Veritas™ System Recovery 16 User's Guide

Linux Edition

VERITAS™

Contents

Introducing Veritas™ System Recovery for Linux

This chapter includes the following topics:

■ About Veritas System Recovery 16 Linux Edition

About Veritas System Recovery 16 Linux Edition

Veritas System Recovery 16 Linux Edition lets you recover from system loss or disasters in minutes, not hours, or days. It provides fast, easy to use system restoration to help you meet your recovery time objectives. Veritas System Recovery 16 Linux Edition lets you capture recovery points of all the partitions and volumes on a live Linux system. The recovery points can include partitions and volumes containing the operating system (OS), applications, system settings, configurations, files, and data.

When you experience a problem with your computer, you can restore a file system partition or an entire drive. This recovery process returns your computer to a previous, functional state with the operating system, applications, and data files intact.

Using Veritas System Recovery 16 Linux Edition you can do the following:

■ Perform backups (create recovery points) of partitions and volumes on your Linux system.

■ Restore volumes and partitions using the recovery points you have created.

■ Create a Veritas Recovery Disk that you can use to recover your computer if it does not start.

■ Mount recovery points so you can restore individual files and folders.

See "About backing up a Linux computer" on page 12.

Installing Veritas System Recovery 16 Linux Edition

This chapter includes the following topics:

- Before you install
- About upgrading to Veritas System Recovery 16 Linux Edition
- Installing Veritas System Recovery 16 Linux Edition
- Uninstalling Veritas System Recovery 16 Linux Edition

Before you install

Installation procedures might vary depending on your work environment and the type of Linux you use. This chapter focuses on installing Veritas System Recovery 16 Linux Edition from a download.

Before you install Veritas System Recovery 16 Linux Edition, ensure that your computer meets the system requirements. Review the Readme file for any known issues.

See "System requirements" on page 5.

See "About supported file systems and removable media " on page 8.

See "Installing Veritas System Recovery 16 Linux Edition" on page 9.

System requirements

The following table lists the system requirements for Veritas System Recovery 16 Linux Edition to function properly.

Table 2-1 Minimum system requirements

Component	Minimum requirements
Operating system	You can find a list of compatible operating systems, platforms, and applications at the following URL:
	https://www.veritas.com/support/en_US/search-results.html?keyword=V-306-17*
	Note: SUSE Linux Enterprise Desktop and Red Hat Enterprise Linux Desktop are not supported.
	All standard kernel versions are supported for the Linux distributions that are listed.
	The binary drivers are already included for all standard kernels that are supported for the listed Linux distributions.
	For custom kernels (recompiled kernels), the installer builds and installs the custom snap driver for the running custom kernel during installation. The system must have the custom kernel headers installed.
RAM	The following are the memory requirements for SUSE Linux, Red Hat Linux, and the CentOS Linux:
	■ SUSE Linux: 1 GB
	■ Red Hat Linux: 1 GB
	■ CentOS Linux: 1 GB
Available hard disk space	The Veritas System Recovery 16 Linux Edition installation requires 50 MB of free disk space. To install and use the option for extracting and creating a Veritas Recovery Disk, you should have at least 200 MB of disk space.
	You should have sufficient hard disk space on a local hard disk or network server for storing recovery points.
	Be aware that the file sizes of resulting recovery points depend on the amount of data that you intend to back up.
DVD-ROM drive	The drive can be any speed, but it must be capable of being used as the startup drive from the BIOS.

Table 2-1 Minimum system requirements *(continued)*

Component	Minimum requirements
Software	Other required software:
	■ The Granular File Recovery option (mount.v2i utility) uses libfuse. Currently, only Fuse 2.7.x is supported. Other versions of Fuse are not supported, but may work.
	■ createSRD uses the squashfs-tools package on RHEL for creating RHEL Veritas Recovery Disks. You must install the required squashfs-tools package on RHEL 5.x and squashfs-tools and genisoimage packages on RHEL 6.x.

Installing Fuse

The Fuse driver and libfuse must be installed before you use the Veritas System Recovery 16 Linux Edition recovery point mount utility. On SUSE Linux and RHEL 6.x, the Fuse driver is installed by default, but, the Fuse library (libfuse) must be installed. On Red Hat 5.x Linux, both, the Fuse driver and the Fuse library must be installed.

You can install the Fuse driver and libfuse from the RPM repository. You can also install Fuse from a downloaded .tar file.

To download and install the Fuse .tar file

1   Log on as root.

2   Download Fuse 2.7.x from http://fuse.sourceforge.net.

3   Extract the .tar.gz file.

4   Change the directory to the Fuse extracted folder.

5   Run the following commands in the order indicated.

```
./configure

make

make install
```

6 Check /etc/ld.so.conf using a text editor (for example, run vi /etc/ld.so.conf).
Look for a line containing '/usr/local/lib'. If it is missing, you must add it.

7 Run ldconfig command

```
ldconfig
```

SUSE requires only the installation of the libfuse rpm libraries. Red Hat requires
both the libfuse rpm library and the fuse module.

See "Installing Veritas System Recovery 16 Linux Edition" on page 9.

See "System requirements" on page 5.

About supported file systems and removable media

Veritas System Recovery 16 Linux Edition supports the following file systems and
removable media:

Supported file systems	Veritas System Recovery 16 Linux Edition supports the following file systems: ■ ReiserFS version 3 ■ EXT2 ■ EXT3 ■ EXT4 ■ FAT16 with 2-GB limit ■ FAT32 ■ XFS **Note:** Veritas System Recovery 16 Linux Edition only supports the listed file systems. Other file systems such as Btrfs, JFS, NSS, and Reiser4 are not supported.
Supported platforms	Veritas System Recovery 16 Linux Edition supports the following new platforms: ■ RHEL 5.11 ■ RHEL 6.6 ■ RHEL 6.5 ■ CentOS 5.10 ■ CentOS 6.5
Removable media	Backing up is not supported to some types of removable media in Veritas System Recovery 16 Linux Edition. You must save recovery points to a local mount point.

See "Before you install" on page 5.

See "Installing Veritas System Recovery 16 Linux Edition" on page 9.

When you delay licensing

If you choose to delay installation of the license key, all features in Veritas System Recovery 16 Linux Edition remain enabled during a 60-day trial period.

Veritas Recovery Disk (SRD), a component of Veritas System Recovery 16 Linux Edition, is available with no trial period. However, you need a valid license key to use the back up feature in Veritas Recovery Disk. If you have created the Veritas Recovery Disk on a computer having licensed version of Veritas System Recovery 16 Linux Edition, the Veritas Recovery Disk is automatically licensed. In such cases, you can perform cold backups using the Veritas Recovery Disk without the need of adding a license key.

