Stratus One View Console and everRun Disaster Recovery User's Guide

Notice

The information contained in this document is subject to change without notice.

UNLESS EXPRESSLY SET FORTH IN A WRITTEN AGREEMENT SIGNED BY AN AUTHORIZED REPRESENTATIVE OF STRATUS TECHNOLOGIES, STRATUS MAKES NO WARRANTY OR REPRESENTATION OF ANY KIND WITH RESPECT TO THE INFORMATION CONTAINED HEREIN, INCLUDING WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PURPOSE.

Stratus Technologies assumes no responsibility or obligation of any kind for any errors contained herein or in connection with the furnishing, performance, or use of this document. Software described in Stratus documents (a) is the property of Stratus Technologies Bermuda, Ltd. or the third party, (b) is furnished only under license, and (c) may be copied or used only as expressly permitted under the terms of the license.

Stratus documentation describes all supported features of the user interfaces and the application programming interfaces (API) developed by Stratus. Any undocumented features of these interfaces are intended solely for use by Stratus personnel and are subject to change without warning.

Copyrights

Manual Name: *Stratus One View Console and everRun Disaster Recovery User's Guide*

Product Release Number: One View Release 1.0.1.0

Publication Date: Tuesday, December 09, 2014

Stratus Technologies, Inc.

111 Powdermill Road

Maynard, Massachusetts 01754-3409

Table of Contents

Part 1: Stratus One View Console and everRun Disaster Recovery Quick Start Guide

Use this Quick Start Guide to get your Stratus One View Console and everRun Disaster Recovery (DR) environment up and running quickly.

- See "Introduction to One View and DR " on page 1 for an overview of the One View and DR environment.
- See "One View and DR Requirements " on page 2 for information about requirements and supported configurations.
- See "Installing One View and Enabling DR Protection for a VM " on page 3 for information about installing your One View and Disaster Recovery environment.
- To test your DR site, see "Testing Your DR Site " on page 9.

1

Chapter 1: Getting Started

The following sections describe how to get your Stratus One View Console and everRun Disaster Recovery (DR) environment up and running quickly.

- See "Introduction to One View and DR " on page 1 for an overview of the One View and DR environment.
- See "One View and DR Requirements " on page 2 for information about requirements and supported configurations.
- See "Installing One View and Enabling DR Protection for a VM " on page 3 for information about installing your One View and Disaster Recovery environment.
- To test your DR site, see "Testing Your DR Site " on page 9.

Introduction to One View and DR

The following items provide a quick introduction to the important features in your One View and DR environment.

- DR protection periodically takes snapshots of virtual machines (VMs) running on a duplex primary everRun system and transfers these snapshots to a remote simplex DR everRun system. This ensures that a recent copy of your VM and its data volumes is always available at the DR site. For more information, see "Disaster Recovery Overview" on page 48.
- If the primary system fails or if you must perform a planned shutdown, you can manually start the VM(s) from their snapshots on the DR system. For more information, see "Failing Over to a DR VM (Unplanned)" on page 66.

> **Note**: Unlike the everRun SplitSite feature, data loss may occur when failing over to a DR VM because the backup VM is booted from the most recent snapshot. However, bandwidth requirements for DR are significantly less than those for the everRun SplitSite feature.

- When you enable DR protection, you must specify the number of snapshots to retain, as well as a recovery point objective (RPO) value that determines the frequency of snapshots and therefore the maximum acceptable period during which data might be lost from a VM. For a definition of RPO, see "Disaster Recovery Terminology" on page 49. See "One View and Disaster Recovery Considerations and Requirements" on page 77 for minimum and recommended maximum RPO values.
- You configure and control DR from the One View Console.
- The One View Console is a web-based interface hosted by the One View appliance, which is a *virtual appliance* supplied by Stratus. This appliance is a CentOS based guest preloaded with the Stratus One View software.
- The One View appliance runs on top of an everRun system, an Avance system, or Virtual Box system. For the One View appliance system requirements, see "One View System Requirements" on page 13. You must install the One View appliance on the DR system or a third site. See "One View and Disaster Recovery Considerations and Requirements" on page 77 for more information.

One View and DR Requirements

The following items provide an overview of One View and DR requirements.

- DR requires two everRun systems: a primary system for running VMs in a production environment and a remote DR system to hold backup copies of the VMs.
- DR is a separately licensed feature. When you purchase the DR feature, you receive the two required licenses listed below. See "Disaster Recovery Licensing" on page 51 for more information.
  - An everRun license with DR enabled for the primary everRun system (if you have a non-DR everRun license, you must update it to include DR support).

> **Note**: If you are connected to the Internet and can access the Stratus licensing server, your everRun license can be updated over the Internet to include DR support. An updated everRun license with DR enabled that can be manually applied to your non-DR everRunsystem will also be sent to the end user on record.

  - A simplex everRun license with DR enabled for the simplex DR system.

- The primary system must be a normal duplex everRun system. To enable DR, the disks holding VM volumes must have a storage capacity of approximately 3.5 times the size of the VM volume you create. The level of VM disk activity and the frequency of snapshots affect the actual storage space requirement. See "Disk Space Usage and Retention" on page 55 for more information.

- The DR system must be a simplex everRun system. Its hardware does not have to be exactly the same as the primary system, but it must have sufficient cores, memory, and networks to run the DR protected VMs, as well as the everRun overhead for those VMs. See Virtual Machine Recommendations and Limits in the *everRun User's Guide* for details. To enable DR, the disks holding VM volumes must have a storage capacity of approximately 3.5 times the size of the VM volume you create. The level of VM disk activity and the frequency of snapshots affect the actual storage space requirement. See "Disk Space Usage and Retention" on page 55 for details.

- The management link handles the synchronization traffic between the primary and DR systems. DR is designed to work with WAN bandwidths (typically less than 100MB/sec) between the primary and DR systems. The higher the bandwidth between the primary and DR systems, the smaller the possible RPO values.

- Only one-to-one Disaster Recovery configurations are supported. An everRun system's DR protected VMs must all be protected on the same everRun system at the DR site. The DR site system can protect VMs from only one other everRun system.

- See "One View and Disaster Recovery Considerations and Requirements" on page 77 for important information about the maximum allowed numbers of DR protected VMs, volumes, and retained snapshots.

Installing One View and Enabling DR Protection for a VM

To install One View and enable DR protection for a VM:

1. Install the duplex primary everRun system, and then create new VMs on it. See the *everRun Quick Start Guide* for details.
2. Install the DR everRun system. Only simplex systems (that is, systems with one physical machine) are supported for the DR system, which is typically located remotely.

   Installing a simplex system is similar to installing a duplex system, except that you perform the installation on only one PM **and** you must obtain a special simplex license from Stratus. For installation instructions, see the *everRun Quick Start Guide*.
3. Install and set up the One View software. See "Installing the Stratus One View Console" on page 13 for details. The software must be installed on the DR system or a third site. Installing the One View appliance on the DR everRun system is an acceptable configuration. Perform the following steps:
   1. a. Prepare your site and system for the installation. See:
      - "One View System Requirements" on page 13

        Describes requirements for the everRun or other system that will host the One View appliance.
      - "Web Browser Requirements" on page 14

        Describes requirements for the web browser on a management system that will run the One View Console.
   2. b. Deploy the One View appliance:
      - i. Download the One View OVF and VHD files to your management PC from the **everRun Downloads and Support** page at http://www.stratus.com/go/support/everrun.
      - ii. Log on to the everRun system with the everRun Availability Console.
      - iii. On the **Virtual Machines** page, click **Import/Restore** to open the import wizard.
      - iv. If prompted, allow the required Java plugins to load in your web browser. For information, see the everRun Availability Console online help and your Java documentation.
      - v. Click **Browse**. In the file browser, select the One View**.ovf** file to import from your management PC and click **Import**.
      - vi. If prompted to **Import** or **Restore**, click **Import** to create a new instance of the VM.

vii. Review the import summary. Optionally, clear the check box for **Auto start Virtual Machine after import** if you want to prevent the One View appliance from starting immediately after the import.

> **Note**: Do not modify the default resource settings of the One View appliance unless specifically instructed by your authorized Stratus service representative.

viii. Click **Import** to begin importing the One View appliance. When the transfer is complete, click **Done** to close the import wizard.

c. Obtain the initial IP address for the One View Console.

i. In the everRun Availability Console, open the **Virtual Machines** page.

ii. Select the One View VM and, if necessary, click **Start** to boot the VM. Wait until the VM is running.

iii. Click **Console** to open the One View VM console window.

iv. At the `login:` prompt, log on to the VM as the **root** user with the default password **admin**.

v. At the command prompt, execute `multisite network --display` and record the IP address from the output.

vi. Type `exit` and press **Enter** to log out of the console.

d. Log on to the One View Console for the first time to configure initial settings.

i. On a remote management system, open a web browser and type the initial IP address for the One View Console. See "Obtaining and Setting the Initial IP Address for the Stratus One View Console" on page 16 for details.

ii. Read the Stratus One View Console EULA and then, if appropriate, click **I Accept** to accept it and continue.

iii. Create the first administrative account. Specify your **Email Address** and **Password**, and then retype your password under **Confirm Password**. Click **Add** to continue.

iv. On the **IP Settings** page, configure the network settings for the One View Console. A static IP address is preferred to DHCP because a DHCP address can be lost, which requires the inconvenience of changing the address in the One View Console . Select either **Use DHCP** or select **Use Static IP Settings** and do the following:

- If you select DHCP (default), click **Next** to continue.
- If you select a static IP address, specify the settings that you obtained from your network administrator and click **Save**. The page reloads from the new address. Click **Next** to continue.

v. On the **SMTP Settings** page, configure the SMTP settings for the One View Console. Click **Save**, and click **Next**.

You must specify an SMTP server to create new users, because the One View Console sends a confirmation link to their email addresses. For details, see "Managing SMTP Settings" on page 35.

vi. On the **Settings for Backup** page, enable periodic backups of your One View Console settings or restore settings from an existing backup as described in "Configuring Backups for the Stratus One View Console" on page 31.

> **Caution**: Enabling One View backups configures the One View Console to save your settings to a backup file inside the One View appliance. To ensure that the backup is available if the One View appliance crashes or is lost, you must copy the backup file to another system on a regular basis.

vii. Click **Finish** to complete the wizard and display the One View login page.

viii. Log on to the One View Console with the administrative account you created earlier, and perform the following post-installation tasks:

- Add additional user accounts to administer the One View Console. See "Adding a User" on page 36.
- Add everRun systems that you will manage from the One View Console. See "Adding a Platform to the One View Console" on page 43.

- Enable backups of your One View configuration settings, if you have not done so already. See "Configuring Backups for the Stratus One View Console" on page 31.
- For security, also set new passwords for the `root` and `admin` users in the guest operating system of the One View VM.

4. Add the primary system and the DR system to the One View Console. Perform the following steps for each system.

   Register the system

   a. In the everRun Availability Console, obtain the **Asset ID** of the system that you want to add to the One View Console. The **Asset ID** appears in the masthead, under the system name.
   b. In the One View Console, click **PLATFORMS** in the masthead.
   c. Click **Register Platform** in the action bar.
   d. In the **Register Platform** dialog box that appears, enter the **Asset ID** (obtained in Step a).
   e. Click **Save**.

   Add the system to the One View **Console**

   a. In the everRun Availability Console, navigate to One View on the **PREFERENCES** page:
      i. Click **Preferences** in the left-hand navigation panel.
      ii. On the **PREFERENCES** page, click One View under **Remote Support.**
   b. With One View selected on the **PREFERENCES** page, click **Enable One View**.
   c. In the **Server** box, enter the IP address or DNS name for the console.
   d. Click **Save**.

      In the One View Console, confirm that the new system appears on the **PLATFORMS** page.

