn=sysaccounts,cn=etc,SUFFIX** のメンバーであることを確認します。

IPATrustControllerPrincipalCheck

このテストでは、現在のホストが **cn=adtrust agents,cn=sysaccounts,cn=etc,SUFFIX** のメンバーであることを確認します。

IPATrustControllerServiceCheck

このテストは、現在のホストが ipactl で ADTRUST サービスを開始することを確認します。

IPATrustControllerConfCheck

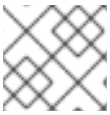
このテストでは、**ldapi** は、**net conf** リストの出力で passdb バックエンドに対して有効になっていることを確認します。

IPATrustControllerGroupSIDCheck

このテストは、admins グループの SID が 512 (Domain Admins RID) で終わることを確認します。

IPATrustPackageCheck

このテストは、信頼コントローラーと AD 信頼が有効になっていない場合に、**trust-ad** パッケージがインストールされていることを確認します。



注記

問題を確認するには、すべての IdM サーバーで上記のテストを実行します。

7.2. HEALTHCHECK ツールを使用した信頼のスクリーニング

本セクションでは、Healthcheck ツールを使用して、Identity Management (IdM) および Active Directory (AD) の信頼ヘルスチェックに関するスタンドアロンの手動テストを説明します。

Healthcheck ツールには多くのテストが含まれるため、以下の方法で結果を短くすることができます。

- 成功したテストをすべて除外する - **--failures-only**
- 信頼テストのみを含める - **--source=ipahealthcheck.ipa.trust**

手順

- 信頼における警告、エラー、および重大な問題ついて Healthcheck を実行するには、次のコマンドを実行します。

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

テストに成功すると、空の括弧が表示されます。

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

関連情報

- **man ipa-healthcheck** を参照してください。

第8章 IDM HEALTHCHECK でシステム証明書の検証

本セクションでは、Identity Management (IdM) の Healthcheck ツールを説明し、システム証明書の問題を特定します。

詳細は「 IdM の Healthcheck 」を参照してください。

8.1. システム証明書の HEALTHCHECK テスト

Healthcheck ツールには、システム (DogTag) 証明書を検証するさまざまなテストがあります。

すべてのテストを表示するには、**--list-sources** オプションを指定して **ipa-healthcheck** を実行します。

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

すべてのテストは、**ipahealthcheck.dogtag.ca** ソースの下にあります。

DogtagCertsConfigCheck
: このテストは、その NSS データベースの CA (認証局) 証明書を、**CS.cfg** に保存されているものと同じ値と比較します。一致しないと、CA は起動できません。
具体的には、以下を確認します。

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

Key Recovery Authority (KRA) がインストールされている場合は、以下になります。

- **ca.connector.KRA.transportCert** の場合は **transportCert cert-pki-kra**

DogtagCertsConnectivityCheck
: このテストでは、接続性を検証します。このテストは、以下の確認を行う **ipa cert-show 1** コマンドと同等です。

- Apache の PKI プロキシー設定
- CA を見つけることができる IdM
- RA エージェントクライアント証明書
- 要求に対する CA 返信の正確性

テストは、**cert-show** を実行し、CA から期待される結果 (証明書または「not fount」) を返すため、シリアル番号 #1 の証明書を確認します。

注記

問題を確認するには、すべての IdM サーバーで上記のテストを実行します。

8.2. HEALTHCHECK を使用したシステム証明書のスクリーニング

本セクションでは、Healthcheck ツールを使用して、Identity Management (IdM) 証明書のスタンドアロンの手動テストを説明します。

Healthcheck ツールには多くのテストが含まれるため、Dogtag テスト (**--source=ipahealthcheck.dogtag.ca**) のみを含めることで結果を絞り込むことができます。

手順

- Healthcheck を Dogtag 証明書に制限して実行するには、次のコマンドを実行します。

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

テストに成功すると、以下のようになります。

```
{
  "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"
    }
}
```

テストに失敗すると、以下のようになります。

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

関連情報

- **man ipa-healthcheck** を参照してください。

第9章 IDM HEALTHCHECK で証明書の検証

本セクションでは、Identity Management (IdM) で Healthcheck ツールを理解して、certmonger が維持する IPA 証明書の問題を特定する方法を説明します。