You can purchase a license key and activate the software at any time (even after the trial period expires) without the need to reinstall. To activate Veritas System Recovery 16 Linux Edition before or after the trial period, you can use the following command:

```
#symsr -addlicense <license key>
```

See "Installing Veritas System Recovery 16 Linux Edition" on page 9.

See "Uninstalling Veritas System Recovery 16 Linux Edition" on page 11.

About upgrading to Veritas System Recovery 16 Linux Edition

You can upgrade Symantec System Recovery 2011, 2013, or 2013 R2 Linux Edition to Veritas System Recovery 16 Linux Edition. When you upgrade, the installation program automatically uninstalls the previous version of Veritas System Recovery Linux Edition from your computer. However, all the configurations, policies, tasks, and recovery points are preserved.

To upgrade to Veritas System Recovery 16 Linux Edition, install 16 Edition on your computer.

See "Installing Veritas System Recovery 16 Linux Edition" on page 9.

Installing Veritas System Recovery 16 Linux Edition

Before you begin, you should review the requirements and scenarios for installing Veritas System Recovery 16 Linux Edition.

Root privileges are required to install the Veritas_System_Recovery.bin.

To install Veritas System Recovery 16 Linux Edition

1   Log on to your computer as the root user.

2   Copy the Veritas_System_Recovery.bin file from the download or the product DVD to a folder on your Linux computer.

3   Make the Veritas_System_Recovery.bin file an executable by changing to the directory where you copied it and entering the following command at the Linux console:

```
chmod +x Veritas_System_Recovery.bin
```

4   Start the installation process by entering the following command at the Linux terminal:

```
./Veritas_System_Recovery.bin
```

Note: The command that you specified assumes that you are currently in the same directory where the Veritas_System_Recovery.bin file is located. If that is not the case, you must either change to that folder or specify the proper path to it.

5   Page through the license agreement and accept it by entering a `y` or `yes` at the prompt.

6   If you want to install the utility for creating a Veritas Recovery Disk, type a `y` or `yes` at the install Veritas Recovery Disk creation utility prompt.

createSRD is a command line utility for creating a Veritas Recovery Disk CD. A Veritas Recovery Disk CD is not included with Veritas System Recovery 16 Linux Edition. You must create the CD manually using the createSRD utility.

See "Creating a Veritas Recovery Disk for Linux" on page 30.

7   If you want to install the Granular File Recovery utility for mounting a recovery point, type a `y` or `yes` at the install Granular File Recovery utility prompt.

Veritas System Recovery 16 Linux Edition includes command line utilities for mounting or unmounting a recovery point so you can restore individual files and folders.

Note: If you choose not to install the utilities you can run the installation process later. The installation program automatically detects that Veritas System Recovery 16 Linux Edition is installed and prompts you to install the utilities that are not installed.

Uninstalling Veritas System Recovery 16 Linux Edition

After installing Veritas System Recovery 16 Linux Edition, you can uninstall it if needed.

To uninstall Veritas System Recovery 16 Linux Edition

1   Log on to your computer as the root user.

2   Uninstall Veritas System Recovery 16 Linux Edition by entering the following command at the Linux terminal:

    symsr-uninstall

Note: Reinstalling Veritas System Recovery 16 Linux Edition prompts you to install over a previous installation. Uninstalling the product is not required before reinstalling it.

Backing up a Linux computer

This chapter includes the following topics:

- About backing up a Linux computer

- Viewing the details of the disk that you want to back up

- Performing an independent backup

- Scheduling a backup

- Running an existing backup job

About backing up a Linux computer

When you perform a backup on a Linux computer, Veritas System Recovery 16 Linux Edition takes a snapshot of an entire partition or volume, capturing all information that is stored on it for later retrieval. All of your files, folders, desktop settings, programs, and your operating system are captured into a recovery point. You can then use that recovery point to restore an individual partition or your entire computer by restoring all volumes on the system individually.

In addition to backing up your computer after installing Veritas System Recovery 16 Linux Edition, you can also perform a backup by booting into Veritas Recovery Disk. This type of backup is sometimes referred to as a cold backup or offline backup. It lets you create recovery points of partitions and volumes without booting to Linux from your hard drive.

The steps for performing a backup using Veritas Recovery Disk are the same as performing a backup from within Veritas System Recovery 16 Linux Edition.

See "About Veritas Recovery Disk" on page 30.

Viewing the details of the disk that you want to back up

Before you perform or schedule backups of a disk, you can view the partitions, file system types, and segments that are available on it.

To view the details of the disk that you want to back up

1 At the Linux server, log on as user root or a user with administrative privileges.

2 Enter the following command in a terminal window:

```
symsr -info disk
```

Performing an independent backup

To perform a backup using Veritas System Recovery 16 Linux Edition

1 At the Linux server, log on as user root or a user with administrative privileges.

2 Enter the following command in a terminal window:

```
symsr -b volume_name options -d destinationrecoverypoint_name
```

Replace *volume_name* with the name and path of the volume block device or mount point.

Replace *options* with the options you want to use with the backup.

See Backup and Restore (symsr utility) on page 40. for a list of the options available with the Veritas System Recovery 16 Linux Edition command line utility.

Replace *destination* with the location where the recovery point is created.

Replace *recoverypoint_name* with the name you want to assign to the recovery point.

For example, if you want to create a recovery point named system_000.v2i of the /dev/sda1 volume in the same directory where the command is executed and using default options, you enter the following command:

```
symsr -b /dev/sda1 -d system_000.v2i
```

Note: Some characters have special meanings and should not be used in recovery point file names and passwords. These characters include colons (:), back slashes (\), question marks (?), ampersand (&), asterisk (*), and caret (^).

Note: When you back up volumes with unsupported file systems, SmartSector copying is disabled (SmartSector backs up only those sectors on the volume that contain data).

See "Viewing the details of the disk that you want to back up" on page 13.

See "Scheduling a backup" on page 14.

Scheduling a backup

Veritas System Recovery 16 Linux Edition lets you schedule backups on a Linux computer. It provides a command line interface that lets you set the backup options and specify a schedule to run the backups.

While scheduling backups, you can choose to create the following types of recovery points:

- **Independent recovery point**
  Creates a complete, independent backup of the specified volumes or comma-separated multiple volumes.

