Red Hat Enterprise Linux 8

テクニカルサポート用の sos レポートの生成

sos ユーティリティーを使用した RHEL サーバーからのトラブルシューティング情報の収集

Last Updated: 2021-10-10

Red Hat Enterprise Linux 8 テクニカルサポート用の sos レポートの生成

sos ユーティリティーを使用した RHEL サーバーからのトラブルシューティング情報の収集

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

法律上の通知

概要

本書は、sos ユーティリティーを使用して設定、診断、およびトラブルシューティングのデータを収集し、そのファイルを Red Hat テクニカルサポートに提供する方法を説明します。

目次

多様性を受け入れるオープンソースの強化

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

RED HAT ドキュメントへのフィードバック (英語のみ)

ご意見ご要望をお聞かせください。ドキュメントの改善点はございませんか。改善点を報告する場合は、以下のように行います。

- 特定の文章に簡単なコメントを記入する場合は、以下の手順を行います。
  1. ドキュメントの表示が **Multi-page HTML** 形式になっていて、ドキュメントの右上端に **Feedback** ボタンがあることを確認してください。
  2. マウスカーソルで、コメントを追加する部分を強調表示します。
  3. そのテキストの下に表示される **Add Feedback** ポップアップをクリックします。
  4. 表示される手順に従ってください。
- より詳細なフィードバックを行う場合は、Bugzilla のチケットを作成します。
  1. Bugzilla の Web サイトにアクセスします。
  2. Component で **Documentation** を選択します。
  3. **Description** フィールドに、ドキュメントの改善に関するご意見を記入してください。ドキュメントの該当部分へのリンクも記入してください。
  4. **Submit Bug** をクリックします。

第1章 テクニカルサポート用の sosレポートの生成

1.1. sos レポートユーティリティーの機能

sos レポートは一般的に、Red Hat テクニカルサポートエンジニアが RHEL システムのサービス要求を分析する際の開始点として使用されます。このユーティリティーは、Red Hat サポートエンジニアがサポートケースで報告された問題の検証時に参照できるように診断情報を標準化された方法で収集します。**sosreport** ユーティリティーを使用すると、データの出力を繰り返し依頼する必要がなくなります。

sosreport ユーティリティは、RHEL システムから以下のような設定情報、システム情報および診断情報を収集します。

- 実行中のカーネルバージョン
- 読み込み済みカーネルモジュール
- システムおよびサービスの設定ファイル
- 診断コマンドの出力
- インストールされているパッケージの一覧

sosreport ユーティリティーは、**sosreport-<host_name>-<support_case_number>-<YYYY-MM-DD>-<unique_random_characters>.tar.xz** という名前のアーカイブに収集データを書き込みます。

また、このユーティリティーは、アーカイブと MD5 チェックサムを **/var/tmp/** ディレクトリーに保存します。

```
[root@server1 ~]# ll /var/tmp/sosreport*
total 18704
-rw-------. 1 root root 19136596 Jan 25 07:42 sosreport-server1-12345678-2021-01-25-tgictvu.tar.xz
-rw-r--r--. 1 root root       33 Jan 25 07:42 sosreport-server1-12345678-2021-01-25-tgictvu.tar.xz.md5
```

関連情報

- **sosreport** の man ページ

1.2. コマンドラインからの sos のインストール

sosreport ユーティリティーを使用するには、**sos** をインストールします。

前提条件

- **root** 権限が必要である。

手順

- **sos** パッケージをインストールするには、以下のコマンドを実行します。

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

検証手順

- **rpm** ユーティリティーを使用して、**sos** 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。

```
[root@server ~]# rpm -q sos
sos-3.9.1-6.el8.noarch
```

1.3. コマンドラインからの sos レポートの生成

sosreport コマンドを使用して、RHEL サーバーから **sos** レポートを収集します。

前提条件

- **sos** をインストールしている。
- **root** 権限が必要である。

手順

1. **sosreport** を実行し、画面の指示に従います。バージョン 3.9 以降の **sos** パッケージでは、**--upload** オプションを追加して、**sos** レポートの生成直後に Red Hat に転送できます。

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

sosreport (version 3.9)

