everRun®

everRun 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.

This document is protected by copyright. All rights are reserved. Stratus Technologies grants you limited permission to download and print a reasonable number of copies of this document (or any portions thereof), without change, for your internal use only, provided you retain all copyright notices and other restrictive legends and/or notices appearing in the copied document.

Copyrights

Table of Contents

Part 1: everRun User's Guide

The *everRun User's Guide* describes everRun systems, how to install them, and how to use them.

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

- *"everRun Quick Start Guide" on page 1*

For system descriptions including modes of operation and storage and network architecture, see:

- "Introduction to everRun Systems" on page 1

For planning and installation information, see:

- "Getting Started" on page 21

The following topics describe how to administer everRun systems.

- "Using the everRun Availability Console" on page 53

- "Upgrading everRun Software" on page 103

- "Migrating From Avance or everRun MX Systems" on page 143

- "Managing Logical Disks" on page 105

- "Managing Physical Machines" on page 111

- "Managing Virtual Machines" on page 121

- "Maintaining Physical Machines" on page 237

1

Chapter 1: Introduction to everRun Systems

For a summary of the steps required to install everRun software, see the *"everRun Quick Start Guide" on page 1*.

See the following topics for an introduction to everRun systems:

- "everRun System Overview" on page 7

- "Modes of Operation" on page 11

- "everRun Storage Architecture" on page 15

- "Network Architecture" on page 17

- "System Usage Restrictions" on page 19

everRun Quick Start Guide

Use the *everRun Quick Start Guide* to get your everRun system up and running as quickly as possible.

An everRun system requires two x86-64 host servers (referred to as *physical machines*, or *PMs*) that can support multiple virtual machines (VMs), and a remote management computer that can run the everRun Availability Console. This guide explains how to set up your PMs and guides you through the basic installation and start-up tasks, including:

- "Assembling Required Items" on page 2

- "Configuring Your RAID Controller" on page 2

- "Cabling Your System" on page 3

- "Burning the Software to a DVD" on page 4

- "Installing the everRun Software" on page 5

- "Logging On to the everRun Availability Console " on page 6

- "Creating a Protected Virtual Machine" on page 7

> **Note**: If you need assistance during the installation process:
>
> - Call 866-763-1813 (U.S. Toll-Free) or 602-852-3094 (International)
>
> - Visit the **Downloads** page at http://www.stratus.com/go/support/everrun

Assembling Required Items

You need the following items/information:

- Two PMs that meet the requirements listed in "System Requirements Overview" on page 22

- Ethernet cables for each network you are connecting

- A remote management computer. This is a general-purpose PC with a supported web browser to access the everRun Availability Console. It must be located on the same business/management network as the PMs being installed. For details, see "everRun Availability Console Requirements" on page 30.

- A monitor, keyboard, and cables, used only during the installation

- The everRun license key you received from Stratus

- The everRun ISO image available for download at the **Downloads** page at http://www.stratus.com/go/support/everrun

- From your network administrator, the IPv4 address, netmask, default gateway address, and DNS address values for everRun and each PM

Configuring Your RAID Controller

Stratus strongly recommends that your everRun system uses a storage RAID controller. The RAID controllers in an everRun system create logical disks from the system's physical disks, and the logical disks are then collected into a storage group. Configuration recommendations follow:

- If the system has a single logical disk, Stratus strongly recommends that you configure the RAID controller so that logical disks presented to the host are backed by redundant physical drives.

- Stratus strongly recommends that RAID controllers have a battery-backed write cache.

- You must configure the RAID controller to boot off the first logical disk.

Cabling Your System

Attach the following cables:

- Private network: Connect an Ethernet cable from the **first embedded port** on the first PM to the **first embedded port** on the second PM. If you plan to use the private network as an A-Link, see "A-Link and Private Networks" on page 18.

- Business/Management network: The first business network is the *management network*. Connect Ethernet cables from the **second embedded port** on each PM, through a network switch to a network, and connect the remote management computer to this network.

- A-Link network(s): For each A-Link network, connect an Ethernet cable from any unused port on the first PM to any unused port on the second PM, either directly or through a network switch.

- Business network(s): For each business network, connect Ethernet cables from a port on the first PM to a port on the second PM, through a network switch to a network.

- Make sure the remote management computer is connected, or routes to, the management network.

- Connect the monitor, keyboard, and mouse to the first PM. See "Site and System Preparation" on page 33 for details.

The following illustration shows these connections:
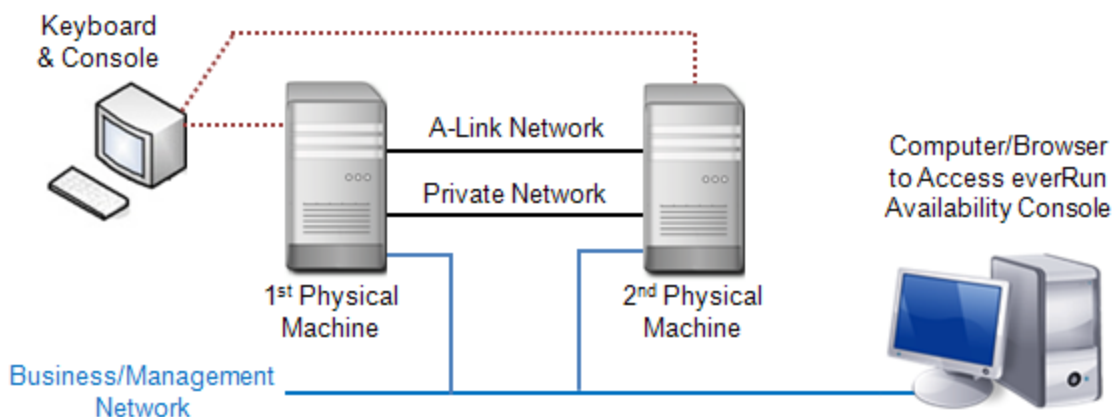
> **Note**: When installing software on the first PM, connect the keyboard and monitor to the first PM. When installing software on the second PM, connect the keyboard and monitor to the second PM. When software installation is complete, disconnect the keyboard and monitor from the system.

Burning the Software to a DVD

Obtain the ISO image, verify it, and burn it to a DVD:

1. From any computer connected to the Internet, go to the **Downloads** page at http://www.stratus.-com/go/support/everrun.

2. To download the everRun software ISO image (everRun_**install-7.**_x.x.x-xxx_.**iso**), under **Product Download**, click **everRun 7.**_x.x.x_ **ISO Image**. Save the ISO image.

   Occasionally a file can be corrupted during the download process. To confirm that the downloaded file is not corrupted, verify the ISO image. After you verify the ISO image, or if you choose to skip verification, go to **Step 3**.

   Verifying the ISO Image (Windows)

   a. Download the Microsoft File Checksum Integrity Verifier (FCIV) executable file from the Microsoft Support Website. Save the file to the directory that contains the downloaded ISO file.

   b. Download the FCIV verification file. Under **Product Download**, click everRun **7.**_x.x.x_ **ISO fciv**. Save the file to the directory that contains the downloaded ISO file.

   c. Open a command prompt. From the directory containing the ISO, executable, and verification files, type the following command to check the ISO image's status:

   fciv -v -xml everRun_install-7._x.x.x-xxx_.**xml**

   d. If the command succeeds (that is, it returns the message `All files verified successfully`), go to **Step 3**. If the command fails, repeat the download.

   Verifying the ISO Image (Linux)

   a. Download the **md5sum** verification file. Under **Product Download**, click everRun **7.**_x.x.x_ **ISO md5sum**. Save the file to the directory that contains the downloaded ISO file.

    b. From the directory containing the ISO and verification files, type the following command to check the ISO image's status:

        md5sum -c everRun_install-7.*x.x.x-xxx*.md5

    c. If the command <u>succeeds</u> (that is, it returns the message `everRun_install-7.x.x.x-xxx.iso: OK`), go to **Step 3**. If the command <u>fails</u>, repeat the download.

3. When the validation is complete, use a commonly available DVD application to burn the ISO image to a DVD. For example, if you have the Roxio application installed, right click the ISO file and select the option to burn a DVD.

For additional information, see "Obtaining everRun Software" on page 34.

Installing the everRun Software

Allow 60 to 90 minutes to complete the everRun software installation process.

1. Install the everRun software on the first PM:

    a. Power on the first PM and insert the DVD.

    b. As the PM powers on, configure the following BIOS settings:

        ○ Set the first boot device to the Optical Drive.

        ○ Enable Virtualization Technology.

        ○ Enable Execute-Disable Bit Capability.

> **Note**: If you need to configure your keyboard for a different layout, see "Mapping Your Keyboard" on page 44.

    c. From the installation software's Welcome screen, use the arrow keys to select **Install ever-Run, Create a new system**, and press **Enter**.

    d. From the **Select interface for private Physical Machine connection** screen, select the first embedded port, **em1** (if it is not already selected), and press **F12.**

    e. From the **Select interface for managing the system (ibiz0)** screen, select the second embedded port, **em2** (if it is not already selected), and press **F12.**

    f. From the **Select the method to configure ibiz0** screen, select **Manual configuration (Static Address)** and press **F12**.

> **Note**: To perform a dynamic IP configuration, select **Automatic configuration via DHCP** instead and skip to **Step 1h**, where you will need to write down the IPv4 address as described in "Recording the Management IP Address" on page 45.

 g. From the **Configure em2** screen, enter the IPv4 address, netmask, default gateway address, and DNS address values that you received from your network administrator, and then press **F12**.

 h. No action from you is necessary until after the PM reboots. At that time, eject the DVD, connect the keyboard/console to the second PM, and go to **Step 2**.

2. Install the everRun software on the second PM:

 a. Power on the second PM and insert the DVD.

 b. As the PM powers on, configure the BIOS as described in **Step 1b**.

 c. From the installation software's Welcome screen, use the arrow keys to select **Replace PM, Join system: Initialize data**, and press **Enter**.

 d. Perform **Steps 1c** through **1f**.

 e. No action from you is necessary until after the second PM reboots. At that time, eject the DVD, disconnect the keyboard/console, and log on to the everRun Availability Console.

Logging On to the everRun Availability Console

1. From the remote management computer, type the IP address of node0 (primary) into a browser address bar.

2. The logon page of the everRun Availability Console appears. Enter **admin** for the **Username** and **admin** for **Password**, and then click **LOGIN**.

3. The Stratus everRun EULA appears. Read the EULA and click **Accept** to accept it.

4. The **INITIAL CONFIGURATION** page appears. Under **NOTIFICATIONS**, the box for **Enable Support Notifications** is checked, by default. If you do not want the everRun system to send health and status notifications to your authorized Stratus service representative, uncheck the box. You can change this setting later (see "Configuring Remote Support Settings" on page 80).

5. Under **SYSTEM IP**, for IP Address, enter the address you obtained from your network

administrator.

After you have entered the network information, click **Continue**.

6. The **Portal Restart Required** window appears. After waiting a minute (as indicated in the window), click **OK** to refresh the console and to continue.

7. The **LICENSE INFORMATION** window appears. Under **Upload License Key**, click **Browse** and navigate to the license **.KEY** file that you received from Stratus. Select the license file and click **Upload**.

For security, change the default user login name and password for the **admin** account on the **Users & Groups** page.

The everRun Availability Console appears. Bookmark or make note of the system IP address for use when logging in to the console in the future.

Creating a Protected Virtual Machine

First, create a virtual CD (VCD) to make software installation media available to the virtual machine (VM).

1. Open the **Virtual CDs** page in the everRun Availability Console

2. Click **Create VCD** to open the **Virtual CD Creation Wizard**.

3. Follow creation wizard prompts. For details, see in the online help.

Next, create a new virtual machine (VM) and install a guest operating system on your everRun system.

1. On the **Virtual Machines** page, click **Create** to open the **VM Creation Wizard**.

2. Follow the creation wizard prompts. For details, see in the online help.

After you install the operating system, perform any other guest OS configuration tasks (for example, initializing disks and installing applications). For details, see in the online help.

everRun System Overview

An everRun system provides uninterrupted operation with no lost data in the event of a hardware failure. See the following topics for descriptions of system features and capabilities.

everRun System Description

everRun software allows two computers to work as a single, highly-available or fault-tolerant system. Each computer is called a physical machine.

Both physical machines (PMs):

- Run the same host operating system (CentOS)

- Contain the same data, memory and storage (synchronized via direct Ethernet links between the two PMs)

- Support virtual machines running supported guest operating systems

The PMs must:

- Have compatible CPUs

- Conform to hardware requirements for everRun systems. See "Physical Machine System Requirements" on page 405 and "System Requirements Overview" on page 22 for more information.

The data and memory contents of the two PMs are synchronized via direct Ethernet links. Other Ethernet connections to a network support virtual machine and management operations.

Related Topics

"System Requirements Overview" on page 22

"Compatible Guest Operating Systems" on page 404

"Network Architecture Overview" on page 18

Physical Machines and Virtual Machines

An everRun system transparently protects applications by creating redundant virtual machines (VMs) that run on two physical machines (PMs).

The everRun management software can create an everRun-protected VM from scratch. It is also possible to import existing VMs from other environments and convert them into an everRun-protected VMs. By creating an identical instance of the selected VM on a second host PM, everRun software provides FT-class protection of the VM. The system administrator manages this single entity from a separate, browser-based management console called the everRun Availability Console.

Neither the application nor the user is exposed to the redundant computing resources on the two host PMs. The application sees only one hostname, one MAC address for each network interface presented to the VM, and one IP address for each VM network interface presented to the VM. A system administrator loads and configures the applications on the protected VM — just as if the system administrator were loading them onto a physical server. If a fault or failure occurs in a disk or network device, everRun software automatically redirects I/O to the paired host PM for continuous operation. Though redundancy is lost until the failure is repaired, the client experiences no interruption in connectivity and no loss of data. The application continues to execute as if nothing had happened. The redundancy, fault detection, isolation, and management are completely transparent to the Windows or Linux environment and the application running within it. Repair of the PM is equally transparent and automatic. When a failed component on the PM is repaired, everRun software automatically incorporates the repaired components into the protected environment and restores redundancy without interrupting the application.

Related Topics

"Using the everRun Availability Console" on page 53

"The Physical Machines Page" on page 84

"The Virtual Machines Page" on page 88

Administrative Operations

You can perform many administrative operations on the everRun system from the everRun Availability Console, a browser-based interface that provides access to the system as a whole as well as to physical machines (PMs), virtual machines (VMs), and other resources. For information, see "The everRun Availability Console" on page 54.

Alerts

everRun system alert messages notify the system administrator whenever an item needs attention. These can include:

- Configuration tasks that should be performed

- Notification of system operational states

- System problems that require attention

Click **Dashboard** in the left-hand navigation panel to see Alert messages and their descriptions. Click **Alerts** in the left-hand navigation panel to see the Alert log.

The following icons indicate the state of an alert message.

 Informational

 Normal or OK state

 Minor, warning, or inconsistent state

 Moderate state

 Broken, failed, or severe state

Remote Support

To access the everRun system's remote support features, click **Preferences** in the left-hand navigation panel. From there, you can configure support and proxy specifications by selecting the following:

- **Support Configuration**—Configure settings to allow remote support access of your system by your authorized Stratus service representative and to enable your system to send health and status notifications to your authorized Stratus service representative. See "Configuring Remote Support Settings" on page 80 for details.

- **Proxy Configuration**—Enables you to configure a proxy server for access to the Internet. See "Configuring Internet Proxy Settings" on page 82 for details.

Lights-Out Management

Some server vendors may provide lights-out capabilities. Lights-out capabilities enable administrators to perform a wide range of system management and operation functions remotely. everRun systems fully support lights-out management on vendor servers.

Third-party Management Tools

You can install third-party management tools on everRun systems. Examples of such tools include vendor- or platform-specific management/monitoring utilities, enterprise management/monitoring utilities, and other miscellaneous management/monitoring software. Note the following:

- In general, management tools that run on the host operating system (CentOS) should run on everRun systems. Possible exceptions are tools that manage/monitor the CentOS KVM-based virtualization. To manage/monitor everRun virtualization, use the integrated everRun management tools.

- Before deploying your everRun system, Stratus recommends that you verify that it operates properly with the management tools installed and operational.

- Stratus recommends that you set up a non-root account for third-party management tools.

- You can access your everRun system via the management network using the IP address(es) specified during the installation process (or supplied by the DHCP server if the interface was configured for DHCP during install).

For information about accessing the host operating system, see "Accessing the Host Operating System" on page 20.

Related Topics

"Getting Started" on page 21

"System Reference Information" on page 404

Modes of Operation

An everRun system provides two modes of operation to set user-defined availability levels for VMs:

- "High Availability Operation" on page 11
- "Fault Tolerant Operation" on page 12

Both HA operation and FT operation achieve their respective level of redundancy by using a pair of physical machines (PMs).

Stratus recommends configuring quorum service for both HA operation and FT operation. The quorum service prevents a condition called *split-brain* where both PMs of an HA operation and FT operation pair are running independently of each other; for information, see "Quorum Servers" on page 14.

High Availability Operation

everRun software provides two user-defined availability levels for VMs: High Availability (HA) and Fault Tolerant (FT).

In HA operation, everRun software automatically detects, isolates, and handles most hardware faults, thereby keeping your applications running. With HA remote-support technology, the everRun software notifies the Stratus support center of various issues, indicating the type of fault and its exact location. This combination of automatic fault detection, isolation, and remote-support technologies ensures speedy access to expert support technicians and rapid problem resolution.

You select a VM's availability level when you create or import the VM by using the everRun Availability Console.

When enabled, HA operation offers basic failover and recovery, with some faults requiring an (automatic) VM reboot for recovery, and return to HA operation:

- Eliminates downtime for many, but not all, CPU, memory, I/O, or other physical machine (PM) failures.

