



# Red Hat Enterprise Linux 9

## Utiliser IdM Healthcheck pour surveiller votre environnement IdM

Effectuer des contrôles d'état et de santé



# Red Hat Enterprise Linux 9 Utiliser IdM Healthcheck pour surveiller votre environnement IdM

---

Effectuer des contrôles d'état et de santé

## Notice légale

Copyright © 2023 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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

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

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> 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<sup>®</sup> 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.

## Résumé

L'utilitaire ipa-healthcheck aide les administrateurs à détecter les problèmes dans un environnement Red Hat Identity Management (IdM). Cela inclut les vérifications de l'état des services IdM, les permissions des fichiers de configuration, les états de réplication et les problèmes liés aux certificats.

## Table des matières

<b>RENDRE L'OPEN SOURCE PLUS INCLUSIF</b> .....	<b>3</b>
<b>FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT</b> .....	<b>4</b>
<b>CHAPITRE 1. INSTALLATION ET EXÉCUTION DE L'OUTIL IDM HEALTHCHECK</b> .....	<b>5</b>
1.1. CONTRÔLE DE SANTÉ DANS L'IDM	5
1.2. INSTALLATION DE IDM HEALTHCHECK	6
1.3. EXÉCUTION DU CONTRÔLE DE SANTÉ DE L'IDM	6
1.4. ROTATION DES GRUMES	6
1.5. CONFIGURATION DE LA ROTATION DES JOURNAUX À L'AIDE DU CONTRÔLE DE SANTÉ IDM	7
1.6. MODIFICATION DE LA CONFIGURATION DU CONTRÔLE DE SANTÉ DE L'IDM	8
1.7. CONFIGURATION DE HEALTHCHECK POUR MODIFIER LE FORMAT DES JOURNAUX DE SORTIE	8
1.8. RESSOURCES SUPPLÉMENTAIRES	9
<b>CHAPITRE 2. VÉRIFICATION DES SERVICES À L'AIDE DE IDM HEALTHCHECK</b> .....	<b>10</b>
2.1. SERVICES TEST DU BILAN DE SANTÉ	10
2.2. SERVICES DE DÉPISTAGE UTILISANT LE HEALTHCHECK	10
<b>CHAPITRE 3. VÉRIFICATION DE L'ESPACE DISQUE À L'AIDE DE IDM HEALTHCHECK</b> .....	<b>12</b>
3.1. TEST DE CONTRÔLE DE L'ESPACE DISQUE	12
3.2. CONTRÔLE DE L'ESPACE DISQUE À L'AIDE DE L'OUTIL HEALTHCHECK	13
<b>CHAPITRE 4. VÉRIFICATION DES AUTORISATIONS DES FICHIERS DE CONFIGURATION IDM À L'AIDE DE HEALTHCHECK</b> .....	<b>14</b>
4.1. AUTORISATIONS DE FICHIERS TESTS DE CONTRÔLE DE SANTÉ	14
4.2. CONTRÔLE DES FICHIERS DE CONFIGURATION À L'AIDE DE HEALTHCHECK	15
<b>CHAPITRE 5. VÉRIFICATION DES ENREGISTREMENTS DNS À L'AIDE DE IDM HEALTHCHECK</b> .....	<b>17</b>
5.1. TEST DE VÉRIFICATION DES ENREGISTREMENTS DNS	17
5.2. VÉRIFICATION DES ENREGISTREMENTS DNS À L'AIDE DE L'OUTIL HEALTHCHECK	17
<b>CHAPITRE 6. VÉRIFICATION DU NOMBRE OPTIMAL DE PROCESSUS DE TRAVAIL DU KDC À L'AIDE D'IDM HEALTHCHECK</b> .....	<b>19</b>
<b>CHAPITRE 7. VÉRIFICATION DE LA RÉPLICATION DE L'IDM À L'AIDE DE HEALTHCHECK</b> .....	<b>21</b>
7.1. TESTS DE CONTRÔLE DE LA SANTÉ DE LA RÉPLICATION	21
7.2. VÉRIFICATION DE LA RÉPLICATION À L'AIDE DE HEALTHCHECK	21
<b>CHAPITRE 8. VÉRIFICATION DE LA CONFIGURATION DE L'IDM ET DE LA CONFIANCE DANS AD À L'AIDE DE IDM HEALTHCHECK</b> .....	<b>23</b>
8.1. TESTS DE CONTRÔLE DE CONFIANCE IDM ET AD	23
8.2. CONTRÔLE DE LA CONFIANCE À L'AIDE DE L'OUTIL HEALTHCHECK	24
<b>CHAPITRE 9. VÉRIFICATION DES CERTIFICATS SYSTÈME À L'AIDE DE IDM HEALTHCHECK</b> .....	<b>25</b>
9.1. CERTIFICATS DE SYSTÈME TESTS DE CONTRÔLE DE SANTÉ	25
9.2. CONTRÔLE DES CERTIFICATS DE SYSTÈME À L'AIDE DE HEALTHCHECK	26
<b>CHAPITRE 10. VÉRIFICATION DES CERTIFICATS À L'AIDE DE IDM HEALTHCHECK</b> .....	<b>27</b>
10.1. CERTIFICATS IDM TESTS DE CONTRÔLE DE SANTÉ	27
10.2. CERTIFICATS DE DÉPISTAGE À L'AIDE DE L'OUTIL HEALTHCHECK	28



## RENDRE L'OPEN SOURCE PLUS INCLUSIF

Red Hat s'engage à remplacer les termes problématiques dans son code, sa documentation et ses propriétés Web. Nous commençons par ces quatre termes : master, slave, blacklist et whitelist. En raison de l'ampleur de cette entreprise, ces changements seront mis en œuvre progressivement au cours de plusieurs versions à venir. Pour plus de détails, voir le [message de notre directeur technique Chris Wright](#).