- **Recovery point set**
  Creates a base recovery point and additional recovery points that contain the incremental changes that are made to the specified volumes or comma-separated multiple volumes

To schedule a backup using Veritas System Recovery 16 Linux Edition

1   At the Linux server, log on as user root or a user with administrative privileges.

2   Enter the following command in a terminal window to start the schedule backup wizard:

    symsr -createjob

Note: To exit the wizard, type **q**, **Q**, or **Quit** at any prompt other than the **Select the source** prompt or the **Select destination** prompt.

3 At the **Select the source** prompt, type the path of the volume block device or the mount point that you want to back up.

You can provide multiple devices or mount points by using a comma (,) separator.

4 At the **Select destination** prompt, type the location where you want to create the recovery points.

5 At the **Create machine specific folder** prompt, type a **y** if you want to create a computer-specific folder in the backup destination.

This option is useful if you use the same backup destination for multiple computers. When you back up a computer, its recovery points are stored in the folder specific to that computer.

6 At the **Select recovery point type** prompt, enter an appropriate option to specify the type of recovery point you want to create.

See "Recovery point type options" on page 16.

7 At the **Select compression level** prompt, enter an appropriate option to set a compression level for the recovery points.

See "Compression level options" on page 17.

8 At the **Select encryption type** prompt, enter an appropriate option to encrypt recovery point data or protect recovery point data using a password.

See "Encryption type options" on page 17.

9 At the **Backup schedule** prompt, enter appropriate options to specify a schedule to run the backups.

The backup schedule options vary depending on the recovery point type you have selected.

See "Scheduling options for starting a new recovery point set (base recovery point)" on page 18.

See "Scheduling options for creating recovery points (incremental recovery points)" on page 19.

See "Scheduling options for an independent recovery point" on page 20.

10 At the **Verify recovery point after creation** prompt, type a **y** if you want to test whether the recovery point is valid or corrupt after it is created.

11 Review the backup job summary and then at the **Save Job** prompt, type a **y** to save the backup job.

12 At the **Provide job name** prompt, enter a name for the backup job.

After you save a backup job, it is available in the system. You can view the details of the existing backups jobs if required.

See "Viewing the details of existing backup jobs" on page 16.

Viewing the details of existing backup jobs

You can see a list of existing backup jobs and their details.

To view the details of existing backup jobs

1 At the Linux server, log on as user root or a user with administrative privileges.

2 Enter the following command in a terminal window:

```
symsr -info job
```

See "Scheduling a backup" on page 14.

Recovery point type options

The following table describes the recovery point type options that you can select while scheduling a backup.

See "Scheduling a backup" on page 14.

Table 3-1   Recovery point type options

Option	Description
Recovery point set (recommended)	Creates a recovery point set of the specified volumes. This backup type requires less storage and is faster that independent recovery point because it contains only the incremental changes that were made to your computer since the previous recovery point **Note:** You can have only one recovery point set defined for each volume at any point of time.
Independent recovery point	Creates a complete, independent backup of the specified volumes. This backup type typically requires more storage space than the recovery point set, especially if you run the backup multiple times.

Compression level options

The following table describes the compression levels that you can apply to the recovery points.

See "Scheduling a backup" on page 14.

Table 3-2   Compression level options

Option	Description
None	Indicates that no compression is applied to the recovery point. Use this option if storage space is not an issue. However, if the backup is saved to a busy network drive, high compression may be faster than no compression because there is less data to write across the network.
Standard (recommended)	Uses low compression for a 40 percent average data compression ratio on recovery points. This option is set by default.
Medium	Uses medium compression for a 45 percent average data compression ratio on recovery points.
High	Uses high compression for a 50 percent average data compression ratio on recovery points. This option is usually the slowest method. When a high compression recovery point is created, CPU usage might be higher than normal. Other processes on the computer might also slow down.

Encryption type options

The following table describes the encryption type options that you can set for the recovery points.

See "Scheduling a backup" on page 14.

Table 3-3   Encryption type options

Option	Description
No password and no encryption	Creates the recovery points without any password protection or encryption. Use this option only if you store your recovery points in a location that is not shared with anyone. Anyone who can access the recovery points can restore from them or view their contents.
Password protected with AES Encryption	Lets you set a password on the recovery point when it is created. Passwords can include standard characters. Passwords cannot include extended characters, or symbols. Use characters with an ASCII value of 128 or lower. Only the users who know the password can restore from or view the contents of the recovery point. Encrypts recovery point data to add another level of protection to your recovery points. Choose from the following encryption levels: ■ **Standard 128-bit (8+ character password)** ■ **Medium 192-bit (16+ character password)** ■ **High 256-bit (32+ character password)**

Scheduling options for starting a new recovery point set (base recovery point)

The following table describes the scheduling options for starting a new recovery point set.

See "Scheduling a backup" on page 14.

Table 3-4   Scheduling options for a new recovery point set

Option	Description
Weekly	Starts a new recovery point set at the defined time and on the days of the week that you specify.

Table 3-4   Scheduling options for a new recovery point set *(continued)*

Option	Description
Monthly	Starts a new recovery point set at the defined time and on the day of the month that you specify.
Quarterly	Starts a new recovery point set at the defined time and on the first day of every quarter.
Yearly	Starts a new recovery point set at the defined time and on the first day of every year.

Scheduling options for creating recovery points (incremental recovery points)

The following table describes the scheduling options for creating recovery points.

See "Scheduling a backup" on page 14.

Table 3-5   Scheduling options for creating recovery points

Option	Description
Schedule	Lets you select the days and a start time for when you want to create the recovery points.
Run more than once per day	Indicates that you want to create recovery points more than once a day to protect the data that you edit or change frequently.
Time between backups	Specifies the time that must occur between two recovery points.
	This option appears only if you have selected to create recovery points more than once in a day.

Table 3-5   Scheduling options for creating recovery points *(continued)*

Option	Description
Number of times	Specifies the number of times the backup should run in a day. This option appears only if you have selected to create recovery points more than once in a day.
	Ensure that you specify a number considering the number of hours that you have specified to occur between two backups. For example, if you have specified a period of 10 hours to occur between backups, you cannot run more than three backups a day.

Scheduling options for an independent recovery point

The following table describes the scheduling options for creating an independent recovery point.

Table 3-6   Scheduling options for an independent recovery point

Option	Description
Weekly	Creates the recovery point at the defined time and on the days of the week that you specify.
Monthly	Creates the recovery point at the defined time and on the day of the month that you specify.
Quarterly	Creates the recovery point at the defined time and on the first day of every quarter
Yearly	Creates the recovery point at the defined time and on the first day of every year.
Run Only Once	Creates the recovery point one time on the date and at the time that you specify.