- Handles failures without IT intervention.

- Provides continuous, active validation of all components.

- Assures redundancy and recovery at all times.

HA is suitable for applications that can tolerate occasional interruptions of a few minutes.

Related Topics

Fault Tolerant Operation

everRun software provides two user-defined availability levels for VMs: High Availability (HA) and Fault Tolerant (FT). In FT operation, an application continues to run without downtime during a fault. Use FT for applications that need the highest levels of availability.

You select a VM's availability level when you create or import the VM by using the everRun Availability Console.

In FT operation, the everRun software transparently protects an application by creating a redundant environment for a VM running across two physical machines (PMs). With an identical instance of the selected VM on a second host, the everRun software provides FT-class protection of the VM.

When enabled, FT operation transparently protects a VM from all faults, with no downtime, and FT operation:

- Eliminates downtime due to any CPU, memory, I/O, or other physical machine (PM) failure.

- Handles failures without IT intervention.

- Ensures no data loss.

- Provides continuous, active validation of all components.

- Assures complete redundancy and recovery at all times.

Related Topics

"The Virtual Machines Page" on page 88

"Using the everRun Availability Console" on page 53

Simplex Operation

A simplex everRun system may only be used in a Disaster Recovery (DR) configuration. In a DR configuration, FT- and/or HA-protected virtual machines (VMs) run on a duplex everRun system at one site and snapshots of those VMs are replicated to a simplex system at another site.

If a failure occurs on the duplex system such that the VMs on it are not able to operate, VMs can be started from the snapshots on the remote simplex system.

A simplex everRun system is part of a DR configuration and should not be confused with simplex mode, wherein an HA or FT VM is temporarily running on a single PM on a duplex system because the partner PM has failed.

SplitSite Configurations

A *SplitSite configuration* connects two physical machines in two separate sites. It is a disaster-tolerant deployment that maintains hardware redundancy as well as redundancy of physical computer rooms and the buildings containing them. Because of the geographic separation, a SplitSite configuration requires careful planning of component placement and more complex networking topologies. **For SplitSite configurations,** Stratus **strongly recommends that you use the quorum service because a SplitSite configuration exposes the A-Link networks to other potential failure scenarios.**

"SplitSite Network Requirements" on page 28 lists the requirements for networks in a SplitSite configuration.

SplitSite and Quorum Service

In a SplitSite configuration, configure two quorum-service computers in compliance with the best practices recommended for quorum deployment (see "Quorum Servers Considerations" on page 31). In any SplitSite configuration, a preferred quorum-service computer is located in a third facility, and an alternate is located in a fourth site (or carefully placed in the third). The networks are interconnected.

Quorum-service computers should be as isolated as possible. If both must be placed in a common (third) site, make sure that they do not depend on common power sources.

Physical connectivity between an everRun PM and the quorum-service computers must not route through the other PM's site.

Placing a quorum-service computer in the same site as one of the everRun PMs ensures data integrity. However, some site failures may then require that the VMs be shut down until manually recovered.

The management network physically connects the everRun PMs and the quorum-service computers. For this to work properly, you must configure each everRun PM to use a different gateway to reach the quorum-service computers. If the two PMs use the same gateway to reach the quorum-service computers, data integrity is ensured during failures. However, some site failures may then require that the VMs be shut down until manually recovered.

Related Topics

"Quorum Servers" on page 14

"Network Architecture Overview" on page 18

Quorum Servers

A *quorum service* is a Windows operating system-based service deployed on a server distinct from the two servers (physical machines or PMs) running HA- or FT-protected virtual machines (VMs). Quorum servers provide data integrity assurances and automatic restart capabilities for specific failures in an ever-Run environment. Stratus strongly recommends using quorum servers, especially for SplitSite operation. You can configure an everRun PM pair with 0, 1, or 2 quorum servers.

Quorum servers ensure the integrity of VMs against multiple network failure scenarios, including split brain, and provide for unattended startup of VMs after specific failures. Quorum server communication occurs via the management network.

Quorum servers are particularly important in SplitSite configurations. Best practice for SplitSite is to place a preferred quorum computer in a third facility and an alternate quorum computer in a fourth facility.

However, you can also place the alternate quorum service computer with the preferred quorum computer and still obtain satisfactory service.

If only two sites are available (thereby preventing the best practices configuration described above) and if one PM goes down and the surviving PM is unable to communicate with the quorum server (for example, because it is on the same site as the down PM), the VMs at the surviving site are automatically shut down to avoid a potential split-brain scenario.

Related Topics

"Quorum Servers Considerations" on page 31

"Configuring Quorum Servers" on page 68

"SplitSite Configurations" on page 13

everRun Storage Architecture

The RAID controllers in an everRun system create logical disks from the system's physical disks. The logical disks are collected into a storage group. Logical disks contain everRun system volumes and virtual machine (VM) volumes. Each volume resides in an associated container that includes the current data on that volume as well as any volume snapshots.

The two physical machines (PM) in an everRun system can have different storage capacities, but only the smaller capacity is available to the system. For example, if one PM has 1 TB of storage in a storage group and the other has 2 TB of storage in that same storage group, only 1 TB is available to the everRun system for that storage group.

For more information about everRun storage, see the following topics:

- "Logical Disks and Physical Disks" on page 15

- "The Storage Group" on page 16

- "Sizing Volume Containers" on page 16

- "Storage Requirements" on page 23

Logical Disks and Physical Disks

In an everRun system, the RAID controller creates logical disks from the system's physical disks. everRun software is able to access logical disks that the RAID controller presents to the operating system. The everRun software detects new logical disks and logical disk failures. You manage logical disks using the everRun Availability Console. For information, see "Managing Logical Disks" on page 105.

You need to use the RAID controller to manage and monitor physical disks. Follow the RAID controller manufacturer's requirements to add a new or replacement physical disk to a RAID array.

Related Topics

"Storage Requirements" on page 23

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

The Storage Group

In an everRun system, a storage group is a collection of logical disks. everRun software creates the **Initial Storage Group**, which contains all logical disks present at install time. You can view information about the storage group from the **Storage Groups** page of the everRun Availability Console. For information, see "The Storage Group Page" on page 95.

Related Topics

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

Sizing Volume Containers

A *volume container* is storage space that holds a volume and VM snapshot data associated with that volume.

You can specify the size of the volume container when you create a VM. As snapshot data accumulates, you may need to increase the size of the volume container. You can expand the volume container, but you cannot decrease its size.

The following factors affect the size of a volume container:

- The volume size
- If snapshots are being taken:
  - The number of snapshots retained
  - How much data changes between snapshots
- Whether DR protection is enabled

> **Note**: The amount of data that changes between snapshots varies for different applications and can have a large impact on what size the volume container should be. In order to properly size a volume container, you must consider the amount of data that your application changes between snapshots.

If you do not take snapshots and do not enable DR protection, the size of the volume container can be the volume size.

If you take snapshots or enable DR protection, the size of the volume container depends largely on the amount of data that is written to the volume between snapshots. This 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 must be more than 3.5 times larger than the volume size.

The following is a general formula to calculate the *approximate* volume container size :

```
VolContSize = 2 * VolSize + [(# SnapshotsRetained + 1)*
SnapshotSize]
```

Related Topics

"Expanding a Volume Container on the everRun System" on page 213

"image-container-resize" on page 310

Network Architecture

See the following topics for information about everRun network architecture.

- "Network Architecture Overview" on page 18

- "A-Link and Private Networks" on page 18

- "Business and Management Networks" on page 19

Network Architecture Overview

Ethernet networks provide pathways for communications between two physical machines (PMs) in an everRun system. The main types of Ethernet networks are:

- *Availability Link networks*, or *A-Link networks*, are assigned to virtual machines (VMs) and are used to synchronize data or migrate VMs between two PMs. One A-Link network must be a *private network*, which connects the two everRun PMs. See "A-Link and Private Networks" on page 18.

- *Business networks* allow your applications to connect to your network. One business network must be a *management network*, which connects to the everRun Availability Console and is used by the quorum servers. See "Business and Management Networks" on page 19.

An everRun system must have a minimum of one private network and one management network per PM.

A-Link and Private Networks

Every everRun system requires one *private* network, referred to as *priv0*, that connects the two everRun physical machines (PMs). The private network is used only for discovery and can have no other entities on it that respond to IPv4 broadcasts.

In addition to the private network, an everRun system has A-Link networks to increase data-replication performance between PMs. *A-Link* networks let you sync disks, shunt networks, migrate, perform heartbeat checks, and sync fault-tolerant memory.

By default, the private network also performs the role of an A-Link network under the following conditions:

- If the private network speed is at least 10 Gb

- If the private network speed is less than 10 Gb and the system contains no other 10 Gb ports (other than the management link). In this situation, you can remove the A-link role later as long as the private network is not currently in use as an A-Link **and** is not the only remaining A-Link.

The private network cannot perform the A-Link role if its speed is less than 10 Gb **and** the system contains any 10 Gb ports (other than the management link). However, you can assign the A-Link role to the private network at a later time.

The simplest private network consists of a single Ethernet cable (crossover or straight-through) that directly connects an embedded Ethernet port on each server. If a networking device other than a single Ethernet cable is used for priv0, see "SplitSite Configurations" on page 13.

Connect A-link networks between PMs either directly (that is, in the same manner that you connect the private network) or through a network switch.

Be sure to set up redundant A-Link networks.

The everRun installation software sets up the private network. It also sets up A-Link networks for any A-Link network ports that are physically connected at the time of the installation. To set up an A-Link network after the installation is complete (recommended if the network includes many additional A-Link network ports), see "Connecting Additional Networks" on page 50.

Related Topics

"Business and Management Networks" on page 19

"A-Link and Private Network Requirements" on page 27

"Network Architecture Overview" on page 18

"Fixing a Network Connection" on page 96

Business and Management Networks

All Ethernet ports--other than those used by A-Link networks (including the private network port)--are considered business-network ports, which your guest operating systems use to connect to your network.

One business network is the *management* network, which accesses the everRun Availability Console and handles miscellaneous management tasks and the quorum server. Each everRun PM has a single management network, referred to as *ibiz0*.

The everRun installation software sets up the management network. It also sets up business networks for any business-network ports that are physically connected at the time of the installation. To set up business networks after the installation is complete, see "Connecting Additional Networks" on page 50.

Related Topics

"A-Link and Private Networks" on page 18

"Business and Management Network Requirements" on page 26

"Network Architecture Overview" on page 18

"Fixing a Network Connection" on page 96

System Usage Restrictions

Observe the restrictions to system usage that are described in the following topics:

- "QEMU" on page 20

- "Accessing the Host Operating System" on page 20

QEMU

Stratus everRun systems support the open-sourced hypervisor QEMU ("Quick EMUlator"), which performs hardware virtualization. When used as a virtualizer, QEMU executes the guest code directly on the host CPU, achieving a high level of performance.

everRun users should make no changes to the QEMU virtualization engine or to its configuration.

Accessing the Host Operating System

After the everRun software installation process completes, you can access the host operating system (CentOS) locally via the PM's physical console, or you can access it remotely via SSH.

If you access the host operating system via SSH, use the management IP addresses specified during the installation process (or supplied by the DHCP server, if the interface was configured for DHCP during installation). See "Recording the Management IP Address" on page 45.

> ⓘ **Note**: Do not use the system IP address to access the host operating system, as it can move from PM to PM.

The default password for the root account is **everRun**.

> ⓘ **Note**: For security reasons, change the username and password as soon as possible.

For information about using third-party management tools on CentOS, see "Third-party Management Tools" on page 10.

2

Chapter 2: Getting Started

The following topics describe the everRun planning, installation and post-installation tasks:

Planning

See the following topics for information about planning your system configuration.

After you have planned the system configuration, continue with "Software Installation" on page 32.

System Requirements Overview

An everRun system requires two x86-64 host servers that can support multiple virtual machines (VMs), and a remote management computer (that is, a general-purpose PC) that can run the everRun Availability Console.

everRun "System Hardware " on page 22 requirements are described below. See "System Software" on page 23 for software requirements.

System Hardware

Supported Servers

Stratus everRun software will run on any systems listed on the Red Hat® Linux Hardware Catalog that support RHEL 6.x and any of the supported processors listed in "Physical Machine System Requirements" on page 405.

A second computer with identical processors is required for use as a redundant server for Protected Virtual Machines (or *PVMs*—virtual machines that are protected by Stratus everRun software). The CPUs for every host computer must have hardware support for virtualization enabled in the firmware (BIOS) setup utility.

RAM

A minimum of 8 GB of RAM (physical memory) is recommended.

Disk Space Requirements

Only internal disks are supported. A minimum of two drives per physical machine is required.

477 MB is required on each internal logical disk for the host CentOS operating system. In addition, 22 GB is required on two of the internal logical disks for everRun system data including logs. The amount of disk space required for a VM's boot volume varies depending on the operating system being used. Additional storage is needed for applications and data on each VM, as well as VM snapshots.

Network

The minimum network configuration includes two ports: one for A-link and one for a shared management/business link.

An optimal network configuration includes two 10-GbE network ports for A-Links (one of which also serves as priv0, the private network), a network interface for the management network, and as many business/production ports as your protected VMs may need. If planning to run multiple protected VMs, consider adding pairs of A-Links, up to the supported total of four pairs.

SplitSite configurations have different network requirements. For information, see "SplitSite Network Requirements" on page 28.

See "Network Architecture Overview" on page 18, "A-Link and Private Networks" on page 18, and "Business and Management Networks" on page 19 for more information.

IP Addresses

Each everRun host must have a static IPv4 IP address assigned for use by the management software. Obtain IP addresses for DNS primary and secondary servers, and gateway and subnet mask information for your management network, from your IT network administrator. See "Obtaining System IP Information" on page 48 for more information.

Ports

everRun systems use port 443 in the local firewall for HTTPS communications, port 22 for ssh, and 5900-59*nn* for each active VNC associated with each VM. Firewalls must allow traffic through the appropriate ports. Firewalls must permit everRun-protected VMs to contact quorum service computers using UDP port 4557. For additional information on TCP and UDP ports, access the Knowledge Base to search for the article *everRun TCP and UDP ports*. See "Accessing Knowledge Base Articles" on page 411.

System Software

See "Compatible Guest Operating Systems" on page 404.

Related Topics

"Physical Machine System Requirements" on page 405

"Important Physical Machine and Virtual Machine Considerations" on page 407

"Virtual Machine Recommendations and Limits" on page 407

"Planning Virtual Machine Resources" on page 122

"Configuring IP Settings" on page 66

Storage Requirements

An everRun system has the following storage requirements and recommendations:

- Each physical machine must contain at least two physical disks.

- Stratus strongly recommends that your system use a storage RAID controller.

  - If the system has a single logical disk, Stratus strongly recommends that you configure the RAID controller so that logical disks presented to the host are backed by redundant physical drives.

  - Stratus strongly recommends that RAID controllers have a battery-backed write cache.

  - You must configure the RAID controller to boot off the first logical disk.

Disk drives support standard format and 512e format with sectors, as follows:

Format	Physical Sectors	Logical Sectors
Standard	512B	512B
512e	4KiB	512B

When planning your system configuration, confirm that your storage configuration meets these requirements and then return to .

Related Topics

Memory Requirements

A minimum of 8 GB of RAM (physical memory) is recommended. The total amount of memory available on an everRun system is equal to the minimum of the amount of memory presented by either physical machine (PM) in the system. For example, in a system where one PM has 32 GB memory and another PM has 16 GB memory, the total amount of memory is 16 GB (the least memory of either PM).

Related Topics

General Network Requirements and Configurations

This topic discusses general network requirements and provides some recommended network configurations.

Requirements

Before you install everRun software, make sure your network meets the following requirement:

- everRun systems utilize full IPv4 and IPv6 protocol access, including IPv6 multicast. Any obstruction of this traffic may prevent a successful installation or compromise the availability of a running everRun system.

In addition, see the following topics for the requirements specific to each network type:

- "A-Link and Private Network Requirements" on page 27

- "Business and Management Network Requirements" on page 26

- "SplitSite Network Requirements" on page 28

Recommended Configurations

Recommendations for possible configurations follow:

- If your system has **two 1 Gb** and **two 10 Gb** Ethernet ports:

    - Set one 10 Gb port as the private network (priv0).

    - Set the other 10 Gb port as an A-Link network.

    - Set one 1 Gb port as the management link.

    - Set the other 1 Gb port as a business link.

- If your system has **four Ethernet ports of the same type** (for example, four 1 Gb or four 10 Gb interfaces):

    - Set one port as the private network (priv0).

    - Set one port as an A-Link network.

    - Set one port as the management link.

    - Set one port as a business link.

> **Note**: A system with four 1 Gb Ethernet ports may not provide sufficient throughput for acceptable performance. The system may require 10 Gb add-on cards to achieve acceptable performance.

Business and Management Network Requirements

Business and management networks have the following requirements:

- The networks use IPv6 link-local addressing.

- The speed of business or management networks should be less than or equal to the speed of A-Link networks.

- The networks do not support bonding or VLAN trunking.

- VMs can use IPv4, IPv6, and other Ethernet protocols.

- All business networks can be used for IPv6 host access if your site has SLAAC or DHCPv6 enabled.

- To reach the everRun Availability Console, use biz0:0, which is the IPv4 address that migrates to the primary management PM. Each PM also has its own IPv4 address (ibiz0) on the management network.

- Each PM requires at least one business network (specifically, the management network), with a maximum of 20 business networks.

To ensure that Ethernet traffic flows unobstructed to and from VMs from either PM:

- The switch ports connected to business networks must not filter ARP packets, including gratuitous ARP packets. An everRun system sends gratuitous ARP packets on behalf of guest VMs in order to prompt Ethernet switches to update their port-forwarding tables to direct VM traffic to the appropriate physical Ethernet port on the appropriate everRun PM.

