Red Hat Enterprise Linux 9

IdM Healthcheck を使用した IdM 環境の監視

ステータスチェックとヘルスチェックの実行

Last Updated: 2024-06-26

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

ステータスチェックとヘルスチェックの実行

法律上の通知

概要

ipa-healthcheck ユーティリティーは、管理者が Red Hat Identity Management (IdM) 環境の問題を検出するのに役立ちます。これには、IdM サービスのステータスチェック、設定ファイルのアクセスパーミッション、レプリケーションステータス、証明書の問題が含まれます。

目次

RED HAT ドキュメントへのフィードバック (英語のみ)

Red Hat ドキュメントに関するご意見やご感想をお寄せください。また、改善点があればお知らせください。

Jira からのフィードバック送信 (アカウントが必要)

1. Jira の Web サイトにログインします。
2. 上部のナビゲーションバーで **Create** をクリックします。
3. **Summary** フィールドにわかりやすいタイトルを入力します。
4. **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追加してください。
5. ダイアログの下部にある **Create** 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

IdM Healthcheck ツールと、ツールのインストールおよび実行方法について詳しく説明します。

1.1. IDM の HEALTHCHECK

Identity Management (IdM) の Healthcheck ツールは、IdM 環境の健全性に影響を与える可能性のある問題を検出するのに役立ちます。

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。

独立したモジュール

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
- ファイルのパーミッションと所有権の正しい設定

2 つの出力形式

Healthcheck 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
: 想定どおりに設定されています。

WARNING
: エラーではありませんが、注意または評価することを推奨します。

ERROR
: 想定どおりに設定されていません。

CRITICAL
: 想定どおりに設定されておらず、影響が受ける可能性が高いと見られます。

1.2. IDM HEALTHCHECK のインストール

以下の手順に従って、IdM Healthcheck ツールをインストールします。

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 インストールが完全に機能していれば、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、手動で実行することも、ログローテーション を使用して自動で実行することもできます。

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 ipa-healthcheck** の man ページ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ます。ファイルは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。

ローテーションとは、設定されたログファイルの最大数を超えると、最新のファイルによって最も古いファイルが書き換えられ、ファイルの名前が変更され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、31 番目のログファイルが 1 番目の (最も古い) ログファイルを置き換えます。

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 でのログローテーションの設定

次の手順に従って、ログローテーションを設定します。

- **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 日間に設定されます。

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** サービスを有効にして実行します。

```
# 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。

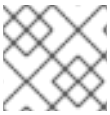
```
# systemctl start ipa-healthcheck
```

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. IDM HEALTHCHECK の設定の変更

Healthcheck の設定を変更するには、目的のコマンドラインオプションを

/etc/ipahealthcheck/ipahealthcheck.conf ファイルに追加します。これは、たとえば、ログローテーションを設定し、ログを自動分析に適した形式にしたいが、新しいタイマーを設定したくない場合に便利です。



注記

この Healthcheck 機能は、RHEL 9.1 以降でのみ利用できます。

変更後、Healthcheck が作成するすべてのログに、新しい設定が反映されます。この設定は、Healthcheck の手動実行にも適用されます。

注記

Healthcheck を手動で実行する場合、設定ファイルの設定は、コマンドラインで指定したオプションよりも優先されます。たとえば、設定ファイルで **output_type** が **human** に設定されている場合、コマンドラインで **json** を指定しても効果はありません。設定ファイルで指定されていないコマンドラインオプションを使用すると、通常どおり適用されます。

関連情報

- IdM Healthcheck でのログローテーションの設定

1.7. 出力ログの形式を変更するための HEALTHCHECK の設定

設定済みのタイマーを使用して Healthcheck を設定するには、次の手順に従ってください。この例では、人間が判読できる形式でログを生成し、エラーだけでなく正常な結果も含めるように Healthcheck を設定します。

前提条件

- システムで RHEL 9.1 以降を実行している。
- **root** 権限がある。
- 以前にタイマーを使用してログローテーションを設定していた。

手順

1. テキストエディターで **/etc/ipahealthcheck/ipahealthcheck.conf** ファイルを開きます。
2. **[default]** セクションに、オプション **output_type=human** と **all=True** を追加します。
3. ファイルを保存してから閉じます。

検証

1. Healthcheck を手動で実行します。

```
# ipa-healthcheck
```

2. **/var/log/ipa/healthcheck/** に移動し、ログの形式が正しいことを確認します。

関連情報

関連情報

- IdM Healthcheck でのログローテーションの設定

1.8. 関連情報

- IdM Healthcheck の使用例は、IdM Healthcheck を使用した IdM 環境の監視 の以下のセクション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
  - ディスク容量の確認
  - IdM 設定ファイルの権限の確認
  - レプリケーションの確認

第2章 IDM HEALTHCHECK を使用したサービスの確認

Healthcheck ツールを使用して、Identity Management (IdM) サーバーによって使用されるサービスを監視できます。

詳細は以下を参照してください。

IdM の Healthcheck

2.1. サービスの HEALTHCHECK テスト

Healthcheck ツールには、実行されていない IdM サービスがないかどうかを確認するテストが含まれています。サービスが実行されていないと他のテストでエラーが発生する可能性があるため、このテストは重要です。したがって、まずすべてのサービスが実行されていることを確認してください。その後、他のすべてのテスト結果を確認します。

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 ソースで、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 を使用したサービスのスクリーニング

Healthcheck ツールを使用して、Identity Management (IdM) サーバー上で実行されているサービスのスタンドアロン手動テストを実行するには、次の手順に従います。

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、および重大な問題について Healthcheck を実行するには、次のコマンドを実行します。