Running an existing backup job

You can run an existing backup at any point of time. This option is useful in the following situations:

- You modify a large number of files and you want to back them up immediately rather than waiting for the scheduled backup to run.

- You want to back up your computer before you install a new application or before you make any changes to the operating system.

To run an existing backup job

1   At the Linux server, log on as user root or a user with administrative privileges.

2   Enter the following command in a terminal window:

```
symsr -runjob <job id>
```

Replace *<job id>* with the ID of the backup job that you want to run.

You can view the details of existing backup jobs to find out the ID of the backup job that you want to run.

See "Viewing the details of existing backup jobs" on page 16.

Restoring a Linux computer

This chapter includes the following topics:

- About recovering a Linux computer
- Starting a Linux-based computer using Veritas Recovery Disk
- Recovering a Linux computer
- Mounting and unmounting a recovery point for granular file and folder recovery

About recovering a Linux computer

If Linux fails to start or does not run normally, you can recover your computer using Veritas Recovery Disk and an available recovery point.

Note: If you can start Linux and the partition that you want to restore is not the system partition, you can restore the partition from within Linux.

Veritas Recovery Disk lets you run a recovery environment that provides temporary access to Veritas System Recovery 16 Linux Edition recovery features.

Starting a Linux-based computer using Veritas Recovery Disk

The Veritas Recovery Disk CD lets you start a computer that can no longer run the Linux operating system. The Veritas Recovery Disk CD is not included with Veritas

System Recovery 16 Linux Edition. You must create the Veritas Recovery Disk CD using the createSRD utility after installing Veritas System Recovery 16 Linux Edition.

See "Creating a Veritas Recovery Disk for Linux" on page 30.

When you start your computer using the Veritas Recovery Disk CD, the recovery process follows the recovery environment process of the rescue disk that you used to create Veritas Recovery Disk.

To start a Linux-based computer using Veritas Recovery Disk

1   If you store your recovery points on a USB device, attach the device now (for example, an external hard drive).

> **Note:** You should attach the device before you restart the computer. Otherwise, the recovery environment might not detect it.

2   Insert the Veritas Recovery Disk CD that you created previously into the media drive of the computer.

3   Restart the computer.

If you cannot start the computer from the CD, you might need to change the startup and BIOS settings on your computer.

4   Boot your computer into the rescue environment.

To activate network into the rescue environment, do one of the following:

- Activate your network from within the Red Hat or SUSE rescue environment.

- Activate your network using the `ifup` command.

5   Check if correct version of Veritas System Recovery Linux Edition is installed on your computer.

To check the version of Veritas System Recovery Linux Edition, open a terminal window (command-line terminal) and enter the following command:

```
symsr -v
```

6   If correct version of Veritas System Recovery Linux Edition is installed on your computer, proceed to restore your system.

See "Recovering a Linux computer" on page 24.

See "Mounting and unmounting a recovery point for granular file and folder recovery" on page 26.

Recovering a Linux computer

You can restore your computer (all volumes and partitions on your computer) using the recover feature of Veritas System Recovery 16 Linux Edition. If you have a recovery point for the partitions or volumes that you want to recover, you can fully recover your computer or another hard drive back to the state it was in when the recovery point was created.

Restoring a system volume might require booting to and performing the recovery from the Veritas Recovery Disk.

Note: If you restore a volume or partition that LVM (Linux Volume Manager) or software RAID managed, before you start the recovery process you must use lvmtools or the RAID tools that are present on the recovery disk to set up LVM or software RAID.

To recover a computer

1   If the computer won't boot, start it using Veritas Recovery Disk. If the computer
     will boot, log on at a terminal window as user root or as a user with
     administrative privileges .

     See "Starting a Linux-based computer using Veritas Recovery Disk" on page 22.

2   If the recovery point is stored on a remote NFS or CIFS share, configure your
     network settings and mount the remote NFS or CIFS share.

3   Enter the following command at the server console:

     ```
     symsr -r recoverypoint_nameoptions -d destination
     ```

     Replace *recovery point_name* with the name of the recovery point you want
     to restore. Recovery points have a .v2i or .iv2i file name extension.

     Replace *options* with the options you want to use with the restore.

     Replace *destination* with the location where the recovery point is restored. The
     destination must be a partition or a volume device.

     For example, if you want to restore an independent recovery point named
     system_000.v2i (the system partition) from the /tmp/path/to directory back to
     its original location (/dev/sda1), you enter the following command:

     ```
     symsr -r /tmp/path/to/system_000.v2i -d /dev/sda1 -active
     ```

     Similarly, to restore an incremental recovery point named system_000_005.iv2i
     from a recovery point set, you enter the following command:

     ```
     symsr -r /tmp/path/to/system_000_005.iv2i -d /dev/sda1 -active
     ```

     Note: The -active option is only used with Veritas System Recovery 16 Linux
     Edition during a restoration of a system volume. Using the -active option allows
     the system to boot from a restored volume. Also, in order for a system to boot
     correctly from a restored system volume, you might be required to fix the Grub
     boot loader using the grub-install tool. You might also need to update the
     /etc/fstab.

See "About restoring to empty disk segments" on page 26.

See "Mounting and unmounting a recovery point for granular file and folder recovery"
on page 26.

About restoring to empty disk segments

Veritas System Recovery 16 Linux Edition lets you restore to an MBR (Master Boot Record) partition, GPT and LVM devices, Software RAID, or to free space on the disk. If you restore to free disk space (an empty disk segment), an MBR partition (on an MBR disk) or a GPT entry (on a GPT disk) is created regardless of the partition type that the recovery point was created from

For example, suppose you have a 40 GB hard disk (/dev/sda) that is partitioned as follows:

```
/dev/sda1=20GB

Free Space=20GB
```

To restore a recovery point named backup01.v2i to free space, you use the following command:

```
symsr -r backup01.v2i -d /dev/sda -seg 1
```

Note: To find the empty segment number, you can use the following command:

```
symsr -info disk
```

After the recovery is complete, the disk has the following partitions with the restored volume on the /dev/sda2 partition:

```
/dev/sda1

/dev/sda2
```

See "Mounting and unmounting a recovery point for granular file and folder recovery" on page 26.

Mounting and unmounting a recovery point for granular file and folder recovery

Veritas System Recovery 16 Linux Edition creates partition or volume-level recovery points. If you want to restore individual files, folders, and documents, you must first mount the recovery point that includes those files and folders. The Granular File Recovery utility is included with Veritas System Recovery 16 Linux Edition and can be used to mount recovery points. After mounting a recovery point using the Granular File Recovery utility, you can restore individual files, folders, and documents.

