Red Hat Enterprise Linux 9

Tirer le meilleur parti de votre expérience en matière de soutien

Collecte d'informations de dépannage sur les serveurs RHEL à l'aide de l'utilitaire sos

Last Updated: 2024-01-18

Red Hat Enterprise Linux 9 Tirer le meilleur parti de votre expérience en matière de soutien

Collecte d'informations de dépannage sur les serveurs RHEL à l'aide de l'utilitaire sos

Notice légale

Résumé

Recueillez les données de configuration, de diagnostic et de dépannage à l'aide de l'utilitaire sos et fournissez ces fichiers à l'assistance technique de Red Hat. L'équipe d'assistance peut analyser et étudier ces données afin de résoudre les demandes de service signalées dans votre dossier d'assistance.

Table des matières

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. GÉNÉRATION D'UN RAPPORT sos POUR LE SUPPORT TECHNIQUE

1.1. CE QUE FAIT L'UTILITAIRE sos

Un rapport **sos** est un point de départ courant pour les ingénieurs du support technique de Red Hat lorsqu'ils effectuent l'analyse d'une demande de service pour un système RHEL. L'utilitaire **sos** (également connu sous le nom de **sosreport**) fournit une méthode standardisée pour collecter des informations de diagnostic auxquelles les ingénieurs de l'assistance technique de Red Hat peuvent se référer tout au long de leur enquête sur les problèmes signalés dans les cas d'assistance. L'utilisation de l'utilitaire **sos** permet de s'assurer que l'on ne vous demandera pas à plusieurs reprises de fournir des données.

L'utilitaire **sos** permet de collecter diverses informations de débogage à partir d'un ou de plusieurs systèmes, de nettoyer éventuellement les données sensibles et de les télécharger sous la forme d'un rapport vers Red Hat. Plus précisément, les trois composants de **sos** effectuent les opérations suivantes :

- **sos report** collecte des informations de débogage à partir du système *one*.

NOTE

Ce programme s'appelait à l'origine **sosreport**. L'exécution de **sosreport** fonctionne toujours puisque **sos report** est appelé à la place, avec les mêmes arguments.

- **sos collect** permet d'exécuter et de collecter des rapports individuels sur le site **sos** à partir d'un ensemble de nœuds spécifiés.
- **sos clean** obscurcit les informations potentiellement sensibles telles que les noms d'utilisateurs, les noms d'hôtes, les adresses IP ou MAC, ou d'autres données spécifiées par l'utilisateur.

Les informations collectées dans un rapport contiennent des détails de configuration, des informations système et des informations de diagnostic d'un système RHEL, comme par exemple :

- La version du noyau en cours d'exécution.
- Modules du noyau chargés.
- Fichiers de configuration du système et des services.
- Sortie de la commande de diagnostic.
- Une liste des paquets installés.

L'utilitaire **sos** écrit les données qu'il recueille dans une archive nommée **sosreport-*<host_name>*-*<support_case_number>*-*<YYYY-MM-DD>*-*<unique_random_characters>*.tar.xz**.

L'utilitaire stocke l'archive et sa somme de contrôle MD5 dans le répertoire /**var**/**tmp**/:

```
[root@server1 ~]# ll /var/tmp/sosreport*
total 18704
-rw-------. 1 root root 19136596 Jan 25 07:42 sosreport-server1-12345678-2022-01-25-tgictvu.tar.xz
```

```
-rw-r--r--. 1 root root      33 Jan 25 07:42 sosreport-server1-12345678-2022-01-25-tgictvu.tar.xz.md5
```

Ressources supplémentaires

- **sosreport(1)** page de manuel

1.2. INSTALLATION DU PAQUETAGE sos À PARTIR DE LA LIGNE DE COMMANDE

Pour utiliser l'utilitaire **sos**, installez le paquetage **sos**.

Conditions préalables

- Vous avez besoin des privilèges de **root**.

Procédure

- Installez le paquetage **sos**.

```
[root@server ~]# dnf install sos
```

Verification steps

- Utilisez l'utilitaire **rpm** pour vérifier que le paquet **sos** est installé.

```
[root@server ~]# rpm -q sos
sos-4.2-15.el9.noarch
```

1.3. GÉNÉRER UN RAPPORT sos À PARTIR DE LA LIGNE DE COMMANDE

Utilisez la commande **sos report** pour obtenir un rapport **sos** à partir d'un serveur RHEL.

Conditions préalables

- Vous avez installé le paquetage **sos**.
- Vous avez besoin des privilèges de **root**.

Procédure

1. Exécutez la commande **sos report** et suivez les instructions à l'écran. Vous pouvez ajouter l'option **--upload** pour transférer le rapport **sos** à Red Hat immédiatement après l'avoir généré.

```
[user@server1 ~]$ sudo sos report
[sudo] password for user:

sos report (version 4.2)

This command will collect diagnostic and configuration information from
this Red Hat Enterprise Linux system and installed applications.
```

```
An archive containing the collected information will be generated in
/var/tmp/sos.qkn_b7by and may be provided to a Red Hat support
representative.

...

Press ENTER to continue, or CTRL-C to quit.
```

2. *(Optional)* Si vous avez déjà ouvert un dossier d'assistance technique avec Red Hat, saisissez le numéro du dossier pour l'incorporer dans le nom du fichier de rapport **sos**, et il sera téléchargé dans ce dossier si vous avez spécifié l'option **--upload**. Si vous n'avez pas de numéro de dossier, laissez ce champ vide. La saisie d'un numéro de dossier est facultative et n'affecte pas le fonctionnement de l'utilitaire **sos**.

```
Veuillez saisir l'identifiant du cas pour lequel vous générez ce rapport [] : <8-
digit_case_number>
```

3. Notez le nom du fichier de rapport **sos** affiché à la fin de la sortie de la console.

```
...
Finished running plugins
Creating compressed archive...

Your sos report has been generated and saved in:
/var/tmp/sosreport-server1-12345678-2022-04-17-qmtnqng.tar.xz

Size    16.51MiB
Owner   root
md5     bba955bbd9a434954e18da0c6778ba9a

Please send this file to your support representative.
```

NOTE

- Vous pouvez utiliser l'option **--batch** pour générer un rapport **sos** sans demander d'entrée interactive.

```
[user@server1 ~]$ sudo sos report --batch --case-id <8-digit_case_number>
```

- Vous pouvez également utiliser l'option **--clean** pour obscurcir un rapport **sos** qui vient d'être collecté.

```
[user@server1 ~]$ sudo sos report --clean
```

Verification steps

- Vérifiez que l'utilitaire **sos** a créé une archive dans **/var/tmp/** correspondant à la description de la sortie de la commande.

```
[user@server1 ~]$ sudo ls -l /var/tmp/sosreport*
[sudo] password for user:
-rw-------. 1 root root 17310544 Sep 17 19:11 /var/tmp/sosreport-server1-12345678-2022-
```

```
04-17-qmtnqng.tar.xz
```

Ressources supplémentaires

- Méthodes pour fournir un rapport **sos** à l'assistance technique de Red Hat .