5. Enable Disaster Recovery protection for VMs on the primary system by following the steps below. See "Enabling Disaster Recovery Protection for a Virtual Machine" on page 59 for details.

   a. On the **VIRTUAL MACHINES** page, click the VM that you want to protect (the primary VM) to open its details page.
   b. On the VM details page, click **DR Protect** to open the DR wizard.
   c. On the **Disaster Recovery Platform** page, select the system where DR will replicate the

primary VM and click **Next**.

d. On the **Disaster Recovery Options** page:

   i. Enter the **Recovery Point Objective**. The Recovery Point Objective (RPO) is the maximum acceptable period during which data might be lost from a VM. For example, if you would not want to lose more than one hour of changes, then enter 1 hour.

   ii. Select the snapshot **Retention** setting. The DR software keeps only the specified number of snapshots. When the limit is reached, the DR software creates a new snapshot. The DR software then *coalesces* the oldest snapshot (that is, it merges it with the next oldest snapshot) and finally deletes the oldest snapshot.

   iii. Select the check box next to **Compress network transfers of snapshot data** if you want to compress the snapshot data for transfers to the DR site.

   iv. Click **Next**.

e. On the Disaster Recovery **VM Name, VCPUs, and Memory** page, if applicable, modify the name and resource settings to use for the DR VM and click **Next**.

f. On the Disaster Recovery **VM Volumes** page, verify the list of volumes that will be replicated and click **Next**.

g. On the Disaster Recovery **VM Network** page:

   i. In the left pulldown menu, select one **Virtual Network** from the primary VM to include in the DR VM.

   ii. In the right pulldown menu, select one **Platform Network** from the DR platform to connect to the chosen **Virtual Network**.

   iii. Click **Next**.

h. On the **Disaster Recovery Configuration Summary** page, verify the summary of DR settings.

i. Click **Finish** to initialize DR protection and return to the VM details page. The details page indicates that **Disaster Recovery is Initializing**.

> **Note**: The system may stay in this state for a long time while it transfers the entire contents of the data volumes to the remote site.

j. When the initialization completes, the VM details page in the One View Console indicates that Disaster Recovery **is Active**.

For further details see "Enabling Disaster Recovery Protection for a Virtual Machine" on page 59.

Testing Your DR Site

Perform the following steps to test your DR site.

> **Notes**:
>
> 1. In order to perform this test procedure, you must stop your VM and its applications and then remap your network to test operation from the DR site.
> 2. This test is optional. Perform it only if you want to validate that your DR site will operate correctly.

1. Perform a test planned migration to a DR VM. See "Migrating to a DR VM (Planned)" on page 65 for details..
   a. In the Stratus One View Console masthead, click **VIRTUAL MACHINES**.
   b. On the **VIRTUAL MACHINES** page, click the primary VM that you want to migrate.
   c. In the action bar, click **Begin Migration**.
   d. When the migration is complete, the message **Disaster Recovery has migrated to the DR VM** appears.
2. Perform a test migration of data back to the primary VM. See "Migrating Current Data Back to the Primary VM" on page 67 for details.
   a. In the Stratus One View Console masthead, click **VIRTUAL MACHINES**.
   b. On the **VIRTUAL MACHINES** page, click the DR VM that corresponds to the primary VM.
   c. In the action bar, click **Begin Migration**.
   d. The system begins to take snapshots on the DR VM and copies them to the primary VM. When the system finishes migrating the data, the **Finish Migration** button appears in the action bar. Click **Finish Migration** to complete this operation.

Part 2: Stratus One View Console User's Guide

The *Stratus One View Console User's Guide* describes the One View Console and how to install, upgrade, and use it.

For descriptions of the One View console, see:

- "Stratus One View Console Overview" on page 11

For a summary of the steps required to install One View software, see:

- "Installing the Stratus One View Console" on page 13

For information about how to use the One View Console, see:

- "Using the Stratus One View Console" on page 23
- "Manage Stratus One View Console Settings" on page 29
- "Managing Virtual Machines" on page 39
- "Managing Platforms" on page 43

2

Chapter 2: Stratus One View Console Overview

The Stratus One View Console is a web-based utility that provides a "single pane of glass" portal through which you remotely manage systems, virtual machines (VMs), and the Disaster Recovery (DR) environment.

With One View, you can monitor the health of all of your systems and VMs by tracking all of their outstanding issues and alerts from a single location.

The Stratus One View Console is available free of charge. However, if you want to protect VMs using the Disaster Recovery feature, you must purchase Disaster Recovery licenses for all of your everRun systems. For information, see "Disaster Recovery Licensing" on page 51

You can also focus on specific platforms in detail, viewing their VMs, physical machines (PMs), alerts, and resource allocations.

One View is deployed as a VM, or appliance, on an everRun, Avance, or Virtual Box system. The best practice is to install the One View appliance at the DR site or at a third site.

One View also supports Disaster Recovery, which restores systems to service after failures caused by certain external events.

See the following topics for more information about the Stratus One View Console.

- "Installing the Stratus One View Console" on page 13
- "Using the Stratus One View Console" on page 23
- "Manage Stratus One View Console Settings" on page 29

- "Managing Virtual Machines" on page 39
- "Managing Platforms" on page 43

See the following topics for an introduction to the Stratus everRun Disaster Recovery feature.

- "Disaster Recovery Overview" on page 48
- "Configuring and Maintaining Disaster Recovery" on page 58
- "Managing Disaster Recovery Operations" on page 64

3

Chapter 3: Installing the Stratus One View Console

When you install the One View software for the first time:

1. Prepare your site and system for the installation. See:
   - "One View System Requirements" on page 13

     Describes requirements for the everRun or other system that will host the One View appliance, or virtual machine (VM).
   - "Web Browser Requirements" on page 14

     Describes requirements for the web browser on a management system that will run the One View Console.
2. Deploy the One View Console. See "Deploying the Stratus One View Console" on page 15.
3. Obtain the initial IP address for the One View Console. See "Obtaining and Setting the Initial IP Address for the Stratus One View Console" on page 16.
4. Log on to the One View Console for the first time to configure initial settings. See "Logging on to the Stratus One View Console for the First Time" on page 18.

When the One View Console installation is complete, see "Stratus One View Console Post-Installation Tasks" on page 19.

One View System Requirements

To install the Stratus One View Console, you deploy the One View appliance, or virtual machine (VM), in a virtualized environment.

You can install the One View appliance on an everRun or Avance system, or on any system on which VirtualBox is installed. It is advisable to install the appliance on a simplex system at a Disaster Recovery site.

To host the One View appliance, the everRun, Avance, or VirtualBox system requires network accessibility to all everRun platforms.

The One View appliance requires the following minimum resources:

- 1 vCPU
- 2048 MB of memory
- 15 GB of storage space

A static IP address is preferred to DHCP because DHCP can be lost, which requires the inconvenience of changing the address.

Web Browser Requirements

A web browser is used to connect to the Stratus One View Console. Use only browsers that support the HTML 5 specification. Using an incompatible browser can result in rendering problems and the omission of some wizards.

The following browsers are compatible with the One View Console.

Compatible Browsers	Release
Microsoft Internet Explorer™	10 or newer
Mozilla® Firefox®	25 or newer
Google® Chrome™	31 or newer

Java™ Requirements

Your system must be running an up-to-date version of Java. If you are running an outdated version, you may see a warning when using a wizard or other feature of the One View Console. If you continue using the feature, it is likely to hang. The warning will advise you to install the latest version of Java and either:

- Reduce your Java security settings to medium.
- Add your everRun system to the Exception Site List.
- Or add a certificate as a Signer CA in Java, using the link in the message.

Deploying the Stratus One View Console

Deploy the One View Console by importing the One View appliance, or virtual machine (VM), onto a system that supports virtual machines. The following procedure describes how to import the appliance on an everRun system, but you can also deploy the appliance on an Avance unit or VirtualBox system.

To deploy the One View appliance on an everRun system, use the everRun Availability Console to import the VM's OVF file and its associated VHD volume file from your management PC.

> **Caution**: If you plan to configure Disaster Recovery protection for your VMs, deploy the One View appliance on a system at your DR site, not at the primary site. If you deploy the One View appliance at the primary site, the One View Console will be unavailable for DR failover operations in the event of a failure at the primary site.

To prepare for deploying the One View appliance

Download the One View OVF and VHD files to your management PC from the **everRun Downloads and Support** page at http://www.stratus.com/go/support/everrun.

To import the One View appliance on an everRun **system**

1. Log on to the everRun system with the everRun Availability Console.
2. On the **Virtual Machines** page, click **Import/Restore** to open the import wizard.
3. If prompted, allow the required Java plugins to load in your web browser. For information, see the everRun Availability Console online help and your Java documentation.
4. Click **Browse**. In the file browser, select the One View**.ovf** file to import from your management PC and click **Import**.
5. If prompted to **Import** or **Restore**, click **Import** to create a new instance of the VM.
6. Review the import summary. Optionally, clear the check box for **Auto start Virtual Machine after import** if you want to prevent the One View appliance from starting immediately after the import.

Note: Do not modify the default resource settings of the One View appliance unless specifically instructed by your authorized Stratus service representative.

7. Click **Import** to begin importing the One View appliance. When the transfer is complete, click **Done** to close the import wizard.

8. Continue the One View installation process by obtaining the initial IP address that you will use to access the One View Console, as described in "Obtaining and Setting the Initial IP Address for the Stratus One View Console" on page 16.

Troubleshooting

If necessary, use the following information to resolve problems with the import process.

To clean up after a canceled or failed import on the everRun system

In the everRun Availability Console, remove the imported VM and any volumes associated with the imported VM.

Obtaining and Setting the Initial IP Address for the Stratus One View Console

Obtain and set the initial IP address of the Stratus One View Console to determine the address that you will use to access the One View Console from a web browser for the first time.

Note: Stratus strongly recommends that you use a static IP address for the Stratus One View Console because a DHCP address can be lost (for example when upgrading or reinstalling One View). Should that occur, you must change the One View Console IP address on each managed platform by using each platform's everRun Availability Console.

The One View appliance, or virtual machine (VM), typically sets its initial IP address by using the Dynamic Host Configuration Protocol (DHCP). If your environment supports DHCP, log on to the console of the One View appliance to collect the initial IP address as described in the first procedure below. You can set a static IP address later when logging on to the One View Console.

If your environment does not have a DHCP server, manually set a static IP address and other network settings at the command line as described in the second procedure.

Both procedures describe how to access the guest operating system of the One View appliance on an everRun system, but you can perform similar steps in the VM console of an Avance unit or VirtualBox system.

To obtain the initial DHCP IP address for the One View Console

1. In the everRun Availability Console, open the **Virtual Machines** page.

2. Select the One View appliance and, if necessary, click **Start** to boot the appliance. Wait until the VM is running.

3. Click **Console** to open the One View appliance console window. If the console is blank, click in the console window and press any key to deactivate the screen saver.

4. At the `login:` prompt, log on as the **root** user with the default password **admin**.

5. At the command prompt, execute `multisite network --display` and record the IP address from the output. In the following example, the IP address is `10.71.160.53`:

   ```
   # multisite network --display
   Network Information:
   ip=10.71.160.53 cidr=16 dns=10.68.40.9 dns=10.68.40.10 gateway=10.71.160.1 bootproto=static
   ```

6. Type `exit` and press **Enter** to log out of the console.

7. Continue the One View installation process by using the IP address you recorded in step 5 to log on to the One View Console, as described in "Logging on to the Stratus One View Console for the First Time" on page 18.

Configuring Static Network Settings

If your environment does not have a DHCP server, use the `multisite network` command to set the initial network settings at the command line of the One View appliance. If you want to display the command options, execute `multisite network --help`.

The following procedure shows an example of configuring the network settings that are typically needed. If you do not know the appropriate network settings for your environment, contact your network administrator.

To manually configure a static IP address and network settings for the One View Console

1. In the everRun Availability Console, open the **Virtual Machines** page.

2. Select the One View appliance and, if necessary, click **Start** to boot the appliance. Wait until the VM is running.

3. Click **Console** to open the One View appliance console window. If the console is blank, click in the

console window and press any key to deactivate the screen saver.