## FOURNIR UN RETOUR D'INFORMATION SUR LA DOCUMENTATION DE RED HAT

Nous apprécions vos commentaires sur notre documentation. Faites-nous savoir comment nous pouvons l'améliorer.

### Soumettre des commentaires sur des passages spécifiques

1. Consultez la documentation au format **Multi-page HTML** et assurez-vous que le bouton **Feedback** apparaît dans le coin supérieur droit après le chargement complet de la page.
2. Utilisez votre curseur pour mettre en évidence la partie du texte que vous souhaitez commenter.
3. Cliquez sur le bouton **Add Feedback** qui apparaît près du texte en surbrillance.
4. Ajoutez vos commentaires et cliquez sur **Submit**.

### Soumettre des commentaires via Bugzilla (compte requis)

1. Connectez-vous au site Web de [Bugzilla](#).
2. Sélectionnez la version correcte dans le menu **Version**.
3. Saisissez un titre descriptif dans le champ **Summary**.
4. Saisissez votre suggestion d'amélioration dans le champ **Description**. Incluez des liens vers les parties pertinentes de la documentation.
5. Cliquez sur **Submit Bug**.



# CHAPITRE 1. INSTALLATION ET EXÉCUTION DE L'OUTIL IDM HEALTHCHECK

Ce chapitre décrit l'outil IdM Healthcheck et explique comment l'installer et l'exécuter.

## 1.1. CONTRÔLE DE SANTÉ DANS L'IDM

L'outil Healthcheck de la gestion des identités (IdM) permet de détecter les problèmes susceptibles d'affecter la santé de votre environnement IdM.



### NOTE

L'outil Healthcheck est un outil de ligne de commande qui peut être utilisé sans authentification Kerberos.

### Les modules sont indépendants

Le Healthcheck se compose de modules indépendants qui testent les éléments suivants

- Problèmes de réplication
- Validité du certificat
- Questions relatives à l'infrastructure de l'autorité de certification
- Questions relatives à la confiance dans IdM et Active Directory
- Autorisations d'accès aux fichiers et paramètres de propriété corrects

### Deux formats de sortie

Healthcheck génère les sorties suivantes, que vous pouvez définir à l'aide de l'option **output-type**:

- **json**: Sortie lisible par la machine au format JSON (par défaut)
- **human**: Sortie lisible par l'homme

Vous pouvez spécifier une autre destination de fichier avec l'option **--output-file**.

### Résultats

Chaque module de contrôle de santé renvoie l'un des résultats suivants :

#### SUCCÈS

configuré comme prévu

#### AVERTISSEMENT

il ne s'agit pas d'une erreur, mais cela vaut la peine de garder un œil ou d'évaluer la situation

#### ERREUR

n'est pas configuré comme prévu

#### CRITIQUE

n'est pas configuré comme prévu, avec un risque élevé d'impact

## 1.2. INSTALLATION DE IDM HEALTHCHECK

Cette section décrit comment installer l'outil IdM Healthcheck.

### Procédure

- Installez le paquetage **ipa-healthcheck**:

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

### Verification steps

- Utilisez l'option **--failures-only** pour que **ipa-healthcheck** ne signale que les erreurs. Une installation IdM fonctionnant parfaitement renvoie un résultat vide de [].

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

### Ressources supplémentaires

- Utilisez **ipa-healthcheck --help** pour voir tous les arguments soutenus.

## 1.3. EXÉCUTION DU CONTRÔLE DE SANTÉ DE L'IDM

Le bilan de santé peut être exécuté manuellement ou automatiquement à l'aide de la [rotation des journaux](#)

### Conditions préalables

- L'outil Healthcheck doit être installé. Voir [Installation de IdM Healthcheck](#).

### Procédure

- Pour exécuter manuellement le contrôle de santé, entrez la commande **ipa-healthcheck**.

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

### Ressources supplémentaires

Pour toutes les options, voir la page de manuel : **man ipa-healthcheck**.

## 1.4. ROTATION DES GRUMES

La rotation du journal crée un nouveau fichier journal chaque jour, et les fichiers sont organisés par date. Les fichiers journaux étant enregistrés dans le même répertoire, vous pouvez sélectionner un fichier journal particulier en fonction de la date.

La rotation signifie qu'un nombre est configuré pour le nombre maximal de fichiers journaux et que, si ce nombre est dépassé, le fichier le plus récent réécrit et renomme le plus ancien. Par exemple, si le nombre de rotation est de 30, le trente et unième fichier journal remplace le premier (le plus ancien).

La rotation des journaux réduit les fichiers journaux volumineux et les organise, ce qui peut faciliter l'analyse des journaux.

## 1.5. CONFIGURATION DE LA ROTATION DES JOURNAUX À L'AIDE DU CONTRÔLE DE SANTÉ IDM

Cette section décrit comment configurer une rotation des journaux avec :

- le minuteur **systemd**
- le service **crond**

La minuterie **systemd** exécute périodiquement l'outil Healthcheck et génère les journaux. La valeur par défaut est fixée à 4 heures du matin tous les jours.