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. **(オプション)** Red Hat でテクニカルサポートケースをすでに起票している場合には、ケース番号を入力して **sos** レポートファイルの名前に追加します。**--upload** を指定している場合は対象のケースにアップロードされます。ケース番号がない場合は、このフィールドを空白にしておきます。ケース番号の入力は任意であるため、**sosreport** ユーティリティーの動作には影響はありません。

```
Please enter the case id that you are generating this report for []: <8-digit_case_number>
```

3. コンソール出力の末尾に表示されている **sos** レポートファイルの名前を書き留めておきます。

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

Your sosreport has been generated and saved in:
```

```
/var/tmp/sosreport-server1-12345678-2020-09-17-qmtnqng.tar.xz

Size    16.51MiB
Owner   root
md5     bba955bbd9a434954e18da0c6778ba9a

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

注記

--batch を使用すると、対話形式で入力を求められることなく、**sos** レポートを生成できます。

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

検証手順

- **sosreport** ユーティリティーが **/var/tmp/** で、コマンド出力の説明と一致するアーカイブを作成したことを確認します。

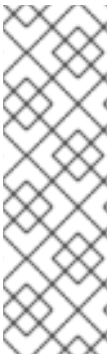
```
[user@server1 ~]$ sudo ls -l /var/tmp/sosreport*
[sudo] password for user:
-rw-------. 1 root root 17310544 Sep 17 19:11 /var/tmp/sosreport-server1-12345678-2020-09-17-qmtnqng.tar.xz
```

関連情報

- Red Hat テクニカルサポートへの **sos** レポートの提出方法

1.4. sos レポートの生成と、GPG パスフレーズ暗号化によるセキュリティーの保護

この手順では、**sos** レポートを生成して、パスフレーズをベースにした GPG2 対称暗号化を使用してセキュリティーを確保する方法を説明します。**sos** レポートは、公共ネットワーク経由で第三者に転送する必要がある場合など、レポートの内容をパスワードで保護することが推奨されます。



注記

暗号化した **sos** レポートを作成する場合には、ディスク領域の倍の容量を一時的に使用するため、十分な領域を確保してください。

1. **sosreport** ユーティリティーでは、 **sos** レポートを暗号化せずに作成します。
2. このユーティリティーは、**sos** レポートを新しいファイルとして暗号化します。
3. 次に、ユーティリティーは暗号化されていないアーカイブを削除します。

前提条件

- **sos** をインストールしている。
- **root** 権限が必要である。

手順

1. **sosreport** コマンドを実行し、**--encrypt-pass** でパスフレーズを指定します。バージョン 3.9 以降の **sos** パッケージでは、**--upload** オプションを追加して、**sos** レポートの生成直後に Red Hat に転送できます。

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

sosreport (version 3.9)

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. **(オプション)** Red Hat でテクニカルサポートケースをすでに起票している場合には、ケース番号を入力して **sos** レポートファイルの名前に追加します。**--upload** を指定している場合は対象のケースにアップロードされます。ケース番号がない場合は、このフィールドを空白にしておきます。ケース番号の入力は任意であるため、**sosreport** ユーティリティーの動作には影響はありません。

```
Please enter the case id that you are generating this report for []: <8-digit_case_number>
```

3. コンソール出力の末尾に表示されている sos レポートファイルの名前を書き留めておきます。

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

Your sosreport has been generated and saved in:
/var/tmp/secured-sosreport-server1-12345678-2021-01-24-ueqijfm.tar.xz.gpg

Size    17.53MiB
Owner   root
md5     32e2bdb23a9ce3d35d59e1fc4c91fe54

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

検証手順

1. **sosreport** ユーティリティーで、以下の要件を満たすアーカイブが作成されたことを確認します。

   - ファイル名が **secured** で始まる。
   - ファイル名が **.gpg** 拡張子で終わる。
   - **/var/tmp/** ディレクトリーにある。