1.4. GÉNÉRER ET COLLECTER DES RAPPORTS SOS SUR PLUSIEURS SYSTÈMES SIMULTANÉMENT

Vous pouvez utiliser l'utilitaire **sos** pour déclencher la commande **sos report** sur plusieurs systèmes. Attendez que le rapport se termine et rassemblez tous les rapports générés.

Conditions préalables

- Vous connaissez le type de *cluster* ou la liste de *nodes* à utiliser.
- Vous avez installé le paquet **sos** sur tous les systèmes.
- Vous disposez des clés **ssh** pour le compte **root** sur tous les systèmes, ou vous pouvez fournir le mot de passe root via l'option **--password**.

Procédure

- Exécutez la commande **sos collect** et suivez les instructions qui s'affichent à l'écran.

NOTE

Par défaut, **sos collect** tente d'identifier le type de *cluster* sur lequel il s'exécute afin d'identifier automatiquement le *nodes* à partir duquel collecter les rapports.

a. Vous pouvez définir manuellement les types *cluster* ou *nodes* à l'aide des options **--cluster** ou **--nodes**.

b. Vous pouvez également utiliser l'option **--master** pour diriger l'utilitaire **sos** vers un nœud distant afin de déterminer le type *cluster* et les listes *node*. Ainsi, il n'est pas nécessaire d'être connecté à l'un des *cluster nodes* pour collecter les rapports **sos**; vous pouvez le faire à partir de votre poste de travail.

c. Vous pouvez ajouter l'option **--upload** pour transférer le fichier **sos report** à Red Hat immédiatement après l'avoir généré.

d. Toute option **sos report** valide peut être fournie et sera transmise à toutes les exécutions de rapports **sos**, telles que les options **--batch** et **--clean**.

```
[root@primary-rhel9 ~]# sos collect --nodes=sos-node1,sos-node2 -o process,apache --log-size=50

sos-collector (version 4.2)

This utility is used to collect sosreports from multiple nodes simultaneously.
It uses OpenSSH's ControlPersist feature to connect to nodes and run commands remotely. If your
system installation of OpenSSH is older than 5.6, please upgrade.

An archive of sosreport tarballs collected from the nodes will be generated in /var/tmp/sos.o4l55n1s
```

```
and may be provided to an appropriate support representative.

The generated archive may contain data considered sensitive and its content should be reviewed by
the originating organization before being passed to any third party.

No configuration changes will be made to the system running this utility or remote systems that it
connects to.


Press ENTER to continue, or CTRL-C to quit


Please enter the case id you are collecting reports for: <8-digit_case_number>

sos-collector ASSUMES that SSH keys are installed on all nodes unless the
--password option is provided.

The following is a list of nodes to collect from:
    primary-rhel9
    sos-node1
    sos-node2


Press ENTER to continue with these nodes, or press CTRL-C to quit


Connecting to nodes...

Beginning collection of sosreports from 3 nodes, collecting a maximum of 4 concurrently

primary-rhel9 : Generating sosreport...
sos-node1  : Generating sosreport...
sos-node2 : Generating sosreport...
primary-rhel9 : Retrieving sosreport...
sos-node1  : Retrieving sosreport...
primary-rhel9  : Successfully collected sosreport
sos-node1 : Successfully collected sosreport
sos-node2 : Retrieving sosreport...
sos-node2 : Successfully collected sosreport

The following archive has been created. Please provide it to your support team.
    /var/tmp/sos-collector-2022-05-15-pafsr.tar.xz

[root@primary-rhel9 ~]#
```

Verification steps

- Vérifiez que la commande **sos collect** a créé une archive dans le répertoire **/var/tmp/** correspondant à la description de la sortie de la commande.

```
[root@primary-rhel9 ~]# ls -l /var/tmp/sos-collector*
-rw-------. 1 root root 160492 May 15 13:35 /var/tmp/sos-collector-2022-05-15-pafsr.tar.xz
```

Ressources supplémentaires

- Pour des exemples d'utilisation des options **--batch** et **--clean**, voir Générer un rapport **sos** à partir de la ligne de commande.

1.5. NETTOYAGE D'UN RAPPORT SOS

L'utilitaire **sos** propose une routine pour obscurcir des données potentiellement sensibles, telles que des noms d'utilisateurs, des noms d'hôtes, des adresses IP ou MAC, ou d'autres mots-clés spécifiés par l'utilisateur. Le fichier original **sos report** ou **sos collect** reste inchangé, et un nouveau fichier ***-obfuscated.tar.xz** est généré et destiné à être partagé avec un tiers.

NOTE

Vous pouvez ajouter la fonctionnalité de nettoyage aux commandes **sos report** ou **sos collect** à l'aide de l'option **--clean**:

[user@server1 ~]$ sudo sos report --clean

Conditions préalables

- Vous avez généré une archive **sos report** ou **sos collect**.
- *(Optional)* Vous disposez d'une liste de mots-clés spécifiques en plus des noms d'utilisateur, des noms d'hôte et d'autres données que vous souhaitez obscurcir.