```
# ipa-healthcheck --source=ipahealthcheck.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 を使用したディスク容量の確認

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できます。

詳細は IdM の Healthcheck を参照してください。

3.1. ディスク容量の HEALTHCHECK テスト

Healthcheck ツールには、利用可能なディスク容量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 テストされるパス

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

テストのリ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 ツールを使用したディスク容量のスクリーニング

Healthcheck ツールを使用して、Identity Management (IdM) サーバー上の利用可能なディスク容量のスタンドアロン手動テストを実行するには、次の手順に従います。

Healthcheck には多くのテストが含まれているため、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

- ディスク容量に関する警告、エラー、および重大な問題について Healthcheck を実行するには、次のコマンドを実行します。

```
# ipa-healthcheck --source=ipahealthcheck.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ています。

関連情報

- **man ipa-healthcheck** を参照してください。

第4章 HEALTHCHECK を使用した IDM 設定ファイルのパーミッションの確認

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について詳しく説明します。

詳細は以下を参照してください。

IdM の Healthcheck

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。

テスト対象のファイルの所有権またはパーミッションが変更されていると、テスト時に **result** セクションに警告が返されます。これは必ずしも設定が機能しないことを意味しませんが、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

このテストでは、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

このテストでは、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

このテストでは、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 を使用した設定ファイルのスクリーニング

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手動テストを実行するには、次の手順に従います。

Healthcheck ツールには多くのテストが含まれています。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. IdM 設定ファイルの所有権とパーミッションについて Healthcheck テストを実行し、警告、エラー、重大な問題のみを表示するには、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 を使用した DNS レコードの確認

Healthcheck ツールを使用して、Identity Management (IdM) の DNS レコードの問題を特定できます。

5.1. DNS レコードの HEALTHCHECK 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。

テストのリ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
```

DNS レコードの確認テストは、**ipahealthcheck.ipa.idns** ソースの下にあります。

IPADNSSystemRecordsCheck

このテストでは、**/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

Healthcheck ツールを使用して Identity Management (IdM) サーバー上で DNS レコードのスタンドアロン手動テストを実行するには、次の手順に従います。

Healthcheck ツールには多くのテストが含まれています。**--source ipahealthcheck.ipa.idns** オプションを追加して、DNS レコードテストだけ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

- **root** ユーザーとして Healthcheck テストを実行する必要があります。

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には、テストの結果として **SUCCESS** が返されます。

```
{
    "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、レコードの数が想定数と一致しないなどの場合には、**WARNING** が返されます。

```
{
    "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 IDM HEALTHCHECK を使用した KDC ワーカープロセスの最適な数の検証

Identity Management (IdM) の Healthcheck ツールを使用して、最適な数の **krb5kdc** ワーカープロセスを使用するように Kerberos Key Distribution Center (KDC) が設定されていることを確認できます。これは、ホストの CPU コアの数と同じにする必要があります。

ipahealthcheck.ipa.kdc ソースの下で、正しい数の KDC ワーカープロセスのテストを見つけることができます。Healthcheck ツールには多くのテストが含まれているため、**--source ipahealthcheck.ipa.kdc** オプションを追加して KDC ワーカー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

- KDC ワーカープロセスの Healthcheck ツールは、RHEL 8.7 以降でのみ使用できます。
- **root** ユーザーとして Healthcheck テストを実行する必要があります。

手順

- KDC ワーカープロセスの確認を実行するには、以下を入力します。

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

KDC ワーカープロセスの数が CPU コアの数と一致する場合、結果として **SUCCESS** が返されます。

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

ワーカープロセスの数が CPU コアの数と一致しない場合、**WARNING** が返されます。次の例では、2 つのコアを持つホストが 1 つの KDC ワーカープロセスのみを持つように設定されています。

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

設定されたワーカーがない場合も、**WARNING** が出力されます。次の例で
は、**KRB5KDC_ARGS** 変数が **/etc/sysconfig/krb5kdc** 設定ファイルにありません。