While mounting a recovery point, you may experience the following error:

```
'mount.v2i: error while loading shared libraries: libfuse.so.2: cannot
open shared object file: No such file or directory'
```

In such cases, you should follow the FUSE installation steps before you attempt to mount the recovery point again.

See "Installing Fuse" on page 7.

To mount a recovery point using the Granular File Recovery utility

1   Open a terminal window (command-line terminal) on the Linux server and log on as a user with mount privileges.

2   Create an empty directory where you want the recovery point mounted.

3   Do one of the following:

To mount a recovery point	Enter the following command in a Linux terminal window:
	``` mount -t v2i sda1recoverypoint.v2i /mnt/image ```
	Replace *sda1recoverypoint.v2i* with the name of the recovery point.
	Replace */mnt/image* with the path to the empty directory you created. The recovery point is mounted here.
	Note: If the recovery point is password protected, you must also use the password option and specify the password. For example, if a password was required for sda1recoverypoint.v2i, you would enter the following command and replace *password* with the actual password for the recovery point:
	``` mount -t v2i sda1recoverypoint.v2i /mnt/image -o password=password ```
	System prompts for a password if you attempt to mount a password-protected recovery point without specifying one.
To mount an incremental recovery point	Enter the following command in a Linux terminal window:
	``` mount -t v2i sda1recoverypoint_nnn.iv2i /mnt/image ```
	Replace *sda1recoverypoint_nnn.v2i* with the name of the incremental recovery point. For example, if you want to mount the fifth incremental recovery point, replace *sda1recoverypoint_nnn.iv2i* with sda1recoverypoint_005.iv2i.
	Replace */mnt/image* with the path to the empty directory you created. The recovery point is mounted here.
	Note: If the recovery point is password protected, you must also use the password option and specify the password. For example, if a password was required for sda1recoverypoint_nnn.iv2i, you would enter the following command and replace *password* with the actual password for the recovery point:
	``` mount -t v2i sda1recoverypoint_nnn.iv2i /mnt/image -o password=password ```
	System prompts for a password if you attempt to mount a password-protected recovery point without specifying one.

To unmount a recovery point

1   Open a terminal window (command-line terminal) on the Linux server and log on as a user with mount privileges.

2   Enter the following command in a Linux terminal window:

    ```
    umount /mnt/image
    ```

    Replace */mnt/image* with the path to where the recovery point is mounted.

See "Recovering a Linux computer" on page 24.

Creating a Veritas Recovery Disk

This chapter includes the following topics:

- About Veritas Recovery Disk
- Creating a Veritas Recovery Disk for Linux

About Veritas Recovery Disk

Veritas Recovery Disk lets you start a computer that can no longer run the Linux operating system. You must create the Veritas Recovery Disk using the createSRD utility after installing Veritas System Recovery 16 Linux Edition. createSRD builds a recovery environment based on the rescue environment of your Linux distribution. In the recovery environment, you can access the recovery features of Veritas System Recovery 16 Linux Edition.

The createSRD utility creates an ISO file which you can burn to a CD or DVD to create a Veritas Recovery Disk. The createSRD utility does not include any CD or DVD burning functionality.

Creating a Veritas Recovery Disk for Linux

To create a Veritas Recovery Disk for Linux you must have a Red Hat Enterprise Linux (RHEL) boot CD/DVD or ISO or a SUSE Linux Enterprise Server (SLES) CD/DVD or ISO.

Note: The ISO must match the distribution and version of Linux that you currently have installed and running.

To create a Veritas Recovery Disk for Linux CD using a Red Hat Enterprise Linux boot CD/DVD iso file

1   Open a terminal window (command-line terminal) on the Linux server and log on as a user with administrative privileges.

2   Enter the following command at the Linux server console:

```
createSRD --iso=/mnt/backup/rhel-5.2-server-i386-dvd.iso -d
/mnt/backup/customSRD.iso
```

Replace */mnt/backup/rhel-5.2-server-i386-dvd.iso* with the path and name of the source ISO file you use to create the Veritas Recovery Disk.

Replace */mnt/backup/customSRD.iso* with the path and name of the Veritas Recovery Disk ISO file that you want to create.

To create a Veritas Recovery Disk using a SUSE Linux Enterprise Server CD/DVD in the drive

1   Open a terminal window (command-line terminal) on the Linux server and log on as a user with administrative privileges.

2   Enter the following command at the Linux server console:

```
createSRD --iso=/media/SLES10SP_001/ -d /mnt/backup/customSRD.iso
```

Replace */media/SLES10SP_001/* with the path to where the CD is mounted.

Replace */mnt/backup/customSRD.iso* with the path and name of the Veritas Recovery Disk ISO file that you want to create.

To create a Veritas Recovery Disk using a SUSE Linux Enterprise Server CD/DVD mounted in the /media directory

1   Open a terminal window (command-line terminal) on the Linux server and log on as a user with administrative privileges.

2   Enter the following command at the Linux server console:

```
createSRD -i /media/SLES10 -d /mnt/backup/customSRD.iso
```

Replace */mnt/backup/customSRD.iso* with the path and name of the Veritas Recovery Disk ISO file that you want to create.

Note: You can also use RHEL 6.2 boot CD to create Veritas Recovery Disk for Linux.

See

Features not supported in Veritas System Recovery for Linux

This chapter includes the following topics:

- Windows product features not supported in this release

Windows product features not supported in this release

This release of Veritas System Recovery 16 Linux Edition includes the functionality to back up and restore Linux computers, partitions, or volumes. Also included is the functionality to create a Veritas Recovery Disk and mount recovery points.

Many features in the 16 for Windows are not included in Veritas System Recovery 16 Linux Edition. The following list identifies the features that 16 for Windows supports, but are not included in Veritas System Recovery 16 Linux Edition.

- Backup and Restore of Windows system volumes from Linux.

- Backing up to and restoring from CD and DVD.

- Backing up to non-mounted network locations including ftp, sftp, and windows shares--CIFS.

- GUI management tool -- No GUI management tool is currently included with Veritas System Recovery 16 Linux Edition. All functions are performed using command line utilities.

- Offsite Copy.

- Backing up individual files and folders.

- Notification area icons and alerts.

- Restore Anyware.

- Virtualization support including physical to virtual conversion.

- Veritas System Recovery 16 Management Solution for Convert to Virtual tasks.

- Veritas System Recovery 16 Management Solution for remote recovery of drives or one or more computers using LightsOut Restore.

- Veritas System Recovery 16 Management Solution for deleting recovery points.