Le service **crond** est utilisé pour la rotation des journaux.

Le nom du journal par défaut est **healthcheck.log** et les journaux en rotation utilisent le format **healthcheck.log-YYYYMMDD**.

### Conditions préalables

- Vous devez exécuter les commandes en tant que root.

### Procédure

1. Activer une minuterie **systemd**:

```
# 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. Lancez la minuterie **systemd**:

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

3. Ouvrez le fichier **/etc/logrotate.d/ipahealthcheck** pour configurer le nombre de journaux à enregistrer.

Par défaut, la rotation des journaux est fixée à 30 jours.

4. Dans le fichier **/etc/logrotate.d/ipahealthcheck**, configurez le chemin d'accès aux journaux. Par défaut, les journaux sont enregistrés dans le répertoire **/var/log/ipa/healthcheck/**.

5. Dans le fichier **/etc/logrotate.d/ipahealthcheck**, configurez l'heure de génération des journaux. Par défaut, un journal est créé quotidiennement à 4 heures du matin.

6. Pour utiliser la rotation des journaux, assurez-vous que le service **crond** est activé et en cours d'exécution :

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

Pour commencer à générer des journaux, démarrez le service de contrôle de santé de l'IPA :

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

Pour vérifier le résultat, allez sur `/var/log/ipa/healthcheck/` et vérifiez si les journaux sont créés correctement.

## 1.6. MODIFICATION DE LA CONFIGURATION DU CONTRÔLE DE SANTÉ DE L'IDM

Vous pouvez modifier les paramètres de Healthcheck en ajoutant les options de ligne de commande souhaitées au fichier `/etc/ipahealthcheck/ipahealthcheck.conf`. Cela peut s'avérer utile lorsque, par exemple, vous avez configuré une rotation des journaux et que vous souhaitez vous assurer que les journaux sont dans un format adapté à l'analyse automatique, mais que vous ne souhaitez pas mettre en place un nouveau minuteur.



### NOTE

Cette fonction de contrôle de santé n'est disponible que sur RHEL 9.1 et les versions plus récentes.

Après la modification, tous les journaux créés par Healthcheck suivent les nouveaux paramètres. Ces paramètres s'appliquent également à toute exécution manuelle de Healthcheck.



### NOTE

Lors de l'exécution manuelle de Healthcheck, les paramètres du fichier de configuration sont prioritaires sur les options spécifiées dans la ligne de commande. Par exemple, si **output\_type** est défini sur **human** dans le fichier de configuration, le fait de spécifier **json** sur la ligne de commande n'a aucun effet. Toutes les options de la ligne de commande que vous utilisez et qui ne sont pas spécifiées dans le fichier de configuration sont appliquées normalement.

### Ressources supplémentaires

- [Configuration de la rotation des journaux à l'aide du contrôle de santé IdM](#)

## 1.7. CONFIGURATION DE HEALTHCHECK POUR MODIFIER LE FORMAT DES JOURNAUX DE SORTIE

Cette procédure décrit comment configurer Healthcheck avec un minuteur déjà configuré. Dans cet exemple, vous configurez Healthcheck pour qu'il produise des journaux dans un format lisible par l'homme et pour qu'il inclue également les résultats positifs au lieu des seules erreurs.

### Conditions préalables

- Votre système est équipé de RHEL 9.1 ou d'une version ultérieure.
- Vous avez des privilèges **root**.
- Vous avez précédemment configuré la rotation des journaux sur une minuterie.

### Procédure

1. Ouvrez le fichier `/etc/ipahealthcheck/ipahealthcheck.conf` dans un éditeur de texte.
2. Ajouter les options `output_type=human` et `all=True` à la section `[default]`.
3. Enregistrez et fermez le fichier.

### Vérification

1. Exécuter le Healthcheck manuellement :

```
█ # ipa-healthcheck
```

2. Allez sur `/var/log/ipa/healthcheck/` et vérifiez que les journaux sont dans le bon format.

### Ressources supplémentaires

- [Configuration de la rotation des journaux à l'aide du contrôle de santé IdM](#)

## 1.8. RESSOURCES SUPPLÉMENTAIRES

- Voir les sections suivantes du guide [Utilisation d'IdM Healthcheck pour surveiller votre environnement IdM](#) pour des exemples d'utilisation d'IdM Healthcheck.
  - [Services de contrôle](#)
  - [Vérification de la configuration de la confiance IdM et AD](#)
  - [Vérification des certificats](#)
  - [Vérification des certificats du système](#)
  - [Vérification de l'espace disque](#)
  - [Vérification des autorisations des fichiers de configuration de l'IdM](#)
  - [Vérification de la réplication](#)

## CHAPITRE 2. VÉRIFICATION DES SERVICES À L'AIDE DE IDM HEALTHCHECK

Cette section décrit les services de surveillance utilisés par le serveur de gestion des identités (IdM) à l'aide de l'outil Healthcheck.

For details, see

[Contrôle de santé dans l'IdM.](#)

### 2.1. SERVICES TEST DU BILAN DE SANTÉ

L'outil Healthcheck comprend un test permettant de vérifier si l'un des services IdM n'est pas en cours d'exécution. Ce test est important car les services qui ne fonctionnent pas peuvent entraîner des défaillances dans d'autres tests. Par conséquent, vérifiez d'abord que tous les services fonctionnent. Vous pouvez ensuite vérifier les résultats de tous les autres tests.

Pour voir tous les tests de services, exécutez **ipa-healthcheck** avec l'option **--list-sources**:

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

Vous trouverez tous les services testés avec le Healthcheck sous la source **ipahealthcheck.meta.services**:

- marchand de cerises
- dirsrv
- gssproxy
- httpd
- ipa\_custodia
- ipa\_dnskeysyncd
- ipa\_otpd
- kadmin
- krb5kdc
- nommée
- pki\_tomcatd
- sssd



#### NOTE

Exécutez ces tests sur tous les serveurs IdM lorsque vous essayez de découvrir des problèmes.

### 2.2. SERVICES DE DÉPISTAGE UTILISANT LE HEALTHCHECK

Cette section décrit un test manuel autonome des services fonctionnant sur le serveur de gestion des identités (IdM) à l'aide de l'outil Healthcheck.

L'outil Healthcheck comprend de nombreux tests, dont les résultats peuvent être abrégés avec :

- à l'exclusion de tout test réussi : **--failures-only**
- ne comprenant que des tests de services : **--source=ipahealthcheck.meta.services**

### Procédure

- Pour lancer le Healthcheck avec les avertissements, les erreurs et les problèmes critiques concernant les services, entrez :

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

Un test réussi affiche des crochets vides :