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

関連情報

- **man ipa-healthcheck**

第7章 HEALTHCHECK を使用した IDM レプリケーションの確認

Healthcheck ツールを使用して、Identity Management (IdM) レプリケーションをテストできます。

詳細は IdM の Healthcheck を参照してください。

7.1. 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。

テストのリ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
```

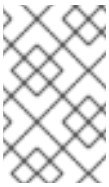
トポロジーのテストは、**ipahealthcheck.ipa.topology** ソースおよび **ipahealthcheck.ds.replication** ソースの下にあります。

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かどうか。
  テストに失敗すると、接続エラーやレプリカ合意が多すぎるなどのエラーが返されます。

  テストに成功すると、設定済みのドメインが返されます。



注記

このテストでは、ドメインおよび ca 接尾辞の両方で **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ています)。

ReplicationConflictCheck

このテストでは、**(&(!(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。

LDAP レプリケーションの競合を解決する方法の詳細は、一般的なレプリケーションの問題解決 を参照してください。

7.2. HEALTHCHECK を使用したレプリケーションのスクリーニング

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と設定のスタンドアロン手動テストを実行するには、次の手順に従います。

Healthcheck ツールには多くのテストが含まれているため、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

- **root** ユーザーとして Healthcheck テストを実行する必要があります。

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 - テストに成功

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

- WARNING - テストには成功したが、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8章 IDM HEALTHCHECK を使用した IDM および AD 信頼設定の検証

Healthcheck ツールを使用して、Identity Management (IdM) での IdM および Active Directory 信頼に関する問題を特定する方法について詳しく説明します。

8.1. 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複数のテストが含まれています。

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
```

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

IPATrustAgentCheck

このテストでは、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** のドメインのリストを、IPA ドメインを除く **ipa trust-find** のドメインのリストと比較して、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

このテストでは、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も検証します。

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

このテストでは、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

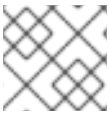
このテストでは、**ldapi** が、**net conf** リストの出力で passdb バックエンドに対して有効になっていることを確認します。

IPATrustControllerGroupSIDCheck

このテストでは、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

このテストでは、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てください。

8.2. HEALTHCHECK ツールを使用した信頼のスクリーニング

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のスタンドアロン手動テストを実行するには、次の手順に従います。

Healthcheck ツールには多くのテストが含まれているため、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、および重大な問題について 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9章 IDM HEALTHCHECK を使用したシステム証明書の検証

Healthcheck ツールを使用して Identity Management (IdM) のシステム証明書の問題を特定する方法について詳しく説明します。

詳細は以下を参照してください。

IdM の Healthcheck

9.1. 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

このテストでは、NSS データベース内の CA (認証局) 証明書を、**CS.cfg** に保存されている同じ値と比較します。一致しない場合、CA は起動に失敗します。
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、以下を確認します。

- **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
- IdM が CA を検出できること
- 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

このテストでは、**cert-show** を実行して CA から期待される結果 (証明書または not found) が返されることを確認する必要があるため、シリアル番号 #1 の証明書がチェックされます。

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てください。

9.2. HEALTHCHECK を使用したシステム証明書のスクリーニング

Healthcheck ツールを使用して Identity Management (IdM) 証明書のスタンドアロン手動テストを実行するには、次の手順に従います。

Healthcheck ツールには多くのテストが含まれているため、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

- DogTag 証明書に限定して Healthcheck を実行するには、次のように入力します。

```
# 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10章 IDM HEALTHCHECK を使用した証明書の検証

Identity Management (IdM) の Healthcheck ツールを使用し、**certmonger** によって維持されている IPA 証明書の問題を特定する方法について詳しく説明します。

詳細は IdM の Healthcheck を参照してください。

10.1. 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 を使用したサービスの IdM 証明書の取得 を参照してください。

この一連のテストでは、有効期限、検証、信頼性、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
```

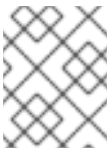
すべてのテストは、**ipahealthcheck.ipa.certs** ソースの下にあります。

IPACertmongerExpirationCheck

このテストでは、**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。ファイルを開いた後、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。

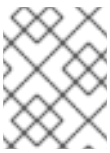


注記

certmonger は、証明書の有効期限に関する独自のビューをロードして維持します。このチェックでは、ディスク上の証明書は検証されません。

IPACertfileExpirationCheck

このテストでは、証明書ファイルまたは NSS データベースを開けないかどうかを確認します。このテストでは、有効期限も確認します。そのため、エラーまたは警告出力の **msg** 属性をよく読んでください。このメッセージは問題を特定するものです。



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、別のエラーが出力される可能性があります。

IPACertNSSTrust

このテストでは、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、追跡される証明書では、期待される値と信頼が比較されます。一致しないとエラーが発生します。

IPANSSChainValidation

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

IPAOpenSSLChainValidation

このテストでは、OpenSSL 証明書の証明書チェーンを検証します。**NSSChain** 検証と比較するために、実行する OpenSSL コマンドを以下に示します。

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

IPARAAgent

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

IPACertRevocation

このテストでは、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 の認証局 (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、IPA という名前の CA があります。IPA 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します。

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。

10.2. HEALTHCHECK ツールを使用した証明書のスクリーニング

Healthcheck ツールを使用して Identity Management (IdM) 証明書ヘルスチェックのスタンドアロン手動テストを実行するには、次の手順に従います。

Healthcheck ツールには多くのテストが含まれているため、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

- **root** ユーザーとして Healthcheck テストを実行する必要があります。

手順

- 証明書に関する警告、エラー、および重大な問題について 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.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]"
  }
}
```

上記の **IPACertfileExpirationCheck** テストは、NSS データベースを開くときに失敗しています。

関連情報

- **man ipa-healthcheck** を参照してください。