- Converting to and restoring from vmdk.

Troubleshooting Veritas System Recovery Linux Edition

This chapter includes the following topics:

- About finding logs for troubleshooting
- About using the gatherLogs utility for troubleshooting
- About troubleshooting cron services issues

About finding logs for troubleshooting

You can find the logs and alerts that can help you to diagnose and troubleshoot issues in the following directory:

/var/log/symsr/

This directory contains the following:

- Debug logs
- Application logs
- Install/Uninstall logs
- Alerts
- History

See "About using the gatherLogs utility for troubleshooting" on page 36.

See "About troubleshooting cron services issues" on page 36.

About using the gatherLogs utility for troubleshooting

The gatherLogs utility is installed along with Veritas System Recovery Linux Edition. You can use the gatherLogs utility to gather the system logs and product logs that are required to diagnose and troubleshoot issues.

Use the following command to run the utility:

```
#gatherLogs
```

The utility gathers the system logs and product logs, and compiles them in a compressed file that is created in the following location:

#/tmp/`Veritas_System_Recovery_for_Linux_logs.<timestamp>.zip`

About troubleshooting cron services issues

If the jobs do not run on the scheduled date and time, you must restart the cron services.

On SUSE Linux, use one of the following commands to restart the cron services:

```
#service cron restart
```

or

```
#/etc/init.d/cron restart
```

On RHEL, use one of the following commands to restart the cron services:

```
#service crond restart
```

or

```
#/etc/init.d/crond restart
```

Veritas System Recovery for Linux Utilities

This appendix includes the following topics:

- Create Veritas Recovery Disk (createSRD utility)

- Backup and Restore (symsr utility)

- Granular File Recovery (mount.v2i utility)

Create Veritas Recovery Disk (createSRD utility)

`Create Veritas Recovery Disk (createSRD utility)` – Create a Veritas Recovery Disk

SYNOPSIS

`createSRD [source]... [destination]`

`createSRD [source]... [install ISO type, disk type]... [destination]`

DESCRIPTION

createSRD is a command line utility for creating a Veritas Recovery Disk (VRD). Veritas Recovery Disk lets you start a computer that can no longer run the Linux operating system. When you boot your computer using the Veritas Recovery Disk CD, a scaled-down version of Linux runs a recovery environment. In the recovery environment, you can access the recovery features of Veritas System Recovery.

OPTIONS

`-h, --help`
Show this help message and exit.

`-i FILE or DIR, --iso=FILE or DIR`
CD ISO file or directory where the CD is mounted. You use this ISO file or directory to create a Veritas Recovery Disk.

`-d FILE, --destination=FILE`
The output ISO file that the script creates.

`-m, --manual-modifications`
Pause after all files are extracted to allow for manual modifications.

`--temp-dir=DIR`
Temporary directory that is used for creating the new ISO file. The default is /tmp/<iso_name>.

`-v --verbose`
Print extra status messages to stdout.

EXAMPLES

createSRD uses POSIX-style options. This is different than the symsr utility, which always uses a single '-' even if the option contains multiple characters. Single-letter

parameters may be specified as a group in POSIX tar -xvf, but cannot be in the symsr utilities.

The following are usage examples for the createSRD utility.

```
createSRD --iso=/mnt/backup/rhel-5.2-server-i386-dvd.iso -d
/mnt/backup/customSRD.iso
```

Create an Veritas Recovery Disk from a Red Hat Enterprise Linux (RHEL) boot CD/DVD iso.

```
createSRD --iso=/media/SLES10SP_001/ -d /mnt/backup/customSRD.iso
```

Create a Veritas Recovery Disk from a SUSE Linux Enterprise Server (SLES) CD/DVD in the drive.

```
createSRD -i /media/SLES10 -d srd.iso
```

Create a Veritas Recovery Disk from a SUSE Linux Enterprise Server (SLES) CD/DVD mounted in the /media/ directory.

SEE ALSO

Man page for Backup and Restore (symsr utility).

Man page for Granular File Recovery (mount.v2i utility).

Backup and Restore (symsr utility)

`Backup and Restore (symsr utility)` – Back up or restore a computer.

SYNOPSIS

`symsr [ACTION] [OPTION]...`

DESCRIPTION

symsr is a command line utility for backing up and restoring a Linux computer or for adding a product license key. The symsr utility captures a recovery point of the entire live Linux system without affecting the productivity. This includes the operating system, applications, system settings, configurations, and files. The recovery point can be saved to various media or disk storage devices, including a SAN, a NAS, and Direct Attached Storage. When systems fail, you can quickly restore them without the need for manual, lengthy, and error-prone processes.

Using the symsr command line utility involves specifying an action and the options that are associated with that action.

ACTIONS

The actions are a group of choices that are used with the symsr command line utility. Only one action can be specified at a time when running symsr. Different options exist for each action. The actions are listed below:

-addlicense <license key>

Adds a license key to Veritas System Recovery 16 Linux Edition.

-b, -backup <device>

Performs a backup of the specified device and creates a recovery point at the specified location.

-createjob

Lets you schedule a backup job for a specific device, comma-separated multiple volumes, or mount points.

-info

Shows information about the existing backup jobs, or the partitions and file system types that are available on the disk.

-r, -restore <recovery point>

Restores the specified recovery point to the specified location.

> **Note:** You cannot restore a recovery point to a destination that is smaller than the size of the volume that was backed up.

`-rmjob <job id>`

Removes an existing backup job from the info job list.

`-runjob <job id>`

Runs an existing backup job immediately, irrespective of the backup job schedule.

`-vrp, -verify-recovery-point <recovery point>`

Verifies the integrity of the specified recovery point.

> **Note:** You cannot verify the integrity of the underlying file system in the recovery point.

OPTIONS

`-?, -help`

Show the help message and exits.

`-active, -set-active`

Sets the restored partition on the destination server to active.

`-cmp, -compress, -compression <level>`

The compression level you want to apply to the recovery point. Valid compression levels include None, Standard, Medium, and High. If you do not specify a compression level, the default is Standard.

`-d, -dest, -destination <file>`

The file or folder where the recovery point is created, or the device where the recovery point is to be restored. If you do not specify a destination, the default is the current directory. A destination is required for performing a recovery.

`-desc, -description <description>`

Use this option to provide a description of the recovery point.

`disk`

Lists the partitions and file system types that are available on the disk.

> **Note:** This option must be used with the `-info` action.