```
[]
```

Si l'un des services échoue, le résultat peut ressembler à cet exemple :

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

### Ressources supplémentaires

- Voir **man ipa-healthcheck**.

## CHAPITRE 3. VÉRIFICATION DE L'ESPACE DISQUE À L'AIDE DE IDM HEALTHCHECK

Cette section décrit comment surveiller l'espace disque libre du serveur de gestion des identités à l'aide de l'outil Healthcheck.

Pour plus de détails, voir [Healthcheck in IdM](#).

### 3.1. TEST DE CONTRÔLE DE L'ESPACE DISQUE

L'outil Healthcheck comprend un test de vérification de l'espace disque disponible. Un espace disque libre insuffisant peut entraîner des problèmes :

- Enregistrement
- Exécution
- Sauvegardes

Le test vérifie les chemins d'accès suivants :

Tableau 3.1. Chemins testés

Chemins vérifiés par le test	Espace disque minimal en Mo
<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

Pour obtenir la liste de tous les tests, exécutez le programme **ipa-healthcheck** avec l'option **--list-sources**:

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

Vous trouverez le test de vérification de l'espace du système de fichiers sur le site **ipahealthcheck.system.filesystemspace** source :

#### Vérification de l'espace du système de fichiers

Ce test vérifie l'espace disque disponible de la manière suivante :

- Le nombre minimum d'octets libres bruts nécessaires.
- Le pourcentage - l'espace disque libre minimum est codé en dur à 20%.



## 3.2. CONTRÔLE DE L'ESPACE DISQUE À L'AIDE DE L'OUTIL HEALTHCHECK

Cette section décrit un test manuel autonome de l'espace disque disponible sur un serveur de gestion des identités (IdM) à l'aide de l'outil Healthcheck.

Comme le bilan de santé comprend de nombreux tests, vous pouvez restreindre les résultats en fonction des critères suivants :

- à l'exclusion de tout test réussi : **--failures-only**
- comprenant uniquement des tests de contrôle de l'espace : **--source=ipahealthcheck.system.filesystemspace**

### Procédure

- Pour exécuter le Healthcheck avec les avertissements, les erreurs et les problèmes critiques concernant l'espace disque disponible, entrez :

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

Un test réussi affiche des crochets vides :

```
[]
```

Par exemple, un test qui a échoué peut s'afficher :

```
{
  "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
  }
}
```

L'échec du test vous informe que le répertoire **/var/lib/dirsrv** n'a plus d'espace disponible.

### Ressources supplémentaires

- Voir **man ipa-healthcheck**.

# CHAPITRE 4. VÉRIFICATION DES AUTORISATIONS DES FICHIERS DE CONFIGURATION IDM À L'AIDE DE HEALTHCHECK

Cette section explique comment tester les fichiers de configuration de la gestion des identités (IdM) à l'aide de l'outil Healthcheck.

For details, see

[Contrôle de santé dans l'IdM.](#)

## 4.1. AUTORISATIONS DE FICHIERS TESTS DE CONTRÔLE DE SANTÉ

L'outil Healthcheck teste la propriété et les permissions de certains fichiers importants installés ou configurés par Identity Management (IdM).

Si vous modifiez la propriété ou les autorisations d'un fichier testé, le test renvoie un avertissement dans la section **result**. Bien que cela ne signifie pas nécessairement que la configuration ne fonctionnera pas, cela signifie que le fichier diffère de la configuration par défaut.

Pour voir tous les tests, exécutez le programme **ipa-healthcheck** avec l'option **--list-sources**:

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

Vous trouverez le test de permissions de fichiers sous la source **ipahealthcheck.ipa.files**:

### IPAFileNSSDBCheck

Ce test vérifie la base de données 389-ds NSS et la base de données de l'autorité de certification (CA). La base de données 389-ds se trouve à l'adresse **/etc/dirsrv/slapd-*<dashed-REALM>*** et la base de données de l'autorité de certification à l'adresse **/etc/pki/pki-tomcat/alias/**.

### IPAFileCheck

Ce test vérifie les fichiers suivants :

- **/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**  
Si PKINIT est activé :
- **/var/lib/ipa/certs/kdc.pem**
- **/var/lib/ipa/private/kdc.key**  
Si le DNS est configuré :
- **/etc/named.keytab**

- **/etc/ipa/dnssec/ipa-dnskeysyncd.keytab**

### TomcatFileCheck

Ce test vérifie certains fichiers spécifiques à Tomcat si une autorité de certification est configurée :

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



#### NOTE

Exécutez ces tests sur tous les serveurs IdM lorsque vous essayez de trouver des problèmes.

## 4.2. CONTRÔLE DES FICHIERS DE CONFIGURATION À L'AIDE DE HEALTHCHECK

Cette section décrit un test manuel autonome des fichiers de configuration d'un serveur de gestion d'identité (IdM) à l'aide de l'outil Healthcheck.

L'outil Healthcheck comprend de nombreux tests. Les résultats peuvent être réduits en fonction des critères suivants

- à l'exclusion de tout test réussi : **--failures-only**
- ne comprenant que des tests de propriété et de permissions : **--source=ipahealthcheck.ipa.files**

### Procédure

1. Pour effectuer des tests de contrôle de santé sur la propriété et les autorisations du fichier de configuration IdM, tout en affichant uniquement les avertissements, les erreurs et les problèmes critiques, entrez :

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

Un test réussi affiche des crochets vides :

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

Les tests qui échouent affichent des résultats similaires à ceux qui suivent : **WARNING:**