4. At the `login:` prompt, log on to the VM as the **root** user with the default password **admin**.

5. At the command prompt, execute the `multisite network` command in the format:

   ```
   # multisite network --ip=staticIpAddress --mask=subnetMask
   --gateway=gatewayIpAddress --dns1=dnsAddr1 --dns2=dnsAddr2
   ```

   For example, to set an IP address of `10.71.160.53` and additional network settings:

   ```
   # multisite network --ip=10.71.160.53 --mask=255.255.0.0
   --gateway=10.71.160.1 --dns1=10.68.40.9 --dns2=10.68.40.10
   ARPING 10.71.160.53 from 0.0.0.0 eth0
   Duplicate:False
   ```

6. Execute the `multisite network --display` command to verify the new network settings. For example, to display the settings specified in the previous step:

   ```
   # multisite network --display
   Network Information:
   ip=10.71.160.53 cidr=16 dns=10.68.40.9 dns=10.68.40.10 gateway=10.71.160.1 bootproto=static
   ```

7. Type `exit` and press **Enter** to log out of the console.

8. Continue the One View installation process by using the static IP address to log on to the One View Console, as described in "Logging on to the Stratus One View Console for the First Time" on page 18.

Logging on to the Stratus One View Console for the First Time

Log on to the Stratus One View Console for the first time to create the first administrative account and configure initial settings.

To log on to the One View Console for the first time

1. On a remote management system, open a web browser and type the initial IP address for the One View Console, which you obtain as described in "Obtaining and Setting the Initial IP Address for the Stratus One View Console" on page 16.

2. Read the Stratus One View Console EULA and then, if appropriate, click **I Accept** to accept it and continue.

3. Create the first administrative account. Specify your **Email Address** and **Password**, and then retype your password under **Confirm Password**. Click **Add** to continue.

4. On the **IP Settings** page, configure the network settings for the One View Console. A static IP address is preferred to DHCP because a DHCP address can be lost, Should that occur, you must change the One View Console IP address on each managed platform by using each platform's everRun Availability Console. Select either **Use DHCP** or select **Use Static IP Settings** and do the following:

   - If you select DHCP (default), click **Next** to continue.
   - If you select a static IP address, specify the settings that you obtained from your network administrator and click **Save**. The page reloads from the new address. Click **Next** to continue.

5. On the **SMTP Settings** page, configure the SMTP settings for the One View Console. Click **Save**, and click **Next**.

   You must specify an SMTP server to create new users, because the One View Console sends a confirmation link to their email addresses. For details, see "Managing SMTP Settings" on page 35.

6. On the **Settings for Backup** page, enable periodic backups of your One View Console settings or restore settings from an existing backup as described in "Configuring Backups for the Stratus One View Console" on page 31.

   > **Caution**: Enabling One View backups configures the One View Console to save your settings to a backup file inside the One View appliance. To ensure that the backup is available if the One View appliance crashes or is lost, you must copy the backup file to another system on a regular basis.

7. Click **Finish** to complete the wizard and display the One View login page.

8. Log on to the One View Console with the administrative account you created in step 3.

9. Complete the tasks described in "Stratus One View Console Post-Installation Tasks" on page 19.

Stratus One View Console Post-Installation Tasks

After installing the One View Console, complete the following post-installation tasks:

- Add additional user accounts to administer the One View Console. See "Adding a User" on page 36.
- Add everRun systems that you will manage from the One View Console. See "Adding a Platform to the One View Console" on page 43.
- Enable backups of your One View configuration settings, if you have not done so already. See "Configuring Backups for the Stratus One View Console" on page 31

