Red Hat Enterprise Linux 9

サポート体験を最大限に活用

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: 2022-05-30

Red Hat Enterprise Linux 9 サポート体験を最大限に活用

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の提供

ご意見ご要望をお聞かせください。ドキュメントの改善点はございませんか。

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

第1章 テクニカルサポート用の sosレポートの生成

1.1. sos 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。**sos** ユーティリティー（ **sosreport**とも呼ばれます）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調査全体で参照できる診断情報を収集するための標準化された方法を提供します。**sos** ユーティリティーを使用すると、データ出力を繰り返し求められないようにするのに役立ちます。

sos ユーティリティーを使用すると、1つ以上のシステムからさまざまなデバッグ情報を収集し、必要に応じて機密データを消去し、レポートの形式でこれを Red Hat にアップロードできます。具体的には、3 つの **sos** コンポーネントは以下を行います。

- **sos report** は、**1つ** のシステムからデバッグ情報を収集します。

注記

このプログラムは、元々 **sosreport** という名前でした。**sosreport** を実行すると、同じ引数を使用して代わりに **sos report** が呼び出されるため、引き続き機能すると言えます。

- **sos collect** を使用すると、指定されたノードセットから個別の **sos** レポートを実行および収集できます。
- そのため、ユーザー名、ホスト名、IP アドレス、またはユーザー指定のデータなどの機密情報が **クリーンアップ** されます。

レポートで収集される情報には、RHEL システムからの設定詳細、システム情報、診断情報が含まれます。以下に例を示します。

- 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

sos 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するデータを書き込みます。

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

関連情報

- **sosreport(1)** man page

1.2. コマンドラインからの sos のインストール

sos ユーティリティーを使用するには、**sos** パッケージ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-4.2-15.el9.noarch
```

1.3. コマンドラインからの sos レポートの生成

sos report 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** パッケージをインストールしている。
- **root** 権限が必要である。

手順

1. **sos report** コマンドを実行し、画面の指示に従います。**--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 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.
```

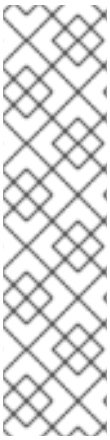
```
...

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

2. **（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** オプションを指定した場合には、そ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り、**sos** ユーティリティーの動作には影響しません。

```
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 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.
```



注記

- **--batch** オプションを使用すると、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 sos report --batch --case-id <8-digit_case_number>
```

- **--clean** オプションを使用して、収集したばかりの **sos** レポートを難読化することもできます。

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

検証手順

- **sos** ユーティリティーが、コマンド出力の説明と一致する **/var/tmp/** に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-server1-12345678-2022-04-17-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. 複数のシステムで同時に SOS レポートを生成および収集する

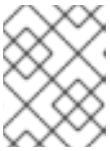
sos ユーティリティーを使用して、複数のシステムで **sos report** コマンドをトリガーできます。レポートが終了するまで待機し、生成されたすべてのレポートを収集します。

前提条件

- 実行する **クラスター** タイプまたは **ノード** の一覧を把握している。
- すべてのシステムに **sos** パッケージをインストールしている。
- すべてのシステムに **root** アカウントの **ssh** キーがあるか、**--password** オプションを使用して root パスワードを指定できます。

手順

- **sosreport** コマンドを実行し、画面の指示に従います。



注記

デフォルトでは、**sos collect** は、レポートを収集する **ノード** を自動的に識別するために実行する **クラスター** のタイプを特定しようとします。

a. **--cluster** または **--nodes** オプションを使用して、**クラスター** または **ノード** の種類を手動で設定できます。

b. **--master** オプションを使用して、リモートノードに **sos** ユーティリティーをポイントし、**クラスター** タイプと **ノード** 一覧を決定することもできます。したがって、**sos** レポートを収集するために **クラスター ノード** のいずれかにログインする必要はなく、ワークステーションから実行できます。

c. **--upload** オプションを追加して、**sos report** の生成直後にこれを Red Hat に転送できます。

d. 有効な **sos レポート** オプションをさらに指定でき、**--batch** オプションや **--clean** オプションなどのすべての **sos** レポートの実行に渡されます。

```
[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 ~]#
```

検証手順

- **sos collect** コマンドが、**/var/tmp/** ディレクトリーで、コマンド出力の説明に一致するアーカイブを作成したことを確認します。

```
[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
```