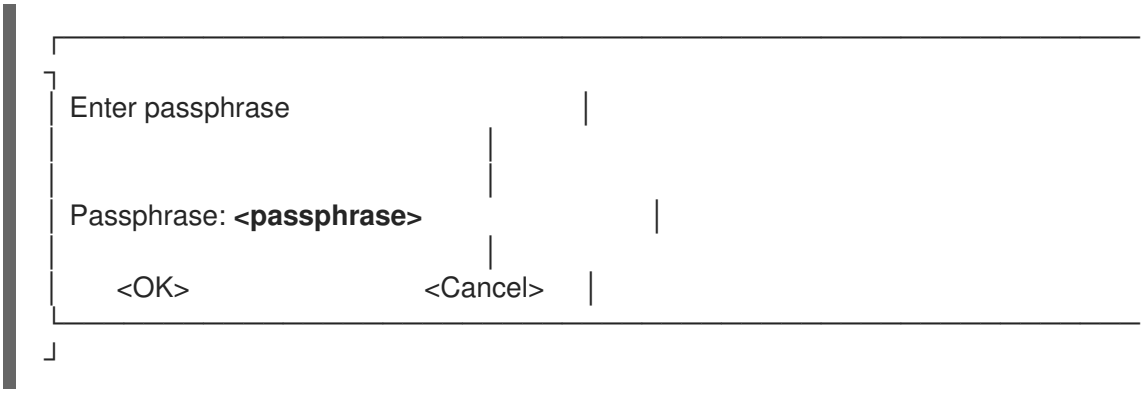
```
[user@server1 ~]$ sudo ls -l /var/tmp/sosreport*
[sudo] password for user:
-rw-------. 1 root root 18381537 Jan 24 17:55 /var/tmp/secured-sosreport-server1-12345678-2021-01-24-ueqijfm.tar.xz.gpg
```

2. アーカイブの暗号化に使用したパスフレーズと同じものを使用して、アーカイブを復号できることを確認します。

   a. **gpg** を使用して、アーカイブを復号します。

   ```
   [user@server1 ~]$ sudo gpg --output decrypted-sosreport.tar.gz --decrypt /var/tmp/secured-sosreport-server1-12345678-2021-01-24-ueqijfm.tar.xz.gpg
   ```

   b. プロンプトが表示されたら、アーカイブの暗号化に使用したパスフレーズを入力します。

   c. **gpg** ユーティリティーが、暗号化されていない、ファイル拡張子が **.tar.gz** のアーカイブを生成したことを確認します。

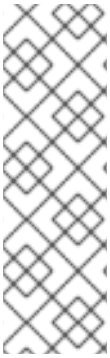
   ```
   [user@server1 ~]$ sudo ls -l decrypted-sosreport.tar.gz
   [sudo] password for user:
   -rw-r--r--. 1 root root 18381537 Jan 24 17:59 decrypted-sosreport.tar.gz
   ```

関連情報

- Red Hat テクニカルサポートへの **sos** レポートの提出方法

1.5. sos レポートの生成と、キーペアをベースにする GPG 暗号化によるセキュリティー保護

この手順では、**sos** レポートを生成し、GPG キーリングからのキーペアをベースにする GPG2 暗号化を使用してセキュリティーを確保する方法を説明します。サーバーに保存されている **sos** レポートを保護する場合など、この種類の暗号化を使用して **sos** レポートのコンテンツを保護できます。



注記

暗号化した **sos** レポートを作成する場合には、ディスク領域の倍の容量を一時的に使用するため、十分な領域を確保してください。

1. **sosreport** ユーティリティーでは、 **sos** レポートを暗号化せずに作成します。
2. このユーティリティーは、**sos** レポートを新しいファイルとして暗号化します。
3. 次に、ユーティリティーは暗号化されていないアーカイブを削除します。

前提条件

- **sos** をインストールしている。
- **root** 権限が必要である。
- GPG2 キーを作成している。

手順

1. **sosreport** コマンドを実行し、**--encrypt-key** オプションで GPG キーリングを所有するユーザー名を指定します。バージョン 3.9 以降の **sos** パッケージでは、**--upload** オプションを追加して、**sos** レポートの生成直後に Red Hat に転送できます。

注記

sosreport コマンドを実行するユーザーは、**sos** レポートの暗号化および復号化に使用する GPG キーリングの所有者で **なければなりません**。ユーザーが **sudo** を使用して **sosreport** コマンドを実行する場合は、**sudo** でキーリングを設定するか、ユーザーがそのアカウントに直接シェルアクセスできる必要があります。

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

sosreport (version 3.9)