```
{
  "source": "ipahealthcheck.ipa.files",
  "check": "IPAFileNSSDBCheck",
  "result": "WARNING",
  "kw": {
    "key": "_etc_dirsrv_slapd-EXAMPLE-TEST_pkcs11.txt_mode",
    "path": "/etc/dirsrv/slappd-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"  
}  
}
```

### Ressources supplémentaires

- Voir **man ipa-healthcheck**.

## CHAPITRE 5. VÉRIFICATION DES ENREGISTREMENTS DNS À L'AIDE DE IDM HEALTHCHECK

Cette section décrit un outil de contrôle de santé dans la gestion des identités (IdM) qui permet d'identifier les problèmes liés aux enregistrements DNS.

### 5.1. TEST DE VÉRIFICATION DES ENREGISTREMENTS DNS

L'outil Healthcheck comprend un test permettant de vérifier que les enregistrements DNS requis pour l'autodécouverte peuvent être résolus.

Pour obtenir la liste de tous les tests, exécutez le programme **ipa-healthcheck** avec l'option **--list-sources**:

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

Vous trouverez le test de vérification des enregistrements DNS sous la source **ipahealthcheck.ipa.idns**.

#### IPADNSSystemRecordsCheck (vérification des enregistrements du système)

Ce test vérifie les enregistrements DNS de la commande **ipa dns-update-system-records --dry-run** en utilisant le premier résolveur spécifié dans le fichier **/etc/resolv.conf**. Les enregistrements sont testés sur le serveur IPA.

### 5.2. VÉRIFICATION DES ENREGISTREMENTS DNS À L'AIDE DE L'OUTIL HEALTHCHECK

Cette section décrit un test manuel autonome des enregistrements DNS sur un serveur de gestion des identités (IdM) à l'aide de l'outil Healthcheck.

L'outil Healthcheck comprend de nombreux tests. Il est possible de réduire les résultats en n'incluant que les tests des enregistrements DNS en ajoutant l'option **--source ipahealthcheck.ipa.idns**.

#### Conditions préalables

- Vous devez effectuer les tests Healthcheck en tant qu'utilisateur **root**.

#### Procédure

- Pour lancer la vérification des enregistrements DNS, entrez :

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

Si l'enregistrement peut être résolu, le test renvoie le résultat **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."  
}
```

Le test renvoie une adresse **WARNING** lorsque, par exemple, le nombre d'enregistrements ne correspond pas au nombre attendu :

```
{  
  "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  
  }  
}
```

### Ressources supplémentaires

- Voir **man ipa-healthcheck**.

## CHAPITRE 6. VÉRIFICATION DU NOMBRE OPTIMAL DE PROCESSUS DE TRAVAIL DU KDC À L'AIDE D'IDM HEALTHCHECK

Vous pouvez utiliser l'outil Healthcheck dans Identity Management (IdM) pour vérifier que le Centre de distribution de clés Kerberos (KDC) est configuré pour utiliser le nombre optimal de processus de travail **krb5kdc**, qui doit être égal au nombre de cœurs de CPU sur l'hôte.

Vous trouverez le test du nombre correct de processus KDC worker sous la source **ipahealthcheck.ipa.kdc**. Comme l'outil Healthcheck comprend de nombreux tests, vous pouvez limiter les résultats en n'incluant que les tests du travailleur KDC en ajoutant l'option **--source ipahealthcheck.ipa.kdc**.

### Conditions préalables

- L'outil KDC worker process Healthcheck n'est disponible que sur RHEL 8.7 ou plus récent.
- Vous devez effectuer les tests Healthcheck en tant qu'utilisateur **root**.