関連情報

- **--batch** および **--clean** オプションの使用例は、Generating an **sos** report from the command line を参照してください。

1.5. SOS レポートのクリーニング

sos ユーティリティーは、ユーザー名、ホスト名、IP アドレス、またはユーザー指定のキーワードなどの機密データを難読化するルーチンを提供します。元の **sos report** または **sos collect** は変更されず、

新しい ***-obfuscated.tar.xz** ファイルが生成され、サードパーティーと共有されることが意図されています。

注記

sos report または **sos collect** コマンドに **--clean** オプションを使用して、クリーナー機能を追加できます。

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

前提条件

- **sos report** または **sos collect** tarball を生成している。
- **(オプション)** 難読化するユーザー名、ホスト名、およびその他のデータ以外の特定のキーワードのリストがあります。

手順

- sos **レポート** または sos で tarball を **収集し、画面の指示に従い、sos clean** コマンドを実行します。
    a. **--keywords** オプションを追加して、特定のキーワードリストをさらにクリーンアップできます。
    b. **--usernames** オプションを追加して、さらに機密性の高いユーザー名を難読化できます。自動ユーザー名クリーニングは、UID が 1000 以上のユーザーの **lastlog** ファイルを通じて報告されたユーザーに対して、自動的に実行されます。このオプションは、実際のログインとして表示されない可能性がある LDAP ユーザーに使用されますが、特定のログファイルで発生する可能性があります。

```
[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
```

検証手順

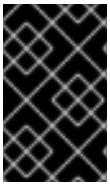
- **sos clean** コマンドが、**/var/tmp/** ディレクトリーで、コマンド出力からの説明に一致する難読化されたアーカイブと難読化マッピングを作成したことを確認します。

```
[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
```

- ***-private_map** ファイルで難読化マッピングを確認します。

```
[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"
    }
}
```



重要

Red Hat サポートは、元の値に変換する必要のある難読化された用語を参照する可能性があるため、元の難読化されていないアーカイブと ***private_map*** ファイルの両方をローカルに保持します。

1.6. 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、パスフレーズに基づいて対称 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。**sos** レポートの内容は、たとえばパブリックネットワークを介してサードパーティーに転送する必要がある場合など、sos レポートのコンテンツをパスワードで保護できます。

注記

暗号化された **sos** レポートを作成する際にはディスク領域を一時的に使用するため、十分な領域があることを確認してください。

1. **sos** ユーティリティーは、**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** パッケージをインストールしている。
- **root** 権限が必要である。

手順

1. **sos report** コマンドを実行し、**--encrypt-pass** オプションでパスフレーズを指定します。**--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 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. **（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** オプションを指定した場合には、そ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り、**sos** ユーティリティーの動作には影響しません。

```
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-server1-12345678-2022-01-24-ueqijfm.tar.xz.gpg

Size    17.53MiB
Owner   root
md5     32e2bdb23a9ce3d35d59e1fc4c91fe54

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

検証手順

1. **sos** 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。
   - ファイル名は、**セキュアな** で始まります。
   - ファイル名は、**.gpg** 拡張子で終わります。
   - **/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-server1-12345678-2022-01-24-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** コマンドを使用して、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-server1-12345678-2022-01-24-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。

```
┌──────────────────────────────────────────────────────────────────────────────┐
│ Enter passphrase                                                             │
```

```
┌                                                    ┐
│                                                    │
│ 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 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

1.7. 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に基づいて 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、このタイプ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

暗号化された **sos** レポートを作成する際にはディスク領域を一時的に使用するため、十分な領域があることを確認してください。

1. **sos** ユーティリティーは、**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** パッケージ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. **sos report** 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。**--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