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. **(オプション)** Red Hat でテクニカルサポートケースをすでに起票している場合には、ケース番号を入力して **sos** レポートファイルの名前に追加します。**--upload** を指定している場合は対象のケースにアップロードされます。ケース番号がない場合は、このフィールドを空白にしておきます。ケース番号の入力は任意であるため、**sosreport** ユーティリティーの動作には影響はありません。

```
Please enter the case id that you are generating this report for []: <8-digit_case_number>
```

3. コンソール出力の末尾に表示されている **sos** レポートファイルの名前を書き留めておきます。

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

Your sosreport has been generated and saved in:
/var/tmp/secured-sosreport-server1-23456789-2021-01-27-zhdqhdi.tar.xz.gpg

Size    15.44MiB
Owner   root
md5     ac62697e33f3271dbda92290583d1242

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

検証手順

1. **sosreport** ユーティリティーで、以下の要件を満たすアーカイブが作成されたことを確認します。
   - ファイル名が **secured** で始まる。
   - ファイル名が **.gpg** 拡張子で終わる。
   - **/var/tmp/** ディレクトリーにある。

```
[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-server1-23456789-2021-01-27-zhdqhdi.tar.xz.gpg
```

2. 暗号化に使用したキーと同じキーでアーカイブを復号化できることを確認します。
   a. **gpg** を使用して、アーカイブを復号します。

```
[user@server1 ~]$ sudo gpg --output decrypted-sosreport.tar.gz --decrypt
/var/tmp/secured-sosreport-server1-23456789-2021-01-27-zhdqhdi.tar.xz.gpg
```

   b. プロンプトが表示されたら、GPG キーの作成に使用したパスフレーズを入力します。

```
┌──────────────────────────────────────────────────────────────────────────────┐
│ 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. **gpg** ユーティリティーが、暗号化されていない、ファイル拡張子が **.tar.gz** のアーカイブを生成したことを確認します。

```
[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
```

関連情報

- Red Hat テクニカルサポートへの **sos** レポートの提出方法

1.6. GPG2 キーの作成

以下の手順では、IdM バックアップユーティリティーなどの暗号化ユーティリティーで使用する GPG2 キーを生成する方法を説明します。

前提条件

- **root** 権限が必要である。

手順

1. **pinentry** ユーティリティーをインストールして設定します。

```
[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. 希望する内容で、GPG キーペアの生成に使用する **key-input** ファイルを作成します。以下に例を示します。

```
[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. **(オプション)** デフォルトでは、GPG2 はキーリングを **~/.gnupg** ファイルに保存します。カスタムキーリングの場所を使用するには、**GNUPGHOME** 環境変数を、root のみがアクセスできるディレクトリーに設定します。

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

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

4. **key-input** ファイルーのコンテンツに基づいて、新しい GPG2 キーを生成します。

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

5. GPG2 キーを保護するパスフレーズを入力します。このパスフレーズを使用して、秘密鍵にアクセスし、復号化します。

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

6. パスフレーズを再度入力して、正しいパスフレーズを確認します。

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

7. 新しい GPG2 キーが正常に作成されたことを確認します。

```
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
```

検証手順

- サーバーの GPG キーの一覧を表示します。