-encryption, -use-aes-encryption <level>

> Use this option to encrypt a recovery point. Encryption levels include high (256-bit), medium (192-bit), and standard (128-bit).
>
> Each encryption level requires a different length password. Password lengths include at least 32 characters for high, at least 16 characters for medium, and at least eight characters for standard.
>
> The default is no encryption if no encryption level is specified.

-force-unmount

> This option attempts to remove any mount points from the destination before a restore. If this option is not specified, the restore fails and an error message displays indicating that you should remove mount points and retry the restore.

-ignore-bad-sectors

> This option lets you run a backup even if there are bad sectors on the hard disk. Although most drives do not have bad sectors, the potential for problems increases during the lifetime of the hard disk. If you have an older hard drive, you should use this option.

job

> Lists all the scheduled backup jobs and their status. The status of a backup job is either active or in progress. Active status indicates that the scheduled job is active for the given recovery point type. In progress status indicates that the backup job is running on the device, after the backup job completes, the status changes back to active.

> **Note:** This option must be used with the `-info` action.

-mnt, -mount-point <path>

> The mount point you want to add to the volume after it is restored (not persistent). <path> must be a valid path.

-nombr, -do-not-restore-mbr

> Do not restore the master boot record that is contained in the recovery point. This option is used only with the Restore action.

-p, -pwd, -password <password>

> Use this option to specify a password for the recovery point file when creating a backup or to supply a password for a password-protected recovery point when restoring.

-prefix, -file-prefix <string>

> Lets you specify a prefix for the recovery point file name. The prefix is used when the destination is not specified or is a directory.

`-raw, -raw-image`

This option instructs Veritas System Recovery 16 Linux Edition to not use SmartSector copy. Instead, the entire volume is captured even if there is no data in some sectors of the volume.

`-reboot, -reboot-on-success`

Restart the computer when the restore is complete.

`-seg, -segment <number>`

You can specify an empty section of the disk to restore the recovery point to (a zero-based index). The number must not be a negative number.

`-span, -split, -span-size <number>`

Use this option to divide the recovery point file into separate chunks. The number is the chunk size in x 500 MB, and cannot be negative.

`-v, -version`

Provides the information about the product name, version, and the license status.

`-verify`

Verify the recovery point after it is created or before it is restored.

OPTIONS FOR CREATE JOB ACTION

Usage: `symsr -createjob`

Note: The `symsr -createjob` action starts the schedule backup wizard. To exit the wizard, type **q**, **Q**, or **Quit** at any prompt of the wizard other than the **Select Source** prompt or the **Select Destination** prompt.

The following options are specific to the `-createjob` action.

`Select Source`

Lets you select the source that you want to back up. The source can be one or more comma-separated devices or a mount point of a device.

`Select Destination`

Lets you select the location where you want to store the recovery points.

`Create a computer specific folder`

Creates a computer-specific folder in the backup destination location. By default, this option is set to no **[n]**.

`Select a recovery point type`

Lets you select the type of backup you want to create. The available backup types are independent backup and recovery point set. The default backup type is recovery point set **[1]**.

`Select compression level`

Lets you select a compression level for the recovery points.

The following compression levels are available:

[1] Standard - 40 percent average data compression ratio on recovery points.

[2] Medium - 45 percent average data compression ratio on recovery points.

[3] High - 50 percent average data compression ratio on recovery points.

[4] No compression for the recovery points.

By default, standard **[1]** compression level is used for the recovery points.

`Select encryption type`

Lets you set a password with or without encryption on the recovery point when it is created.

The following encryption types are available:

[1] No password and no encryption

[2] Password protected without any encryption

[3] Standard 128-bit (8+ character password)

[4] Medium 192-bit (16+ character password)

[5] High 256-bit (32+ character password)

By default, this option is set to no password and no encryption **[1]**.

Note: If you select an encryption type that requires a password, you are prompted to enter and confirm the password.

`Start a new recovery point set`

Lets you specify a schedule to run the base backup for a recovery point set.

The following scheduling options are available:

[1] Weekly

Runs the backup on the day of the week you specify. By default, the backup is run on Sunday **[SUNDAY]**.

[2] Monthly

Runs the backup on the days of the month you specify. You can choose to run the backup every day, on a specific day, or on the last of day of the month. By default, the backup runs on the first day of the month **[1]**.

[3] Quarterly

Runs the backup on the first day of every quarter. If you choose this option, the backup runs on the first day of January, April, July, and October.

[4] Yearly

Runs the backup on the first day of January.

Note: The default schedule for running backups is Monthly **[2]**.

Specify backup start time

Runs the backup at the time and on the days specified by you.

Note: Veritas System Recovery Linux Edition adjusts the time you specify a backup to run to the nearest quarter of an hour. For example, if you schedule a backup to run at 2:20 P.M., the time to run the backup is adjusted to 2:30 P.M.

The default schedule for running backups is Weekly **[1]**.

`Create recovery points`

Lets you schedule a backup to create recovery points.

The following scheduling options are available:

Schedule recovery points

Lets you specify whether you want to create recovery points. By default, this option is set to yes **[y]**.

Recur every week

Runs the backup on the days of the week you specify. You can choose to run the backup on one day or multiple days in a week. By default, the backup runs on Sunday **[SUNDAY]**

Run more than once a day

Runs the backup more than once a day to protect the data that you change frequently. By default, this option is set to no **[n]**.

Time between backups

Specifies the maximum time period that should occur between two backups. This option appears only if you have selected to run backups more than once a day.

Number of backups

Specifies the number of times the backup should run in a day. Ensure that you specify a number considering the number of hours that you have specified to occur between two backups. For example, if you have specified a period of 10 hours to occur between backups, you cannot run more than three backups a day.

`Specify independent recovery point schedule`

Lets you schedule backups to create independent recovery points.

The following scheduling options are available:

[1] Weekly

Runs the backup on the day of the week you specify. By default, the backup runs on Sunday **[SUNDAY]**.

[2] Monthly

Runs the backup on the days of the month you specify. You can choose to run the backup every day, on a specific day, or on the last of day of the month. By default, the backup runs on the first day of the month **[1]**.

[3] Quarterly

Runs the backup on the first day of every quarter. If you choose this option, the backup runs on the first day of January, April, July, and October.

[4] Yearly

Runs the backup on the first day of January.

[5] Run only once

Runs the backup only once.

Note: The default schedule for running backups is Weekly **[1]**.

Recur every week

Runs the backup on the days of the week you specify. You can choose to run the backup on one or more days of the week. By default, the backup runs on Sunday **[SUNDAY]**.

Specify backup start time

Runs the backup at the time on the days that you specified.