sos report 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 キーリングを所有するユーザーである **必要** があります。ユーザーが **sudo** を使用して **sos report** 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 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. **（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** オプションを指定した場合には、そ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り、**sos** ユーティリティーの動作には影響しません。

```
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-server1-23456789-2022-02-27-zhdqhdi.tar.xz.gpg

Size    15.44MiB
Owner   root
md5     ac62697e33f3271dbda92290583d1242

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

検証手順

1. **sos** 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。
   - ファイル名は、**セキュアな** で始まります。
   - ファイル名は、**.gpg** 拡張子で終わります。

- **/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-server1-23456789-2022-01-27-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** コマンドを使用して、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-server1-23456789-2022-01-27-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

1.8. GPG2 キーの作成

以下の手順では、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 プライバシーガード

1.9. 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 **レスキュー環境** で起動できます。

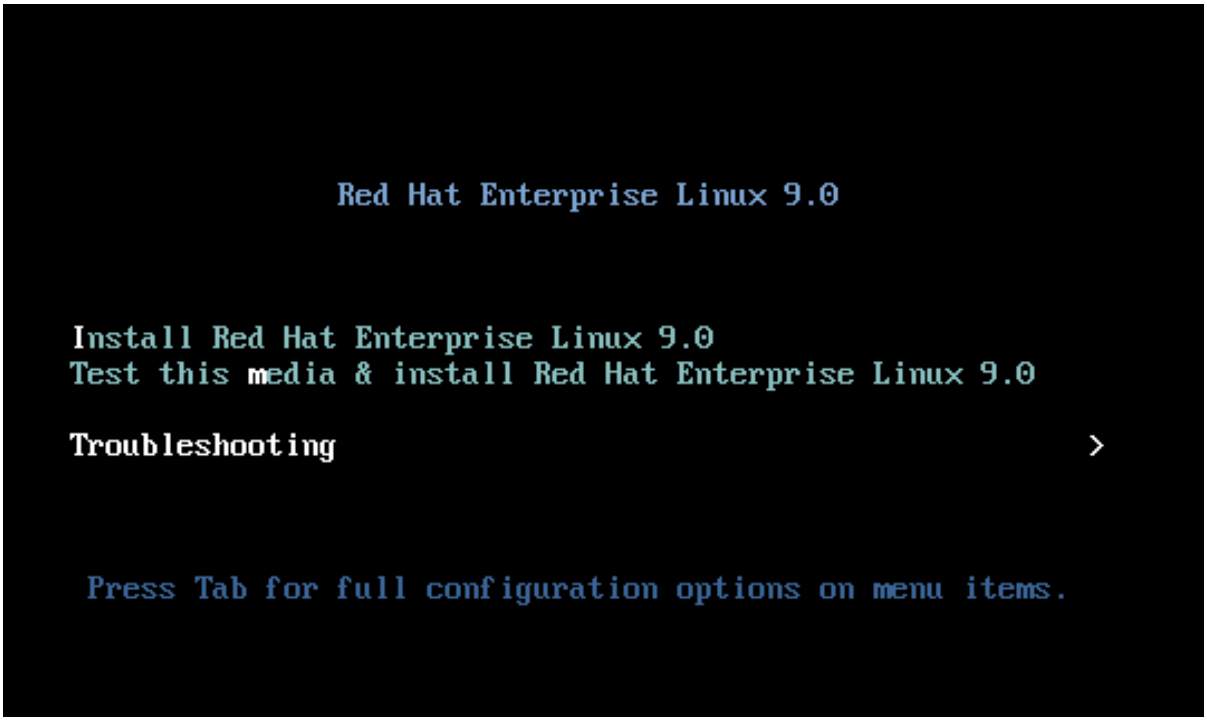
レスキュー環境を使用すると、**/mnt/sysimage** にターゲットシステムをマウントし、そのコンテンツにアクセスして、**sos report** コマンドを実行できます。

前提条件

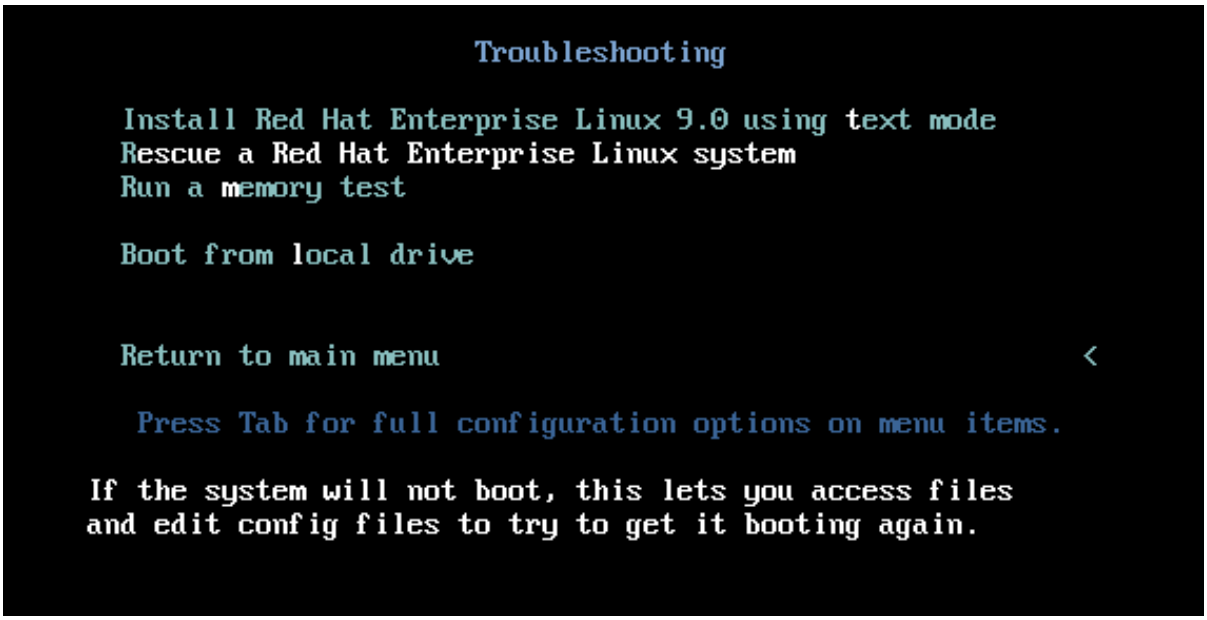
- ホストがベアメタルサーバーの場合は、マシンへの物理アクセスが必要である。
- ホストが仮想マシンの場合は、ハイパーバイザーにある仮想マシンの設定へのアクセス権が必要である。
- RHEL インストールを行うための ISO イメージファイル、インストール DVD、netboot CD、PXE (Preboot Execution Environment) 設定などの RHEL インストールソース。

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。