- The switch ports connected to business networks must allow layer2 multicasts (address: 01:E0:09:05:00:02) with ethertype: 0x8807.

- If you configure RHEL or Centos guests to have multiple NICs on same subnet, you may experience guest network connectivity issues due to asymmetric routing. To avoid this problem, modify the **/etc/sysctl.conf** file on the Protected Virtual Machine (PVM) to contain the following lines, save the file, and reboot the PVM.

- - `net.ipv4.conf.default.rp_filter = 2`

  - `net.ipv4.conf.all.rp_filter = 2`

- The switches connected to business networks must not enable any MAC address security features that would disable the movement of a MAC address from one business link to the matching business link on the other PM.

- For optimal failover response, configure any switches connected to your everRun system to have MAC aging timeout values of less than one second.

If these requirements are not met, or if the switch does not properly update its forwarding table when a VM is migrated from one everRun PM to the other, the VM may experience a blackout in which network traffic is not properly directed to and from the VM.

Related Topics

"Network Architecture Overview" on page 18

"Business and Management Networks" on page 19

"network-info" on page 334 and "network-change-mtu" on page 332

A-Link and Private Network Requirements

A-Link and private networks have the following requirements:

- The networks use IPv6 link-local addressing.

- All A-Link and private networks on one PM of an everRun system must be in the same L2 broadcast domain as its matching links on the other PM, without any protocol filtering.

- Ethernet packets sent between two everRun PMs must not be obstructed or rate-limited. Ensure that they are not routed or switched by any L3 network infrastructure.

- Each PM can have one to eight A-Link networks; however, a minimum of two is recommended.

- The networks use 1 Gb to 10 Gb Ethernet ports. The speed of A-Link networks should be equal to or greater than the speed of business or management networks.

- Network traffic for storage replication between PMs is sent over A-Link networks. A-Link networks are not required to be directly connected; instead, they can connect to a network switch.

- Private networks have no network hosts connected other than the everRun end-points.

- The system assigns each VM to a minimum of <u>one</u> or a maximum of <u>two</u> A-Link networks. However, each A-Link network can have multiple VMs assigned to it.

Related Topics

"A-Link and Private Networks" on page 18

SplitSite Network Requirements

This topic describes the requirements for networks in a SplitSite configuration.

- "A-Link Network Requirements" on page 28

- "Private Network Requirements" on page 29

- "Business Network Requirements" on page 29

- "Management Network Requirements" on page 29

General Network Requirements

All network components in a SplitSite configuration must have more than 155 Mbps minimum capacity, end-to-end.

A-Link Network Requirements

A-Link networks in a SplitSite configuration require the following:

- NICs must be at least 1 Gb and full-duplex; use 10 Gb, if possible.

- For systems running FT-protected virtual machines (VMs), A-Links require:

    - A minimum bandwidth of 1 Gbps per VM

    - A maximum inter-site latency of 2 ms, round-trip time

- For systems running only HA-protected VMs, A-Links require:

    - A minimum bandwidth of 155 Mbps per VM

    - A maximum inter-site latency of 10 ms, round-trip time

- Do not use a common card (multiport NIC) for both A-Links.

- A-Links can be dedicated point-to-point fiber connections. If they are not, they must be configured on a VLAN. The A-Links can share a single VLAN, or they can use separate VLANs. Multiple ever-Run systems can share the same VLAN(s) for use by the A-Links.

- When fault-tolerant SMP is used, the A-Link networks must be a minimum of 1Gbps.

Private Network Requirements

The private network in a SplitSite configuration requires the following:

- NICs must be at least 1 Gb and full-duplex; use 10 Gb, if possible.

- A minimum bandwidth of 155 Mbps per VM.

- A maximum inter-site latency of 10 ms, round-trip time. Switches and/or fiber-to-copper converters connected to the private network must be non-routed and non-blocking, with a round-trip latency that does not exceed 10 ms. Calculate latency at 1 ms for each 100 miles of fiber, plus any latency added by non-routed, non-blocking switches or fiber converters.

- The private network can be a dedicated point-to-point fiber connection. If it is not, it must be configured on a private VLAN. VLANs used to connect the private-network ports must not add any filtering on any of the network equipment between the two VLAN switch ports that are connected to the everRun PMs.

Business Network Requirements

Business networks in a SplitSite configuration require the following:

- Configure the network on a business VLAN. The business network for both nodes must be on this VLAN.

- The nodes must be in the same layer-2 multicast domain.

- Connect the business networks on each PM to a switch separate from the other PM's switch.

- An everRun system requires at least one business network. All of these requirements apply to each business network.

Management Network Requirements

A management network in a SplitSite configuration requires the following:

- By default, the management network is shared with a business network. In this case, all requirements for a business network apply.

- Configure gateways to a business LAN for remote management.

Related Topics

"SplitSite Configurations" on page 13

"Network Architecture Overview" on page 18

everRun Availability Console Requirements

The everRun Availability Console provides browser-based remote management of the everRun system, its physical machines (PMs), and virtual machines (VMs).

- Your computer must be able to access the subnet containing the everRun system.

- Use a supported browser. See "Compatible Internet Browsers" on page 30.

- Make sure your computer has a recent release of Java 7 or later. Your browser may require you to update to the latest version. Java downloads are available at http://www.java.com.

For more information, see "Using the everRun Availability Console" on page 53.

Compatible Internet Browsers

A browser is used to connect to the everRun Availability Console. Use only browsers that are compatible with everRun systems. Using an incompatible browser can result in some rendering problems and the omission of some wizards.

The following browsers are compatible with everRun systems.

Compatible Browsers	Release
Microsoft Internet Explorer™	IE9 or newer[1]
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 everRun Availability 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:

---

[1]IE8 is not recommended and it does not support some everRun functionality.

- 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

Quorum Servers Considerations

Enabling or configuring quorum service is a post-install configuration task. Stratus recommends configuring two quorum service computers: a preferred quorum server and an alternate. For an overview of quorum servers, see "Quorum Servers" on page 14.

Quorum service software, if deployed, can be installed on any general-purpose computer or laptop running the Windows operating system with these requirements:

- OS: Windows Server 2012, Windows Server 2008, Windows Server 2003, Windows Vista, Windows 7, or Windows 8; always powered on

- Disk space: 100 MB (minimum)

- NIC: at least one (1)

- Connectivity: Available to the everRun configuration via the management network

To install quorum server software:

1. Open the **Downloads** page at http://www.stratus.com/go/support/everrun: scroll down to the **Software Downloads** section and then, for **Select Product & Version**, select **everRun** and the appropriate version number.

2. Scroll down to the **Drivers and Tools** section and then click **Quorum Service** to download the quorum server software installer file to the quorum server.

3. On the quorum server, double click the installer file.

> **Note**: When upgrading to a more recent version of quorum server software, you do **not** need to uninstall the previous version.

In addition, consider the following for quorum service best practices:

- Configure two quorum service computers with minimum common networking between the quorum computers and the hosts.

- As installed, protected VMs contact quorum service computers using UDP port 4557. Firewalls must permit everRun-protected VMs to contact quorum service computers using UDP port 4557. (If this port assignment conflicts with your local infrastructure, you can use different port numbers when you configure the quorum servers using the everRun Availability Console.)

- Quorum service computers should not reside on the same site as any host when deploying in a SplitSite. If both preferred and alternate quorum computers fail for a common reason, VMs will gracefully downgrade redundancy, and then continue to operate using one host, pending recovery of a quorum computer. However, if a host and the elected quorum computer fail for a common reason, the VMs running on the surviving server shut themselves down. For additional information about quorum servers and SplitSite configurations, see "SplitSite Network Requirements" on page 28 and "SplitSite Configurations" on page 13.

- If the preferred and alternate quorum service computers must reside on a common site, power them from separate AC power sources (phases) or configure them on separate UPS devices.

Related Topics

"Physical Machines and Virtual Machines" on page 8

"Configuring Quorum Servers" on page 68

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

Power Requirements and Considerations

To ensure maximum availability, Stratus strongly recommends that everRun's fault-tolerant (FT) software run on physical machines (PMs) that are powered by redundant power supplies. In addition, each PM power supply should connect to a separate power source.

See "Connecting Power" on page 33 for illustrations of some sample power-connection configurations.

Also, refer to your server vendor documentation for other power-related information.

Software Installation

When you install the everRun software for the first time:

1. Prepare your site and system for the installation. See "Site and System Preparation" on page 33.

2. Connect power to your system. See "Connecting Power" on page 33.

3. Install the everRun software. See "Installing everRun Software" on page 37.

When the software installation is complete, see "Post-Installation Tasks" on page 48.

Related Topics

"Upgrading everRun Software" on page 103

Site and System Preparation

Before you install everRun software, make sure that your site and system meet the following requirements:

- The system meets all of the requirements described in "System Requirements Overview" on page 22.

- The storage configuration meets all of the requirements described in "Storage Requirements" on page 23.

- Provide keyboard and console access to each physical machine. This access can be in the form of a physical keyboard and monitor, a keyboard-video-mouse switch, or a properly-configured remote-management card capable of providing remote console and keyboard access. Connect the keyboard/console access as described in the vendor's documentation (for example, through direct VGA or USB connections).

  > **Note**: You cannot install everRun software from a serial console.

- Provide a remote management computer for the everRun Availability Console, and make sure it meets all of the requirements described in "everRun Availability Console Requirements" on page 30.

- Determine the best configuration for your network. See "General Network Requirements and Configurations" on page 24.

- Use either an internal DVD drive or a USB DVD drive for the installation.

After confirming that your site and system meet the preceding requirements, return to "Software Installation" on page 32.

Connecting Power

To connect power, configure your everRun server with redundant power supplies connected to separate

sources. After connecting power, return to "Software Installation" on page 32.

UPS (Optional)

The illustrations show how to connect one or two optional uninterruptible power supplies (UPS) to the ever-Run system.

Single UPS:
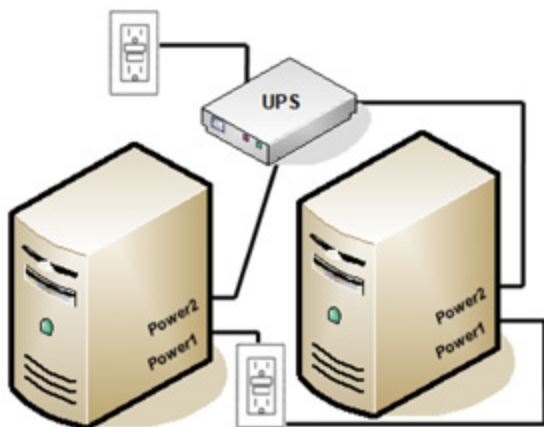
Dual UPS:
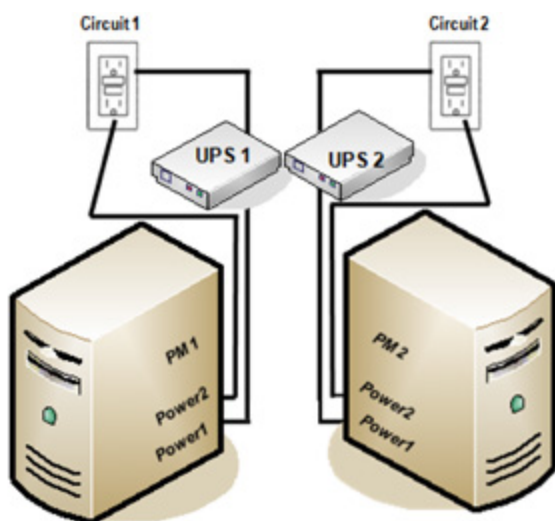
Related Topics

"Power Requirements and Considerations" on page 32

Obtaining everRun Software

Stratus provides the everRun software as an ISO image. You can boot from it directly, or you can burn it to a DVD.

> **Note**: You cannot boot the ISO image from a flash drive.

Obtaining the ISO Image

1. From any computer connected to the Internet, go to the **Downloads** page at http://www.stratus.-com/go/support/everrun.

2. To download the everRun software ISO image (everRun_**install-7.*x.x.x-xxx*.iso**), under **Product Downloads**, click **everRun 7.*x.x.x* ISO Image**. Save the ISO image.

> **Note**: Depending on your Internet connection, the download can take up to 30 minutes.

Occasionally a file can be corrupted during the download process. To confirm that the downloaded file is not corrupted, verify the ISO image. After you verify the ISO image, or if you choose to skip verification, go to the final step.

To verify the integrity of the ISO image, use the associated `fciv` checksum file and the Microsoft File Checksum Integrity Verifier (FCIV) executable file, if you have already downloaded these files to your system. Otherwise, use the MD5 checksum hash function.

Using fciv

Open a command prompt window. From the directory containing the ISO, executable, and verification files, type a command similar to the following to verify the ISO image:

fciv -v -xml everRun_install-7.*x.x.x-xxx*.xml

If the command succeeds (that is, it returns the message `All files verified successfully`), go to the next step. If the command fails, repeat the download.

Using MD5

Open a command prompt window as an administrator, and enter the following:

```
CertUtil -hashfile path_to_file MD5
```

The `CertUtil` command displays a message indicating whether or not it completed successfully. If the command succeeds, continue with the next step. If the command fails, repeat the download.

Final Step

When the verification is complete, or if you have skipped the verification, do one of the following:

- Burn the ISO image to a DVD using a commonly available application, and then perform the next step in "Installing everRun Software" on page 37.

- If you are not burning the ISO image to a DVD, perform the next step in "Installing everRun Software" on page 37.

Configuring Settings in the Firmware Setup Utility

Before you install the software, you must modify settings in the firmware (BIOS) setup utility. You can also modify some optional, though recommended, settings.

After you modify the settings, save them and perform the next step in the installation procedure (either "Installing Software on the First PM" on page 40 or "Installing Software on the Second PM" on page 46).

> **Note**: This topic provides general information about settings in the firmware setup utility. Because settings--including setting names--vary, refer to the manufacturer's documentation for specific instructions for modifying any setting.

Required Settings

The following settings are required.

First Boot Device	Controls which device boots the operating system. Set the first boot device to the Optical Drive.
Virtualization Technology	Allows the processor to use virtualization technology. Set this to Enabled.
Execute-Disable Bit Capability	Allows the processor to classify areas in memory where application code can or cannot execute. Set this to Enabled to help prevent malicious code attacks.

Recommended Settings

The following settings are optional but recommended.

AC Power Recovery	Determines whether the server automatically powers on and boots after a power cycle. The recommended setting is ON.
F1/F2 Prompt on Error **(Dell systems only)**	Terminates booting if an error is detected during the process. Set this to Disable, as the everRun system may be able to provide more information once the server is running.

Installing everRun Software

Follow these instructions to install everRun software for the first time on a system.

> ⬣ **Warning**: Installing everRun software erases all hard drives.

To install everRun software for the first time:

1. On a remote management computer, obtain the everRun software. See "Obtaining everRun Software" on page 34

2. On your everRun system:

   a. Provide keyboard and console access to your physical machines (PMs), if you have not already done so (see "Site and System Preparation" on page 33).

   b. Connect Ethernet cables for the networks you are configuring. See "Connecting Ethernet Cables" on page 37.

3. Perform the installation on the first PM. See "Installing Software on the First PM" on page 40.

4. After you have finished installing the software on the first PM, perform the installation on the second PM. See "Installing Software on the Second PM" on page 46.

The installation is now complete. To perform the required post-installation configuration steps, see "Post-Installation Tasks" on page 48.

Connecting Ethernet Cables

Before you install everRun software for the first time, you need to connect Ethernet cables for your networks.

> ⓘ **Note**: To install additional networks <u>after</u> you have completed the software installation, see
>
> "Connecting Additional Networks" on page 50.

On each physical machine (PM), assign one network port as the private network (priv0), and assign another network port as the management network (ibiz0). Although you can use any network port (1 Gb or 10 Gb) for the private network or management network, Stratus recommends that you use embedded network ports. Use CAT5E, CAT6, or CAT7 network cables for all network ports.

The following illustration shows an example of an everRun network configuration.
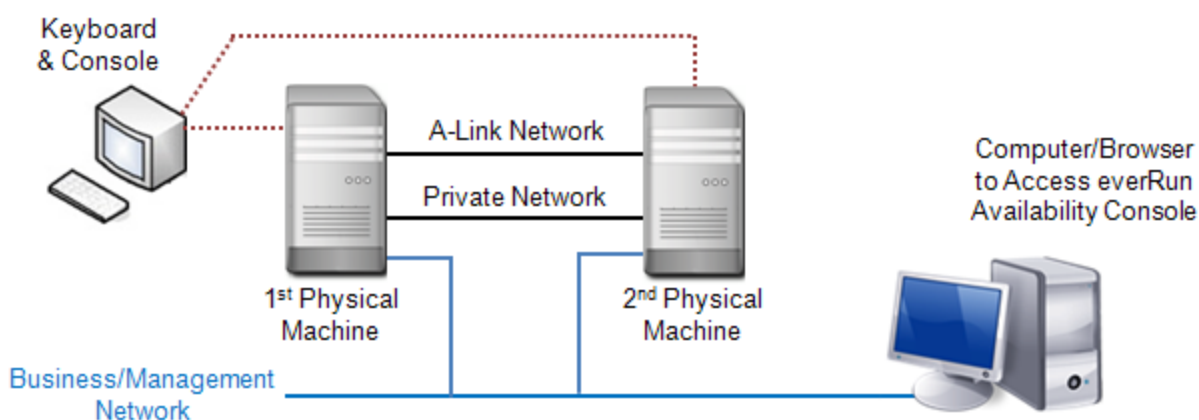
Stratus recommends the following Ethernet cable configurations:

- For the private network, directly connect an Ethernet cable from any embedded port on the first PM to the same embedded port on the second PM. If you plan to use the private network as an A-Link, connect the cable to 10 Gb ports, if installed.