For security, also set new passwords for the `root` and `admin` users in the guest operating system of the One View appliance. Open the VM console, log on as each user (with the default password: **admin**), and execute the `passwd` command. For example:

```
$ passwd
Changing password for user admin.
Changing password for admin.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

After completing these initial tasks, you can manage your One View environment as described in:

- "Manage Stratus One View Console Settings" on page 29
- "Managing Virtual Machines" on page 39
- "Managing Platforms" on page 43

To manage your Disaster Recovery configuration , see the "Stratus everRun Disaster Recovery User's Guide" on page 47.

4

Chapter 4: Upgrading the Stratus One View Console

When you upgrade the One View Console from a previous version:

1. Back up the configuration settings from your old One View Console. See "Configuring Backups for the Stratus One View Console" on page 31.
2. Transfer the most current One View Console backup file from your old One View appliance to a management system. See "Configuring Backups for the Stratus One View Console" on page 31 for information about how to transfer the file.
3. If the old One View appliance is using a static IP address, record it so that you can apply it to the new One View appliance after it is installed.
4. Shut down the old One View appliance, and then do one of the following:
   - If you want to preserve the old appliance until you are certain that the new appliance is running correctly, rename the old VM and its boot volume.
   - If you do not want to preserve the old appliance, delete it now.

   Note: Disaster Recovery operations continue to run in the background on the protected everRun systems when the One View appliance is unavailable.
5. Deploy the new One View appliance. See "Deploying the Stratus One View Console" on page 15.
6. Obtain or set the initial IP address for the One View Console. See "Obtaining and Setting the Initial IP Address for the Stratus One View Console" on page 16.

7. Log on to the One View Console for the first time to configure initial settings. If the old One View appliance used a static IP address, use that same address which you recorded in step 3. See "Logging on to the Stratus One View Console for the First Time" on page 18.
8. Transfer the One View backup settings file from your management system to the new One View appliance. See "Configuring Backups for the Stratus One View Console" on page 31 for information about how to transfer the file.
9. Restore your One View backup settings by using the file that you transferred from the old One View appliance. See "Configuring Backups for the Stratus One View Console" on page 31.
10. When you are confident that the new One View appliance is running properly, delete the old appliance, if you have not already done so.

> **Note**: If you are using a DHCP IP address and the IP address for the newly installed One View appliance has changed, you must change the One View Console IP address on each managed platform by using each platform’s everRun Availability Console.

Related Topics

"Installing the Stratus One View Console" on page 13

5

Chapter 5: Using the Stratus One View Console

The following topics explain how to use the Stratus One View Console:

- "The Stratus One View Console Interface" on page 24
- "Logging On to the Stratus One View Console" on page 23
- "The PLATFORMS Page" on page 26
- "The VIRTUAL MACHINES Page" on page 26
- "The SETTINGS Page" on page 27
- "The ALERTS Page" on page 25
- "Sorting and Filtering Views" on page 28

Related Topics

"Managing Your Account" on page 29

"Managing the System" on page 31

"Managing Users" on page 35

Logging On to the Stratus One View Console

Log on to the Stratus One View Console console to manage your everRun systems and virtual machines, and if applicable, configure Disaster Recovery protection for your environment.

To log on to the One View Console

1. Start a supported web browser and open the One View Console for your environment.
2. Type your **Email Address** and **Password**. (Your password is case-sensitive.)
3. Optionally, specify additional settings for your login session:
   - Click **Remember Me** to remain logged on until you explicitly log off.
   - Click the flag to select the language to display for your login session. The One View Console retains this setting for future sessions.
   - If you forget your password, click **Forgot your password?** to receive an email that will enable you to reset your password.
4. Click **Login**.

To log off from the One View Console

Click the logout button in the far-right corner of the masthead.

Related Topics

"Logging on to the Stratus One View Console for the First Time" on page 18

"Web Browser Requirements" on page 14

The Stratus One View Console Interface

You access the features of the Stratus One View Console interface by clicking the following items, which are found on the console masthead.

- The **PLATFORMS** page: Displays the platform boxes of all platforms in the One View environment. From this page, you can use the buttons in the action bar to sort and filter the information displayed on the page (see "Sorting and Filtering Views" on page 28) and register another everRun system for the One View Console (see "Adding a Platform to the One View Console" on page 43). You can also click a platform to view and manage that platform (see "Viewing Platform Resources and Alerts" on page 44).
- The **VIRTUAL MACHINES** page: Displays the VM boxes of all the VMs in the One View environment as well as two buttons you use to sort the VM names in ascending or descending order. From this page, you can monitor and manage your platform's VMs. See "The VIRTUAL MACHINES Page" on page 26 and "Sorting and Filtering Views" on page 28 for more details.

- The **ALERTS** page: Displays an overview of the status and health of the everRun systems in your environment. You can use the buttons in the action bar to filter the information displayed on the page. See "The ALERTS Page" on page 25 for details.
- The **SETTINGS** page: Allows you to configure settings for email and password accounts, IP addresses, backup operations, diagnostic files, SMTP configuration, and users. See "The SETTINGS Page" on page 27 for details.
- The **Help** icon: Displays the online Help system.
- The **Logout** icon. Logs you off the system and returns you to the login page.

The ALERTS Page

Click **ALERTS** in the masthead to display an overview of the status and health of the everRun systems in your environment. The page displays alerts according to the following levels of severity:

- Critical (red icon)
- Serious (red icon, same as for Critical)
- Moderate (orange icon)
- Minor (yellow icon)
- Info (blue icon)
- Normal (no icon)

Alerts appear in table form, arranged in the following columns (from left to right):

- Time since the alert was generated (for example, "a day ago"). Hover the cursor over the elapsed time value to view the exact date and time of the alert (for example, 11/18/2014 11:32:00 PM).
- A description of the event (for example, "Single PM Detected").
- The affected platform (for example, syssw.eng.cmpny.com).

Clicking any item in a column launches the platforms detail page for the corresponding platform (the same page you launch by clicking a particular platform on the **PLATFORMS** page).

You can use the following **ALERTS** page buttons to view selected subsets of alerts of the monitored platforms:

- Show Platform Alerts
- Show One View Only Alerts

- Show Ignored
- Show History

See "Sorting and Filtering Views" on page 28 for more details.

The VIRTUAL MACHINES Page

Click **VIRTUAL MACHINES** in the masthead to display all of the VMs on systems within your One View environment. On this page, you can use the sort buttons to display the VMs in ascending or descending order.

You can also click an individual VM to perform several actions, including:

- Subscribe or unsubscribe to email updates (see "Managing Email Notifications" on page 29).
- Initiate Disaster Recovery protection (see "Disaster Recovery Overview" on page 48 and related topics).
- Start or stop the VM (see "Starting, Shutting Down, or Powering off a Virtual Machine" on page 42).
- Invoke the VM's console (see "Opening a Virtual Machine Console Session" on page 40).

Related Topics

"Managing Virtual Machines" on page 39

The PLATFORMS Page

Click **PLATFORMS** in the masthead to display an overview of the status of all of the everRun systems in your One View environment.

The **PLATFORMS** page action bar includes several buttons that you can use to sort and filter views of the platforms and VMs monitored by the Stratus One View Console. You can use the buttons (described from left to right) to:

- Display platforms by the severity level of their alerts.
- Display platforms based on descending order of severity of alert.
- Display platforms in ascending or descending alphabetical order.
- Register your everRun system for One View, as explained in "Adding a Platform to the One View Console" on page 43.

Note: If no platforms match your filtering selection, the message "There's nothing here" appears.

To manage a specific platform, on the **PLATFORMS** page click the desired platform. A platform details page displays platform information, and controls for managing the platform, in the following panes:

- **Alerts**
- **Virtual Machines**
- **Physical Machines**
- **Resource Allocations**

Related Topics

"Viewing Platform Resources and Alerts" on page 44

"Sorting and Filtering Views" on page 28

The SETTINGS Page

Click **SETTINGS** in the masthead to configure global settings for the One View environment.

The following table describes the configurable settings and provides links to detailed information.

The SETTINGS Page

Setting	Function	Topic
Account	(Un)subscribe to email alerts. Change your password.	"Managing Email Notifications" on page 29
IP	Configure IP settings, including DHCP, static IP, netmask, gateway, and primary and secondary DNS.	"Configuring IP Settings" on page 31
Backup	Specify backup settings and restore a system from backup.	"Configuring Backups for the Stratus One View Console" on page 31
Diagnostics	Create diagnostic (log) files.	"Generating Diagnostic Files" on

Setting	Function	Topic
		page 34
SMTP	Specify SMTP settings.	"Managing SMTP Settings" on page 35
Users	List, and edit roles of, current users and add new users.	"Managing Users" on page 35

Sorting and Filtering Views

The **ALERTS** page displays alerts for your One View system. Click the appropriate button to display one of the following sets of alerts:

- **Show Platform Alerts**: Shows all non-Disaster Recovery (DR) alerts. These are the same alerts that appear on the everRun system **ALERTS** page.
- **Show One View Only Alerts**: Shows alerts that are generated by both the One View VM and DR.
- **Show Ignored**: Shows alerts that are ignored on the everRun platform.
- **Show History**: Shows alerts on platforms that are currently inactive.

The system reports alerts of the following levels:

- **Critical**: Immediate threat to the operation of a platform or VM. These require immediate attention.
- **Serious**: Could soon develop into a threat to the operation of a platform or VM.
- **Moderate**: A condition that needs eventual correction.
- **Minor**: A condition that merits continued monitoring.
- **Info**: Information that does not demand action.
- **Normal**: The platform or VM is operating correctly.

Hovering your cursor over an alert's time indication (for example, "3 hours ago") toggles the displayed value to the date and time of the alert.

6

Chapter 6: Manage Stratus One View Console Settings

To manage Stratus One View Console settings, refer to the following topics.

- "Managing Your Account" on page 29
- "Managing the System" on page 31
- "Managing Users" on page 35

Managing Your Account

Refer to the following topics to manage your user account on the Stratus One View Console.

- "Changing Your Password" on page 30
- "Managing Email Notifications" on page 29

Managing Email Notifications

You can subscribe to receive email updates either from specific virtual machines (VMs) or platforms, or from all VMs or platforms.

To receive email updates about particular VMs or platforms

1. On the One View Console, click **VIRTUAL MACHINES** or **PLATFORMS** in the masthead.
2. Click the box of the desired VM or platform.
3. Click **Get Email Updates** in the actions bar.

   The button changes to **Unsubscribe** and the console returns to the **PLATFORMS** page.

To receive all email updates

1. On the One View Console, click the settings icon.
2. Click **Account** in the actions bar.
3. Under **Email Preferences**, click **Subscribe to All Email Updates**.

To unsubscribe from the email updates

1. On the One View Console, click **VIRTUAL MACHINES** or **PLATFORMS** in the masthead.
2. Click the box of the desired VM or platform.
3. Click **Unsubscribe** in the actions bar.

   The button changes to **Get Email Updates** and the console returns to the **PLATFORMS** page.

To unsubscribe from all email updates

1. On the One View Console, click the settings icon.
2. Click **Account** in the actions bar.
3. Under **Email Preferences**, click **Unsubscribe from All Email Updates**.

Related Topics

"The PLATFORMS Page" on page 26

"The VIRTUAL MACHINES Page" on page 26

"The SETTINGS Page" on page 27

Changing Your Password

To change your password

1. Click **SETTINGS** in the masthead.
2. Click the **Account** button.
3. Under **Change Password**, supply these values:
   - **Current Password.** Enter the current password.
   - **New Password.** Enter the new password.

     You may use upper- and lower-case letters, numbers, and symbols for passwords. (Passwords may consist of any Unicode characters.)

     While there is no minimum or maximum number of characters allowed for a password, it should be long enough to provide a sufficient level of security.

- **Confirm Password**. Re-enter the new password.

4. Click **Save** to save the new password, or click **Reset** to clear the fields.

Related Topic

"Logging on to the Stratus One View Console for the First Time" on page 18

Managing the System

Refer to the following topics to manage your One View system.

- "Managing SMTP Settings" on page 35
- "Configuring Backups for the Stratus One View Console" on page 31
- "Configuring IP Settings" on page 31
- "Generating Diagnostic Files" on page 34

Configuring IP Settings

Configure Internet Protocol (IP) settings for the Stratus One View Console system to set or modify the IP address of the system, as well as values for applicable settings such as network mask, gateway address, and Domain Name System (DNS) server. On the **IP Settings** page, required fields are marked with a star.

To configure IP settings

1. Click **SETTINGS** in the masthead.
2. Click **IP.**
3. On the **IP Settings** page, click the **Use DHCP** or **Use Static IP Settings** button.

   If you choose **Use DHCP**, the system automatically supplies values for all of the required fields. Press **Save** to keep, or **Reset** to clear, the settings.

   If you choose **Use Static IP Settings**, continue to the next step.
4. Obtain the following values from your system administrator: IP address, netmask, gateway, primary and (optionally) secondary DNS address.
5. Press **Save** to keep, or **Reset** to clear, the settings.

Configuring Backups for the Stratus One View Console

You can back up your Stratus One View Console configuration settings, enable periodic backups, start a backup, and restore your console's configuration settings from an existing backup file. One View creates backups in the form of .tgz files.

To start any of the backup procedures, click **SETTINGS** in the masthead and click **Backup**. The **Backup** page presents two panes: the **Settings for Backup** pane and the **Restore from Backup** pane.

> **Caution**: Enabling One View backups configures the One View Console to save your settings to a backup file that is stored inside the One View VM. To ensure that the backup is available if the One View VM crashes or is lost, you must copy the backup file to another system on a regular basis.

To enable periodic backups or start a backup of your One View **settings**