```
[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>
```

関連情報

- GNU Privacy Guard

1.7. レスキュー環境からの sos レポートの生成

Red Hat Enterprise Linux (RHEL) ホストが適切に起動しない場合は、**sos** レポートを収集するために、ホストを起動して **レスキュー環境** を作成してください。

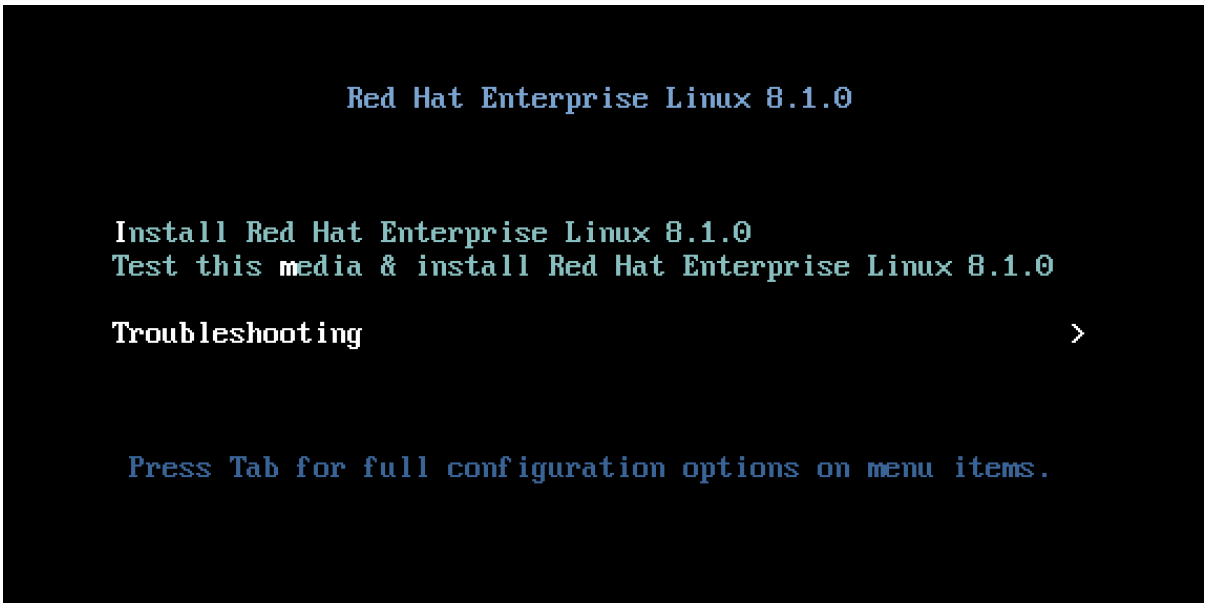
レスキュー環境を使用すると、**/mnt/sysimage** にターゲットシステムをマウントし、そのコンテンツにアクセスして、**sosreport** コマンドを実行できます。

前提条件

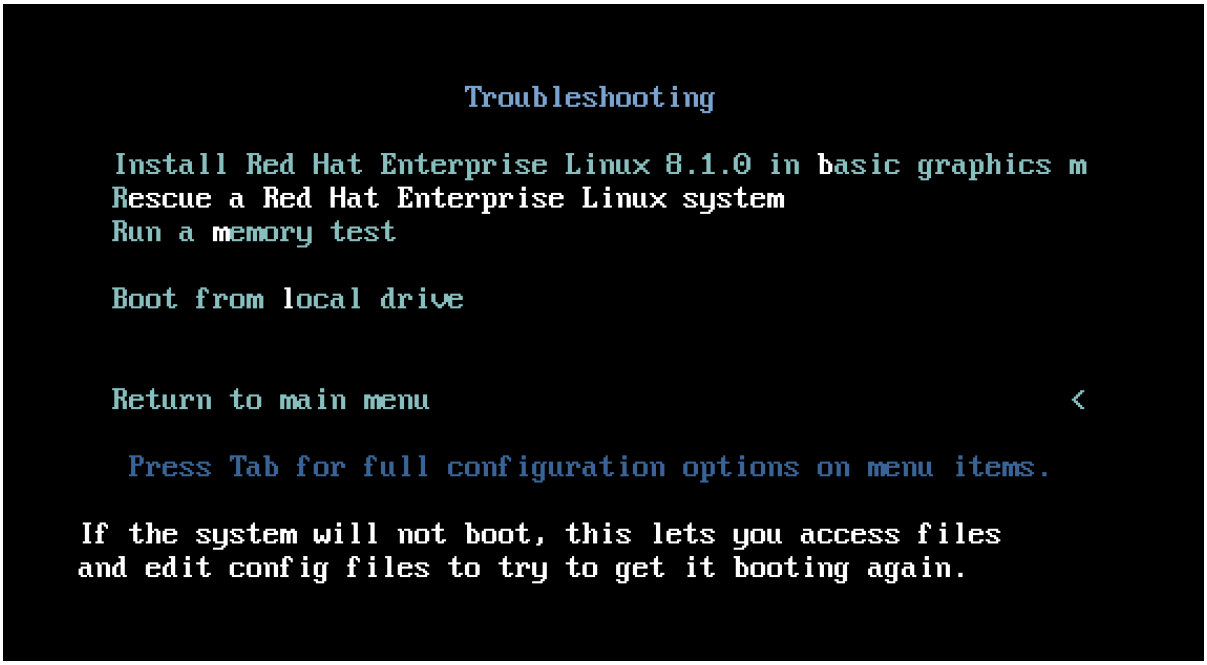
- ホストがベアメタルサーバーの場合は、マシンへの物理アクセスが必要である。
- ホストが仮想マシンの場合は、ハイパーバイザーにある仮想マシンの設定へのアクセス権が必要である。