- For the management network, connect Ethernet cables from an embedded port on each PM to a network that is accessible from the remote management computer.

> ⓘ **Note**: Take note of the ports you used for the private and management networks. The installation software will prompt you for this information.

- For each A-Link network, connect an Ethernet cable from a port on the first PM to a port on the second PM, either directly or through a network switch.

> **Note**: Stratus recommends that you configure at least <u>one</u> A-Link network in addition to the private network. See "A-Link and Private Network Requirements" on page 27

- For each business network, connect an Ethernet cable from a port on the first PM to a port on the second PM, through a network switch.

After you connect these Ethernet cables, perform the next step in "Installing everRun Software" on page 37.

Related Topics

"A-Link and Private Network Requirements" on page 27

"Business and Management Network Requirements" on page 26

"everRun Availability Console Requirements" on page 30

"Connecting Additional Networks" on page 50

Installation Options

When you begin the installation, the Welcome screen appears with the following list of installation-related options. Use the up and down arrow keys to select an option based on the task you want to perform. You can then press the **Tab** key to modify the command line. Finally, press the **Enter** key to boot the installation program from the DVD.

Task	Option	Description
Perform initial installation on the first PM	`Install everRun, Create a new system`	Deletes all partitions on all connected disks, installs the CentOS and everRun software, and creates a new system. See "Installing Software on the First PM" on page 40.
Perform initial installation on the second PM;	`Replace PM, Join system: Initialize`	Deletes all partitions on all connected disks, installs CentOS and everRun software, and attempts to connect to an existing system. See "Installing Software on the Second PM" on page 46 and "Replacing Physical Machines, Motherboards, NICs, or RAID Controllers"

Task	Option	Description
replace a PM	`data`	on page 242.
Recover failing PM	`Recover PM, Join system: Preserving data`	Preserves all data but re-creates the `/boot` and `root` file systems, reinstalls the CentOS and everRun software, and attempts to connect to an existing system. See "Recovering a Failed Physical Machine" on page 116.
Boot to rescue mode	`Rescue the installed system`	Boots to rescue mode.
Boot from local drive	`Boot from local drive`	Boots from a local drive.
Perform memory test	`Memory test`	Performs a memory test.

Installing Software on the First PM

This topic describes how to perform an initial installation of the everRun software on node0, which is the first physical machine (PM).

> ℹ **Note**: To perform an installation by mounting the ISO image, you must first configure your system's remote-management feature (for example, iDRAC on a Dell system). See the manufacturer's documentation for instructions.

To perform an initial installation of the software on the first PM:

1. Power on the first PM, if it is not already powered on, and either insert the installation software DVD or mount the ISO image.

2. As the system powers on, enter the firmware (BIOS) setup utility, and configure the required and optional settings described in "Configuring Settings in the Firmware Setup Utility" on page 36.

> **Note**: If you need to configure your keyboard for a different language, see "Mapping Your Keyboard" on page 44.

3. When the installation software loads, the **Welcome** screen appears and displays the options shown in "Installation Options" on page 39. From this screen, you can choose to perform the initial installation in one of two ways:

   - **Method 1**: Installing via the user interface. This method is best for users who are not familiar with the installation process and who prefer to follow a GUI-based procedure with prompts.

   - **Method 2**: Installing via the command line. This method allows you to automate the installation. You can enter the IP settings in advance, and the installation proceeds without human intervention. This method is especially useful when you need to reinstall the software and you know all of the IP settings in advance.

Method 1: Installing via the User Interface

   i. Use the arrow keys to select **Install everRun, Create a new system**, and press **Enter**.

   > **Note**: No action from you is required until the screen described in the next step appears.

   iii. The **Select interface for private Physical Machine connection** screen sets the physical interface to use for the private network. To use the first embedded port, use the arrow keys to select **em1** (if it is not already selected), and then press **F12** to save your selection and go to the next screen.

> **Notes**:
>
>   1. If you are not sure of which port to use, use the arrow keys to select one of the ports, and click the **Identify** button. The LED on the selected port will then flash for 30 seconds, allowing you to identify it. Since the LED may also flash due to activity on that network, Stratus recommends that you leave the cable disconnected during the identification process. Reconnect the cable immediately after identification is complete.
>
>   2. If the system contains no embedded ports, select the first option interface instead.

iv. The **Select interface for managing the system (ibiz0)** screen sets the physical interface to use for the management network. To use the second embedded port, use the arrow keys to select **em2** (if it is not already selected), and then press **F12** to save your selection and go to the next screen.

> **Note**: If the system contains only one embedded port, select the first option interface. If the system contains no embedded ports, select the second option interface.

v. The **Select the method to configure ibiz0** screen sets the management network for node0 as either a dynamic or static IP configuration. Typically, you set this as a static IP configuration, so use the arrow keys to select **Manual configuration (Static Address)** and press **F12** to save your selection and go to the next screen. However, to set this as a dynamic IP configuration, select **Automatic configuration via DHCP** and press **F12** to save your selection and go to the next screen.

vi. If you selected **Manual configuration(Static Address)** in the previous step, the **Configure em2** screen appears. Enter the following information and press **F12**.

   - IPv4 address

   - Netmask

   - Default gateway address

   - Domain name server address

See your network administrator for this information.

> **Note**: If you enter invalid information, the screen redisplays until you enter valid information.

Method 2: Installing via the Command Line

   i. Press the **Tab** key to bring up the command line.

   ii. Set the value for the private network (**priv0**).

- To use the first embedded interface, type:

  priv0=em1

- To automatically select the default interface, type:

  priv0=auto

- To use the interface with a MAC address, type one of the following:

  priv0=AA-BB-CC-DD-EE-FF or **priv0=AABBCCDDEEFF**

   iii. Set the value for the management network (**ibiz0**).

- To use the second embedded interface with BOOTP:

  ibiz0=em2:bootp

- To automatically choose an interface and use DHCP:

  ibiz0=auto:dhcp

- To use a static configuration with IP address 10.83.51.116, netmask 255.255.0.0 , default gateway 10.83.0.1, and two DNS servers 134.111.24.254 and 134.111.18.14:

  ibiz0=em2:10.83.51.116/16:10.83.0.1:134.111.24.254,134.111.18.14

- To query the system administrator to configure the default interface:

  ibiz0=auto

   iv. After entering the desired values on the command line, press **Enter**.

4. At this point, the installation continues without additional prompts. No action from you is required until the first PM reboots. After it reboots:

a. Remove the DVD, or unmount the ISO image.

b. If you configured the IP address <u>dynamically</u>, record its IP address as described in "Record-
   ing the Management IP Address" on page 45

5. Perform the next step in "Installing everRun Software" on page 37.

Mapping Your Keyboard

You can configure your keyboard for a different layout either during or after installation.

Supported keyboard layouts include:

Layout	Language
de	German
de-latin1	German (latin1)
de-latin1-nodeadkey	German (latin1 without dead keys)
dvorak	Dvorak
jp106	Japanese
sg	Swiss German
sg-latin1	Swiss German (latin1)
uk	United Kingdom
us	U.S. English
us-acentos	U.S. International

To configure your keyboard layout during installation:

1. As the first PM boots, select **Install**, **Recover**, or **Replace** from the boot menu.

2. Press **Tab** to access the kernel command line.

3. Specify the `keymap` kernel argument to configure the correct keyboard layout. The following

example configures the Japanese keyboard layout:

```
keymap=jp106
```

4. Press **Enter** to continue the boot sequence.

5. Repeat the preceding steps on the second PM.

To configure your keyboard layout after installation:

1. Log in to the first PM as `root`.

2. From the command line, use the `system-config-keyboard` command to select a key mapping that matches the console keyboard. You do not need to reboot. The following example configures the German keyboard layout:

```
system-config-keyboard de
```

3. Press **Enter**.

4. Repeat the preceding steps on the second PM.

Related Topics

Recording the Management IP Address

Your network administrator may require the management IP address for each physical machine (PM) in order to configure the system IP address. Perform this procedure if you configured the management network to have a dynamic IP address. (Your network administrator already has this information if the management network has a static IP address.)

1. When the PM completes its installation and reboots, a login screen similar to the following appears:

```
everRun

    IPv4 address 10.84.52.117

    IPv6 address 3d00:feed:face:1083:225:64ff:fe8d:1b6e

    IPv6 address fe80: :225:64ff:fe8d:1b6e
```

2. Record the IPv4 address shown on the screen.

3. Give this IP address to your network administrator.

Return to to see the next step.

Installing Software on the Second PM

This topic describes how to perform an initial installation of the everRun software on node1, which is the second physical machine (PM).

> **Note**: To perform an installation by mounting the ISO image, you must first configure your system's remote-management feature (for example, iDRAC on a Dell system). See the manufacturer's documentation for instructions.

To perform an initial installation of the software on the second PM:

1. Power on the second PM, if it is not already powered on, and either insert the installation software DVD or mount the ISO image.

2. As the system powers on, enter the firmware (BIOS) setup utility, and configure the required and optional settings described in .

3. When the installation software loads, the **Welcome** screen appears and displays the options shown in . From this screen, you can perform the initial installation using either the user interface or the command line. This topic describes how to perform the installation with the user interface. To perform the installation with the command line, see "Method 2: Installing via the Command Line" in .

4. Use the arrow keys to select **Replace PM, Join system: Initialize data**, and press **Enter**.

> **Note**: No action from you is required until the screen described in the next step appears.

5. The **Select interface for private Physical Machine connection** screen sets the physical interface to use for the private network. To use the first embedded port, use the arrow keys to select **em1** (if it is not already selected), and then press **F12** to save your selection and go to the next screen.

> **Notes**:
>
>   1. If you are not sure of which port to use, use the arrow keys to select one of the ports, and click the **Identify** button. The LED on the selected port will then flash for 30 seconds, allowing you to identify it. Since the LED may also flash due to activity on that network, Stratus recommends that you leave the cable disconnected during the identification process. Reconnect the cable immediately after identification is complete.
>
>   2. If the system contains no embedded ports, select the first option interface instead.

6. The **Select interface for managing the system (ibiz0)** screen sets the physical interface to use for the management network. To use the second embedded port, use the arrow keys to select **em2** (if it is not already selected), and then press **F12** to save your selection and go to the next screen.

> **Note**: If the system contains only one embedded port, select the first option interface. If the system contains no embedded ports, select the second option interface.

7. The **Select the method to configure ibiz0** screen sets the management network for node1 as either a dynamic or static IP configuration. Typically, you set this as a static IP configuration, so use the arrow keys to select **Manual configuration (Static Address)** and press **F12** to save your selection and go to the next screen. However, to set this as a dynamic IP configuration, select **Automatic configuration via DHCP** and press **F12** to save your selection and go to the next screen.

8. If you selected **Manual configuration(Static Address)** in the previous step, the **Configure em2** screen appears. Enter the following information and press **F12**.

   - IPv4 address

   - Netmask

   - Default gateway address

   - Domain name server address

   See your network administrator for this information.

> **Note**: If you enter invalid information, the screen redisplays until you enter valid information.

9. At this point, the installation continues without additional prompts. No action from you is required until the second PM reboots. After it reboots:

   a. Remove the DVD, or unmount the ISO image.

   b. If you configured the IP address <u>dynamically</u>, record its IP address as described in "Recording the Management IP Address" on page 45

10. Perform the next step in "Installing everRun Software" on page 37.

Post-Installation Tasks

After completing system installation, you must complete several post-installation tasks, including:

- "Obtaining System IP Information" on page 48

- "Logging on to the everRun Availability Console for the First Time" on page 49

- Configuring Required System Preferences:

  - "Configuring Date and Time" on page 70

  - "Configuring Remote Support Settings" on page 80

  - "Configuring Quorum Servers" on page 68

  - "Specifying Owner Information" on page 62

- "Configuring Active Directory" on page 71

- "Managing Local User Accounts" on page 98

- "Resolving Outstanding Alerts on the Dashboard" on page 56

- "Connecting Additional Networks" on page 50

Obtaining System IP Information

After you install the everRun software, you need the node0 IP address to log on to the everRun Availability Console for the first time (see "Logging on to the everRun Availability Console for the First Time" on page 49). To complete the initial logon procedure, you also need system IP information, which the network administrator should provide. Give the network administrator the node0 and node1 IP addresses (see

"Recording the Management IP Address" on page 45), which helps the network administrator determine system IP information. The system IP address must be a static IP address. Do not use a dynamic IP address.

Related Topics

"Software Installation" on page 32

"Post-Installation Tasks" on page 48

Logging on to the everRun Availability Console for the First Time

After completing the installation of the everRun software, log on to the everRun Availability Console to accept the end-user license agreement (EULA) and to manage the everRun system.

> **Prerequisites**: To log on to the everRun Availability Console the first time, you need the following:
>
> - The node0 (primary) IP address—You note this address during installation. See "Recording the Management IP Address" on page 45.
>
> - The system IP address—The network administrator provides this information. See "Obtaining System IP Information" on page 48.
>
> - The license **.KEY** file that you received from Stratus when you purchased the everRun software—You must upload this file to the everRun Availability Console to complete the initial logon. Locate the file before you begin the initial logon.

To log on to the everRun Availability Console **for the first time**

1. From the remote management computer, type the IP address of node0 (primary) into a browser address bar.

   The logon page of the everRun Availability Console appears.

2. Enter **admin** for the **Username** and **admin** for **Password**, and then click **LOGIN**

   The Stratus everRun EULA appears.

3. Read the EULA and then, if appropriate, click **Accept** to accept it.

   The **INITIAL CONFIGURATION** page appears.

4. Under **NOTIFICATIONS**, the box for **Enable Support Notifications** is checked, by default. If you

do not want the everRun system to send health and status notifications to your authorized Stratus service representative, uncheck the box. You can change this setting later (see "Configuring Remote Support Settings" on page 80).

5. Under **SYSTEM IP**, for IP Address, enter the address you obtained from your network administrator.

   After you have entered the network information, click **Continue**.

6. The **Portal Restart Required** window appears. After waiting a minute (as indicated in the window), click **OK** to refresh the console and to continue.

7. The **LICENSE INFORMATION** window appears. Under **Upload License Key**, click **Browse** and navigate to the license **.KEY** file that you received from Stratus. Select the license file and click **Upload**.

The initial logon is complete, and the everRun Availability Console appears. Bookmark or otherwise make note of the system IP address for use when logging in to the console in the future.

For security, change the default user login name and password for the **admin** account on the **Users & Groups** page. See "Managing Local User Accounts" on page 98.

Related Topics

"Software Installation" on page 32

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

Connecting Additional Networks

The everRun installation software connects networks for all network ports that are physically connected at the time of the installation. This topic describes how to connect additional networks after the software installation is complete.

To connect a network:

1. Connect an Ethernet cable from a port on the first PM to a port on the second PM. Ideally, use the same NIC slot and port number in each PM. Connect the cable either directly (for an A-Link network) or through a network switch (for an A-Link or business network).

2. In the everRun Availability Console, go to the **Networks** page.

    a. The new shared-network name should appear within a minute or so. If not, either your cable is on different subnets or the NIC ports between the PMs are incompatible (for example, if one end is connected to a 10 Gb port and the other end is connected to a 1 Gb port).

    b. Click the **Config** button to select whether the network should be an A-Link or a business network. If the connection is direct, the network must be an A-Link. Otherwise, the network can be either an A-Link or a business network.

    c. Verify that the new shared network displays a green check.

3. Connect additional network cables to both PMs, one pair at a time. Ideally, use the same NIC slot and port number in each PM.

Related Topics

"Connecting Ethernet Cables" on page 37

"A-Link and Private Network Requirements" on page 27

"Business and Management Network Requirements" on page 26

"General Network Requirements and Configurations" on page 24

3

Chapter 3: Using the everRun Availability Console

The everRun Availability Console is a browser-based interface that provides management and monitoring of an everRun system from a remote management computer. For an overview of the console, see "The everRun Availability Console" on page 54.

For information on pages within the everRun Availability Console, see the following topics:

The everRun Availability Console

The everRun Availability Console is a browser-based interface that provides management and monitoring of an everRun system from a remote management computer. You can perform many administrative operations from the console because it provides access to the system as a whole as well as to physical machines (PMs), virtual machines (VMs), and other resources.

For information on the requirements of the remote management computer that runs the everRun Availability Console, see "everRun Availability Console Requirements" on page 30.

Using the everRun Availability Console, you can perform a variety of administrative functions:

- Read system alerts from the Dashboard. See "The Dashboard Page" on page 55.

- View VM, CPU, memory, and storage statistics, and reboot or shutdown the system from the System page. See "The System Page" on page 57.

- Set preferences for the system, diagnostics, notifications (e-Alerts and SNMP configuration), and remote support (notification and access). System preferences include owner information and configuration values for IP address, quorum services, date and time, etc. See "The Preferences Page" on page 59.

- View alerts and audit logs. See "The Alerts Page" on page 83 and "The Audits Page" on page 84.

- Monitor, manage, and maintain resources:

  - PM status, storage, disks, network, and sensors: see "The Physical Machines Page" on page 84.

  - VM status and management tasks such as creating, importing/restoring, managing, and maintaining VMs: see "The Virtual Machines Page" on page 88.

  - Snapshot status and management tasks such as exporting and deleting snapshots: see "The Snapshots Page" on page 93.

  - Volumes, including their state, size, and storage group: see "The Volumes Page" on page 93.

  - Storage groups, including name, size used, size, and number of volumes: see "The Storage Group Page" on page 95.

  - Networks, including state, physical interface, speed, MAC address, and network bandwidth: see "The Networks Page" on page 95.

- Virtual CDs, including their state, name, size, and storage group: see "The Virtual CDs Page" on page 97.

● Monitor and manage upgrade kits, and users and groups in the LIBRARY. See "The Upgrade Kits Page" on page 97 and "The Users & Groups Page" on page 98.