Procédure

- Exécutez la commande **sos clean** sur une archive **sos report** ou **sos collect** et suivez les instructions à l'écran.
  a. Vous pouvez ajouter l'option **--keywords** pour nettoyer davantage une liste donnée de mots-clés.
  b. Vous pouvez ajouter l'option **--usernames** pour obscurcir d'autres noms d'utilisateurs sensibles.
  Le nettoyage automatique des noms d'utilisateur sera automatiquement exécuté pour les utilisateurs signalés dans le fichier **lastlog** pour les utilisateurs dont l'UID est égal ou supérieur à 1000. Cette option est utilisée pour les utilisateurs LDAP qui n'apparaissent pas comme des connexions réelles, mais qui peuvent apparaître dans certains fichiers journaux.

```
[user@server1 ~]$ sudo sos clean /var/tmp/sos-collector-2022-05-15-pafsr.tar.xz
[sudo] password for user:

sos clean (version 4.2)

This command will attempt to obfuscate information that is generally considered to be potentially
sensitive. Such information includes IP addresses, MAC addresses, domain names, and any user-
provided keywords.

Note that this utility provides a best-effort approach to data obfuscation, but it does not guarantee that
such obfuscation provides complete coverage of all such data in the archive, or that any obfuscation
is provided to data that does not fit the description above.

Users should review any resulting data and/or archives generated or processed by this utility for
remaining sensitive content before being passed to a third party.
```

```
Press ENTER to continue, or CTRL-C to quit.

Found 4 total reports to obfuscate, processing up to 4 concurrently

sosreport-primary-rhel9-2022-05-15-nchbdmd :      Extracting...
sosreport-sos-node1-2022-05-15-wmlomgu :      Extracting...
sosreport-sos-node2-2022-05-15-obsudzc :      Extracting...
sos-collector-2022-05-15-pafsr :                  Beginning obfuscation...
sosreport-sos-node1-2022-05-15-wmlomgu :      Beginning obfuscation...
sos-collector-2022-05-15-pafsr :                  Obfuscation completed
sosreport-primary-rhel9-2022-05-15-nchbdmd :      Beginning obfuscation...
sosreport-sos-node2-2022-05-15-obsudzc :      Beginning obfuscation...
sosreport-primary-rhel9-2022-05-15-nchbdmd :      Re-compressing...
sosreport-sos-node2-2022-05-15-obsudzc :      Re-compressing...
sosreport-sos-node1-2022-05-15-wmlomgu :      Re-compressing...
sosreport-primary-rhel9-2022-05-15-nchbdmd :      Obfuscation completed
sosreport-sos-node2-2022-05-15-obsudzc :      Obfuscation completed
sosreport-sos-node1-2022-05-15-wmlomgu :      Obfuscation completed

Successfully obfuscated 4 report(s)

A mapping of obfuscated elements is available at
   /var/tmp/sos-collector-2022-05-15-pafsr-private_map

The obfuscated archive is available at
   /var/tmp/sos-collector-2022-05-15-pafsr-obfuscated.tar.xz

   Size    157.10KiB
   Owner    root

Please send the obfuscated archive to your support representative and keep the mapping file private
```

Verification steps

- Vérifiez que la commande **sos clean** a créé une archive obscurcie et un mappage d'obscurcissement dans le répertoire **/var/tmp/** correspondant à la description de la sortie de la commande.

```
[user@server1 ~]$ sudo ls -l /var/tmp/sos-collector-2022-05-15-pafsr-private_map
/var/tmp/sos-collector-2022-05-15-pafsr-obfuscated.tar.xz
[sudo] password for user:

-rw-------. 1 root root 160868 May 15 16:10 /var/tmp/sos-collector-2022-05-15-pafsr-
obfuscated.tar.xz
-rw-------. 1 root root  96622 May 15 16:10 /var/tmp/sos-collector-2022-05-15-pafsr-
private_map
```

- Consultez le fichier ***-private_map** pour connaître le mappage de l'obfuscation :

```
[user@server1 ~]$ sudo cat /var/tmp/sos-collector-2022-05-15-pafsr-private_map
[sudo] password for user:

{
    "hostname_map": {
```

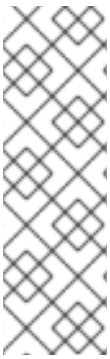
```
        "pmoravec-rhel9": "host0"
    },
    "ip_map": {
        "10.44.128.0/22": "100.0.0.0/22",
..
    "username_map": {
        "foobaruser": "obfuscateduser0",
        "jsmith": "obfuscateduser1",
        "johndoe": "obfuscateduser2"
    }
}
```

IMPORTANT

Conservez l'archive originale non obscurcie et les fichiers ***private_map** localement car l'assistance de Red Hat peut se référer aux termes obscurcis que vous devrez traduire en valeurs originales.

1.6. GÉNÉRER UN RAPPORT sos ET LE SÉCURISER AVEC UN CHIFFREMENT PAR PHRASE SECRÈTE GPG

Cette procédure décrit comment générer un rapport **sos** et le sécuriser par un chiffrement symétrique GPG2 basé sur une phrase de passe. Vous pouvez vouloir sécuriser le contenu d'un rapport **sos** à l'aide d'un mot de passe si, par exemple, vous devez le transférer à un tiers via un réseau public.



NOTE

Veillez à disposer de suffisamment d'espace lors de la création d'un rapport **sos** crypté, car il utilise temporairement le double de l'espace disque :

1. L'utilitaire **sos** crée un rapport **sos** non crypté.
2. L'utilitaire crypte le rapport **sos** dans un nouveau fichier.
3. L'utilitaire supprime ensuite l'archive non chiffrée.

Conditions préalables

- Vous avez installé le paquetage **sos**.
- Vous avez besoin des privilèges de **root**.

Procédure

1. Exécutez la commande **sos report** et spécifiez une phrase d'authentification avec l'option **--encrypt-pass**. Vous pouvez ajouter l'option **--upload** pour transférer le rapport **sos** à Red Hat immédiatement après l'avoir généré.

```
[user@server1 ~]$ sudo sos report --encrypt-pass my-passphrase
[sudo] password for user:

sosreport (version 4.2)

This command will collect diagnostic and configuration information from
```

```
this Red Hat Enterprise Linux system and installed applications.

An archive containing the collected information will be generated in
/var/tmp/sos.6lck0myd and may be provided to a Red Hat support
representative.

...

Press ENTER to continue, or CTRL-C to quit.
```

2. *(Optional)* Si vous avez déjà ouvert un dossier d'assistance technique avec Red Hat, saisissez le numéro du dossier pour l'incorporer dans le nom du fichier de rapport **sos**, et il sera téléchargé dans ce dossier si vous avez spécifié l'option **--upload**. Si vous n'avez pas de numéro de dossier, laissez ce champ vide. La saisie d'un numéro de dossier est facultative et n'affecte pas le fonctionnement de l'utilitaire **sos**.

```
Veuillez saisir l'identifiant du cas pour lequel vous générez ce rapport [] : <8-digit_case_number>
```

3. Notez le nom du fichier de rapport **sos** affiché à la fin de la sortie de la console.

```
Finished running plugins
Creating compressed archive...

Your sosreport has been generated and saved in:
/var/tmp/secured-sosreport-server1-12345678-2022-01-24-ueqijfm.tar.xz.gpg

Size    17.53MiB
Owner   root
md5     32e2bdb23a9ce3d35d59e1fc4c91fe54

Please send this file to your support representative.
```