1. On the **Settings for Backup** pane, click the **Enable Backup** button.

   Two boxes drop down with fields for required values.

2. Specify the following values in the drop-down boxes:

   - **Backup Location:** the full path name of the backup location, ending with the name of the .tgz file; for example, /home/admin/backup.tgz.
   - **Interval (hours)**: the interval, in number of hours, at which you want the system to automatically back up configuration settings; for example, 24.

3. Click **Save** to save the specified values or **Reset** to clear them.

4. To start a backup now, click the **Backup Now** button.

To restore your console's settings from an existing backup file

1. On the **Restore from Backup** pane, supply the full path name of the backup file in the required **Location of Backups** field.

2. Click **Restore** to restore the configuration settings to those in the backup file, or click **Reset** to clear the path name.

Transferring Backup Files to and from the One View VM

To ensure that your One View backup is available if the One View VM crashes or is lost, you must copy the backup file from the guest operating system of the One View VM to another system on a regular basis by using a secure copy (SCP) utility. The CentOS guest operating system that runs in the One View VM already supports SCP, but you may need to download additional software to your remote management system to establish an SCP connection:

Linux-based Remote Systems

On many Linux and UNIX systems, standard SCP utilities are already installed and enabled by default. See `scp(1)` for information about how to use these utilities.

The following examples show how to log on to the One View VM and transfer a backup file to or from a remote Linux-based system; however, you could also initiate the SCP connection from the remote system and use different commands.

To transfer the backup file to a Linux- or UNIX-based system

Perform this procedure after creating a backup file to copy the file to another system for safekeeping (for example to any Physical Machine in any everRun system).

1. Open the console window of the One View VM, or connect to the VM with an SSH utility.
2. Log on as the `admin` user. The default password is **admin**, if you have not changed it yet.
3. Locate the file that you need to transfer. For example, if you stored the file in the `admin` user's home directory, it may be `/home/admin/backup.tgz`.
4. Consider renaming the backup file with a unique name or time stamp.
5. Transfer the file to the remote system with an `scp` command in the format:

   ```
   $ scp backup_fileuser@remote_system:/target_directory
   ```

   For example, to transfer the file to the `/home/admin` directory on the remote system `ocean.xyz.com`:

   ```
   $ scp /home/admin/backup.tgz admin@ocean-
   .xyz.com:/home/admin/
   backup.tgz           100% 4122     4.0KB/s    00:00
   ```

To transfer the backup file from a Linux- or UNIX-based system to the One View VM

Perform this procedure to transfer a backup file from a remote system to the One View VM for a restore operation.

1. Open the console window of the One View VM, or connect to the VM with an SSH utility.
2. Log on as the `admin` user. The default password is **admin**, if you have not changed it yet.

3. Transfer the backup file to the One View VM with an `scp` command in the format:

   ```
   $ scp user@remote_system:/directory/backup_file /target_directory
   ```

   For example, to transfer the file from the remote system `ocean.xyz.com` to the `/home/admin` directory of the One View VM:

   ```
   $ scp admin@ocean.xyz.com:/home/admin/backup.tgz /home/admin
   backup.tgz            100% 4122      4.0KB/s     00:00
   ```

Windows-based Remote Systems

If you want to connect to the One View VM from a Windows management PC, you can download and use PuTTY, a suite of open-source SSH clients:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

In particular, PuTTY includes the `pscp.exe` command-line utility that allows you to securely transfer files from the One View VM to your management PC.

If you prefer a secure copy (SCP) client with a graphical user interface, you can also try the open-source WinSCP utility:

http://winscp.net/eng/index.php

The steps to transfer files depend on the utility that you choose. For more information, see the documentation for your SCP utility.

Generating Diagnostic Files

Diagnostic files maintain a record of your system's activities and events.

To create a diagnostic file

1. Click **SETTINGS** in the masthead.
2. Click **Diagnostics**.
3. Click **Generate Diagnostic File**.

   As the file is generated, a box appears, showing the date and time and an activity indicator.
   When the file has been generated, the system displays a box showing the log file's date and time of creation.

To read a diagnostic file

1. Click the diagnostic file to download it. The resulting diagnostic file will be in the browser's download area.
2. Extract the downloaded .tar.xz diagnostic file to read it.

To delete a diagnostic file

1. On the **Diagnostics** page, hover your cursor over the diagnostic file you want to delete and click **Delete Diagnostics?** when it appears.
2. In the **Confirm Delete** window, click **Yes**.
   The system deletes the file.

Managing SMTP Settings

Click **SETTINGS** in the masthead and then click **SMTP** to manage SMTP settings.

Under **SMTP Settings**, set the following values:

- **SMTP Host**: The name of the email host for your network (for example, host1.se.yourcompany.com).
- **Mail Sender**: The email address of the email sender.
- **Use TLS?**: Check this box if you want to use Transport Layer Security (TLS).
- **Use SMTP Auth?**: Check this box if you want to use SMTP Authentication.

After providing the SMTP settings, click **Save** to save the values or **Reset** to clear the values.

Click **Send Test Email** to verify that you have set up SMTP settings correctly.

Managing Users

The Stratus One View Console uses password-protected user accounts. You can perform the following user-management tasks:

- "Adding a User" on page 36
- "User Roles" on page 35
- "Editing a User Role" on page 36
- "Deleting a User" on page 37

User Roles

When adding a user to the system (see "Adding a User" on page 36), you assign one of the following roles to each user:

Administrator is the highest permission level granted to a user. Administrators can manage all aspects of platforms, VMs, and all settings. They may also create, delete, and modify user accounts. The wrench icon in the user box on the **Users** page indicates an administrator.

Platform Manager can completely manage platforms, VMs, and all settings. They may not create, delete, or modify user accounts. The pencil icon in the user box indicates a platform manager.

Read-only users can monitor platform and VM status, view all settings, and subscribe to notifications. The magnifying glass icon in the user box indicates read-only permission.

Related Topics

"Adding a User" on page 36

"Editing a User Role" on page 36

"Deleting a User" on page 37

Adding a User

You can add multiple user accounts to your One View environment.

To add a user

1. Click **SETTINGS** in the masthead.
2. Click **Users** and then click **Add User**.
3. Enter the user's email address and, in the **Role** box, select a role for the new user. (See "User Roles" on page 35 for an explanation of user roles.)
4. Click **Save**.

Related Topics

"Editing a User Role" on page 36

"Deleting a User" on page 37

Editing a User Role

You can modify a user's role.

To modify a user role

1. Click **SETTINGS** in the masthead.
2. Click **Users** and click the box of the user to be modified.
3. From the **Edit User Role** window, select the user's new role. (See "User Roles" on page 35 for an explanation of user roles.)
4. Click **Save**.

Related Topics

"Adding a User" on page 36

"Deleting a User" on page 37

Deleting a User

You can delete a user.

To delete a user

1. Click **SETTINGS** in the masthead.
2. Click **Users** and hover your mouse over the user to be deleted.
3. When the **Delete User?** link appears, click it.
4. On the **Delete User** box, click **Yes** to delete or **No** to retain the user.

Related Topics

"Adding a User" on page 36

"Editing a User Role" on page 36

7

Chapter 7: Managing Virtual Machines

Manage your virtual machines (VMs) to view their status and resources, control their operation, and manage their Disaster Recovery (DR) protection.

To manage a VM, click a VM box on the **VIRTUAL MACHINES** page (see "The VIRTUAL MACHINES Page" on page 26) of the Stratus One View Console. To perform specific management tasks on the VM details page, see:

- "Managing Virtual Machine Resources" on page 39
- "Opening a Virtual Machine Console Session" on page 40
- "Starting, Shutting Down, or Powering off a Virtual Machine" on page 42
- "Managing Email Notifications" on page 29

To manage DR protection for a VM, see:

- "Configuring and Maintaining Disaster Recovery" on page 58
- "Managing Disaster Recovery Operations" on page 64

Managing Virtual Machine Resources

Open the details page for a specific virtual machine (VM) to view the VM's resources, controls, and Disaster Recovery settings.

To view the VM details page

1. On the One View Console, click **VIRTUAL MACHINES** in the masthead.
2. Click a VM to manage. The VM details page is displayed, as follows:
   - The left-hand pane displays the VM's resources. It also provides the controls for:
     - "Opening a Virtual Machine Console Session" on page 40
     - "Starting, Shutting Down, or Powering off a Virtual Machine" on page 42
   - The **Disaster Recovery** pane, if present, displays the status of the associated DR VM and provides controls for managing DR protection. For information about managing your Disaster Recovery environment, see the "Stratus everRun Disaster Recovery User's Guide" on page 47.

Related Topics

"The VIRTUAL MACHINES Page" on page 26

Opening a Virtual Machine Console Session

Open a virtual machine (VM) console session to display the console of the guest operating system running in the VM. The following procedure describes how to open a VM console in the Stratus One View Console, but you can also use a remote desktop application for this purpose.

To open a VM console

1. On the **VIRTUAL MACHINES** page, click a VM to open its details page.
2. Ensure that the VM is in a running state.
3. Click **Console**.
4. If prompted, allow the required Java™ plugins to load in your web browser.

Troubleshooting

To resolve an issue where the VM console window does not open

Allow the required Java™ plugins to load in your web browser. For information about enabling Java, see "Web Browser Requirements" on page 14.

If you still have problems opening the VM console session, you may need to ask your network administrator to open ports 6900-6999 (inclusive).

To resolve an issue where the VM console window is blank

Verify that the VM is powered on and not in the process of booting. Also, click in the console window and press any key to deactivate the screen saver.

To resolve an issue where more than one VM console window is displayed and they are behaving erratically

Close all console windows and open only one console window.

To resolve an issue where the VM console window hangs on the everRun system

For Ubuntu-based VMs, the VM console hangs if you do not properly set the `gfxmode` parameter. In the guest operating system, edit the `/boot/grub/grub.cfg` file and change the `gfx-mode` parameter to `text` (for example, `set gfxmode=text`).

If the console hangs before you can set the parameter, do the following:

1. Restart the VM.
2. At the GRUB menu, press `e` to edit the grub command.
3. On the next screen, on the `gfxmode` line, change `$linux_gfx_mode` to `text` so the line reads:

   ```
   gfxmode text
   ```

4. Press **Ctrl-x** or **F10** to boot the guest operating system.
5. To update the setting so it persists for each boot cycle, edit the `/boot/-grub/grub.cfg` file and change the `gfxmode` parameter to `text` so the line reads:

   ```
   set gfxmode=text
   ```

6. Save the `/boot/grub/grub.cfg` file.

To change the terminal type in a Linux-based VM if the console screen is unreadable

By default, the Linux operating system sets the `TERM` variable to `vt100-nav`, which is not properly supported by the `vncterm` program, the basis for the VM console. If you use anything other than the command line, the screen becomes unreadable. To resolve this issue, change the terminal type in the Linux guest operating system:

1. Open the `inittab` file in the guest operating system.
2. In the following line, replace `vt100-nav` with `vt100` by deleting `-nav` at the end of the line.

   The updated line appears as follows:

   ```
   # Run gettys in standard runlevels co:2345:respawn:/sbin/agetty
   xvc0 9600 vt100
   ```

3. Save the **inittab** file.

Starting, Shutting Down, or Powering off a Virtual Machine

Start, shut down, or power off a virtual machine (VM) to control the state of the guest operating system running on the virtual machine.

To access the VM controls, click a VM on the **VIRTUAL MACHINES** page of the Stratus One View Console.

In the left panel of the VM details page, you can:

- Click **Start** to boot the guest operating system.
- Click **Shutdown** to begin an orderly shutdown of the guest operating system.
- Click **Power Off** to stop the virtual machine without properly shutting down the operating system.

Caution: Use the **Power Off** command only if the **Shutdown** command or guest operating system commands fail. Powering off a virtual machine is similar to pulling the power cord, which may result in data loss.

8

Chapter 8: Managing Platforms

Manage platforms to view information about alerts, virtual machines (VMs), physical machines (PMs), and resource allocations, and to perform specific management tasks.

To manage platforms, click **PLATFORMS** in the masthead of the Stratus One View Console (see "The PLATFORMS Page" on page 26).

To manage a specific platform, click a platform box on the **PLATFORMS** page, which opens a platform details page.

To perform specific management tasks, see the following topics:

- "Adding a Platform to the One View Console" on page 43
- "Managing Email Notifications" on page 29
- "Launching a Portal to a Target Platform" on page 45
- "Unmanaging a Platform" on page 45
- "Viewing Platform Resources and Alerts" on page 44

Adding a Platform to the One View Console

Add a platform to the One View Console to begin managing the platform from the console. The procedure consists of **Part A** and **Part B:**

Part A: Registering a platform

1. In the everRun Availability Console, obtain the **Asset ID** of the system that you want to add to the One View Console. The **Asset ID** appears in the masthead, under the system name.

2. In the One View Console, click **PLATFORMS** in the masthead.
3. Click **Register Platform** in the action bar.
4. In the **Register Platform** dialog box that appears, enter the **Asset ID** (obtained in Step 1).
5. Click **Save**.

Part B: Adding the platform to the One View Console

1. In the everRun Availability Console, navigate to **One View** on the **PREFERENCES** page:
    a. Click **Preferences** in the left-hand navigation panel.
    b. On the **PREFERENCES** page, click **One View** under **Remote Support**.
2. With **One View** selected on the **PREFERENCES** page, click **Enable One View.**
3. In the **Server** box, enter the IP address or DNS name for the One View Console. (If you need to obtain the IP address, see "Obtaining and Setting the Initial IP Address for the Stratus One View Console" on page 16.)
4. Click **Save**.

   In the One View Console, confirm that the new system appears on the **PLATFORMS** page.

Related Topics

"The PLATFORMS Page" on page 26

"Installing the Stratus One View Console" on page 13

Viewing Platform Resources and Alerts

You can view information about a specific platform's resources and alerts.

To view platform resources and alerts

1. On the One View Console, click **PLATFORMS** in the masthead.
2. Click the box of the desired platform.
3. View alerts, physical machines, virtual machines, and resource allocations:

- The **Alerts** pane lists platform alerts.
    - Click **Show Ignored** to view ignored alerts.