### Procédure

- Pour vérifier les processus de travail du KDC, entrez :

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

Si le nombre de processus de travail du KDC correspond au nombre de cœurs de l'unité centrale, le test renvoie **SUCCESS**:

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

Le test renvoie une adresse **WARNING** si le nombre de processus de travail ne correspond pas au nombre de cœurs de l'unité centrale. Dans l'exemple suivant, un hôte avec 2 cœurs est configuré pour n'avoir qu'un seul processus KDC :

```
{
  "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}"
  }
}

```

Le test produit également un message **WARNING** s'il n'y a pas de travailleurs configurés. Dans l'exemple suivant, la variable **KRB5KDC\_ARGS** est absente du fichier de configuration **/etc/sysconfig/krb5kdc**:

```

{
  "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}"
  }
}

```

### Ressources supplémentaires

- **man ipa-healthcheck**



## CHAPITRE 7. VÉRIFICATION DE LA RÉPLICATION DE L'IDM À L'AIDE DE HEALTHCHECK

Cette section décrit comment tester la réplication de la gestion des identités (IdM) à l'aide de l'outil Healthcheck.

Pour plus de détails, voir [Healthcheck in IdM](#).

### 7.1. TESTS DE CONTRÔLE DE LA SANTÉ DE LA RÉPLICATION

L'outil Healthcheck teste la configuration de la topologie de la gestion des identités (IdM) et recherche les conflits de réplication.

Pour obtenir la liste de tous les tests, exécutez le programme **ipa-healthcheck** avec l'option **--list-sources**:

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

Les tests de topologie sont placés sous les sources **ipahealthcheck.ipa.topology** et **ipahealthcheck.ds.replication**:

#### IPATopologyDomainCheck (vérification de l'opologie du domaine)

Ce test permet de vérifier

- si la topologie n'est pas déconnectée et s'il existe des chemins de réplication entre tous les serveurs.
- si les serveurs n'ont pas plus que le nombre recommandé d'accords de réplication. Si le test échoue, il renvoie des erreurs, telles que des erreurs de connexion ou un trop grand nombre d'accords de réplication.

Si le test réussit, il renvoie les domaines configurés.



#### NOTE

Le test exécute la commande **ipa topologysuffix-verify** pour les suffixes domain et ca (en supposant que l'autorité de certification soit configurée sur ce serveur).

#### ReplicationConflictCheck

Le test recherche dans LDAP les entrées correspondant à **(&(!(objectclass=nstombstone))(nsds5ReplConflict=\*))**.



#### NOTE

Exécutez ces tests sur tous les serveurs IdM lorsque vous essayez de vérifier s'il y a des problèmes.

### 7.2. VÉRIFICATION DE LA RÉPLICATION À L'AIDE DE HEALTHCHECK

Cette section décrit un test manuel autonome de la topologie et de la configuration de la réplication d'Identity Management (IdM) à l'aide de l'outil Healthcheck.

L'outil Healthcheck comprend de nombreux tests, ce qui vous permet d'abrégier les résultats :

- Test de conflit de réplication : **--source=ipahealthcheck.ds.replication**
- Test de topologie correct : **--source=ipahealthcheck.ipa.topology**

### Conditions préalables

- Vous devez effectuer les tests Healthcheck en tant qu'utilisateur **root**.

### Procédure

- Pour exécuter les vérifications de conflit de réplication et de topologie Healthcheck, entrez :

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

Quatre résultats différents sont possibles :

- SUCCESS - le test s'est déroulé avec succès.

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

- AVERTISSEMENT - le test a réussi mais il pourrait y avoir un problème.
- ERROR - le test a échoué.

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

- CRITIQUE - le test a échoué et affecte la fonctionnalité du serveur IdM.

### Ressources supplémentaires

- Voir **man ipa-healthcheck**.

## CHAPITRE 8. VÉRIFICATION DE LA CONFIGURATION DE L'IDM ET DE LA CONFIANCE DANS AD À L'AIDE DE IDM HEALTHCHECK

Cette section vous aide à comprendre et à utiliser l'outil Healthcheck de la gestion des identités (IdM) pour identifier les problèmes liés à IdM et à une confiance Active Directory.

### 8.1. TESTS DE CONTRÔLE DE CONFIANCE IDM ET AD

L'outil Healthcheck comprend plusieurs tests permettant de vérifier l'état de votre gestion des identités (IdM) et de votre confiance dans Active Directory (AD).

Pour voir tous les tests de confiance, exécutez **ipa-healthcheck** avec l'option **--list-sources**:

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

Vous trouverez tous les tests sous la source **ipahealthcheck.ipa.trust**:

#### IPATrustAgentCheck

Ce test vérifie la configuration SSSD lorsque la machine est configurée en tant qu'agent de confiance. Pour chaque domaine dans **/etc/sss/sss.conf** où **id\_provider=ipa** s'assurer que **ipa\_server\_mode** est **True**.

#### Vérification des domaines de confiance (IPATrustDomainsCheck)

Ce test vérifie si les domaines de confiance correspondent aux domaines SSSD en comparant la liste des domaines de **sssctl domain-list** à la liste des domaines de **ipa trust-find**, à l'exclusion du domaine IPA.

#### Vérification du catalogue IPATrust

Ce test résout un utilisateur AD, **Administrator@REALM**. Les valeurs du catalogue global AD et du contrôleur de domaine AD sont ainsi renseignées dans la sortie **sssctl domain-status**.

Pour chaque domaine de confiance, recherchez l'utilisateur dont l'identifiant est le SID 500 (l'administrateur), puis vérifiez la sortie de **sssctl domain-status <domain> --active-server** pour vous assurer que le domaine est actif.

#### IPAsidgenpluginCheck

Ce test vérifie que le plugin **sidgen** est activé dans l'instance IPA 389-ds. Ce test vérifie également que les plugins **IPA SIDGEN** et **ipa-sidgen-task** dans **cn=plugins,cn=config** incluent l'option **nsslapd-pluginEnabled**.