```
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. 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。

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

```
  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_
```

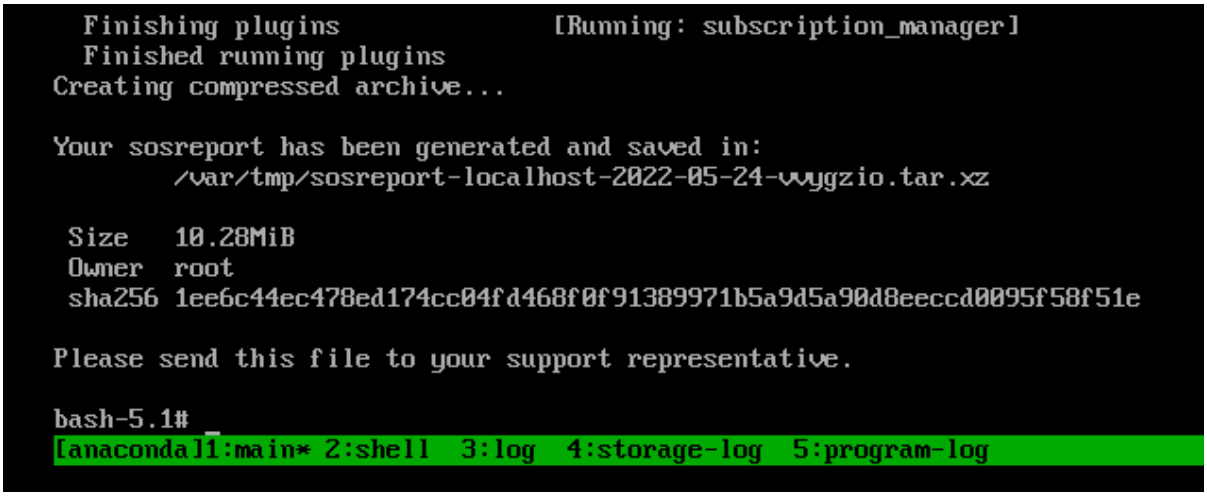
7. **sos report** コマンドを実行し、画面の指示に従います。**--upload** オプションを追加して、**sos** レポートの生成直後に Red Hat に転送できます。

```
bash-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. **(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り、**sos** ユーティリティーの動作には影響しません。

```
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. 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

- **sos** 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

1.10. 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。

sos report コマンドでのアップロード

--upload オプションを使用すると、**sos** レポートの生成直後に 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** オプションを使用すると、**sos** 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や、認証を行わない場合は、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指定して、アクセスできるようにします。

```
[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
```

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の 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。

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方法は、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供する方法（vmcore、Projected 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。