- RHEL インストールを行うための ISO イメージファイル、インストール DVD、netboot CD、PXE (Preboot Execution Environment) 設定などの RHEL インストールソース。

手順

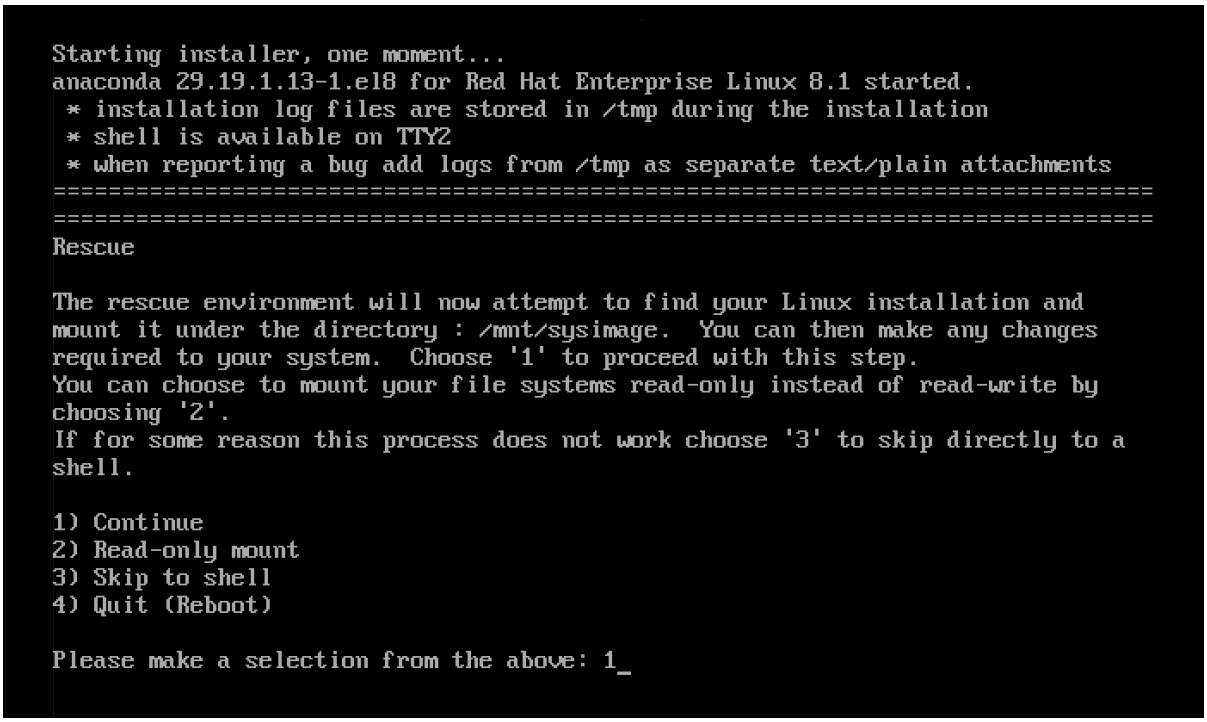
1. インストールソースからホストを起動します。
2. インストールメディアのブートメニューで、**トラブルシューティング** を選択します。



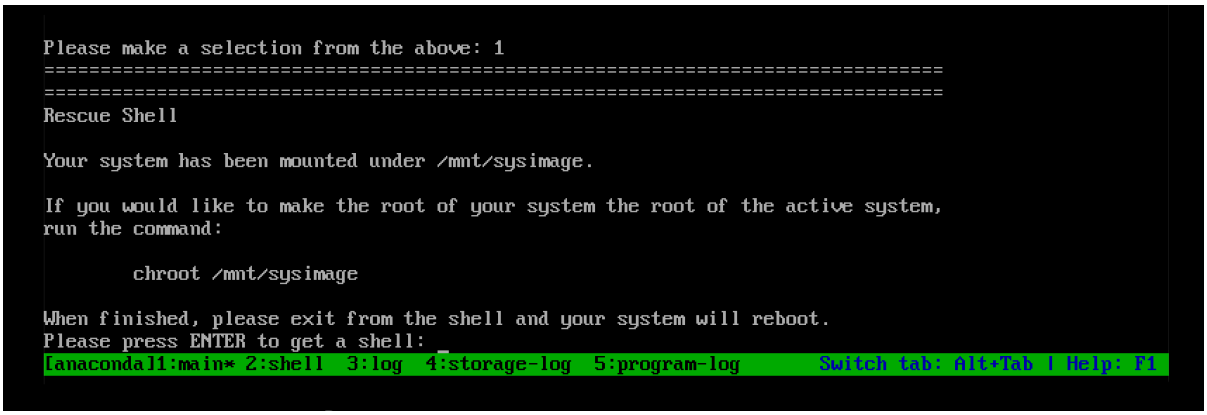
3. トラブルシューティング メニューで **Red Hat Enterprise Linux システムのレスキュー** オプションを選択します。



4. レスキューメニューで **1** を選択し、**Enter** キーを押して続行し、**/mnt/sysimage** ディレクトリーにシステムをマウントします。



5. プロンプトが表示されたら、**Enter** キーを押してシェルを取得します。



6. **chroot** コマンドを使用して、root ディレクトリーに見せかけたディレクトリーを **/mnt/sysimage** ディレクトリーのレスキューセションに変更します。