詳細は「 IdM の Healthcheck 」を参照してください。

9.1. IDM 証明書の HEALTHCHECK テスト

Healthcheck ツールには、Identity Management (IdM) の certmonger が維持する証明書の状況を確認するさまざまなテストが含まれています。certmonger の詳細は、「certmonger で サービスの IdM 証明書の取得」を参照して ください。

このテストスイートは、有効期限、検証、信頼、およびその他の問題を確認します。根本的な問題 1 つに対して、複数のエラーが発生する可能性があります。

すべての証明書テストを表示するには、**--list-sources** オプションを指定して **ipa-healthcheck** を実行します。

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

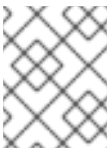
すべてのテストは、**ipahealthcheck.ipa.certs** ソースの下にあります。

IPACertmongerExpirationCheck

このテストは、**certmonger** の有効期限を確認します。
証明書の有効期限が切れている場合は、エラーが報告されます。

証明書の有効期限が間近な場合は、警告が表示されます。デフォルトでは、このテストは、証明書の有効期限が 28 日以内のものを対象としています。

/etc/ipahealthcheck/ipahealthcheck.conf ファイルで日数を設定できます。ファイルを開くと、デフォルトセクションにある **cert_expiration_days** オプションを変更します。

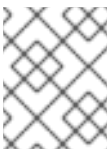


注記

certmonger は証明書の有効期限に関する独自のビューを読み込んで維持します。この確認では、ディスク上の証明書は検証されません。

IPACertfileExpirationCheck

このテストは、証明書ファイルまたは NSS データベースを開けないかを確認します。このテストでは、有効期限も確認します。したがって、エラー出力または警告の出力で、**msg** 属性を慎重に読み取ります。このメッセージは問題を指定します。



注記

このテストでは、ディスク上の証明書が確認されます。証明書がない、読み取りができないなどの問題が発生した場合は、別のエラーを出力することもできます。

IPACertNSSTrust

このテストは、NSS データベースに保存されている証明書の信頼を比較します。NSS データベースで期待される、追跡された証明書では、信頼が、期待される値と比較され、一致しないとエラーが発生します。

IPANSSChainValidation

このテストは、NSS 証明書の証明書チェーンを検証します。テストは、**certutil -V -u V -e -d [dbdir] -n [nickname]** を実行します。

IPAOpenSSLChainValidation

このテストは、OpenSSL 証明書の証明書チェーンを検証します。**NSSChain** 検証を比較するには、以下を実行する OpenSSL コマンドになります。

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

IPARAAgent

このテストは、ディスクの証明書を、**uid=ipara,ou=People,o=ipaca** の LDAP の同等のレコードと比較します。

IPACertRevocation

このテストは certmonger を使用して、証明書が取り消されていないことを確認します。したがって、テストでは certmonger でのみメンテナンスされる証明書に接続している問題を見つけることができます。

IPACertmongerCA

このテストでは、certmonger の Certificate Authority (CA) の設定を検証します。IdM は、CA を使用しない証明書を発行できません。
certmonger は、CA ヘルパーのセットを維持します。IdM には、IdM を介して証明書を発行し、ホストまたはサービスの証明書に対して、ホストまたはユーザーのプリンシパルとして認証する IPA という名前の CA があります。

また、CA サブシステム証明書を更新する **dogtag-ipa-ca-renew-agent** および **dogtag-ipa-ca-renew-agent-reuse** があります。

注記

問題を確認するには、すべての IdM サーバーで上記のテストを実行します。

9.2. HEALTHCHECK ツールで証明書のスクリーニング

本セクションでは、Healthcheck ツールを使用した Identity Management (IdM) 証明書のヘルスチェックのスタンドアロンの手動テストを説明します。

Healthcheck ツールには多くのテストが含まれるため、以下の方法で結果を短くすることができます。

- 成功したテストをすべて除外する - **--failures-only**
- 証明書テストのみを含める - **--source=ipahealthcheck.ipa.certs**

前提条件

- Healthcheck テストは root ユーザーで実行する。

手順

- 証明書に関する警告、エラー、および重大な問題で Healthcheck を実行するには、次のコマンドを実行します。

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

テストに成功すると、空の括弧が表示されます。

```
[]
```

失敗したテストでは、以下の出力が表示されます。

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

この **IPACertfileExpirationCheck** テストは、NSS データベースを開く際に失敗します。

関連情報

- **man ipa-healthcheck** を参照してください。