Related Topics

Logging on to the everRun Availability Console

Log on to the everRun Availability Console to manage the everRun system. Using the console, you can manage the system, including its physical machines (PMs), virtual machines (VMs), storage, and networks. You can also generate statistics and view alerts and logs.

To log on to the everRun Availability Console

1. Type the everRun system's IP address or name that is a fully qualified domain name (FQDN) into a browser address bar:

   http://*IP_address*

   OR

   http://*FQDN_name*

   IP_address is the everRun system's static IP address, supplied during installation.

   FQDN_name is the FQDN corresponding to that IP address.

2. When the logon page appears, enter your **Username** and **Password**.

3. Click **LOGIN**.

Related Topics

The Dashboard Page

The **Dashboard** page displays a summary of outstanding alerts on the everRun system. To open this page, click **Dashboard** in the left-hand navigation panel.

To display additional information about outstanding alerts, click an alert symbol (for example, 🛈) in the everRun system diagram or click an entry in the list of alerts below the system diagram. The alert information includes:

- The component associated with the issue (for example, the everRun system, physical machine (PM), or virtual machine (VM)).

- A description of the activity or task that requires attention.

- The reason the issue should be resolved, if available.

Resolve active alerts as soon as possible (see "Resolving Outstanding Alerts on the Dashboard" on page 56).

Understanding the everRun System Diagram

The system diagram on the **Dashboard** page displays a graphical representation of system status. A star symbol indicates the primary PM. Alert symbols, if present, represent informational or critical alerts that require attention. Click an alert symbol to display information about the alert.

Related Topics

"The Physical Machines Page" on page 84

"The System Page" on page 57

"The Virtual Machines Page" on page 88

Resolving Outstanding Alerts on the Dashboard

After completing system installation, resolve any outstanding alerts that appear on the Dashboard page.

To resolve outstanding alerts

On the everRun Availability Console Dashboard page, view any alerts listed in the lower portion of the page. Your options are as follows:

- Resolve the alert.

  For instance, if you see the message **Support Notification service should be enabled to ensure the best possible support from Stratus**, then enable support notification service.

- Click **Ignore** (beneath the **Action** column) to ignore the alert and remove it from the list. Minor alerts

can be ignored rather than resolved. Clicking **Ignore** hides the alert.

To restore the ignored alert to the list, click **Ignored**, above the alerts list, and then **Restore**, under the **Action** column.

Related Topics

The System Page

The **System** page displays information about the everRun system, and enables you to reboot or shut down the system. The page also displays resource allocations for the everRun system. To open this page, click **System** in the left-hand navigation panel.

You can use the **System** page for administrative tasks including:

-

-

You perform many other administrative tasks on the everRun system using the everRun Availability Console. For information, see .

To manage everRun system resources, see .

Related Topics

Rebooting the System

Reboot the everRun system using the everRun Availability Console to safely restart both PMs without incurring downtime for the VMs.

> **Caution**: Rebooting the everRun system by any method other than following (for example, rebooting from the PMs individually) may result in data loss.

> **Note**: You can reboot the system only if both PMs are running, healthy, and not in maintenance mode.

> **Prerequisite**: Confirm that both PMs are running before rebooting.

To reboot the everRun system

1. Select **System** in the left-hand navigation panel.

2. Click the **Reboot** button. A message appears, asking you to confirm the reboot. Click **Yes** to continue.

   Rebooting can take up to 15 minutes. You can observe the process in the **Dashboard** and the masthead of the everRun Availability Console. The system's PMs sequentially enter and then exit maintenance mode (for information on maintenance mode, see "Maintenance Mode" on page 111).

3. Verify that the PMs restart and that all VMs continue running as expected.

After you initiate a reboot, a message in the masthead shows the status of the reboot. If necessary, you can cancel the reboot by clicking **Cancel Reboot** in the masthead.

> **Caution**: If you cancel a reboot, the system is left in its current state and you need to manually restore it to a healthy state.

Related Topics

"The everRun Availability Console" on page 54

"The System Page" on page 57

"Using the everRun Availability Console" on page 53

Shutting Down the System

Use the everRun Availability Console to shut down the everRun system. Doing so performs an orderly shutdown by first shutting down the virtual machines (VMs) and then the physical machines (PMs). Use only this method to shutdown the everRun system. Make sure both PMs are running before shutting down.

> **Cautions**:
>
> 1. Shutting down the everRun system takes the VMs offline, so shutdown the system only during a planned maintenance period.
>
> 2. Shutting down the everRun system by any other method (for example, removing power from both PMs individually) may result in data loss.

To shut down the everRun system

1. Confirm that both PMs are running so that the disks can synchronize between nodes.

2. Select **System** in the left-hand navigation panel.

3. Click the **Shutdown** button. A warning appears: *It will shut down the entire system and stop one or more VMs!* Click **Yes** to shutdown or **No** to cancel the shutdown. After clicking **Yes**, a second warning appears, asking you to confirm the shutdown. Click **Yes** (again) to shutdown or **No** to cancel the shutdown.

You can observe some of the shutdown process in the **Dashboard** and the masthead of the everRun Availability Console as the system's PMs sequentially enter maintenance mode (for information on maintenance mode, see "Maintenance Mode" on page 111). When the system shuts down completely, though, the everRun Availability Console is unavailable and the masthead displays **Lost Communication**.

After the system shuts down, you lose the connection to the console. If the everRun system cannot shutdown completely, a VM may not be shutting down properly. Do one of the following to shut down the VM:

- Use the VM console or a remote desktop application to log on to the VM. Use operating system commands to shut down the VM.

- Log on to the everRun Availability Console. Click **Virtual Machines** in the left-hand navigation panel, select the VM, and then click **Power Off**.

Related Topics

"Managing the Operation of a Virtual Machine" on page 198

"The everRun Availability Console" on page 54

"The System Page" on page 57

"Using the everRun Availability Console" on page 53

The Preferences Page

The **Preferences** page enables you to configure everRun system settings. To open this page, click **Preferences** in the left-hand navigation panel.

The following table lists and describes the preferences.

Preference	Description
System	

Preference	Description
Owner Information	Allows you to specify and then view the name and contact information for an everRun system administrator. This information is also provided in response to Simple Network Management Protocol (SNMP) requests. See "Specifying Owner Information" on page 62.
Product License	Allows you to view and manage the everRun product license. See "Managing the everRun Product License" on page 62.
IP Configuration	Allows you to view and specify the Internet Protocol (IP) address and network settings for the everRun system. See "Configuring IP Settings" on page 66.
Quorum Servers	Allows you to view existing and new Quorum servers. Quorum servers provide data integrity assurances and automatic restart capabilities for specific failures in the everRun environment. See "Quorum Servers" on page 14 and "Configuring Quorum Servers" on page 68.
Date & Time	Allows you to view the system time, specify values for Network Time Protocol (NTP) (recommended), or to manually set the time and date on the everRun system. See "Configuring Date and Time" on page 70.
System Resources	Allows you to specify the number of virtual CPUs (VCPUs) and the amount of memory reserved for the everRun software. See "Configuring System Resources" on page 71.
Active Directory	Allows you to enable (and disable) Active Directory. When enabled, Active Directory allows you to authorize existing users or groups from the Active Directory domain to log on to the everRun Availability Console and manage the everRun system. See "Configuring Active Directory" on page 71.
Import/Export Settings	Allows you to enable compression and encryption for import/export procedures in the everRun Availability Console. See "Configuring the Virtual Machine Import Option" on page 73.

Preference	Description
Diagnostics	
Diagnostics	Allows you to generate a diagnostic file for your authorized Stratus service representative. See "Managing Diagnostic Files" on page 74.
Notification	
e-Alerts	Allows you to enable email alerts (e-Alerts) for system administrators. See "Configuring e-Alerts" on page 76.
SNMP Configuration	Allows you to enable Simple Network Management Protocol (SNMP) requests and traps for remote system monitoring. See "Configuring SNMP Settings" on page 78.
Remote Support	
Support Configuration	Allows you to configure remote access and notifications. Remote access enables your authorized Stratus service representative to log on to the system remotely for troubleshooting. When enabled, the everRun system can send notifications to your authorized Stratus service representative about problems with the system. See "Configuring Remote Support Settings" on page 80.
Proxy Configuration	Allows you to configure proxy settings for the everRun system if your organization requires a proxy server to access the Internet and you have a service agreement with Stratus or another authorized everRun service representative. everRun software uses proxy server information for support notification messaging and remote support access features. See "Configuring Internet Proxy Settings" on page 82.
One View	Allows you to enter the IP address or host name of the One View server. See "Configuring One View Settings" on page 83.

Related Topics

Specifying Owner Information

Specify the name and contact information for an administrator or owner of the everRun system to make this information available for support purposes.

This contact information is available in the everRun Availability Console and provided in response to Simple Network Management Protocol (SNMP) requests.

To specify system owner information

1. Click **Preferences** in the left-hand pane.

2. On the **Preferences** page, click **Owner Information**.

3. Supply information in the **Full Name**, **Phone Number**, **Email**, and **Site Address** fields.

4. Click **Save**.

Related Topics

Managing the everRun Product License

Manage the product license for the everRun system 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 an everRun system, 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 Support** page at http://www.stratus.com/services-support/customer-support.

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.

Follow the procedure below that is appropriate for your needs.

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. Click **Preferences** in the left-hand navigation panel, to open the **Preference** page.

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 **Choose File** (in Google Chrome) or **Browse** (in Firefox or Internet Explorer), 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 with a connection 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 **Choose File** 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
  Computer B and the everRun system are **not** connected to the Internet.

On Computer B

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.

On Computer A

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 is automatically downloaded.

4. Copy the license .key file to the USB flash drive.

5. Remove the USB flash drive.

On Computer B

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 **Choose File**, 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**.

   Click the **License Check and Activation** bar.

3. 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	*month dd*, 20*yy*, *time*

If a license activation fails, the License Activation Server (or ALAS) returns a numeric error code. The following drop-down menu lists the error codes.

To view the 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

"The everRun Availability Console" on page 54

"The Preferences Page" on page 59

"Using the everRun Availability Console" on page 53

Configuring IP Settings

Configure Internet Protocol (IP) settings for the everRun system to set or modify the IP address of the system and nodes as well as values for applicable settings such as network mask, gateway address, and Domain Name System (DNS) server.

During installation and post-installation of everRun software, you configure three IP addresses: one for the everRun system and one for each node. You can change the IP addresses and other IP settings after installation using the appropriate procedure below. You must specify a static IPv4 address for the everRun system.

> **Warnings**:
>
> 1. Do not change the IP configuration settings, especially on systems with running VMs, without the advice and knowledge of your network administrator. Doing so could make the system and all its VMs inaccessible.
>
> 2. You must use the everRun Availability Console to change IP addresses. Do not use Linux tools.

> **Notes**:
>
> 1. The procedure you use to configure IP settings depends on whether the everRun system stays on the same subnet or moves to a new subnet. See the "everRun Release 7.2.2.0 Release Notes" on page 248 for instructions on how to move the system to a new subnet. Follow the appropriate procedure for your needs.
>
> 2. Changing IP settings for a new subnet typically includes changing the node's physical network connections (for example, disconnecting and then re-attaching network cables if moving the PMs). Before you disconnect cables from nodes, you must shut down the nodes.
>
> 3. In a single-node system, the **IP Configuration** page displays settings for only one node.

To change the system and/or node IP settings with the system on same subnet

The everRun system and all virtual machines (VMs) continue to run throughout this procedure; however, the everRun Availability Console briefly loses its connection to the system if you change the system IP address. You can access the everRun Availability Console at the new system IP address within 1-2 minutes. (You can change node IP addresses on each node, individually, but the console connection is not lost.)

1. Click **Preferences** in the left-hand navigation panel, to open the **Preference** page.

2. Click **IP Configuration**.

3. In the **Static System IP** box, type the static system IP address that you obtained from your net-work administrator.

4. Click the **Static** button and type valid, unique values for **Primary DNS** and **Secondary DNS**.

5. Verify that the displayed **NetMask** value is correct.

6. For **Node0** and **Node1**, enter appropriate values for **IP Address** and **Gateway IP**.

7. Click **Save** to save the values (or click **Reset** to restore previous values).

   If you have changed the system IP address, the **Portal Restart Required** dialog box appears. Wait about a minute and then click **OK**. This redirects the browser to the new system IP address.

Related Topics

"Software Installation" on page 32

"Obtaining System IP Information" on page 48

"Logging on to the everRun Availability Console for the First Time" on page 49

"The Preferences Page" on page 59

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

Configuring Quorum Servers

When you log on to the everRun system for the first time, configure quorum servers.

> **Prerequisite**: Before you configure quorum servers, read "Quorum Servers" on page 14 and "Quorum Servers Considerations" on page 31.

> **Note**: For a VM to recognize quorum server configuration changes, you must reboot the VM by shutting it down and then restarting it. See "Shutting Down a Virtual Machine" on page 198 and "Starting a Virtual Machine" on page 198.

To configure quorum servers

1. Click **Preferences** in the left-hand navigation panel, to open the **Preferences** page.

2. Click **Quorum Servers**.

3. Click **Add Quorum Server**.

4. In the **Add Preferred Quorum Server** dialog box, enter the following values (if a preferred quorum server already exists, the **Add Alternate Quorum Server** dialog box appears):

   - **DNS or IP Address**—Type the fully-qualified **DNS** host name or **IP address** for the pre-ferred quorum server.

   - **Port** (the default value is 4557)—Type the port number if it is different from the default.

   Click **Save** to save the values.

5. Repeat steps 4 and 5 to configure a second, alternate quorum server. Stratus recommends con-figuring two quorum servers.

6. To enable quorum service, select the **Enabled** check box and click **Save**.

To remove a quorum server

> **Caution**: If you remove the preferred quorum server, the alternate quorum server becomes the preferred quorum server. If no alternate quorum server exists, removing the preferred quorum server automatically disables quorum service.

1. Navigate to the **Preferences** page of the everRun Availability Console.

2. Click **Quorum Servers**.

3. Locate the entry for the quorum server you want to remove.

4. In the right-most column, click **Remove**.

> **Note**: If a VM is using the quorum server that you are removing, you must reboot the VM so that it no longer recognizes the quorum server, which allows the removal process to finish.

Related Topics

"The everRun Availability Console" on page 54

"The Preferences Page" on page 59

"Using the everRun Availability Console" on page 53

Configuring Date and Time

When you log on to the everRun system for the first time, configure the date and time to enable the Network Time Protocol (NTP) service. Using the NTP service automatically sets the system clock and ensures that it does not drift from the actual time.

> **Caution**: When you change the date and time settings, the primary physical machine (PMs) may reboot and the secondary PM may shutdown if system time has drifted from actual time. All virtual machines (VMs) are stopped and business processing is interrupted until the reboot is complete.

> **Note**: The clock swaps between time zones whenever VMs migrate or restart. To ensure that the time zone in VMs does not change:
>
> - Set the time zone in all VMs to correspond to the time zone configured for the everRun system.
>
> - Configure all VMs to use the same NTP servers as those configured for the everRun system.

To configure date and time settings

1. Click **Preferences** in the left-hand navigation panel, to open the **Preferences** page.

2. On the **Preferences** page, click **Date & Time**.

3. In the **Date & Time** display, the default setting for **Configure Time Zone** is **America, New York**. Select a time zone appropriate for your location, if necessary.

4. Select one of the following for **Configure Date and Time**:

   - **Automatically (Recommended)** enables NTP service. Type NTP server addresses in the text area, one per line. Specifying multiple NTP servers provides redundancy.

   - **Manually** allows you to manually enter settings.

     > **Note**: If you configure time manually, the everRun system's time may drift from actual time.

5. Click **Save** (or click **Reset** to restore the previously-saved values).

If the system requires a reboot because of time drift, a message appears in the everRun Availability Console masthead telling you that the system will reboot. In this case, the primary physical machine (PM) reboots and the secondary PM shuts down. While the primary PM reboots, you lose your connection to the everRun Availability Console. When the reboot is complete, the PM re-establishes a connection to the console and you receive an alert telling you to restart the secondary PM.

Related Topics

"The everRun Availability Console" on page 54

"The Preferences Page" on page 59

"Using the everRun Availability Console" on page 53

Configuring System Resources

Configure system resources to specify how the everRun system manages virtual CPUs (vCPUs) and memory. Use default values; change a value only if your service representative instructs you to.

To configure system resources for the everRun system

1. In the everRun Availability Console, click **Preferences** in the left-hand navigation panel, to open the **Preference** page.

2. Click **System Resources**.

3. Modify the settings only if your service representative instructs you to:

    - **System VCPUs**, which sets the number of VCPUs reserved for the everRun software. Values are **2** (the default) and **4**.

    - **System Memory**, which sets the amount of memory reserved for the everRun software. Values are **1024 MB**, **2048 MB** (the default), and **4096 MB**.

4. Scroll to the bottom of the **System Resources** section and click **Save** (or click **Reset** to restore the previously-saved values).

Related Topics

"The everRun Availability Console" on page 54

"The Preferences Page" on page 59

"Using the everRun Availability Console" on page 53

Configuring Active Directory

Configure Active Directory for the everRun system to authorize existing users or groups from an Active Directory domain to log on to the everRun Availability Console with their Active Directory credentials.

After you add the everRun *system to an Active Directory domain*, you can assign administrative privileges to domain users using the **Grant Access** wizard, which you start from the **Users & Groups** page (see "The Users & Groups Page" on page 98).

To add the everRun **system to an Active Directory domain**

1. Click **Preferences** in the left-hand navigation panel, to open the **Preferences** page.

2. Click **Active Directory**.

3. Click **Enable Active Directory**.

4. Next to **Active Directory Domain**, type the name of the domain to use.

5. Click **Add System to Active Directory**.

6. Type the **Username** and **Password** of an Active Directory Administrator in order to add this everRun system to the domain.