#### IPATrustAgentMemberCheck (vérification des membres de l'agent de confiance)

Ce test vérifie que l'hôte actuel est membre de **cn=adtrust agents,cn=sysaccounts,cn=etc,SUFFIX**.

#### IPATrustControllerPrincipalCheck (vérification du principe)

Ce test vérifie que l'hôte actuel est membre de **cn=adtrust agents,cn=sysaccounts,cn=etc,SUFFIX**.

#### IPATrustControllerServiceCheck

Ce test vérifie que l'hôte actuel démarre le service ADTRUST dans ipactl.

#### IPATrustControllerConfCheck (vérification de la confiance)

Ce test vérifie que **ldapi** est activé pour le backend passdb dans la sortie de **net conf list**.

#### IPATrustControllerGroupSIDCheck (vérification de l'identité du groupe)

Ce test vérifie que le SID du groupe admins se termine par 512 (Domain Admins RID).

### IPATrustPackageCheck (vérification du paquet)

Ce test vérifie que le paquet **trust-ad** est installé si le contrôleur de confiance et la confiance AD ne sont pas activés.



#### NOTE

Exécutez ces tests sur tous les serveurs IdM lorsque vous essayez de trouver un problème.

## 8.2. CONTRÔLE DE LA CONFIANCE À L'AIDE DE L'OUTIL HEALTHCHECK

Cette section décrit un test manuel autonome d'un contrôle de confiance de la gestion des identités (IdM) et d'Active Directory (AD) à l'aide de l'outil Healthcheck.

L'outil Healthcheck comprend de nombreux tests, ce qui vous permet d'abrégier les résultats :

- à l'exclusion de tout test réussi : **--failures-only**
- ne comprenant que des tests de confiance : **--source=ipahealthcheck.ipa.trust**

### Procédure

- Pour lancer le Healthcheck avec les avertissements, les erreurs et les problèmes critiques dans la confiance, entrez :

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

Un test réussi affiche des parenthèses vides :

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

### Ressources supplémentaires

- Voir **man ipa-healthcheck**.

## CHAPITRE 9. VÉRIFICATION DES CERTIFICATS SYSTÈME À L'AIDE DE IDM HEALTHCHECK

Cette section décrit un outil de contrôle de santé dans la gestion des identités (IdM) qui permet d'identifier les problèmes liés aux certificats du système.

For details, see

[Contrôle de santé dans l'IdM.](#)

### 9.1. CERTIFICATS DE SYSTÈME TESTS DE CONTRÔLE DE SANTÉ

L'outil Healthcheck comprend plusieurs tests de vérification des certificats du système (DogTag).

Pour voir tous les tests, exécutez le programme **ipa-healthcheck** avec l'option **--list-sources**:

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

Vous trouverez tous les tests sous la source **ipahealthcheck.dogtag.ca**:

#### DogtagCertsConfigCheck

Ce test compare les certificats de l'autorité de certification (CA) dans sa base de données NSS aux mêmes valeurs stockées dans **CS.cfg**. S'ils ne correspondent pas, l'autorité de certification ne démarre pas.

Plus précisément, il vérifie :

- **auditSigningCert cert-pki-ca** contre **ca.audit\_signing.cert**
- **ocspSigningCert cert-pki-ca** contre **ca.ocsp\_signing.cert**
- **caSigningCert cert-pki-ca** contre **ca.signing.cert**
- **subsystemCert cert-pki-ca** contre **ca.subsystem.cert**
- **Server-Cert cert-pki-ca** contre **ca.sslserver.cert**

Si Key Recovery Authority (KRA) est installé :

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

#### DogtagCertsConnectivityCheck (contrôle de connectivité)

Ce test vérifie la connectivité. Ce test est équivalent à la commande **ipa cert-show 1** qui vérifie :

- La configuration du proxy PKI dans Apache
- IdM capable de trouver une autorité de certification
- Le certificat du client de l'agent RA
- Exactitude des réponses de l'AC aux demandes

Notez que le test vérifie un certificat avec le numéro de série #1 parce que vous voulez vérifier qu'un **cert-show** peut être exécuté et obtenir un résultat attendu de la part de l'autorité de certification (soit le certificat, soit un résultat non trouvé).

**NOTE**

Exécutez ces tests sur tous les serveurs IdM lorsque vous essayez de trouver un problème.

## 9.2. CONTRÔLE DES CERTIFICATS DE SYSTÈME À L'AIDE DE HEALTHCHECK

Cette section décrit un test manuel autonome des certificats de gestion d'identité (IdM) à l'aide de l'outil Healthcheck.

Comme l'outil Healthcheck comprend de nombreux tests, vous pouvez restreindre les résultats en n'incluant que les tests DogTag : **--source=ipahealthcheck.dogtag.ca**

### Procédure

- Pour lancer un contrôle de santé limité aux certificats DogTag, entrez :

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

Un exemple de test réussi :

```
{
  "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"
  }
}
```

Exemple d'échec d'un test :

```
{
  "source: ipahealthcheck.dogtag.ca",
  "check: DogtagCertsConfigCheck",
  "result: CRITICAL",
  "uuid: 59d66200-1447-4b3b-be01-89810c803a98",
  "when: 20191008135912Z",
  "duration: 0.002022",
  "kw:" {
    "exception": "NSDB /etc/pki/pki-tomcat/alias not initialized",
  }
}
```

### Ressources supplémentaires

- Voir **man ipa-healthcheck**.