Verification steps

1. Vérifiez que l'utilitaire **sos** a créé une archive répondant aux exigences suivantes :
   - Le nom du fichier commence par **secured**.
   - Le nom du fichier se termine par une extension **.gpg**.
   - Situé dans le répertoire /**var**/**tmp**/.

```
[user@server1 ~]$ sudo ls -l /var/tmp/sosreport*
[sudo] password for user:
-rw-------. 1 root root 18381537 Jan 24 17:55 /var/tmp/secured-sosreport-server1-12345678-2022-01-24-ueqijfm.tar.xz.gpg
```

2. Vérifiez que vous pouvez déchiffrer l'archive avec la même phrase de passe que celle utilisée pour la chiffrer.
   a. Utilisez la commande **gpg** pour décrypter l'archive.

```
[user@server1 ~]$ sudo gpg --output decrypted-sosreport.tar.gz --decrypt
/var/tmp/secured-sosreport-server1-12345678-2022-01-24-ueqijfm.tar.xz.gpg
```

b. Lorsque vous y êtes invité, saisissez la phrase de passe que vous avez utilisée pour crypter l'archive.

```
┌──────────────────────────────────────────────────────┐
│ Enter passphrase                                     │
│                                                      │
│ Passphrase: <passphrase>                             │
│                                                      │
│     <OK>                    <Cancel>                 │
└──────────────────────────────────────────────────────┘
```

c. Vérifiez que l'utilitaire **gpg** a produit une archive non chiffrée avec une extension de fichier **.tar.gz**.

```
[user@server1 ~]$ sudo ls -l decrypted-sosreport.tar.gz
[sudo] password for user:
-rw-r--r--. 1 root root 18381537 Jan 24 17:59 decrypted-sosreport.tar.gz
```

Ressources supplémentaires

- Méthodes pour fournir un rapport **sos** à l'assistance technique de Red Hat .

1.7. GÉNÉRER UN RAPPORT sos ET LE SÉCURISER AVEC UN CHIFFREMENT GPG BASÉ SUR UNE PAIRE DE CLÉS

Cette procédure décrit comment générer un rapport **sos** et le sécuriser avec un cryptage GPG2 basé sur une paire de clés provenant d'un trousseau GPG. Vous pouvez vouloir sécuriser le contenu d'un rapport **sos** avec ce type de cryptage si, par exemple, vous souhaitez protéger un rapport **sos** stocké sur un serveur.

NOTE

Veillez à disposer de suffisamment d'espace lors de la création d'un rapport **sos** crypté, car il utilise temporairement le double de l'espace disque :

1. L'utilitaire **sos** crée un rapport **sos** non crypté.
2. L'utilitaire crypte le rapport **sos** dans un nouveau fichier.
3. L'utilitaire supprime ensuite l'archive non chiffrée.

Conditions préalables

- Vous avez installé le paquetage **sos**.
- Vous avez besoin des privilèges de **root**.
- Vous avez créé une clé GPG2.

Procédure

1. Exécutez la commande **sos report** et spécifiez le nom d'utilisateur qui possède le trousseau de clés GPG avec l'option **--encrypt-key**. Vous pouvez ajouter l'option **--upload** pour transférer le rapport **sos** à Red Hat immédiatement après l'avoir généré.

NOTE

L'utilisateur qui exécute la commande **sos report must** est le même que celui qui possède le trousseau GPG utilisé pour chiffrer et déchiffrer le rapport **sos**. Si l'utilisateur utilise **sudo** pour exécuter la commande **sos report**, le trousseau doit également être configuré à l'aide de **sudo**, ou l'utilisateur doit avoir un accès direct à ce compte.

```
[user@server1 ~]$ sudo sos report --encrypt-key root
[sudo] password for user:

sosreport (version 4.2)

This command will collect diagnostic and configuration information from
this Red Hat Enterprise Linux system and installed applications.

An archive containing the collected information will be generated in
/var/tmp/sos.6ucjclgf and may be provided to a Red Hat support
representative.

...

Press ENTER to continue, or CTRL-C to quit.
```

2. *(Optional)* Si vous avez déjà ouvert un dossier d'assistance technique avec Red Hat, saisissez le numéro du dossier pour l'incorporer dans le nom du fichier de rapport **sos**, et il sera téléchargé dans ce dossier si vous avez spécifié l'option **--upload**. Si vous n'avez pas de numéro de dossier, laissez ce champ vide. La saisie d'un numéro de dossier est facultative et n'affecte pas le fonctionnement de l'utilitaire **sos**.

```
Veuillez saisir l'identifiant du cas pour lequel vous générez ce rapport [] : <8-digit_case_number>
```

3. Notez le nom du fichier de rapport **sos** affiché à la fin de la sortie de la console.

```
...
Finished running plugins
Creating compressed archive...

Your sosreport has been generated and saved in:
/var/tmp/secured-sosreport-server1-23456789-2022-02-27-zhdqhdi.tar.xz.gpg

Size    15.44MiB
Owner   root
md5     ac62697e33f3271dbda92290583d1242

Please send this file to your support representative.
```

Verification steps

1. Vérifiez que l'utilitaire **sos** a créé une archive répondant aux exigences suivantes :
   - Le nom du fichier commence par **secured**.
   - Le nom du fichier se termine par une extension **.gpg**.
   - Situé dans le répertoire **/var/tmp/**.

     ```
     [user@server1 ~]$ sudo ls -l /var/tmp/sosreport*
     [sudo] password for user:
     -rw-------. 1 root root 16190013 Jan 24 17:55 /var/tmp/secured-sosreport-server1-23456789-2022-01-27-zhdqhdi.tar.xz.gpg
     ```

2. Vérifiez que vous pouvez décrypter l'archive avec la même clé que celle utilisée pour la crypter.
   a. Utilisez la commande **gpg** pour décrypter l'archive.

      ```
      [user@server1 ~]$ sudo gpg --output decrypted-sosreport.tar.gz --decrypt /var/tmp/secured-sosreport-server1-23456789-2022-01-27-zhdqhdi.tar.xz.gpg
      ```

   b. Lorsque vous y êtes invité, saisissez la phrase de passe que vous avez utilisée lors de la création de la clé GPG.