7. Click **Add**.

8. Assign administrative privileges to domain users on the **Users & Groups** page, as described in "Managing Domain User Accounts" on page 100.

To remove an everRun system from an Active Directory domain

1. In the everRun Availability Console, click **Preferences** in the left panel, to open the **Preferences** page.

2. Click **Active Directory**.

3. Click **Remove System from Active Directory**.

4. Type a **Username** and **Password** that provides you with administrative privileges within the domain.

5. Click **Remove**.

To disable domain authentication

1. In the everRun Availability Console, click **Preferences** in the left panel, to open the **Preferences** page.

2. Click **Active Directory**.

3. Click **Disable Active Directory**.

> **Note**: Disabling Active Directory prevents the use of domain authentication for author-
> izing administrators of the everRun system; however, it does not remove the system
> from the domain. To restore the use of domain authentication, click **Enable Active Dir-
> ectory**. You do not need to retype the name of the controller or restore domain users on
> the **Users & Groups** page.

Related Topics

Configuring the Virtual Machine Import Option

Configure the virtual machine import option to enable encryption that improves security for the everRun
system.

To configure an import option for the everRun system

1. In the everRun Availability Console, click **Preferences** in the left panel, to open the **Preferences**
    page.

2. Click **Import**.

3. Select a setting, as appropriate for your system:

    -   **Import** , which enables encrypted data communication using a secure version of the Hyper
        Text Transfer Protocol (HTTPS). Encryption can be time consuming, so enable it only when
        security is a concern. By default, this setting is disabled.

4. Click **Save** (or click **Reset** to restore the previously-saved values).

Related Topics

Managing Diagnostic Files

Diagnostic files provide a snapshot of an everRun system's log files and configuration information. This information enables your authorized Stratus service representative to resolve an issue with the system.

When you create diagnostic files, you can choose to include log files from the last 24 hours, the previous seven days, or all available log information and statistics for the everRun system. You can also choose to include only performance statistics.

For additional information, see:

- "Creating a Diagnostic File" on page 74

- "Deleting a Diagnostic File" on page 76

- "Uploading a Diagnostic File to Customer Support" on page 75

Related Topics

Creating a Diagnostic File

Diagnostic files provide a snapshot of an everRun system's log files and configuration information. You create a diagnostic file to help your authorized Stratus service representative resolve issues with the system.

> **Note**: everRun software allocates a fixed amount of storage space for diagnostic files. If sufficient space is not available when you create a diagnostic file, the system will delete previously created files.

To create diagnostic files

1. Click **Preferences** in the left-hand navigation panel, to open the **Preference** page.

2. In the **Diagnostics** category, click **Diagnostics**.

3. Select an option from the pulldown menu:

- **Minimal** diagnostics contain log information for the last 24 hours.

- **Medium** diagnostics contain log information for the last 7 days.

- **Full** diagnostics contain all available log information with statistics for the everRun system.

4. Click **Generate Diagnostic File**.

5. Upload the file to your authorized Stratus service representative, as described in "Uploading a Diagnostic File to Customer Support" on page 75.

Related Topics

"The everRun Availability Console" on page 54

"The Preferences Page" on page 59

"Using the everRun Availability Console" on page 53

Uploading a Diagnostic File to Customer Support

Upload a diagnostic file to the Stratus everRun Customer Support web site to help resolve an issue with the everRun system. (To create a diagnostic file, see "Creating a Diagnostic File" on page 74.)

To upload a diagnostic file to Customer Support

1. Click **Preferences** in the left-hand navigation panel, to open the **Preference** page.

2. In the **Diagnostics** category, click **Diagnostics**

3. Do one of the following:

   - If the everRun system has Internet connectivity, upload the diagnostic file directly to the Stratus everRun Customer Support web site by clicking **Upload**. An **Alert** appears with the message that the diagnostic was uploaded successfully, if the upload succeeds.

   - If the everRun system does not have Internet connectivity or if the **Upload** fails, you can manually upload the diagnostic file to the **Stratus Diagnostic File Upload** web page. First, click **Download** on the everRun Availability Console to download the diagnostic file as a .zip file to your local computer. Transfer the diagnostic zip file to a computer with Internet connectivity . Open a web browser, and in its address bar, enter http://diags.stratus.com/DiagUpload.html. On the **Stratus Diagnostic File Upload** page, click **Choose File**, select the zip file on the computer, and click **Submit**.

If you need help with this procedure, call everRun Customer Support at the phone number listed on the **everRun Support** page at http://www.stratus.com/services-support/customer-support.

After you are certain that you no longer need the file (for example, Customer Support confirms that the file uploaded correctly), you can optionally delete it from the everRun system, as described in "Deleting a Diagnostic File" on page 76.

Related Topics

"The everRun Availability Console" on page 54

"The Preferences Page" on page 59

"Using the everRun Availability Console" on page 53

Deleting a Diagnostic File

Delete a diagnostic file from the everRun system after you have uploaded it to your authorized Stratus service representative.

To delete a diagnostic file

1. Click **Preferences** in the left-hand navigation panel, to open the **Preference** page.

2. In the **Diagnostics** category, click **Diagnostics**.

3. Select the diagnostic file and click **Delete**.

Related Topics

"The everRun Availability Console" on page 54

"The Preferences Page" on page 59

"Using the everRun Availability Console" on page 53

Configuring e-Alerts

Configure email alerts (e-Alerts) to enable the everRun system to send email to system administrators whenever the system detects an event requiring administrator attention.

To enable e-Alerts

1. Click **Preferences** in the left-hand navigation panel, to open the **Preference** page.

2. Under **Notification**, click **e-Alerts**.

3. Click the **Enable e-Alerts** box. Boxes for specifying or selecting the following settings appear:

- **SMTP Server** (required)—Enter the name of the Simple Mail Transfer Protocol (SMTP) server that your company uses to send email.

- **e-Alerts Language**—Select a language from the pull-down menu.

- **Sender's Email Address**—Enable e-Alert delivery by specifying a valid sender's email address in either of the following cases:

  - You have not specified a DNS server on the everRun system **and** your SMTP server is not configured to accept domain literals (`From` addresses in the form `noreply@IP_address`).

  - You want the e-Alert to provide a different sender's email address (for example, noreply@company.com).

  Any email address that the SMTP server accepts is sufficient.

- **Connect using TLS**—Click this box if the SMTP server requires Transport Layer Security (TLS).

- **Enable Authentication**—Click this box if the SMTP server requires authentication to send email and type the **Username** and **Password** for the SMTP account.

- **List of Recipients** (required)—Enter email addresses for all e-Alert recipients.

4. Click **Save** (or click **Reset** to restore the previously-saved values).

> **Note**: When you enable or update the e-Alert configuration, generate a test alert to confirm that you receive the alerts.

To generate a test alert

Click **Generate Test Alert**. The everRun software generates a test alert and sends a sample email with the subject "Test Alert" to all email recipients; SNMP sends traps to recipients of SNMP traps, if configured (see "Configuring SNMP Settings" on page 78); and Support Configuration sends a notification to your authorized Stratus service representative, if configured (see "Configuring Remote Support Settings" on page 80). Watch the Alerts History log (see "The Alerts Page" on page 83) for delivery status.

You can also test e-Alerts by putting the secondary physical machine into maintenance mode (see "Maintenance Mode" on page 111), and then removing it from maintenance mode. Verify that you receive e-Alerts for both maintenance mode events.

Related Topics

Configuring SNMP Settings

Configure Simple Network Management Protocol (SNMP) settings for your everRun system to allow SNMP management applications to remotely monitor your systems. (SNMP information pertains only to systems and not individual PMs.) You can enable SNMP requests and SNMP traps:

- SNMP request—a request sent to the everRun system to retrieve the values of objects listed in the Management Information Bases (MIBs) supported by the everRun software. These MIBs include an everRun-specific MIB that is a collection of objects describing the everRun system. You can download a copy of the MIB file from the **Drivers and Tools** section of the **Downloads** page at http://www.stratus.com/go/support/everrun.

- SNMP trap—a message initiated by one of the nodes in the everRun system after an event such as an alert that is then sent to an identified list of recipients, typically a network management station (NMS).

To specify the desired security parameters, you must edit the standard `/etc/snmp/snmpd.conf` file on both nodes. For example, to allow SNMP requests by any user using the default `public` community, comment out or delete the following lines from that file on each node:

```
com2sec notConfigUser default public

group notConfigGroup v1 notConfigUser
group notConfigGroup v2c notConfigUser

view systemview included .1.3.6.1.2.1.1
view systemview included .1.3.6.1.2.1.25.1.1

access notConfigGroup "" any noauth exact systemview none none
```

After you save the edited files, you must restart the `snmpd` process on each node by entering the following command:

```
service snmpd restart
```

Follow the appropriate procedure to enable SNMP requests or traps.

To enable SNMP requests

1. Click **Preferences** in the left-hand navigation panel, to open the **Preference** page.

2. Under **Notification**, click **SNMP Configuration**.

3. Activate the check box next to **Enable SNMP Requests**.

4. Click **Save**. (Or click **Reset** to restore the previously-saved values.)

To enable SNMP traps

> **Note**: When you enable or modify the SNMP trap settings, generate a test alert to confirm that traps are received.

1. Click **Preferences** in the left-hand navigation panel, to open the **Preference** page.

2. Under **Notification**, click **SNMP Configuration**.

3. Activate the check box next to **Enable SNMP Traps**.

4. Type the name of the SNMP **Community**, or keep the default (**public**).

5. Next to **List of Recipients for SNMP traps**, type the IP address or host name for each recipient, one per line.

6. Click **Save**. (Or click **Reset** to restore the previously saved values.)

7. Configure your organization's firewall to allow SNMP operations, which enables SNMP management systems to receive alerts from and send traps to the everRun system. To do so, configure your organization's firewall to open the SNMP port:

   Message Type: SNMP
   Protocol: SNMP
   Port: 161 (Get/Walk) 162 (Traps)

8. Generate a test alert by clicking **Generate Test Alert**.

   The everRun software generates a test alert and SNMP sends traps to recipients of SNMP traps; e-Alerts send a sample email with the subject "Test Alert" to all email recipients of e-Alerts, if configured (see "Configuring e-Alerts" on page 76); and Support Configuration sends a notification to your authorized Stratus service representative, if configured (see "Configuring Remote Support Settings" on page 80). Watch the Alerts History log (see "The Alerts Page" on page 83) for delivery status.

Related Topics

Configuring Remote Support Settings

When you log on to the everRun system for the first time, configure support configuration settings that enable the everRun system to send support notifications (alerts) to your authorized Stratus service representative when an event requires attention.

To configure support configuration settings

> **Note**: When you enable or modify support configuration settings, generate a test alert to confirm that your authorized Stratus service representative can receive system health messages from your system.

1. Click **Preferences** in the left-hand navigation panel, to open the **Preferences** page.

2. Under **Remote Support**, click **Support Configuration**.

3. Modify the settings, as appropriate for your system:

   - **Enable Remote Support Access** allows your authorized Stratus service representative to remotely connect to the everRun system for troubleshooting purposes. Note that you can enable and then disable this setting, as needed.

   - **Enable Notifications** allows the everRun system to send health and status notifications to your authorized Stratus service representative.

     ○ **Enable Support Notifications** sends an alert for any event that requires attention.

     ○ **Enable Periodic Reporting** sends a daily summary of system information to help improve product and service quality.

4. Click **Save** (or click **Reset** to restore the previously saved values).

5. Configure your organization's firewall to allow support messages.

   To configure your firewall to allow support messages

Use the following information to configure your organization's firewall to allow com-munication with your authorized Stratus service representative:

Message Type: Call-Home and Licensing

Protocol: TCP

Port: 443

Stratus support server address: *.stratus.com

Message Type: Support Diagnostics

Protocol: TCP

Port: 443

Stratus support server address: *.stratus.com

Message Type: Dial-In

Protocol: TCP

Port: 443, Default proxy port: 3128 (You can change the default proxy port number.)

Stratus support server address: *.ecacsupport.com

Message Type: e-Alert

Protocol: SMTP

Port: 25

(For additional information on TCP and UDP ports, access the Knowledge Base to search for the article *TCP and UDP ports used by everRun 7* (KB-2123). See "Accessing Know-ledge Base Articles" on page 411.)

To enable SNMP management systems to receive alerts and send traps to the everRun sys-tem, configure the firewall for the following:

Message Type: SNMP

Protocol: SNMP

Port: 161(Get/Walk) 162(Traps)

6. Generate a test alert.

To generate a test alert

Click **Generate Test Alert**. The everRun software generates a test alert and Support Con-figuration sends a notification to your authorized Stratus service representative; e-Alerts send a sample email with the subject "Test Alert" to all email recipients of e-Alerts, if

configured (see "Configuring e-Alerts" on page 76); and SNMP sends traps to recipients of SNMP traps, if configured (see "Configuring SNMP Settings" on page 78). Watch the Alerts History log (see "The Alerts Page" on page 83) for delivery status. A subsequent alert will be generated if the support notification fails.

Related Topics

"The everRun Availability Console" on page 54

"The Preferences Page" on page 59

"Using the everRun Availability Console" on page 53

Configuring Internet Proxy Settings

Configure proxy settings for the everRun system if your organization requires a proxy server to access the Internet and you have a service agreement with Stratus or another authorized everRun service representative.

A proxy server provides a secure bridge between the everRun system and the Internet. everRun software uses proxy server information for only outbound HTTP traffic related to support notification messaging and remote support access features.

To configure Internet proxy settings

1. Click **Preferences** in the left-hand navigation panel, to open the **Preferences** page.

2. Under **Remote Support**, click **Proxy Configuration**.

3. To enable proxy service, click the **Enable Proxy** box.

4. In the **Proxy Server** box, type the fully-qualified proxy server host name or IP address.

5. In the **Port Number** box, type the port number if it is different from the default number (3128).

6. If the proxy server requires authentication, click the **Enable Authentication** box and type the **Username** and **Password**.

7. Click **Save** (or click **Reset** to restore the previously-saved values).

Related Topics

"The everRun Availability Console" on page 54

"The Preferences Page" on page 59

"Using the everRun Availability Console" on page 53

Configuring One View Settings

You must register your everRun system with the One View Console before you can enable One View connections on your system. The procedure consists of "Part A: Registering a Platform" on page 83 and "Part B: Adding a Platform to the One View Console" on page 83.

Part A: Registering a Platform

1. In the everRun Availability Console, obtain the **Asset ID** of the system you want to add to the 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 a 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 necessary, see your system administrator to obtain the IP address.)

4. Click **Save**.

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

Related Topics

"Obtaining System IP Information" on page 48

The Alerts Page

The **Alerts** page displays messages about events on the everRun system.

To open the **Alerts** page, click **Alerts** in the left-hand navigation panel of the everRun Availability Console. (To view a log of user activity on the everRun system, see "The Audits Page" on page 84.)

To view alert information, scroll through the alerts, which are, by default, listed in reverse chronological order. Click an alert to display information about the problem and resolution (if available), and whether **Support Notifications**, an **e-Alert**, or an **SNMP Trap** was sent for this alert.

> **Note**: Support notification alerts, e-Alerts, and SNMP traps are generated only when you enable them in the everRun Availability Console console. For information see:
>
> - "Configuring Remote Support Settings" on page 80
> - "Configuring e-Alerts" on page 76
> - "Configuring SNMP Settings" on page 78

Related Topics

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

The Audits Page

The **Audits** page displays a log of user activity in the everRun Availability Console. To open this page, click **Audits** in the left-hand navigation panel. (To display information about events on the everRun system, see "The Alerts Page" on page 83.)

To view log information, scroll through the log entries, which are, by default, listed in reverse chronological order. The information includes:

- **Time**—The date and time of the action.
- **Username**—The name of the user that initiated the action.
- **Originating Host**—The IP address of the host on which the everRun Availability Console was running.
- **Action**—The action performed in the everRun Availability Console.

Related Topics

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

The Physical Machines Page

The **Physical Machines** page enables you to manage the physical machines (PMs) in the everRun system. (PMs are also referred to as nodes.) To open this page, click **Physical Machines** in the left-hand navigation panel.

State, **Activity**, **Name**, **Model**, and **# of VMs** columns appear immediately under the **PHYSICAL MACHINES** heading and masthead. To manage a specific PM, click **node0 (primary)** or **node1** under **Name**. To interpret PM states and activities, see "Physical Machine States and Activities" on page 87.

The bottom pane displays action buttons for and details about the selected node:

- Action buttons: Various action buttons appear, depending upon the state of the selected node. The **Work On** button ( ) appears initially. To perform most maintenance tasks, click **Work On**, which places a node into maintenance mode (for information, see "Maintenance Mode" on page 111). To learn about additional PM actions available in maintenance mode, see "Physical Machine Actions" on page 85 or the help topic for the task you want to complete.

- Detailed information: To view detailed information or statistics about the selected node, click one of the following tabs:

  - **Summary** (in the initial display), which displays the model,overall state, activity, and configuration (memory and logical disks) for the selected node.

  - **Description**, which displays a window where you can enter information about the node.

  - **Storage**, which displays the state, logical ID, size, controller an current action (if any) of storage.

  - **Network**, which displays the state, name, speed, and MAC address of networks.

  - **Sensors**, which displays the name and current state of sensors.

  - **Virtual Machines**, which displays the state, activity, and name of virtual machines.

  - **Details**, which displays the manufacturer, model, and serial number of the selected node.

Related Topics

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

Physical Machine Actions

When you select a physical machine (PM), some or all of the following action buttons appear, depending on the PM's state and activity.

> **Caution**: Use the **Physical Machines** page of the everRun Availability Console when you perform maintenance on a PM. Do not use controls on the computer (for example, the power switch on the PC) because the everRun Availability Console protects the everRun system from most actions that are potentially disruptive.