## CHAPITRE 10. VÉRIFICATION DES CERTIFICATS À L'AIDE DE IDM HEALTHCHECK

Cette section aide à comprendre et à utiliser l'outil Healthcheck de la gestion des identités (IdM) pour identifier les problèmes liés aux certificats IPA gérés par certmonger.

For details, see

[Contrôle de santé dans l'IdM.](#)

### 10.1. CERTIFICATS IDM TESTS DE CONTRÔLE DE SANTÉ

L'outil Healthcheck comprend plusieurs tests permettant de vérifier l'état des certificats gérés par certmonger dans Identity Management (IdM). Pour plus d'informations sur certmonger, voir [Obtention d'un certificat IdM pour un service à l'aide de certmonger.](#)

Cette série de tests vérifie l'expiration, la validation, la confiance et d'autres aspects. Plusieurs erreurs peuvent être générées pour le même problème sous-jacent.

Pour voir tous les tests de certificats, exécutez le programme **ipa-healthcheck** avec l'option **--list-sources**:

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

Vous trouverez tous les tests sous la source **ipahealthcheck.ipa.certs**:

#### IPACertmongerExpirationCheck (contrôle d'expiration)

Ce test vérifie les expirations dans **certmonger**.

Si une erreur est signalée, le certificat a expiré.

Si un avertissement apparaît, cela signifie que le certificat va bientôt expirer. Par défaut, ce test s'applique dans un délai de 28 jours ou moins avant l'expiration du certificat.

Vous pouvez configurer le nombre de jours dans le fichier **/etc/ipahealthcheck/ipahealthcheck.conf**. Après avoir ouvert le fichier, modifiez l'option **cert\_expiration\_days** située dans la section default.



#### NOTE

Certmonger charge et maintient sa propre vue de l'expiration du certificat. Cette vérification ne valide pas le certificat sur disque.

#### IPACertfileExpirationCheck (vérification de l'expiration du fichier de certification)

Ce test vérifie si le fichier de certificat ou la base de données NSS ne peut pas être ouvert. Ce test vérifie également l'expiration. Par conséquent, lisez attentivement l'attribut **msg** dans le message d'erreur ou d'avertissement. Le message précise le problème.



#### NOTE

Ce test vérifie le certificat sur disque. Si un certificat est manquant, illisible, etc., une erreur distincte peut également être soulevée.

### IPACertNSSTrust

Ce test compare la confiance dans les certificats stockés dans les bases de données du NSS. Pour les certificats suivis attendus dans les bases de données du SSN, la confiance est comparée à une valeur attendue et une erreur est soulevée en cas de non-concordance.

### IPANSSChainValidation

Ce test valide la chaîne de certificats des certificats NSS. Le test s'exécute : **certutil -V -u V -e -d [dbdir] -n [nickname]**

### IPAOpenSSLChainValidation

Ce test valide la chaîne des certificats OpenSSL. Pour être comparable à la validation **NSSChain**, voici la commande OpenSSL que nous exécutons :

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

### IPARAAgent

Ce test compare le certificat sur disque avec l'enregistrement équivalent dans LDAP à l'adresse **uid=ipara,ou=People,o=ipaca**.

### IPACertRevocation

Ce test utilise certmonger pour vérifier que les certificats n'ont pas été révoqués. Par conséquent, le test peut détecter les problèmes liés aux certificats gérés par certmonger uniquement.

### IPACertmongerCA

Ce test permet de vérifier la configuration de l'autorité de certification (AC) de certmonger. L'IdM ne peut pas délivrer de certificats sans autorité de certification.

Certmonger gère un ensemble d'aides d'AC. Dans IdM, il existe une autorité de certification nommée IPA qui délivre des certificats par l'intermédiaire d'IdM, en s'authentifiant en tant qu'hôte ou utilisateur principal, pour des certificats d'hôte ou de service.

Il y a aussi **dogtag-ipa-ca-renew-agent** et **dogtag-ipa-ca-renew-agent-reuse** qui renouvellent les certificats du sous-système de l'autorité de certification.



#### NOTE

Exécutez ces tests sur tous les serveurs IdM lorsque vous essayez de vérifier s'il y a des problèmes.

## 10.2. CERTIFICATS DE DÉPISTAGE À L'AIDE DE L'OUTIL HEALTHCHECK

Cette section décrit un test manuel autonome du contrôle de santé d'un certificat de gestion d'identité (IdM) à l'aide de l'outil Healthcheck.

L'outil Healthcheck comprend de nombreux tests, ce qui vous permet d'abrégier les résultats :

- à l'exclusion de tout test réussi : **--failures-only**
- ne comprenant que des tests de certificats : **--source=ipahealthcheck.ipa.certs**

#### Conditions préalables

- Vous devez effectuer les tests Healthcheck en tant qu'utilisateur **root**.



## Procédure

- Pour exécuter le contrôle de santé avec les avertissements, les erreurs et les problèmes critiques concernant les certificats, entrez :

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

Un test réussi affiche des parenthèses vides :

```
[]
```

L'échec du test se traduit par la sortie suivante :

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

Ce test **IPACertfileExpirationCheck** a échoué lors de l'ouverture de la base de données NSS.

## Ressources supplémentaires

- Voir **man ipa-healthcheck**.