      ```
      ┌──────────────────────────────────────────────────────┐
      │ Please enter the passphrase to unlock the OpenPGP secret key: │
      │ "GPG User (first key) <root@example.com>"                     │
      │ 2048-bit RSA key, ID BF28FFA302EF4557,                        │
      │ created 2020-01-13.                                           │
      │                                                               │
      │                                                               │
      │ Passphrase: <passphrase>                                      │
      │                                                               │
      │       <OK>                          <Cancel>                  │
      └──────────────────────────────────────────────────────┘
      ```

   c. Vérifiez que l'utilitaire **gpg** a produit une archive non chiffrée avec une extension de fichier **.tar.gz**.

      ```
      [user@server1 ~]$ sudo ll decrypted-sosreport.tar.gz
      [sudo] password for user:
      -rw-r--r--. 1 root root 16190013 Jan 27 17:47 decrypted-sosreport.tar.gz
      ```

Ressources supplémentaires

- Méthodes pour fournir un rapport **sos** à l'assistance technique de Red Hat .

1.8. CRÉATION D'UNE CLÉ GPG2

La procédure suivante décrit comment générer une clé GPG2 à utiliser avec les utilitaires de cryptage.

Conditions préalables

Conditions préalables

- Vous avez besoin des privilèges de **root**.

Procédure

1. Installer et configurer l'utilitaire **pinentry**.

```
[root@server ~]# dnf install pinentry
[root@server ~]# mkdir ~/.gnupg -m 700
[root@server ~]# echo "pinentry-program /usr/bin/pinentry-curses" >> ~/.gnupg/gpg-agent.conf
```

2. Créez un fichier **key-input** utilisé pour générer une paire de clés GPG avec les détails de votre choix. Par exemple :

```
[root@server ~]# cat >key-input <<EOF
%echo Generating a standard key
Key-Type: RSA
Key-Length: 2048
Name-Real: GPG User
Name-Comment: first key
Name-Email: root@example.com
Expire-Date: 0
%commit
%echo Finished creating standard key
EOF
```

3. *(Optional)* Par défaut, GPG2 stocke son trousseau de clés dans le fichier **~/.gnupg**. Pour utiliser un emplacement de trousseau personnalisé, définissez la variable d'environnement **GNUPGHOME** dans un répertoire accessible uniquement par root.

```
[root@server ~]# export GNUPGHOME=/root/backup

[root@server ~]# mkdir -p $GNUPGHOME -m 700
```

4. Générer une nouvelle clé GPG2 basée sur le contenu du fichier **key-input**.

```
[root@server ~]# gpg2 --batch --gen-key key-input
```

5. Saisissez une phrase de passe pour protéger la clé GPG2. Cette phrase d'authentification permet d'accéder à la clé privée pour le décryptage.

```
┌──────────────────────────────────────────────────────┐
│ Please enter the passphrase to                       │
│ protect your new key                                 │
│                                                      │
│ Passphrase: <passphrase>                             │
│                                                      │
│  <OK>                          <Cancel>              │
└──────────────────────────────────────────────────────┘
```

6. Confirmez la phrase d'authentification correcte en la saisissant à nouveau.

```
┌──────────────────────────────────────────────────────┐
│ Please re-enter this passphrase                      │
│                                                      │
│ Passphrase: <passphrase>                             │
│                                                      │
│  <OK>                          <Cancel>              │
└──────────────────────────────────────────────────────┘
```

7. Vérifiez que la nouvelle clé GPG2 a été créée avec succès.

```
gpg: keybox '/root/backup/pubring.kbx' created
gpg: Generating a standard key
gpg: /root/backup/trustdb.gpg: trustdb created
gpg: key BF28FFA302EF4557 marked as ultimately trusted
gpg: directory '/root/backup/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/backup/openpgp-
revocs.d/8F6FCF10C80359D5A05AED67BF28FFA302EF4557.rev'
gpg: Finished creating standard key
```

Étapes de la vérification

- Liste des clés GPG sur le serveur.

```
[root@server ~]# gpg2 --list-secret-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
/root/backup/pubring.kbx
------------------------
sec   rsa2048 2020-01-13 [SCEA]
      8F6FCF10C80359D5A05AED67BF28FFA302EF4557
uid           [ultimate] GPG User (first key) <root@example.com>
```

Ressources supplémentaires

- GNU Privacy Guard

1.9. GÉNÉRER UN RAPPORT sos À PARTIR DE L'ENVIRONNEMENT DE SAUVETAGE

Si un hôte Red Hat Enterprise Linux (RHEL) ne démarre pas correctement, vous pouvez démarrer l'hôte sur *rescue environment* pour obtenir un rapport **sos**.

En utilisant l'environnement de secours, vous pouvez monter le système cible sous **/mnt/sysimage**, accéder à son contenu et exécuter la commande **sos report**.