Note: Veritas System Recovery Linux Edition adjusts the time you specify a backup to run to the nearest quarter of an hour. For example, if you schedule a backup to run at 2:20 P.M., the time to run the backup is adjusted to 2:30 P.M.

Verify recovery point after creation

Verifies whether the recovery point is valid after it is created.

Save Job

Lets you save or cancel a backup job. By default, this option is set to yes **[y]**.

Provide Job Name

Lets you specify a name for the backup job you want to save. You must enter a job name. The job name cannot be blank and cannot contain only spaces.

EXAMPLES

The following are usage examples for the symsr command-line utility.

symsr -b /dev/sda1 -d sda1backup.v2i

Creates a recovery point named sda1backup.v2i for volume sda1 using default options and storage. The recovery point is created in the same folder where the command is run.

symsr -b /boot -d sda1backup.v2i

Creates a recovery point named sda1backup.v2i for the mount point /boot. The recovery point is created in the same folder where the command is run.

symsr -b /dev/mapper/vg0-lv0 -d lvmbackup.v2i

Creates a recovery point of an LVM volume. The recovery point is created in the same folder where the command is run.

symsr -b /dev/sda1 or , **symsr -b /boot**

Creates a recovery point of volume sda1 with the default file name. This creates the recovery point in the current folder using the name *volume_name*_NNN.v2i.

symsr -b /dev/sda1 -d *machinename_volumename* or , **symsr -b /boot -d *machinename_volumename***

Creates a recovery point of volume sda1 with the supplied file name. This creates the recovery point in the current folder using the name *machinename_volumename*_NNN.v2i.

`symsr -b /dev/sda1 -create-machine-folder` or , `symsr -b /boot -create-machine-folder`

> Creates a folder using the computer name and place the recovery point of volume sda1 in that folder.

`symsr -b /dev/sda1 -d /machine_subfolder/machinename_volumename` or , `symsr -b /boot -d /machine_subfolder/machinename_volumename`

> Creates a recovery point of volume sda1 in the specified computer subfolder with the specified file name. This creates the recovery point in the specified computer subfolder using the name `machinename_volumename_`NNN.v2i.

`symsr -b /boot -d /mnt/backup/sda1backup.v2i -ignore-bad-sector`

> Creates a recovery point that skips over the bad sectors on the hard disk.

`symsr -b /boot -d /mnt/backup/sda1backup.v2i -p recoverypointpassword`

> Creates a recovery point with password protection.

`symsr -b /boot -d /mnt/backup/sda1backup.v2i -cmp high`

> Creates a recovery point with high compression.

`symsr -b /boot -d /mnt/backup/sda1backup.v2i -desc "This backup was taken on July 25 2009 at 10:00AM"`

> Creates a recovery point with an embedded recovery point description.

`symsr -b /boot -d /mnt/backup/sda1backup.v2i -span 2`

> Creates a recovery point that spans multiple files that are each 1000 MB. The chunk size in x 500 MB.

`symsr -b / -d /mnt/backup -use-aes-encryption high -password XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX`

> Creates a recovery point using AES-256 encryption. For high AES encryption, the password length must be at least 32 characters.

`symsr -info disk`

> Shows the partitions and file system types that are available on the disk.

`symsr -info job`

> Shows a list of existing backup jobs and their details.

`symsr -r system_000.v2i -d /dev/sda1`

> Restores the system partition back to its original location (/dev/sda1).

`symsr -r system_000_005.iv2i -d /dev/sda1`

> Restores the fifth incremental recovery point of the system partition back to its original location (/dev/sda1).

`symsr -r system_000.v2i -d /dev/sda -segment 0`

> Restores the system partition back to its original location (/dev/sda1) on a new or empty disk.

`symsr -r lvm2_000.v2i -d /dev/mapper/vg0-lv1`

> Restores an LVM device back to its original location (/dev/mapper/vg0-lvl).

`symsr -rmjob job-1`

> Removes the backup job corresponding to the specified job ID.

`symsr -runjob job-4`

> Runs the backup job corresponding to the specified job ID immediately, irrespective of the backup schedule.

`symsr -v`

> Shows the information about the product name, version, and the license status.

`symsr -vrp system_000.v2i`

> Verifies the integrity of the recovery point.

`symsr -vrp system_000_s01.v2i`

> Verifies the integrity of the spanned recovery point and the recovery point chain.

Note: Some characters have special meanings and should not be used in recovery point file names and passwords. These characters include colons (:), back slashes (\), question marks (?), ampersand (&), asterisk (*), and caret(^).

SEE ALSO

Man page for Create Veritas Recovery Disk (createSRD utility).

Man page for Granular File Recovery (mount.v2i utility).

Granular File Recovery (mount.v2i utility)

`Granular File Recovery (mount.v2i utility)` – Mount a recovery point file for restoring files and folders.

SYNOPSIS

`mount -t v2i [recovery point]... [mount point]... [options]...`

DESCRIPTION

mount.v2i mounts a recovery point. It is usually invoked indirectly by the mount(8) command when using the `-t v2i` option. This command requires the FUSE driver and the FUSE shared library (libfuse.so.2).

mount -t v2i is a command line utility for mounting a recovery point file on a Linux computer so you can restore files and folders.

Using the mount -t v2i command line utility involves specifying the image file name, the location where the recovery point will be mounted, and any desired options. You must use the -o flag when specifying options.

Use `umount` command to unmount the.v2i file that is mounted using the mount `-t v2i` command.

OPTION

password=<password>

If the recovery point is assigned a password, use this option to supply the password when mounting or unmounting the file.

If a password is not supplied for the password-protected recovery point, it prompts you for the password.

EXAMPLES

The following are usage examples for mounting a recovery point using mount -t v2i and unmounting a recovery point using unmount.

mount -t v2i *image.v2i* /mnt/image

Mount a recovery point in the /mnt/image directory. Replace *image.v2i* with the name of the recovery point.

```
mount -t v2i image_nnn.iv2i /mnt/image
```
Mount an incremental recovery point in the /mnt/image directory. Replace *image_nnn.iv2i* with the name of the incremental recovery point. For example, if you want to mount the fifth incremental recovery point, replace *image_nnn.iv2i* with image_005.iv2i.

```
mount -t v2i image.v2i /mnt/image -o password=password
```
Mount a password-protected recovery point in the /mnt/image directory. Replace *image.v2i* with the name of the recovery point and *password* with the password.

```
umount /mnt/image
```
Unmount a recovery point in the /mnt/image directory.

SEE ALSO

Man page for Create Veritas Recovery Disk (createSRD utility).

Man page for Backup and Restore (symsr utility).