    - Click **Show History** to view the alert history.

- The **Virtual Machines** pane displays VM boxes. Click the box of a virtual machine to open its details window.
- The **Physical Machines** pane displays node boxes with information about the nodes for you to view.
- The **Resource Allocations** pane displays bar graphs of CPU, memory and storage resources for you to view.

Related Topics

"The PLATFORMS Page" on page 26

Unmanaging a Platform

Discontinue managing a platform to remove the platform from the One View Console. The platform, though, remains registered.

To discontinue managing a platform

1. On the One View Console, click **PLATFORMS** in the masthead.
2. Click the box of the desired platform.
3. On the platform details page, click **Unmanage** in the actions bar.
4. Click **Yes** in the confirmation dialog box to discontinue management.

   When the console returns to the **PLATFORMS** page, confirm that the platform you removed no longer appears.

Related Topics

"Adding a Platform to the One View Console" on page 43

"The PLATFORMS Page" on page 26

Launching a Portal to a Target Platform

You can open a portal to a target platform's everRun Availability Console from the Stratus One View Console.

To launch a portal to a target platform

1. Log in to the One View Console.
2. Click **PLATFORMS** in the masthead of the home page.

3. Click the target platform.

4. On the platform details page, click **Launch Portal** in the actions bar.

5. Log in to the portal.

Related Topics

"The PLATFORMS Page" on page 26

Part 3: Stratus everRun Disaster Recovery User's Guide

The *Stratus everRun Disaster Recovery User's Guide* describes the everRun Disaster Recovery feature and how to configure and use it.

For Disaster Recovery overview descriptions, including terminology and types of DR operations, see:

- "Disaster Recovery Overview" on page 48

For setup and configuration information, see:

- "Configuring and Maintaining Disaster Recovery" on page 58

For information about how to manage Disaster Recovery operations, see:

- "Managing Disaster Recovery Operations" on page 64

9

Chapter 9: Disaster Recovery Overview

The Stratus everRun Disaster Recovery (DR) feature enables you to protect VMs running on everRun systems.

DR protection involves taking snapshots of VMs running on a primary system and replicating the VMs and their snapshots to a DR system located at a separate DR site. The VMs running on the first system are called *primary VMs*. The backup VMs on the system at the DR site are called *DR VMs*.

You can control how often snapshots are taken and the number of snapshots to be retained, up to the allowed maximum. Should a failure occur, DR protection provides for the recovery of VMs with minimal data loss. For maintenance and other planned outages, it provides the ability to move a running VM to a different system with no data loss.

For information about DR terminology and types of operations, see:

- "Disaster Recovery Terminology" on page 49
- "Disaster Recovery Operations" on page 50

For information about system licensing requirements, see:

- "Disaster Recovery Licensing" on page 51

For information about DR platform configurations, including important considerations, see:

- "Network Considerations" on page 56
- "Disk Space Usage and Retention" on page 55
- "Data Compression" on page 56

For information about setting up and configuring DR protection, see:

- "Configuring and Maintaining Disaster Recovery" on page 58

Disaster Recovery Terminology

You should be familiar with the following Disaster Recovery terminology.

Terminology	Description
Coalesce	To remove the oldest snapshot by merging it with the next oldest snapshot.
Destination VM	The VM to which the source VM is being replicated. Depending on the situation, either the primary VM or the DR VM can be the destination VM.
DR VM	Initially, the everRun VM to which the primary VM is being replicated. Under normal operating circumstances, the DR VM is not running or serving clients. In the case of either a planned maintenance period or unplanned failure of the everRun system on which the primary VM exists, you can manually start the DR VM to serve clients
Primary VM	Initially, the everRun VM that is under DR protection. Under normal operating circumstances, the primary VM is running and serving clients, and snapshots of it are taken periodically and are replicated to another everRun system.
Recovery Point Objective (RPO)	The RPO value determines the frequency of snapshots and therefore the maximum acceptable period during which data might be lost from a VM. The RPO value depends on the speed of the network between the primary VM and the DR VM sites, as well as how quickly data changes between snapshots. See "One View and Disaster Recovery Considerations and Requirements" on page 77 for the allowed RPO values.
Recovery Time Objective (RTO)	The targeted duration of time within which a VM must be restored in order to avoid unacceptable consequences. The RTO value depends on the time it takes an administrator to perform external network reconfigurations to make the DR VM available to clients that previously accessed the primary VM.

Terminology	Description
Source VM	The VM that is currently running and serving clients, and that is capable of being replicated to a remote site. Depending on the situation, either the primary VM or the DR VM can be the source VM.

Disaster Recovery Operations

This topic provides an overview of the DR operations.

Migrating to a DR VM (Planned)

When a system containing primary VMs must be shut down (for example, when performing maintenance), you can migrate each primary VM to a DR VM running on a second system with no data loss. Once the DR VMs are running, you can then shut down the first system. See "Migrating to a DR VM (Planned)" on page 65 for details.

Failing Over to a DR VM (Unplanned)

If a primary VM fails, you can recover--with minimal data loss--by failing over to the DR VM. In this case, the DR VM is started using data from a selected snapshot. See "Failing Over to a DR VM (Unplanned)" on page 66 for details.

Migrating Current Data Back to the Primary VM

If a DR VM has been running long enough to accumulate new data that you want to preserve, you can migrate this data back to the primary VM with no data loss. See "Migrating Current Data Back to the Primary VM" on page 67 for details.

Reverting to the Original Data on the Primary VM

If a DR VM has been running for a brief period of time and has not accumulated any data that you wish to preserve, you can revert back to the primary VM with its original data. You might choose to do this if the primary VM unexpectedly becomes available soon after an unplanned failover. See "Reverting to the Original Data on the Primary VM" on page 68 for details.

Taking an Unscheduled Snapshot

If you suspect that a system failure is imminent, or if you are about to perform an activity that could result in a system failure, you can take an unscheduled snapshot to capture the most recent data. See "Taking an Unscheduled Snapshot" on page 69 for details.

Disaster Recovery Licensing

Every everRun system in your DR-protected environment must have a Disaster Recovery enabled license. This includes the systems where primary VMs reside, as well as the system where DR VMs reside.

After registering the Disaster Recovery enabled licenses, you can enable DR protection of VMs. The roles of the VMs (primary and DR) are established when you initially enable DR protection for a VM.

Note: The Disaster Recovery license package includes a simplex everRun license for the DR system. You cannot use a standard duplex everRun license to register a simplex everRun system.

Managing the Disaster Recovery Product License

Manage the Disaster Recovery product license by:

- Uploading a license .key file saved on a computer.
- Downloading an activated license .key file to a computer and then uploading it to the everRun system.
- Activating, renewing, or checking the status of an existing license.

When you purchase Disaster Recovery, Stratus provides you with a license .key file (via email). Save the license .key file to a location on a computer (not your everRun system) that you can access when you need to upload (and activate) the license to the everRun system.

If you do not yet have a license, or if you need to upgrade or renew a license or support, you must contact everRun Customer Support or your authorized Stratus service representative. See the **everRun Downloads and Support** page at http://www.stratus.com/go/support/everrun.

Your license is automatically activated/renewed each time you upload a license .key file to an everRun system that has Internet connectivity to the Stratus `alas.stratus.com` server via port 443 (https). The everRun system also attempts to activate/renew your license every 24 hours. If your everRun system does not have Internet connectivity, you can manually download an activated .key file to a computer and then upload it to the everRun system.

To upload a new license .key file to an everRun system with internet connectivity

After you have saved a license.key file to a computer, use this procedure to upload the license.key file to the everRun system. The everRun system must have internet connectivity.

1. In the everRun Availability Console, click **Preferences** in the left-hand navigation panel.
2. On the **Preferences** page, click **Product License**.
3. Click the **New License** bar to display its options.
4. Under **Upload New License Key**, click **Browse** and navigate to the location of the license .key file on your computer. Select the license .key file and click **Open.** Then click **Upload** to upload the file to the everRun system. The everRun system contacts the Stratus server to activate the license.

To license an everRun system with no Internet connectivity (but is connected to a computer that has Internet connectivity)

If your everRun system is not connected to the Internet but has private intranet connectivity to a computer that is connected to the Internet, perform the following steps to download an activated license and then upload it to an everRun system.

1. In the everRun Availability Console, click **Preferences** in the left-hand navigation panel.
2. On the **Preferences** page, click **Product License**.
3. Click the **License Check and Activation** bar to display its options.
4. Under Step 1, **Download Activated License Key**, click **Activated License** to activate and download a license .key file to a computer (not the everRun system).

   The **Opening av_*number*_A.key** dialog box appears. In the dialog box, select **Save File** and select a location on the computer to save the downloaded .key file. (Depending on the browser, the default location for saving the file may be the Downloads folder.)
5. Under Step 2, **Upload Activated License Key**, click **Browse** and navigate to the license .key file that you saved in the previous step. Then, click **Upload** to upload it to the everRun system.

To license an everRun system with no Internet connectivity

If your everRun system is not connected to the Internet and has no private intranet connectivity to a computer that is connected to the Internet, perform the following steps to obtain an activated license and then move it to an everRun system.

For this procedure:

- You will need a USB flash drive and two computers (A and B) in addition to the everRun system.
- Computer A has internet access and has no connection to the everRun system.
- Computer B has access to the everRun Availability Console on the everRun system, but both of these computers are **not** connected to the internet.

<u>On Computer B</u>

1. Insert a USB flash drive into a USB port.
2. Log on to the everRun Availability Console.
3. Click **Preferences** in the left-hand navigation panel.
4. On the **Preferences** page, click **Product License**.
5. Click the **License Check and Activation** bar to display its options.
6. Under Step 1, right-click the **Activate License** link and select your browser's option to copy the link (for example, **Copy Link Location** or **Copy Link Address**).
7. Open a text editor (notepad.exe), paste the copied URL in to it, and save the contents of the editor to a text file on the USB flash drive.
8. Remove the USB flash drive.

<u>On Computer A</u>

1. Insert the USB flash drive into a USB port.
2. In a text editor, open the text file on the USB flash drive. Copy the URL in the text editor to the clipboard.
3. Open a web browser and paste the URL into the address bar. Press **Enter**. A license .key file will be downloaded.
4. Copy the license .key file to the USB flash drive.
5. Remove the USB flash drive.

<u>On Computer B</u>

1. Insert the USB flash drive into a USB port.
2. Click **Preferences** in the left-hand navigation panel.
3. On the Preferences page, click **Product License**.
4. Click the **License Check and Activation** bar to display its options.
5. Click **Browse**, navigate to the license .key file on the USB flash drive, and select it. Click **Open**.
6. In the **Product License** pane, click **Upload**.

To check the status of a license

Use this procedure to check the status of a license .key file that you have already uploaded on a computer that has Internet connectivity to the Stratus `alas.stratus.com` server via port 443 (https).

1. In the everRun Availability Console, click **Preferences** in the left-hand navigation panel.
2. On the **Preferences** page, click **Product License**.
3. Click the **License Check and Activation** bar.
4. Click **Check License Now**. The console displays the status of the license:

    STATUS: License is activated and expires in *nn* days *nn* hours

    TYPE OF LICENSE: Enterprise Edition (volume)

    EXPIRATION: *month dd*, 20*yy*, *time*

    LAST CHECK: *month dd*, 20*yy*, *time*

    Asset ID: *asset_id*

License Activation Error Codes

If a license activation fails, the License Activation Server (or ALAS) returns one of the following numeric error codes.

2.1: ALAS_UNKNOWN_SITEID

The specified Asset ID key does not exist in the Stratus customer database Atlas. If the license was just created (for example, with trial IDs), the license information might not yet have propagated to ALAS. Wait 15 minutes and try again. If the activation fails again, contact your authorized Stratus service representative and provide them with the return code.

3.1: ALAS_INVALID_ARG

The ALAS URL was called without an Asset ID parameter. This error can occur with an improperly formed license key that does not include the Asset ID.

3.2: ALAS_INVALID_SITEID

The Asset ID parameter has been specified but does not contain a value. This error can occur with an improperly formed license key that includes a blank Asset ID.

3.3: ALAS_NO_SIGN

ALAS cannot communicate with the SSL certificate signing server.

3.4: ALAS_NO_ATLAS_UPDATE

ALAS failed to update activation information, OS release number, and/or other information in Atlas. This error occurs on the ALAS side of the license activation.

3.5: ALAS_NO_MORE_ACTIVATION

The site has exceeded the number of activations allowed (typically 3). If necessary, your authorized Stratus service representative can change the limit.

9.0: ALAS_UNKNOWN

Unknown error.

Related Topics

"Registering the Disaster Recovery Product License" on page 58

"Enabling Disaster Recovery Protection for a Virtual Machine" on page 59

Disk Space Usage and Retention

An everRun system that takes snapshots and has DR protection enabled requires a larger volume container. The size of the volume container depends largely on the amount of data that is written to the volume between snapshots. This amount varies for different applications and different RPO values.

For a typical case with 10 or fewer DR-retained snapshots and with an additional 3 user-created snapshots:

- For a VM created with a separate boot disk, or for applications that write relatively small amounts of data between snapshots, a reasonable volume-container size is 2.6 times larger than the volume size.

- For applications that write moderate amounts of data between snapshots, a reasonable volume-container size is approximately 3.5 times larger than the volume size.
- For applications that write larger amounts of data between snapshots, the volume-container size may be more than 3.5 times larger than the volume size.