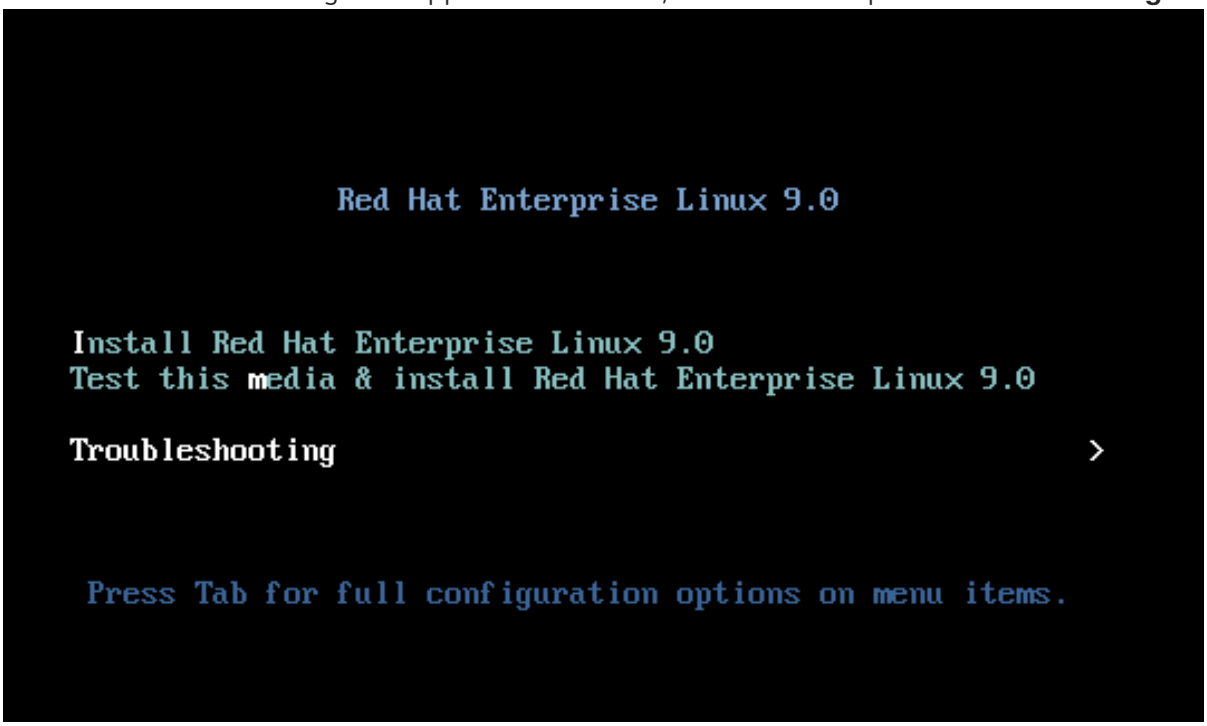
Conditions préalables

- Si l'hôte est un serveur bare metal, vous devez avoir un accès physique à la machine.
- Si l'hôte est une machine virtuelle, vous devez avoir accès aux paramètres de la machine virtuelle dans l'hyperviseur.

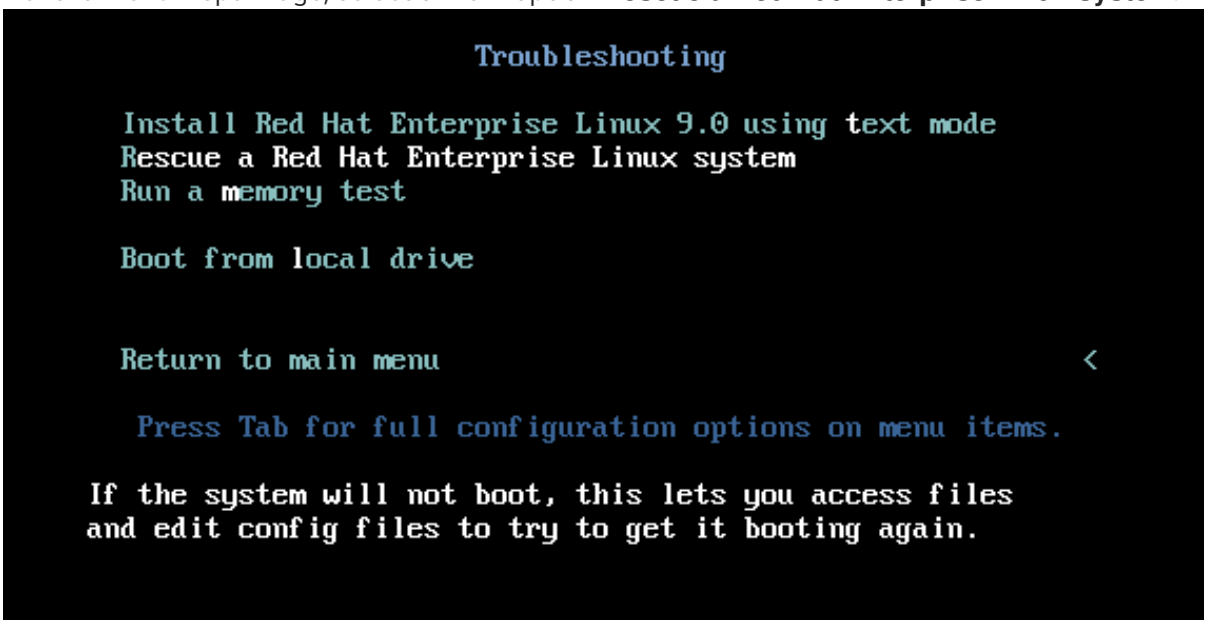
- Une source d'installation RHEL, telle qu'un fichier image ISO, un DVD d'installation, un CD netboot ou une configuration Preboot Execution Environment (PXE) fournissant une arborescence d'installation RHEL.

Procédure

1. Démarrer l'hôte à partir d'une source d'installation.
2. Dans le menu de démarrage du support d'installation, sélectionnez l'option **Troubleshooting**.



3. Dans le menu Dépannage, sélectionnez l'option **Rescue a Red Hat Enterprise Linux system**.



4. Dans le menu Rescue, sélectionnez **1** et appuyez sur la touche **Entrée** pour continuer et monter le système sous le répertoire **/mnt/sysimage**.

```
Starting installer, one moment...
anaconda 34.25.0.29-1.el9_0 for Red Hat Enterprise Linux 9.0 started.
 * installation log files are stored in /tmp during the installation
 * shell is available on TTY2
 * when reporting a bug add logs from /tmp as separate text/plain attachments
================================================================================
================================================================================
Rescue

The rescue environment will now attempt to find your Linux installation and
mount it under the directory : /mnt/sysroot.  You can then make any changes
required to your system.  Choose '1' to proceed with this step.
You can choose to mount your file systems read-only instead of read-write by
choosing '2'.
If for some reason this process does not work choose '3' to skip directly to a
shell.



1) Continue
2) Read-only mount
3) Skip to shell
4) Quit (Reboot)

Please make a selection from the above: 1_
```

5. Appuyez sur la touche **Entrée** pour obtenir un shell lorsque vous y êtes invité.

```
--------------------------------------------------------------------------------
Rescue Shell

Your system has been mounted under /mnt/sysroot.

If you would like to make the root of your system the root of the active system,
run the command:

        chroot /mnt/sysroot

When finished, please exit from the shell and your system will reboot.

Please press ENTER to get a shell:
bash-5.1#
```

6. Utilisez la commande **chroot** pour changer le répertoire racine apparent de la session de sauvetage en répertoire /**mnt**/**sysimage**.

```
  Rescue Shell

  Your system has been mounted under /mnt/sysroot.

  If you would like to make the root of your system the root of the active system,
  run the command:

          chroot /mnt/sysroot

  When finished, please exit from the shell and your system will reboot.

  Please press ENTER to get a shell:
  bash-5.1# chroot /mnt/sysimage_
```