Commands	Description
Work On	Enters a PM into maintenance mode. VMs running on this PM migrate to the other PM, if it is in service. (Otherwise, you are asked to re-confirm the request and then shut down VMs.) When VMs are migrated or shut down, the PM displays **running (in Maintenance)**. See "Maintenance Mode" on page 111.
The following actions are available after clicking the **Work On** button, when the PM has entered maintenance mode.	
Finalize	Removes a PM from the state **running (in Maintenance)**. See "Maintenance Mode" on page 111.
Shutdown	Shuts down a PM. The PM transitions to **off (in Maintenance)**. See "Shutting Down a Physical Machine" on page 113.
Reboot	Reboots the PM. The PM transitions to **preparing for reboot (in Maintenance)**. See "Rebooting a Physical Machine" on page 113.
Remove	Causes the everRun software to delete the PM from the everRun system's database, so that you can replace the PM or one of its components. See "Replacing Physical Machines, Motherboards, NICs, or RAID Controllers" on page 242.
The following actions may be available when a PM has failed or when everRun software has removed a PM from service and powered it off, due to an excessive failure rate.	

Commands	Description
Reset Device	Resets the mean time between failures (MTBF) counter for a PM so it can be brought back into service. See "Resetting MTBF for a Failed Physical Machine" on page 118.
Recover	Recovers a failed PM. In some cases, the everRun Availability Console displays the state of a failed PM as **Unreachable (Syncing/Evacuating…)**. See "Recovering a Failed Physical Machine" on page 116.

Related Topics

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

"The Physical Machines Page" on page 84

Physical Machine States and Activities

The following states and activities apply to physical machines (PMs). Only certain actions are enabled during each state and activity.

State	Activity	Available Commands	Description
✔	▶ Running	**Work On**	PM is running normally.
↻	▶ Evacuating	**Finalize**	Virtual machines are migrating from this PM to its partner.
⚠	▶ Running	**Work On**	PM is predicted to fail.
✖	▶ Running	**Work On**	PM failed.
✖	✖ Powered Off	**Work On** **Reset Device**	everRun has powered off the PM because of an excessive failure rate. The PM is left powered off until **Reset Device** is clicked. See "Resetting MTBF for a Failed Physical

			Machine" on page 118.
🧰	❌ Booting	**Finalize**	PM is booting.
🧰	⌛ Rebooting	**Finalize**	PM is rebooting.
🧰	▶ Running	**Finalize** **Shutdown** **Reboot** **Recover** **Replace**	PM is running in Maintenance Mode. See "Maintenance Mode" on page 111.

Related Topics

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

"The Physical Machines Page" on page 84

The Virtual Machines Page

Use the **Virtual Machines** page to manage the virtual machines (VMs) running on your everRun system. To open this page, click **Virtual Machines** in the left-hand navigation panel of the everRun Availability Console.

To manage a specific VM, click the name of a VM in the top pane of the **Virtual Machines** page. The bottom pane displays controls and information for managing the VM.

To interpret VM status as displayed on the **Virtual Machines** page, see "Virtual Machine States and Activities" on page 91. To learn more about the controls on this page, see "Virtual Machine Actions" on page 89 or the help topic for a specific task.

You can use the **Virtual Machines** page for administrative tasks including:

- Creating, importing, or restoring VMs, as described in "Creating and Migrating Virtual Machines" on page 127

- "Opening a Virtual Machine Console Session" on page 200

- "Reprovisioning Virtual Machine Resources" on page 204

- Creating VM snapshots that can be restored or exported, as described in "Creating a Snapshot" on page 220

- Controlling the power state of a VM, as described in:

  - "Starting a Virtual Machine" on page 198

  - "Shutting Down a Virtual Machine" on page 198

  - "Powering Off a Virtual Machine" on page 200

- "Removing a Virtual Machine" on page 202 or "Renaming a Virtual Machine" on page 202

- Performing advanced tasks or troubleshooting, as summarized in "Advanced Topics (Virtual Machines)" on page 231

- Viewing information about a VM, including its name, description, and resources in the tabs of the bottom pane

Related Topics

"Managing Virtual Machines" on page 121

"Using the everRun Availability Console" on page 53

Virtual Machine Actions

When you select a virtual machine (VM), the following action buttons can appear, depending on the VM's state and activity.

Action	Description
Create	Launches the Create VM Wizard. See "Creating a New Virtual Machine" on page 128.
Import/Restore	Imports a VM from a set of OVF and VHD files. See "Creating and Migrating Virtual Machines" on page 127. The import wizard allows you to *import* a VM to create a new instance of the VM or *restore* a VM to create an identical VM with the same hardware IDs provided in the OVF and VHD files. Open Virtual Machine Format (OVF) is an open standard for packaging and dis-

Action	Description
	tributing physical or virtual machine data. The OVF format contains meta-data information about the VM. A Virtual Hard Disk (VHD) is a file that contains the virtual disk information.
The following actions are available for use if the VM is running.	
Console	Opens a console for the selected VM. See "Opening a Virtual Machine Console Session" on page 200.
Snapshot	Creates a VM snapshot that you can export to OVF and VHD files. See "Managing Snapshots" on page 219.
Shutdown	Shuts down the selected VM. See "Shutting Down a Virtual Machine" on page 198.
Power Off	Immediately stops processing in the selected VM and destroys its memory state. Use this only as a last resort, when the VM cannot be successfully shutdown. See "Powering Off a Virtual Machine" on page 200.
The following actions are available if the VM is shut down or stopped.	
Config	Launches the **Reprovision Virtual Machine** wizard. The VM must be shut down prior to launching this wizard. See "Reprovisioning Virtual Machine Resources" on page 204
Restore	Recovers an existing VM on your everRun system by overwriting the VM from a previous backup copy of OVF and VHD files. See "Replacing a Virtual Machine from an OVF File" on page 185.
Snapshot	Creates a VM snapshot that you can export to OVF and VHD files. See "Managing Snapshots" on page 219.

Action	Description
Start	Boots the selected VM. See "Starting a Virtual Machine" on page 198.
Boot From CD	Boots a VM from the selected virtual CD. See "Booting from a Virtual CD" on page 218.

The following action is available if the everRun software has removed the VM from service and powered it off because an excessive failure rate.

Reset Device	Resets the mean time between failures (MTBF) counter for a VM so it can be brought back into service. See "Resetting MTBF for a Failed Virtual Machine" on page 234. When a VM crashes, the everRun software automatically restarts it, unless it has fallen below its MTBF threshold. If the VM is below the MTBF threshold, the ever-Run software leaves it in the crashed state. If necessary, you can click **Reset Device** to restart the VM and reset the MTBF counter.

Related Topics

"Managing the Operation of a Virtual Machine" on page 198

"The Virtual Machines Page" on page 88

"Using the everRun Availability Console" on page 53

Virtual Machine States and Activities

A virtual machine (VM) can have the following states and activities, during which only certain actions are enabled.

State	Activity	Enabled Actions	Description
↻	⊙ installing		everRun software is installing the boot volume for a new VM.

State	Activity	Enabled Actions	Description
	■ stopped	Start Config Snapshot Boot From CD Remove	VM has been shut down or powered off.
↻	▷ booting	Console Power Off	VM is starting.
✔	▷ running	Console Snapshot Shutdown Power Off	VM is operating normally on redundant physical machines
⚠	✖ running	Console Shutdown Power Off	VM is operating normally, but is not running on fully redundant resources.
↻	✖ stopping	Power Off Remove	VM is being shut down in response to the **Shutdown** action, or shut down because the remaining physical machine is transitioning into maintenance mode.
↻	✖ crashed		VM crashed and is restarting. If enabled, e-Alerts and support notification messages are sent.
🧰	✖ crashed		VM crashed too many times and exceeded its MTBF threshold. The VM is left in a crashed state until **Reset Device** is clicked. See "Resetting

State	Activity	Enabled Actions	Description
			MTBF for a Failed Virtual Machine" on page 234.

Related Topics

"Managing the Operation of a Virtual Machine" on page 198

"The Virtual Machines Page" on page 88

"Using the everRun Availability Console" on page 53

The Snapshots Page

Use the **Snapshots** page to manage virtual machine (VM) snapshots, which represent an image of a VM at a particular point in time. You can use a snapshot to restore a VM on the everRun system or you can export a snapshot for use in a new VM. To open this page, click **Snapshots** in the left-hand navigation panel of the everRun Availability Console.

To create a snapshot (on the **Virtual Machines** page), see "Creating a Snapshot" on page 220.

To manage an existing snapshot, click the name of a snapshot in the top pane of the **Snapshots** page. The bottom pane displays a description of the snapshot.

You can use the **Snapshots** page for administrative tasks including:

- "Exporting a Snapshot" on page 224

- "Removing a Snapshot" on page 230

- Adding a description for each volume, in the **Description** text box

Related Topics

"Managing Snapshots" on page 219

"Using the everRun Availability Console" on page 53

The Volumes Page

The **Volumes** page displays information about volumes that are attached to virtual machines (VMs) in the everRun system. To open this page, click **Volumes** in the left-hand navigation panel of the everRun Availability Console. The **Volumes** page displays the following columns with information about volumes in the top pane:

- **State**

- **Name**

- **Size**

- **Storage Group**

- **Used By**, which displays one of the following:

  - A link to a VM when a VM is using the volume.

  - A link to the physical machine (PM) page (**node0** or **node1**) when the volume is **root** or **swap**.

  - *System* for a shared volume (**shared.fs**) .

  - *None* when the volume is not a system volume and is not used by a VM.

Click the name of a volume in the top pane of the **Volumes** page to display additional information about the volume in the bottom pane. You can perform some administrative tasks on volumes from the bottom pane, including:

- Add a description for each volume in the **Description** text box.

- Rename a volume (see "Renaming a Volume on the everRun System" on page 213).

- View information about the volume container, including the volumes and snapshots it contains, on the **Container** tab.

- Expand a volume container on the **Container** tab (see "Expanding a Volume Container on the ever-Run System" on page 213).

- Remove a volume by clicking **Remove**. Note, though, that the **Remove** button does not appear when a VM is using a volume.

You perform other volume management tasks from the virtual machines page. These tasks include:

- "Attaching a Volume to a Virtual Machine" on page 208

- "Creating a Volume in a Virtual Machine" on page 207

- "Detaching a Volume from a Virtual Machine" on page 210

- "Removing a Volume from a Virtual Machine" on page 211

Related Topics

"The everRun Availability Console" on page 54

The Storage Group Page

The **Storage Group** page displays information about disks in the everRun system. To open this page, click **Storage Group** in the left-hand navigation panel of the everRun Availability Console.

You can use the **Storage Group** page to view information about the storage group, including the name, size used, size, and number of volumes. You can also add a description for the storage group using the **Description** tab in the bottom pane.

To view information about the storage group, click the storage group name in the top pane of the **Storage Group** page. The bottom pane displays additional information about the storage group.

> **Caution**: The everRun software automatically synchronizes disks on the secondary physical machine (PM) with disks on the primary PM, when, for example, you change disks or when you upgrade or restore PMs. During synchronization of volumes between PMs, a busy icon (🔄) appears on **System** and **Volumes** in the left-hand navigation panel. Do not remove either PM during synchronization.

For more information about storage and everRun systems, see .

Related Topics

The Networks Page

The **Networks** page displays information about the shared networks attached to the everRun system. To open this page, click **Networks** in the left-hand navigation panel of the everRun Availability Console.

You can use the **Networks** page to view information about a specific network, including its state, type, number of Virtual Machines, and speed. You can also add a description for the network using the **Description** tab in the bottom pane.

To manage a specific network or simply view information about it, click the network name under **Shared Network** in the top pane of the **Networks** page, or click a port in the network connectivity diagram on the **Summary** tab. The bottom pane displays additional information about nodes on the network. Columns in the **Summary** tab display information about the node's state, physical interface, speed, MAC address,

slot, and port. To display or hide columns, move the cursor to the right of a column heading, click the down-arrow that appears, and then click **Columns**, selecting or de-selecting the columns that you want to show or hide.

You can use the **Networks** page for administrative tasks, including:

- "Connecting Additional Networks" on page 50.

- "Fixing a Network Connection" on page 96.

- Viewing a list of the physical adapters that compose the network, on the **Summary** tab.

- Adding a description for a network, on the **Description** tab.

- Viewing a list of virtual machines that use the network, on the **Virtual Machines** tab.

For additional information on networks, see the following topic:

- "General Network Requirements and Configurations" on page 24

- "SplitSite Network Requirements" on page 28

> **Note**: The **Networks** page displays only networks that have physical connectivity on both physical machines. If a network that you expect to see does not appear, check that both network connections are cabled correctly and that their LINK is active.

Related Topics

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

Fixing a Network Connection

The everRun system software monitors and analyzes network connections. If it determines that an existing network connection is not optimal (for example if a 1Gb port is connected to a 10Gb port), and it cannot automatically reconfigure the network, it issues an alert stating that cabled network ports could not be paired automatically. In this case, perform the following procedure to reconfigure network connections so that they are optimal.

To reconfigure non-optimal network connections

1. Place the secondary PM into maintenance mode. See "Maintenance Mode" on page 111 for details.

2. Open the **Networks** page in the everRun Availability Console.

3. Click the **Fix Network** button. As the everRun system software reconfigures the networks, the connection topology displayed in the diagram on the **Networks** page will change to show the new optimal configuration.

4. Remove the secondary PM from maintenance mode. See "Maintenance Mode" on page 111 for details.

Related Topics

"The Networks Page" on page 95

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

The Virtual CDs Page

Use the **Virtual CDs** page to create virtual CDs (VCDs). Use VCDs to make software installation or recovery media available to the virtual machines on your everRun system. To open this page, click **Virtual CDs** in the left-hand navigation panel of the everRun Availability Console.

To manage a specific VCD, click the name of a VCD in the top pane of the **Virtual CDs** page. The bottom pane displays a description of the VCD.

You can use the **Virtual CDs** page for administrative tasks including:

- "Creating a Virtual CD" on page 216

- "Removing a Virtual CD" on page 219

- "Renaming a Virtual CD" on page 218

- Adding a description for each volume, in the **Description** text box

To complete other VCD management tasks, see "Managing Virtual CDs" on page 215.

Related Topics

"Using the everRun Availability Console" on page 53

The Upgrade Kits Page

The **everRun Upgrade Kits** page enables you to upload and manage software kits that you use to upgrade your system to newer versions of everRun. To open the **Upgrade Kits** page, click **Upgrade Kits** in the left-hand navigation panel in the everRun Availability Console.

For information about upgrading your everRun software, see "Upgrading everRun Software" on page 103.

Related Topics

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

The Users & Groups Page

Use the **Users & Groups** page to add, modify, or remove user accounts on, or to grant access for Active Directory users to manage your everRun system. To open this page, click **Users & Groups** in the left-hand navigation panel of the everRun Availability Console.

To manage local user accounts

To add a new user, click **Add** in the right side of the top pane. To modify an existing user, click the name of a user account and click **Edit** or **Remove**. For more information, see "Managing Local User Accounts" on page 98.

To manage domain user accounts

For information about enabling the Active Directory service on your everRun system, see "Configuring Active Directory" on page 71. To grant or remove access for domain users to manage the everRun system, see "Managing Domain User Accounts" on page 100.

> **Note**: If you are logged on as administrator to a system that has Active Directory users or groups configured, the **Grant Access** button will appear in the upper-right corner of the **Users & Groups** page. Clicking the **Grant Access** button launches the Grant Access wizard. The "Managing Domain User Accounts" on page 100 topic discusses using the Grant Access wizard.

To sort and locate user accounts

If you have a large number of accounts, you can click a column heading to sort the accounts by parameter. You can sort accounts by **Type**, **Username**, **Real Name**, **Email** address, or **Role**.

Related Topics

"Configuring Active Directory" on page 71

"Managing Domain User Accounts" on page 100

"Managing Local User Accounts" on page 98

Managing Local User Accounts

You add, edit, or remove users, specify passwords, and assign user roles to local-user accounts on the **User & Groups** page in the everRun Availability Console. (To grant or deny access for established user accounts in an Active Directory domain, see .)

Local user accounts reside on the everRun system itself, as opposed to a central domain server. You can find local accounts on the **Users & Groups** page by looking for entries labeled **Local User** in the **Type** column.

User roles are:

- **Administrator**: full system administrator privileges

- **Platform Manager**: system administrator privileges except for adding, removing, and modifying users

- **Read-only**: ability to view but not to change system configuration or to install system software

To add a user account

1. In the left-hand navigation panel, select **Users & Groups**.

2. In the top pane, click **Add**.

3. In the **Role** drop-down window, select **Administrator**, **Platform Manager**, or **Read-only**.

4. Provide values for the **User Name**, **Password** (and **Confirm Password**), **Email Address**, and **Real Name** fields. User names and passwords may be from 1 to 64 characters long, and must include no white space.

5. Click **Save**.

To edit a user account

1. In the left-hand navigation panel, select **Users & Groups**.

2. Under **USERS & GROUPS**, select the account you want to edit.

3. In the top pane, click **Edit**.

4. To change a user's role, in the **Role** drop-down window, select **Administrator**, **Platform Manager**, or **Read-only**.

5. Click **Save**.

To remove a user account

1. Under **USERS & GROUPS**, select the account to remove.

2. Click **Remove**.

3. Click **Yes** in the Confirm dialog box.

> **Note**: You cannot delete the default **admin** account, although you should change its name and password by editing the account.

Related Topics

"Configuring Active Directory" on page 71

"Managing Domain User Accounts" on page 100

"The Users & Groups Page" on page 98

Managing Domain User Accounts

You can grant Active Directory (AD) domain user accounts access to the everRun Availability Console. Domain user accounts are managed on a central AD domain server, as opposed to the local everRun system.