A general formula for calculating the approximate volume-container size is:

VolContSize = 2 * *VolSize* + [(*NumSnapshotsRetained* + 1) * *SnapshotSize*]

> **Note**: *NumSnapshotsRetained* is the value you specify for **Maximum number of snapshots to keep** when you are enabling DR protection. See "Enabling Disaster Recovery Protection for a Virtual Machine" on page 59 for details.

Before you use the preceding formula, you must calculate *SnapshotSize*:

1. During peak business hours, take four or more snapshots of the primary VM in sequence with a time of (*TargetRPO*) / 2 between them. For example, if the RPO is set for 2 hours, the software takes a snapshot every hour.
2. Then, for each of the VM's volumes, look into its volume container.
   a. Ignore the first volume snapshot.
   b. For the remaining volume snapshots, calculate the average of the three largest volume snapshots. This average is *SnapshotSize*.

Related Topics

"Disaster Recovery Terminology" on page 49

Data Compression

When DR protection is enabled for a VM, snapshot data is transferred between the primary VM and its associated DR VM. Disaster Recovery provides the option to compress data during these transfers. Depending on the size of the VMs to be transferred and the bandwidth of your network link(s), you can choose to use compressed or uncompressed data during these transfers.

See "Enabling Disaster Recovery Protection for a Virtual Machine" on page 59 for information about how to configure DR protection to use data compression.

Network Considerations

Before you enable DR protection on the primary VM, consider the following:

- You set the recovery time objective (RTO) value based on how long it will take for the DR VM to enter a running state. Because the primary and DR VMs are in different IP subnets, when a failover or migration occurs, the DNS servers need to know about the new IP address. When you are determining the RTO value, you need to be aware of the speed at which the network can propagate the DNS name change to the secondary DNS servers.
- An appropriate recovery point objective (RPO) value depends on the network connectivity between the primary VM and DR VM sites, as well as the rate of data being changed between snapshots. Therefore, no minimum RPO value can be guaranteed.

Related Topics

"Enabling Disaster Recovery Protection for a Virtual Machine" on page 59

"Disaster Recovery Terminology" on page 49

10

Chapter 10: Configuring and Maintaining Disaster Recovery

Configure your Disaster Recovery (DR) environment to activate the DR features of the Stratus One View Console and to start enabling DR protection for your virtual machines.

To initially configure and maintain your DR environment, see:

- "Registering the Disaster Recovery Product License" on page 58
- "Enabling Disaster Recovery Protection for a Virtual Machine" on page 59
- "Modifying Disaster Recovery Protection for a Virtual Machine" on page 62
- "Disabling Disaster Recovery Protection for a Virtual Machine" on page 63

To manage DR failover and failback operations after the initial configuration, see "Managing Disaster Recovery Operations" on page 64.

Registering the Disaster Recovery Product License

Register your Disaster Recovery (DR) product license to activate the DR features of the Stratus One View Console.

The DR software is installed automatically as a component of the Stratus everRun and One View software. To activate the DR features, register your DR-enabled product license on each everRun system that you want to include in your DR-protected environment.

Every everRun system in your DR-protected environment must have a Disaster Recovery enabled license. This includes the systems where primary VMs reside, as well as the systems where DR VMs reside.

To register your product license on an everRun system

1. In the everRun Availability Console, click **Preferences** in the left-hand navigation panel.
2. On the **Preferences** page, click **Product License**.
3. Upload a license key file. For details, see the everRun online help.

After registering your product license, you can continue configuring your DR environment as described in "Configuring and Maintaining Disaster Recovery" on page 58.

Enabling Disaster Recovery Protection for a Virtual Machine

Enable Disaster Recovery (DR) protection for a virtual machine (VM) to begin snapshot replication of the primary VM to a DR VM at the DR site.

Prerequisites:

- Review the information in "One View and Disaster Recovery Considerations and Requirements" on page 77 to verify that your planned DR configuration is supported.
- Ensure that you have finished creating the VM and installing the guest operating system. If necessary, open the VM console and verify that the guest is healthy and responsive.
- Configure the power button action in the guest operating system to shut down the guest. (For information, see the everRun help and your operating system documentation.) If the DR software cannot automatically shut down a VM with the power button action in the event of a DR migration, the operation may be delayed until you log on to the VM console and manually shut down the guest operating system.
- Verify that the storage group on the everRun system has enough free storage space to support DR operations. For example, enabling DR protection automatically increases the size of each volume container associated with the primary VM (by approximately 3.5 times larger than the volume size) if the volume containers are not large enough to store DR snapshots.

To enable DR protection for a VM

1. If you have not already done so, add your everRun systems to the One View Console as described in "Adding a Platform to the One View Console" on page 43. Add the everRun system that contains the primary VM as well as the system at the DR site where you want to replicate the VM snapshots and maintain the DR VM.

2. On the **VIRTUAL MACHINES** page, click the VM that you want to protect (the primary VM) to open its details page.

3. On the VM details page, click **DR Protect** to open the DR wizard.

4. On the **Disaster Recovery Platform** page, select the system where DR will replicate the primary VM and click **Next**.

   > **Note**: Valid DR-site systems must be simplex everRun systems that are managed by the One View Console. Each DR-site system must also have an activated, DR-enabled product license as described in "Registering the Disaster Recovery Product License" on page 58.

5. On the **Disaster Recovery Options** page:

   a. Enter the **Recovery Point Objective**. The Recovery Point Objective (RPO) is the maximum acceptable period during which data might be lost from a VM. For example, if you would not want to lose more than one hour of changes, then enter 1 hour.

   b. Select the snapshot **Retention** setting. The DR software keeps only the specified number of snapshots. When the limit is reached, the DR software creates a new snapshot. The DR software then *coalesces* the oldest snapshot (that is, it merges it with the next oldest snapshot) and finally deletes the oldest snapshot.

   c. Select the check box next to **Compress network transfers of snapshot data** if you want to compress the snapshot data for transfers to the DR site.

   d. Click **Next**.

6. On the Disaster Recovery **VM Name, VCPUs, and Memory** page, if applicable, modify the name and resource settings to use for the DR VM and click **Next**.

   > **Caution**: To ensure that the DR VM will function properly during a failover event, do not modify these settings unless you have specific needs.

7. On the Disaster Recovery **VM Volumes** page, verify the list of volumes that will be replicated and click **Next**.

8. On the Disaster Recovery **VM Network** page:

   a. In the left pulldown menu, select one **Virtual Network** from the primary VM to include in the DR VM.

   b. In the right pulldown menu, select one **Platform Network** from the DR platform to connect to the chosen **Virtual Network**.

   c. Click **Next**.

   Notes:

   - When you initially configure DR protection, only one **Virtual Network** from the primary VM is replicated to DR VM; however, you can add more networks later.
   - If you migrate or fail over to the DR VM, the DR VM starts with the network disabled, which allows you to modify any network settings in the guest operating system before the DR VM becomes the active VM.
   - When needed, you can add or enable networks by using the **Reprovision Virtual Machine** wizard in the everRun Availability Console on the DR platform.

9. On the **Disaster Recovery Configuration Summary** page, verify the summary of DR settings.

10. Click **Finish** to initialize DR protection and return to the VM details page. The VM details page indicates that Disaster Recovery **is Initializing**.

After a few minutes, a new **DR** pane appears on the VM details page of the One View Console to display the information about the DR VM and the status of the DR initialization process.

As the process continues, DR replicates the primary VM to the DR site. DR also creates a snapshot of the primary VM and immediately replicates the snapshot to the DR site. Unless modified, each DR VM and DR snapshot at the DR site is assigned a unique name based on the Asset ID from the primary site.

You can monitor DR activity on the VM details page of the One View Console and also on the **Virtual Machines** and **Snapshots** pages of the everRun Availability Console for each primary and DR site.

When the initialization completes, the VM details page in the One View Console indicates that Disaster Recovery **is Active**. The amount of time to complete the initialization depends on the number and size of the volumes that must be replicated at the DR site. Thereafter, the DR snapshots continue based on the RPO and snapshot-retention settings, which you can modify as described in "Modifying Disaster Recovery Protection for a Virtual Machine" on page 62. The DR software automatically manages the inventory of

DR snapshots. If necessary, you can create an unscheduled DR snapshot as described in "Taking an Unscheduled Snapshot" on page 69, but you cannot manually remove any DR snapshots or the DR VM in the everRun Availability Console unless you disable DR protection.

When DR is active, the DR VM appears in the list of VMs on the **VIRTUAL MACHINES** page of the One View Console, where both the primary VM and DR VM are displayed as stacked boxes to indicate that these VMs are DR protected.

Because DR protection runs in the background of the everRun systems, snapshot replication continues running as long as both systems are online and even if the One View VM goes offline; however, you must have access to the One View Console to monitor DR status, maintain your DR configuration, and manage failover operations if needed.

Related Topics

"Modifying Disaster Recovery Protection for a Virtual Machine" on page 62

"Disabling Disaster Recovery Protection for a Virtual Machine" on page 63

"Pausing Disaster Recovery Protection for a Virtual Machine" on page 65

Modifying Disaster Recovery Protection for a Virtual Machine

Modify Disaster Recovery (DR) protection for a virtual machine (VM) if you need to change its Recovery Point Objective (RPO) or snapshot-retention settings.

To modify DR protection for a VM

1. On the **VIRTUAL MACHINES** page, click a protected VM to open its details page.
2. In the **DR** pane, next to the **RPO** and **Retention** summary, click the edit button.
3. In the **Modify Recovery** dialog box:
    a. Enter the **Recovery Point Objective**. The Recovery Point Objective (RPO) is the maximum acceptable period during which data might be lost from a VM. For example, if you would not want to lose more than one hour of changes, then enter 1 hour.

    b. Select the snapshot **Retention** setting. The DR software keeps only the specified number of snapshots. When the limit is reached, the DR software creates a new snapshot. The DR software then *coalesces* the oldest snapshot (that is, it merges it with the next oldest snapshot) and finally deletes the oldest snapshot.

   c. Select the check box next to **Compress network transfers of snapshot data** if you want to compress the snapshot data for transfers to the DR site.

4. Click **Save**.

The new settings are displayed in the **DR** pane of the VM details page. If needed, DR creates new snapshots or coalesces snapshots to comply with the updated settings.

Disabling Disaster Recovery Protection for a Virtual Machine

Disable Disaster Recovery (DR) protection for a virtual machine (VM) to stop snapshot replication of the VM to the DR site.

To disable DR protection for a VM

1. On the **VIRTUAL MACHINES** page, click a VM to open its details page.
2. On the VM details page, click **DR Unprotect**.
3. Confirm that you want to delete the DR VM and its snapshots. (Or, if failover has occurred, confirm that you want to delete the primary VM.)

In a few moments, DR protection is stopped and the Disaster Recovery pane is removed from the right-hand side of the VM details page. If any DR snapshots remain, you can delete them in the everRun Availability Console after DR protection is disabled.

11

Chapter 11: Managing Disaster Recovery Operations

The following topics describe how to manage DR operations:

Note: You must be registered as an administrator or platform manager to perform DR operations.

Ongoing DR Protection

Ongoing DR protection occurs in the background and protects the primary VM with scheduled snapshot updates from the primary VM to the DR VM.

When you set up a schedule for the snapshots to occur, be aware that snapshots occur twice during that time period: once at the beginning, and once at the halfway point. For example, if you schedule snapshots to occur every 60 minutes, the system takes a snapshot in the first minute and then again in 30 minutes. If an update cycle has not completed before the next scheduled update, the system defers the next update.

You also need to set how many snapshots the system should retain, up to a maximum of 12. The volume container must be large enough to hold all of the snapshots.

Related Topics

"Disk Space Usage and Retention" on page 55

Pausing Disaster Recovery Protection for a Virtual Machine

Pause Disaster Recovery (DR) protection for a virtual machine (VM) to temporarily pause snapshot replication of the VM to a DR site.

For example, you can temporarily pause snapshot replication if you expect a planned network outage in your environment, and then resume DR protection when network connectivity is restored.

> **Caution**: DR protection is maintained as long as the existing snapshots on the DR site are within the Recovery Point Objective (RPO) and you resume protection before the RPO is exceeded. If you do not resume DR protection before the RPO is exceeded, recovery is possible only to the point in time when the last snapshot was taken.

To pause DR protection for a VM

1. On the **VIRTUAL MACHINES** page, click a VM to open its details page.
2. On the VM details page, click **Pause DR**.

To resume DR protection for a VM

1. On the **VIRTUAL MACHINES** page, click a VM to open its details page.
2. On the VM details page, click **Resume DR**.

Migrating to a DR VM (Planned)

For planned outages (for example, system or site maintenance), you can migrate to a DR VM. When you migrate to a DR VM:

- DR protection is paused.
- The primary VM is gracefully shut down.
- A snapshot of the final state of the primary VM is taken.

- The final snapshot is replicated to the DR VM.
- The DR VM boots from the final snapshot.

Notes:

1. No data is lost during a planned migration. However, for a period of time, neither the primary VM nor the DR VM will be running.
2. During the failover, monitor the primary VM to make sure it shuts down. If it does not, shut it down manually by going into the guest operating system and performing a shutdown. See "Enabling Disaster Recovery Protection for a Virtual Machine" on page 59 for more information.
3. After a planned migration, the DR VM is not DR protected (that is, no snapshots of it are taken). Snapshots and updates start when you click **Begin Migration**. To provide maximum protection, do this as soon as the other system is running again and connected.