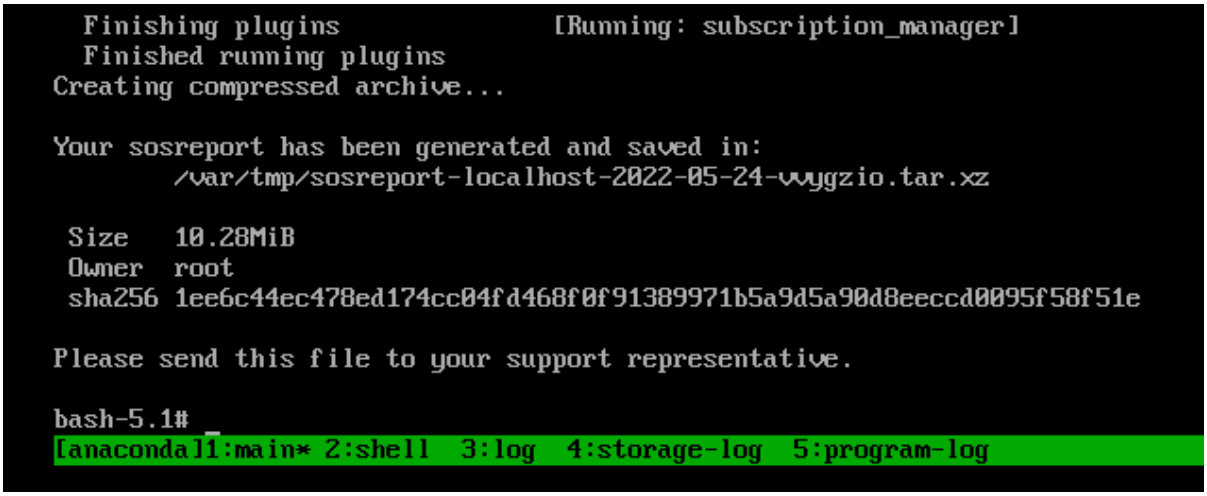
7. Exécutez la commande **sos report** et suivez les instructions à l'écran. Vous pouvez ajouter l'option **--upload** pour transférer le rapport **sos** à Red Hat immédiatement après l'avoir généré.

```
bash-5.1# sos report

sosreport (version 4.2)

This command will collect diagnostic and configuration information from
this Red Hat Enterprise Linux system and installed applications.

An archive containing the collected information will be generated in
/var/tmp/sos.awiu1v8n and may be provided to a Red Hat support
representative.

Any information provided to Red Hat will be treated in accordance with
the published support policies at:

        Distribution Website : https://www.redhat.com/
        Commercial Support   : https://www.access.redhat.com/

The generated archive may contain data considered sensitive and its
content should be reviewed by the originating organization before being
passed to any third party.

No changes will be made to system configuration.

Press ENTER to continue, or CTRL-C to quit.
```

8. *(Optional)* Si vous avez déjà ouvert un dossier d'assistance technique auprès de Red Hat, entrez le numéro du dossier pour l'incorporer dans le nom du fichier de rapport **sos**, et il sera téléchargé dans ce dossier si vous avez spécifié l'option **--upload** et que votre hôte est connecté à Internet. Si vous n'avez pas de numéro de cas, laissez ce champ vide. La saisie d'un numéro de dossier est facultative et n'affecte pas le fonctionnement de l'utilitaire **sos**.

```
bash-5.1# sos report

sosreport (version 4.2)

This command will collect diagnostic and configuration information from
this Red Hat Enterprise Linux system and installed applications.

An archive containing the collected information will be generated in
/var/tmp/sos.awiu1v8n and may be provided to a Red Hat support
representative.

Any information provided to Red Hat will be treated in accordance with
the published support policies at:

        Distribution Website : https://www.redhat.com/
        Commercial Support   : https://www.access.redhat.com/

The generated archive may contain data considered sensitive and its
content should be reviewed by the originating organization before being
passed to any third party.

No changes will be made to system configuration.

Press ENTER to continue, or CTRL-C to quit.

Optionally, please enter the case id that you are generating this report for []:
[anaconda]1:main* 2:shell  3:log  4:storage-log  5:program-log
```

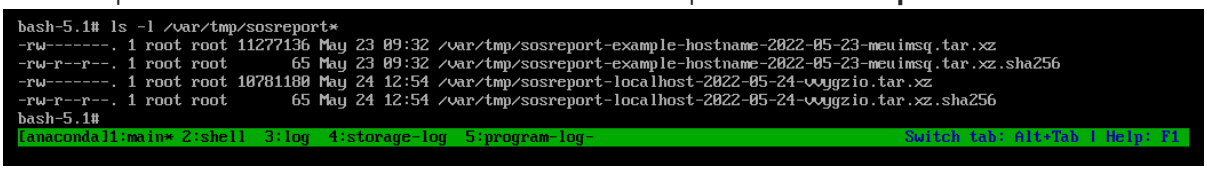
9. Notez le nom du fichier de rapport **sos** affiché à la fin de la sortie de la console.



10. Si votre hôte ne dispose pas d'une connexion à Internet, utilisez un utilitaire de transfert de fichiers tel que **scp** pour transférer le rapport **sos** vers un autre hôte de votre réseau, puis téléchargez-le vers un dossier d'assistance technique de Red Hat.

Verification steps

- Vérifiez que l'utilitaire **sos** a créé une archive dans le répertoire **/var/tmp/**.



Ressources supplémentaires

- Pour télécharger une ISO du DVD d'installation de RHEL, visitez la section des téléchargements du portail client de Red Hat. Voir Téléchargements de produits.
- Méthodes pour fournir un rapport **sos** à l'assistance technique de Red Hat .

1.10. MÉTHODES POUR FOURNIR UN RAPPORT sos À L'ASSISTANCE TECHNIQUE DE RED HAT

Vous pouvez utiliser les méthodes suivantes pour télécharger votre rapport **sos** vers l'assistance technique de Red Hat.

Télécharger avec la commande sos report

Vous pouvez utiliser l'option **--upload** pour transférer le rapport **sos** à Red Hat immédiatement après l'avoir généré.