```
================================================================================
================================================================================
Rescue Shell

Your system has been mounted under /mnt/sysimage.

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

        chroot /mnt/sysimage

When finished, please exit from the shell and your system will reboot.
Please press ENTER to get a shell:
sh-4.4# chroot /mnt/sysimage
bash-4.4#
[anaconda]1:main* 2:shell  3:log  4:storage-log  5:program-log       Switch tab: Alt+Tab | Help: F1
```

7. **sosreport** を実行し、画面の指示に従います。バージョン 3.9 以降の **sos** パッケージでは、**--upload** オプションを追加して、**sos** レポートの生成直後に Red Hat に転送できます。

```
bash-4.4# sosreport

sosreport (version 3.7)

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.d5z2riw6 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:

  https://access.redhat.com/support/

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.

[anaconda]1:main* 2:shell  3:log  4:storage-log  5:program-log       Switch tab: Alt+Tab | Help: F1
```

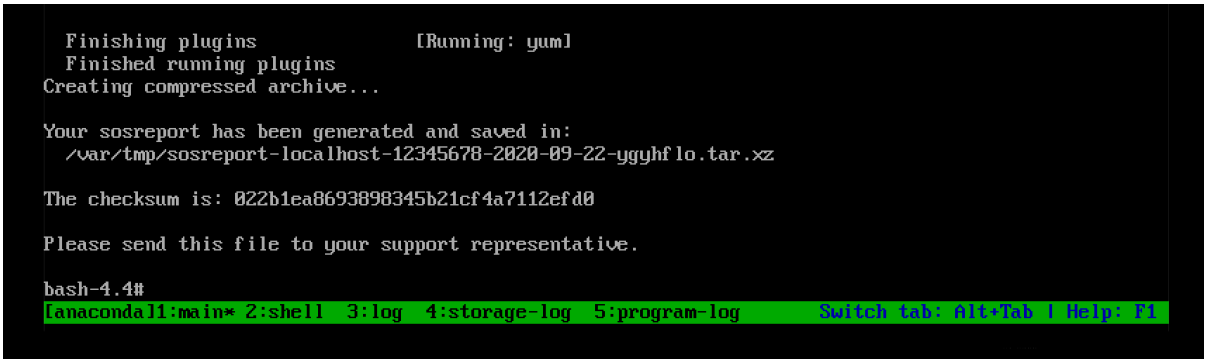
8. **(オプション)** Red Hat でテクニカルサポートケースをすでに起票している場合には、ケース番号を入力して **sos** レポートファイルの名前に追加します。**--upload** を指定しており、ホストがインターネットに接続されている場合は対象のケースにアップロードされます。ケース番号がない場合は、このフィールドを空白にしておきます。ケース番号の入力は任意であるため、**sosreport** ユーティリティーの動作には影響はありません。

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

Please enter the case id that you are generating this report for []: 12345678_

[anaconda]1:main* 2:shell  3:log  4:storage-log  5:program-log       Switch tab: Alt+Tab | Help: F1
```