4. When the DR VM is booted, it starts up with all network interfaces disabled. You can enable the networks by using the **Reprovision Virtual Machine** wizard in the everRun Availability Console on the DR system.

To migrate to a DR VM (Planned)

1. In the Stratus One View Console masthead, click **VIRTUAL MACHINES**.
2. On the **VIRTUAL MACHINES** page, click the primary VM that you want to migrate.
3. In the action bar, click **Start Migration**.
4. When the migration is complete, the message **Disaster Recovery has migrated to the DR VM** appears.

Failing Over to a DR VM (Unplanned)

You can recover from a primary VM failure by starting its DR VM and using a recent snapshot. When you recover from a VM failure:

- DR protection is paused.
- The failed primary VM is shut down if possible.
- The DR VM boots from whichever snapshot you select.

Caution: Data that accumulated between the time when the most recent snapshot of the primary VM was completed and the time of the failure is lost.

You can minimize the amount of lost data by setting an appropriate value for your Recovery Point Objective (RPO) when you enable DR protection for your VM (see "Enabling Disaster Recovery Protection for a Virtual Machine" on page 59). Be aware, though, that bandwidth increases as your RPO value drops, so you may not want to set the value too low.

Notes:

1. During the failover, monitor the primary VM to make sure it shuts down. If it does not, shut it down manually by going into the guest operating system and performing a shutdown. See "Enabling Disaster Recovery Protection for a Virtual Machine" on page 59 for more information.
2. After an unplanned failover, the DR VM is not DR protected (that is, no snapshots of it are taken). Snapshots and updates start when you click **Begin Migration**. To provide maximum protection, do this as soon as the other system is running again and connected.
3. When the DR VM is booted, it starts up with all network interfaces disabled. You can enable the networks by using the **Reprovision Virtual Machine** wizard in the everRun Availability Console on the DR system.

To fail over to a DR VM (Unplanned)

1. In the Stratus One View Console masthead, click **VIRTUAL MACHINES**.
2. On the **VIRTUAL MACHINES** page, click the DR VM that corresponds to the failed primary VM.
3. On the VM pane for the DR VM, click the desired snapshot (here, called a *recovery point*).
4. Click **Recover**.

Migrating Current Data Back to the Primary VM

If a DR VM has been running long enough to accumulate new data that you want to preserve, you can migrate this data back to the primary VM with no data loss. When you migrate data back to a primary VM:

- The direction of DR protection is reversed (that is, snapshots are sent from the DR VM to the primary VM).
- DR protection is resumed for the reverse direction.
- The DR VM is shut down, and a final snapshot of it is taken. The user clicks **Finish Migration** to initiate the final steps.
- The final snapshot is replicated to the site where the primary VM resides.
- The primary VM is started.
- The direction of DR protection is returned to normal operation (snapshots sent from primary VM to DR VM).

No data is lost migrating back to the primary VM. However, for a period of time, neither the DR VM nor the primary VM will be running.

To migrate current data back to the primary VM

1. In the Stratus One View Console masthead, click **VIRTUAL MACHINES**.
2. On the **VIRTUAL MACHINES** page, click the DR VM that corresponds to the primary VM.
3. In the action bar, click **Begin Migration**.
4. The system begins to take snapshots on the DR VM and copies them to the primary VM. When the system finishes migrating the data, the **Finish Migration** button appears in the action bar. Click **Finish Migration** to complete this operation.

   The DR VM is shut down. One more snapshot is taken and copied to the primary VM. The primary VM is started.

   Note: This operation automatically enables DR protection on the primary VM; you do not need to enable it manually.

Reverting to the Original Data on the Primary VM

If a DR VM has been running for a brief period of time and has not accumulated any data that you wish to preserve, you can revert back to the primary VM with its original data. When you revert to the primary VM:

- The recently created DR VM is shut down and is then deleted.
- The original primary VM is booted.
- DR protection is resumed.

> **Caution**: Data accumulated by the DR VM while it was running is lost.

To revert back to the original data on the primary VM

1. In the Stratus One View Console masthead, click **VIRTUAL MACHINES**.
2. On the **VIRTUAL MACHINES** page, click either the original primary VM or its corresponding DR VM.
3. In the action bar, click **Abort Migration**. (This option is visible only after the primary VM has been migrated to the DR VM.)

   > **Note**: This operation automatically enables DR protection on the primary VM; you do not need to enable it manually.

Taking an Unscheduled Snapshot

If you suspect that a system failure is imminent, or if you are about to perform an activity that could result in a system failure, you can take an unscheduled snapshot to capture the most recent data.

To take an unscheduled snapshot

1. In the Stratus One View Console masthead, click **VIRTUAL MACHINES**.
2. On the **VIRTUAL MACHINES** page, click the primary VM for which you want to take a snapshot.
3. On the VM pane, click **DR Snapshot**.
4. At the prompt, click **yes** to take an unscheduled snapshot.

Recovering From a Primary Site Disaster

To recover from a primary site disaster, perform the following procedure for each DR-protected VM.

1. In the One View Console, failover to the DR system by following the steps in "Failing Over to a DR VM (Unplanned)" on page 66 for details. A new VM will be booted from a DR snapshot. Wait until the VM boot completes.

2. Delete the Primary site instance of the VM from One View. In the One View Console, disable DR protection for the VM by following the procedure in "Disabling Disaster Recovery Protection for a Virtual Machine" on page 63 and the instructions below:

   - At the prompt **We have lost contact with one of your VMs. Are you sure you want to unprotect? This may cause undesired results** click **Yes.**
   - At the prompt **Are you sure you want to unprotect and delete the primary VM *name*?** click **Yes**.

3. Delete the primary site platform from One View. In the One View Console, unmanage the lost primary system by following the procedure in "Unmanaging a Platform" on page 45.
4. Shutdown the DR instance of the VM. In the DR system’s everRun Availability Console on the **Virtual Machines** page, select the DR instance of the VM and click **Shutdown**.
5. Take a snapshot of the DR instance of the VM. In the DR system’s everRun Availability Console on the **Virtual Machines** page, select the DR instance of the VM and click **Snapshot**. Then click **Create Snapshot**. See Creating a Snapshot in the *everRun User's Guide* for details.
6. Export the DR instance of the VM. In the DR system’s everRun Availability Console, on the **Snapshots** page, select the snapshot of the DR VM and click **Export**. Follow the prompts. See Exporting a Snapshot in the *everRun User's Guide* for details.
7. Install a new everRun system at the primary site. See the everRun Quick Start Guide for details.
8. In the new primary system's everRun Availability Console, import the DR instance of the VM. For instructions, see Importing an OVF File from an everRun 7.x System in the *everRun User's Guide*. When using the import wizard, select **Restore** to restore the original hardware information (MAC address, HW id, etc.) that may be required by a software license.
9. Start the restored VM. In the new primary system's everRun Availability Console on the **Virtual Machines** page, select the restored VM and click **Start**.
10. In the DR system’s everRun Availability Console, delete the instance of the VM that you exported in step 6.
11. In the One View Console, add the new primary site platform to One View. See "Adding a Platform to the One View Console" on page 43 for instructions.
12. In the One View Console, enable DR protection of the restored VM on the new primary system. See "Enabling Disaster Recovery Protection for a Virtual Machine" on page 59 for instructions.

Wait for DR initialization to complete. When complete, the One View Console displays the message Disaster Recovery **is Active**.

Part 4: Supporting Documents

See the following support documents for release information, and reference information.

12

Chapter 12: Stratus One View Console Release 1.0.1.0 Release Notes

These release notes are for the Stratus One View Console release 1.0.1.0 (updated at 3:02 PM on 12/9/2014). See the following sections:

- Important Considerations
- Known Issues
- New Features, Enhancements, and Bug Fixes
- Getting Help

> ℹ **Note**: For the latest technical information and updates, see the English version of the Stratus One View Console User's Guide at the **everRun Downloads and Support** page at http://www.stratus.com/go/support/everrun.

Important Considerations

See the "Stratus One View Console and everRun Disaster Recovery Quick Start Guide" on page 1 for instructions on how to get your Stratus One View Console and everRun Disaster Recovery (DR) environment up and running quickly.

See "One View and Disaster Recovery Considerations and Requirements" on page 77 for important information about system configuration requirements and software configuration limits.

Known Issues

Removing User or DR Snapshots Temporarily Prevents Some VM and DR Operations

When either a user or the DR software removes a snapshot on an everRunsystem, the system must coalesce the snapshot by merging it with the next oldest snapshot. **While the system is coalescing snapshots**:

- A user cannot create a new snapshot in the everRun Availability Console or create an unscheduled DR snapshot in the One View Console. If you try, an error indicates that the system is busy.
- The DR software cannot create DR snapshots of the primary VM. If DR snapshots are delayed long enough, DR protection may temporarily fall below your snapshot retention and recovery point objective (RPO) thresholds until DR snapshots resume.
- A user cannot start the VM associated with the snapshot(s) if the VM is currently stopped. The **Start** button is temporarily unavailable on the **Virtual Machines** page of the everRun Availability Console and on the VM details page of the One View Console.
- A user cannot enable or resume DR protection for a VM. An alert on the **Alerts** page of the everRun Availability Console or the One View Console may indicate that there is not enough storage space for the snapshot, because the coalescing snapshots continue to occupy space in the volume container(s) until they are finally removed.

Avoid removing snapshots if you have an immediate need to perform any of these operations. After you remove a snapshot, wait at least 10-15 minutes before attempting any of these operations, or retry the operation if needed. You may need to wait much longer depending on the size of your volumes, the amount of VM activity, and the number of snapshots you remove.

For DR-protected VMs, if DR snapshot replication appears to stop or fall below your thresholds, check the **Alerts** page of the everRun Availability Console and the One View Console for more information.

Coalescing Snapshots Can Affect RPO

When snapshots are coalescing, new snapshots cannot be taken until coalescing completes. If the RPO is set to be near or lower than the typical coalesce time for a VM's activity level, the VM will periodically fall out of RPO. For systems with moderate work load and RPOs in the 1 - 6 hour range, this is unlikely to happen but should this occur, it is necessary to increase the RPO time to avoid falling out of RPO.

DR Protect VMs With QCOW2 Disk Image Format Only

Only DR protect VMs whose volumes have QCOW2 disk image formats. If the VM has a raw disk format volume, do not DR protect it.

Note: VMs created on releases earlier than 7.2 do not use the QCOW2 format and are not candidates for DR protection in this release.

Do Not Remove DR Protection During DR Site Network Connectivity Failure

If the DR system loses network connectivity and can no longer communicate with the primary system, do not remove DR protection from its VMs. After DR system connectivity is restored, DR protection of the VMs will resume and it is then safe to remove DR protection from VMs.

Note: If the DR system's network connectivity cannot or will not be restored, contact everRun Customer Support or your authorized Stratus service representative. See the **everRun Downloads and Support** page at http://www.stratus.com/go/support/everrun.

Primary and DR VM Snapshot Sizes May Be Different

The One ViewConsole displays the disk space allocated to the primary and DR VM snapshots, not the size of the data within the snapshots. The primary VM snapshot and its corresponding DR VM snapshot are located on different file systems on different physical machines and their allocated sizes are likely to be different.

New Features, Enhancements, and Bug Fixes

Major new features, enhancements, and/or bug fixes are listed below under the release in which they became available.

Fixed in One View Release 1.0.1.0

- bz-28713 - Changing the RPO does not take effect until after the next scheduled snapshot
- bz-28776 - DR takes an unwanted snapshot as part of the lossless failback process
- bz-28777 - Changing the retention count does not take effect on the source VM
- bz-28778 - Create lossless failback cancel state machine so **Cancel** button is enabled
- bz-28564 - Show whitelisted platforms in One View UI

Getting Help

If you have a technical question about the Stratus One View Console software, you can find the latest documentation at the the **everRun Downloads and Support** page at http://www.stratus.com/go/support/everrun.

If you are unable to resolve your questions with the online documentation, and the system is covered by a service agreement, please contact everRun Customer Support or your authorized Stratus service representative. For information see the One View Support page at http://www.stratus.com/go/support/everrun.

13

Chapter 13: One View and Disaster Recovery Considerations and Requirements

You should be aware of the following important One View and Disaster Recovery considerations and requirements.

System and Configuration Requirements

- If you plan to enable Disaster Recovery, do not install the One View appliance, or virtual machine (VM), on the everRun system where your primary VMs are running. Otherwise, the One View Console will be unavailable for DR failover operations in the event of a failure at the primary site. Instead, install the One View appliance on the everRun system (or on an Avance or Virtual Box system) at the DR site.
- Do not enable DR protection for the One View appliance.
- Only one-to-one Disaster Recovery configurations are supported. An everRun system's DR protected VMs must all be protected on the same everRun system at the DR site. The DR site system can protect VMs from only one other everRun system.
- The physical machine (PM) on which a DR VM is running must have the same amount of resources as one of the two source PMs.
- The everRun system at the DR site must be a simplex system with only a single PM.

Software Configuration Limits and Considerations

- One View supports the monitoring of only everRun 7.2 systems.
- The Stratus One View Console supports the monitoring of up to 64 systems.
- One everRun system can have a maximum of 6 DR protected VMs.

> **Note**: Although the system will allow you to configure more than the maximum number of DR protected VMs, do not configure more than 6 .

- A DR protected VM can have a maximum of 6 volumes.

> **Note**: Although the system will allow you to configure more than the maximum number of volumes, do not configure more than 6.

- The minimum RPO is 1 hour; the maximum recommended RPO is 24 hours.
- A DR VM can retain a maximum of 12 snapshots.
- You cannot reprovision a DR protected VM.

Related Topics

"Disaster Recovery Terminology" on page 49

"Configuring and Maintaining Disaster Recovery" on page 58

"Installing the Stratus One View Console" on page 13