- Si vous fournissez un numéro de dossier lorsque vous y êtes invité, ou si vous utilisez les options **--case-id** ou **--ticket-number**, l'utilitaire **sos** télécharge le rapport **sos** dans votre dossier après que vous vous soyez authentifié avec votre compte Red Hat Customer Portal.
- Si vous ne fournissez pas de numéro de dossier ou si vous ne vous authentifiez pas, l'utilitaire télécharge le rapport **sos** sur le site SFTP public de Red Hat. Fournissez aux ingénieurs du support technique de Red Hat le nom de l'archive du rapport **sos** afin qu'ils puissent y accéder.

```
[user@server1 ~]$ sudo sos report --upload
```

```
[sudo] password for user:

sosreport (version 4.2)

This command will collect diagnostic and configuration information from
this Red Hat Enterprise Linux system and installed applications.
...

Please enter the case id that you are generating this report for []: <8-digit_case_number>
Enter your Red Hat Customer Portal username (empty to use public dropbox):
<Red_Hat_Customer_Portal_ID>
Please provide the upload password for <user@domain.com>:
...

Attempting upload to Red Hat Customer Portal
Uploaded archive successfully
```

Télécharger des fichiers via le portail client de Red Hat

En utilisant votre compte utilisateur Red Hat, vous pouvez vous connecter à la section **Support Cases** du site web Red Hat Customer Portal et télécharger un rapport **sos** vers un cas d'assistance technique.
Pour vous connecter, rendez-vous sur la page Cas de support.

Ressources supplémentaires

- Pour des méthodes supplémentaires sur la manière de fournir au support technique de Red Hat votre rapport **sos**, telles que SFTP et **curl**, consultez l'article de la base de connaissances de Red Hat intitulé Comment fournir des fichiers au support technique de Red Hat (vmcore, rhev logcollector, sosreports, heap dumps, fichiers journaux, etc.)

CHAPITRE 2. GÉNÉRER ET MAINTENIR LES RAPPORTS DE DIAGNOSTIC À L'AIDE DE LA CONSOLE WEB RHEL

Générer, télécharger et supprimer les rapports de diagnostic dans la console web RHEL.

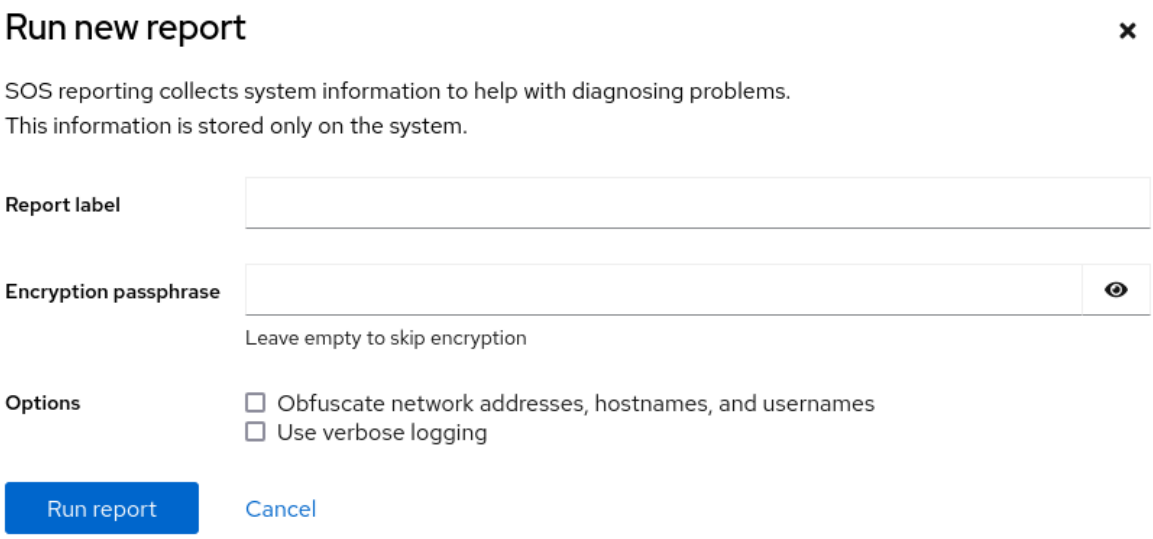
2.1. GÉNÉRER DES RAPPORTS DE DIAGNOSTIC À L'AIDE DE LA CONSOLE WEB RHEL

Conditions préalables

- La console web RHEL a été installée. Pour plus de détails, voir Installation de la console web .
- Le paquetage **cockpit-storaged** est installé sur votre système.
- Vous disposez de privilèges d'administrateur.

Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Dans le menu de gauche, sélectionnez **Tools >> Diagnostic reports**.
3. Pour générer un nouveau rapport de diagnostic, cliquez sur le bouton **Exécuter le rapport**.



4. Saisissez l'étiquette du rapport que vous souhaitez créer.
5. *(Optional)* Personnalisez votre rapport.
   a. Saisissez la phrase de passe de cryptage pour crypter votre rapport. Si vous souhaitez ignorer le cryptage du rapport, laissez le champ vide.
   b. Cochez la case **Obfuscate network addresses, hostnames, and usernames**pour obscurcir certaines données.
   c. Cochez la case **Use verbose logging** pour augmenter la verbosité de la journalisation.

6. Cliquez sur le bouton **Exécuter le rapport** pour générer un rapport et attendre la fin du processus. Vous pouvez arrêter la génération du rapport en cliquant sur le bouton **Arrêter le rapport**.

2.2. TÉLÉCHARGEMENT DE RAPPORTS DE DIAGNOSTIC À L'AIDE DE LA CONSOLE WEB RHEL

Conditions préalables

- La console web RHEL a été installée. Pour plus de détails, voir Installation de la console web.
- Vous disposez de privilèges d'administrateur.
- Un ou plusieurs rapports de diagnostic ont été générés.

Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Dans le menu de gauche, sélectionnez **Tools >> Diagnostic reports**.
3. Cliquez sur le bouton **Télécharger** à côté du rapport que vous souhaitez télécharger. Le téléchargement démarre automatiquement.

Prochaines étapes

Pour savoir comment fournir votre rapport de diagnostic à l'équipe d'assistance technique de Red Hat, reportez-vous à Méthodes pour fournir un rapport **sos** à l'équipe d'assistance technique de Red Hat .

2.3. SUPPRESSION DES RAPPORTS DE DIAGNOSTIC À L'AIDE DE LA CONSOLE WEB RHEL

Conditions préalables

- La console web RHEL a été installée. Pour plus de détails, voir Installation de la console web.
- Vous disposez de privilèges d'administrateur.
- Un ou plusieurs rapports de diagnostic ont été générés.

Procédure

1. Connectez-vous à la console web RHEL. Pour plus d'informations, voir Connexion à la console web.
2. Dans le menu de gauche, sélectionnez **Tools >> Diagnostic reports**.
3. Cliquez sur l'ellipse verticale près du bouton **Télécharger** à côté du rapport que vous souhaitez supprimer, puis cliquez sur le bouton **Supprimer**.
4. Dans la fenêtre **Delete report permanently?**, cliquez sur le bouton **Supprimer** pour supprimer le rapport.