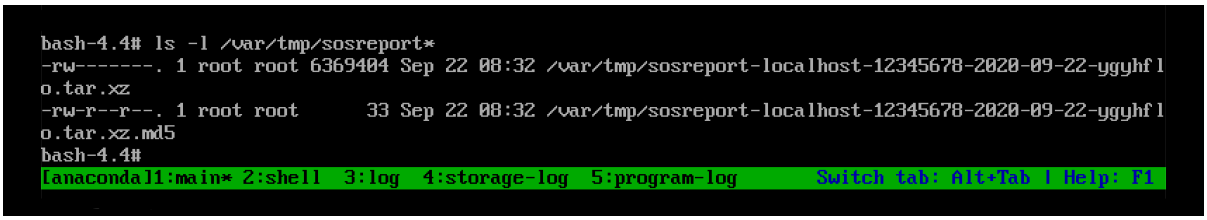
9. コンソール出力の末尾に表示されている **sos** レポートファイルの名前を書き留めておきます。



10. ホストがインターネットに接続されていない場合は、**scp** などのファイル転送ユーティリティーを使用して、ネットワーク上の別のホストに **sos** レポートを転送して Red Hat テクニカルサポートケースにアップロードします。

検証手順

- **sosreport** ユーティリティーが、**/var/tmp/** ディレクトリーにアーカイブを作成したことを確認します。



関連情報

- RHEL インストール DVD の ISO をダウンロードするには、Red Hat カスタマーポータルの downloads セクションに移動してください。製品のダウンロード を参照してください。
- Red Hat テクニカルサポートへの **sos** レポートの提出方法

1.8. RED HAT テクニカルサポートへの SOS レポートの提供方法

以下の方法を使用して、**sos** レポートを Red Hat テクニカルサポートにアップロードできます。

sosreport コマンドでのアップロード

バージョン 3.9 以降の **sos** パッケージでは、**--upload** を使用して、レポートの生成直後に、**sos** レポートを Red Hat に転送できます。

- プロンプトが表示されたらケース番号を指定するか、**--case-id** または **--ticket-number** のオプションを使用すると、**sosreport** ユーティリティーは、Red Hat カスタマーポータルアカウントの認証後に、**sos** レポートをケースにアップロードします。
- ケース番号を指定しない場合、または認証を行わない場合には、sos ユーティリティーにより、**sos** レポートが Red Hat 公開 FTP サイトにアップロードされます。Red Hat テクニカルサポートエンジニアに、**sos** レポートのアーカイブ名を提示し、エンジニアがアーカイブにアクセスできるようにします。

```
[user@server1 ~]$ sudo sosreport --upload
[sudo] password for user:

sosreport (version 3.9)
```

```
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
```

Red Hat カスタマーポータルからのファイルのアップロード

Red Hat ユーザーアカウントを使用して、Red Hat カスタマーポータル Web サイトの **サポートケース** セクションにログインし、テクニカルサポートケースに **sos** レポートをアップロードできます。ログインするには、サポートケース にアクセスします。

Red Hat Support Tool を使用したファイルのアップロード

Red Hat Support Tool を使用すると、コマンドラインから Red Hat テクニカルサポートケースにファイルを直接アップロードできます。ケース番号が必要です。

```
[user@server1 ~]$ redhat-support-tool addattachment -c <8-digit_case_number>
</var/tmp/sosreport_filename>
```

関連情報

- *FTP、**curl** など、Red Hat テクニカルサポートに **sos** レポートを提出する他の方法については、Red Hat ナレッジベースの記事「Red Hat サポートにファイルを提出する方法 (vmcore、rhev logcollector、sosreports、ヒープダンプ、ログファイルなど)」を参照してください。*