After granting access to domain accounts, you can use the Grant Access wizard (on the Users & Groups page) to view, manage, and sort the AD accounts that have access to the system.

> **Prerequisites**: You must add the everRun system to an Active Directory domain before you can manage domain accounts. (See "Configuring Active Directory" on page 71.) If Active Directory is not configured, or if the user who is logged onto the interface does not have administrator privileges, the Grant Access button does not appear on the Users & Groups page.

To grant access to a domain user account

1. In the left-hand navigation panel, select the **Users & Groups** page.

2. In the upper right-hand corner, click **Grant Access**.

3. In the **everRun - Grant Access Wizard**, specify the search range in the **Search for** menu.

4. Type the name or group for which to search. Partial names and text are allowed.

5. Click **Search**.

6. Click the green plus sign (**+**) next to the users or groups you want to add as everRun Availability Console Global Users or Groups of the system.

7. Use the drop-down menus in the Role column to assign a role to the user or group to which you have just granted access. You can assign the following roles:

   - **Administrator** –Enables performance of the full range of system administration activities.

   - **Platform Admin**–Enables Administrator privileges, except for managing user accounts.

   - **Read Only**–Enables read access but no management functions.

   - **Everyone** –Enables only limited read access to certain information.

8. Click **Finish**. The new domain users are displayed in the Grant Access wizard.

To remove access for a domain user account

1. In the left-hand navigation panel, select the **Users & Groups** page.

2. In the upper right-hand corner, click **Grant Access**.

3. In the **everRun - Grant Access Wizard**, click the check box next to users or groups you want to remove.

4. Click **Deny Access**, then click **Finish**.

Related Topic

"Configuring Active Directory" on page 71

4

Chapter 4: Upgrading everRun Software

This topic describes how to upload an upgrade kit and then use the kit to upgrade everRun software.

> **Prerequisite**: All PMs and VMs in must be in good health before performing an upgrade of ever-Run software. Before starting an upgrade, examine the everRun Availability Console to verify that there are no alerts indicating PM or VM problems.

To upgrade the system using an upgrade kit

1. In the everRun Availability Console, click **Upgrade Kits** in the left-hand navigation panel.

2. On the **Upgrade Kits** page, click the **Add a Kit** button beneath the masthead, which opens the **everRun - Kit Upload Wizard**.

3. In the **everRun - Kit Upload Wizard** dialog box, click **Choose File** (in Google Chrome) or **Browse** (in Firefox or Internet Explorer), and then browse to select a .kit file.

4. After you have selected a .kit file, click **Upload** or **Finish** (they perform the same function).The message **Uploading file (DO NOT CLOSE WIZARD)** appears while the file is uploading. The upload may require up to two minutes for a file stored locally, to ten or more minutes for a file stored over a network.

5. After the upload is complete, the message **Kit uploaded successfully.** Click **OK** to close the wizard.

   The **Upgrade Kits** page now lists the state and version number of the upgrade kit. The **Upgrade** and **Delete** buttons also appear with the **Add a Kit** button.

6. If more than one upgrade kit is loaded, select the one to use.

7. Click **Upgrade** to upgrade the everRun system.

   First, the everRun software upgrades and reboots the secondary PM. The newly upgraded

   PM becomes primary, and then the everRun software upgrades and reboots the other PM.

> **Note**: The everRun software upgrade also upgrades the AVCLI software on the everRun system; however, if you have installed AVCLI on a remote management computer, you must manually upgrade AVCLI to the most recent version on the remote computer. You can obtain AVCLI software from the **Drivers and Tools** section of the **Downloads** page at http://www.stratus.com/go/support/everrun. For information about how to manually install AVCLI on a remote computer see "AVCLI Command Overview" on page 260.

Related Topics

"The Upgrade Kits Page" on page 97

"The everRun Availability Console" on page 54

"Using the everRun Availability Console" on page 53

5

Chapter 5: Managing Logical Disks

Manage logical disks using the everRun Availability Console. For overview information see "Logical Disk Management" on page 105 as well as "Logical Disks and Physical Disks" on page 15.

To perform tasks, see the following:

- "Responding to a Failed Logical Disk" on page 106
- "Activating a New Logical Disk" on page 108

Logical Disk Management

In an everRun system, use the everRun Availability Console to manage logical disks by activating a new logical disk and responding to a failed logical disk.

In some cases, you need to activate a new logical disk even though the everRun software automatically recognizes new logical disks that the RAID controller presents to the operating system. For information, see "Activating a New Logical Disk" on page 108.

You need to respond to alerts regarding missing or failed logical disks. everRun software may detect a logical disk failure when a physical disk is removed or fails. The everRun software then generates an alert that appears on the DASHBOARD. The following alerts are examples:

- **System has missing or failed Logical Disks**.
- **Logical Disk - 1 on PM node1 has failed**.

On the **Physical Machines** page of the everRun Availability Console, the Storage tab for each PM identifies logical disks that have failed. For information, see "The Physical Machines Page" on page 84.

When a logical disk has failed, system storage is frozen. You cannot allocate new volumes until you have responded to the alert. Your response might require using the RAID controller BIOS or the **Repair** button on the masthead. For information, see "Responding to a Failed Logical Disk" on page 106

Related Topics

"Logical Disks and Physical Disks" on page 15

"The everRun Availability Console" on page 54

"Storage Requirements" on page 23

Responding to a Failed Logical Disk

When everRun software detects a missing or broken logical disk, it displays a failed logical disk alert on the DASHBOARD page of the everRun Availability Console. (For examples of alerts, see "Logical Disk Management" on page 105.) You can also view the alert on the ALERT HISTORY page. The everRun Availability Console continues to display the alert until you respond to the problem using one of the following methods, as appropriate for your situation:

- If a physical disk has been pulled, reinsert the appropriate physical disk. In this case, the physical machine restores the disk and you may need to use RAID controller software to complete the logical disk restoration.

- If a logical disk is broken or missing, you can attempt to use RAID controller software to recover it. If you are able to use RAID controller software to restore the logical disk to service, the everRun software will detect the restored logical disk and start using its data

- If a logical disk is broken or missing, and you cannot recover the logical disk using RAID controller software (for example, a failed physical disk needs to be replaced), click the **Repair** button in the masthead to complete the repair. After clicking the **Repair** button, the everRun software:

  - Dismisses the alert.

  - Evacuates all failed logical disks.

  - Removes all failed logical disks from their storage groups.

  - Attempts to repair any volumes that had been using the failed logical disks.

> **Caution:**
>
> 1. Clicking the **Repair** button removes all data on failed logical disks.
>
> 2. Repairing storage causes virtual machines (VMs) that are using failed logical disks to become simplex until repair is complete.
>
> 3. In some configurations, if you need to repair a logical disk that is the boot disk, you may need to reconfigure the RAID controller to boot from one of the remaining logical disks. Any logical disk that is not affected by the failed disk is able to boot the server. The ever-Run software mirrors the boot files for each node, in order to maximize overall availability. However, some systems may be able to boot from only the predefined boot logical disk in the RAID controller, and may be unable to boot from an alternate logical disk, if the predefined boot logical disk is present but not bootable. After the node has recovered and the logical disk with the replacement drive has been brought up to date, you should restore the boot device to the original value in the RAID controller.

To repair a failed logical disk

1. Click the **Repair** button that appears in the masthead of the everRun Availability Console.

2. Click **Yes** in the Confirm message box if you want to continue with the repair.

   After you click the **Repair** button, the everRun software attempts to repair all broken volumes by migrating data to other logical disks. When other logical disks have enough space for the data, the everRun software can successfully complete the repair. When other logical disks do not have enough space for the data, the everRun software generates the alert **Not enough space for repair**. In this case, you need to add more storage to the storage group by creating new logical disks or by deleting some existing volumes.

   When enough space for the data exists, the everRun software automatically re-mirrors broken volumes.

After the repair is complete, use RAID controller software to remove the failed logical disk and to create a new logical disk. everRun software automatically recognizes the new logical disk and brings it into service if the disk does not contain data. If the disk contains data, the DASHBOARD displays the message **Logical Disk - _n_ on PM node_n_ is foreign and should be activated or removed**. To activate the logical disk, see .

Related Topics

Activating a New Logical Disk

In an everRun system, the RAID controller creates logical disks from the system's physical disks. The everRun software is able to access logical disks that the RAID controller presents to the operating system. When the everRun software recognizes a new logical disk, it performs one of the following actions:

- If the logical disk does not contain data, the everRun software brings the logical disk into service.

- If it is a known logical disk that was not evacuated, the everRun software starts using the logical disk and its data.

- If the disk contains unknown data, the DASHBOARD displays the message **Logical Disk - *n* on PM node*n* is foreign and should be activated or removed**. In this case, you can activate or remove the disk now, or you can do nothing now, but later activate or remove the disk.

> **Caution**: Activating the logical disk causes all data on the disk to be lost.

> **Prerequisite**: Note any relevant requirements in "Storage Requirements" on page 23.

To activate a new logical disk

1. Click **Physical Machines** in the left-hand navigation panel.

2. On the **Physical Machines** page, select either **node0** or **node1** in the top pane.

3. On the **Physical Machines** page, click the **Storage** tab in the bottom pane.

4. In the **Action** column, click the **Activate Foreign** button to activate the corresponding logical disk.

5. When the **Confirm** message box appears, click **Yes** to confirm activating the logical disk. Activating the logical disk causes all data on the disk to be lost.

The everRun software partitions the new logical disk, adds it to the Initial Storage Group, and begins to use the disk.

Related Topics

6

Chapter 6: Managing Physical Machines

Manage a physical machine (PM) to control its operation and perform maintenance.

You view and manage PMs using the **Physical Machines** page of everRun Availability Console; for information, see "The Physical Machines Page" on page 84.

Many of the tasks you perform from the **Physical Machines** page require maintenance mode; for information, see "Maintenance Mode" on page 111.

To manage the operational state of a PM (in maintenance mode), see:

- "Rebooting a Physical Machine" on page 113

- "Shutting Down a Physical Machine" on page 113

- "Load Balancing" on page 115

To troubleshoot a PM by recovering a failed PM or resetting MTBF for a failed machine, see "Troubleshooting Physical Machines" on page 115.

To perform maintenance tasks, see "Maintaining Physical Machines" on page 237.

Maintenance Mode

When a physical machine (PM) enters maintenance mode, it goes offline for service. When you finalize service, the PM exits maintenance mode and goes back online, becoming available for running virtual machines (VMs).

When one PM enters maintenance mode, the PM migrates the VMs running on it to the other PM, which protects the VMs from any potential disruption caused by the service.

When the primary PM (**node*x* (primary)**) enters maintenance mode, the other PM becomes primary.

When both PMs enter maintenance mode, the PMs perform an orderly shutdown of all VMs, which protects their memory state before the PMs shut down or reboot.

Shut down the PMs only from the **Physical Machines** page with the PM in maintenance mode because the everRun Availability Console protects the system from disruptive action that results from manually powering down a PM.

> **Cautions**:
>
> 1. An everRun system is not fault tolerant when a PM is in maintenance mode. For continuous uptime, finalize service as soon as possible so that the PM can exit maintenance mode and go back online.
>
> 2. Avoid entering both PMs into maintenance mode at the same time. To keep the virtual machines running, at least one PM must be up and running normally. (If you need to shut down the entire everRun system, see "Shutting Down a Physical Machine" on page 113.)

> **Note**: If you want both PMs in maintenance mode, first enter the secondary PM into maintenance mode, and then enter the primary PM into maintenance mode. This sequence avoids the unnecessary migration of VMs.

To enter a PM into maintenance mode

1. Select a PM from the **Physical Machines** page.

2. Click **Work On**.

   When the PM is in maintenance mode, its state displays 🧰.

To finalize and exit a PM from maintenance mode

1. Select a physical machine from the **Physical Machines** page.

2. Click **Finalize**, which exits the PM from maintenance mode.

Related Topics

"The everRun Availability Console" on page 54

"Managing Physical Machines" on page 111

"Physical Machines and Virtual Machines" on page 8

Rebooting a Physical Machine

Reboot a physical machine (PM) to restart its everRun software, and optionally exit the PM from main-tenance mode. (If you need to reboot both PMs in the everRun system, see "Rebooting the System" on page 57.)

To reboot a PM

1. Determine which PM (node0 or node1) you want to reboot.

2. In the everRun Availability Console, click **Physical Machines** in the left-hand navigation panel.

3. Select the appropriate PM (node0 or node1) and then click **Work On**, which changes the PM's **Overall State** to **Maintenance Mode** and the **Activity** state to **running (in Maintenance)**.

4. Click **Reboot**. As the PM reboots, the **Activity** state displays:

   - **preparing for reboot (in Maintenance)**

   - **rebooting (in Maintenance)**

   - **booting (in Maintenance)**

   - **running (in Maintenance)**.

5. To exit the PM from maintenance mode and make it available for running virtual machines, click **Fin-alize**.

Related Topics

"Maintenance Mode" on page 111

"The everRun Availability Console" on page 54

"Managing Physical Machines" on page 111

"The Physical Machines Page" on page 84

Shutting Down a Physical Machine

Shut down a physical machine (PM) to stop it from running when you need to service or replace the PM. Use this procedure to shut down one and only one PM.

> **Cautions**:
>
> 1. Using this procedure to shut down both PMs will result in data loss. If you need to stop both PMs, shut down the everRun system (which also shuts down the virtual machines (VMs)), as described in "Shutting Down the System" on page 58.
>
> 2. Do not use the `-f` (force) option with the `halt`, `poweroff`, or `reboot` command of the CentOS operating system. Doing so causes FT guests that are active on the same node to hang. Instead, use the everRun Availability Console and maintenance mode to shutdown a PM, as described in the procedure below.
>
> 3. The everRun system is not fault tolerant when you shut down a PM. For continuous uptime, bring an offline PM back into service as soon as possible.

To shut down a PM, you must place the PM into maintenance mode, which migrates any virtual machines running on that PM to the remaining PM.

To shut down a PM

1. Determine which PM you want to shut down.

2. In the everRun Availability Console, click **Physical Machines** in the left-hand navigation panel.

3. Select the appropriate PM (node0 or node1) and then click **Work On**, which changes the PM's **Overall State** to **Maintenance Mode** and the **Activity** state to **running (in Maintenance)**.

4. After the PM displays **running (in Maintenance)**, click **Shutdown**.

> **Caution**: If the PM does not turn off after you click **Shutdown**, you must manually power off the PM, though doing so destroys its memory state. **Manually power off a PM only as a last resort.**

After the PM has shutdown, its activity is ❌ **off (in Maintenance)**. You must manually restart the PM.

Related Topics

"Maintenance Mode" on page 111

"The everRun Availability Console" on page 54

"Managing Physical Machines" on page 111

"The Physical Machines Page" on page 84

Load Balancing

HA Load Balancing distributes VMs across both PMs to improve performance and availability. Load balancing is configured per VM and is enabled automatically on everRun systems.

If a PM is out of service, all VMs will run on the surviving PM. VMs automatically migrate back as soon as the PM they are targeted to run on returns to service and is fully synchronized.

Modes of Operation

Load balancing is set for a VM on its **Load Balance** tab on the **Virtual Machines** page. The following modes are supported:

- **automatically balance**. This provides automatic load balancing of a VM. When a VM is set to balance automatically, it will run on the available PM with the most resources. When the system determines that better load balancing can be achieved by moving one or more VMs with the automatic setting, an alert is generated. The alert appears on the Dashboard, and a Load Balancing notification appears on the masthead.
  Click **Load Balance** to initiate automatic load balancing of a VM.
  The icon on the **Virtual Machines** page under **Current PM** column indicates VMs that will migrate imminently.

- **manually place on node***N*. Advanced users can manually assign a preferred PM (node) for each individual VM, rather than relying on the automatic policy, if preferred.

A graphic appears on the **Virtual Machine** page under the **Current PM** tab for each VM. It indicates the current status of the VM's load-balancing state, the PM the VM is running on, and its preference.

The following sample graphic indicates that the VMs are currently at PM 0 and that PM 1 is the preference.

everRun policy ensures that a VM is always running. In the event that one PM is predicted to fail, is under maintenance, or is taken out of service, the VM will run on the healthy PM. When both PMs are healthy, a VM migrates to its preferred PM.

Related Topic

"Selecting a Preferred PM for a Virtual Machine" on page 232

Troubleshooting Physical Machines

The following topics describe troubleshooting procedures for PMs:

- "Recovering a Failed Physical Machine" on page 116
- "Resetting MTBF for a Failed Physical Machine" on page 118

Recovering a Failed Physical Machine

Recover a physical machine (PM) when it cannot boot or if it fails to become a PM in the everRun system. In some cases, the everRun Availability Console displays the state of a failed PM as **Unreachable (Syncing/Evacuating…)**.

To recover a PM, you must reinstall the everRun release that the PM has been running using an install ISO. Recovering a failed PM, though, is different from installing the software for the first time. The recovery preserves all data, but it re-creates the /boot and root file systems, re-installs CentOS and the everRun software, and attempts to connect to an existing system.

> **Warning**: This procedure deletes all software you may have installed on the PM and all PM configuration information you may have entered before recovery. After you complete this procedure, you must manually re-install all your software and reconfigure the PM to match your original settings.

> **Note**: If you need to repair or replace the PM, see "Replacing Physical Machines, Motherboards, NICs, or RAID Controllers" on page 242, which requires the **Remove** operation of a node in maintenance mode.

Prerequisites:

1. Determine which PM you need to recover.

2. Obtain installation software for the everRun release that the PM has been running by using one of the following methods:

   ▪ Download an install ISO from your authorized Stratus service representative.

   ▪ Extract an install ISO into the current working directory from the most recently used upgrade kit by executing a command similar to the following (*x.x.x.x* is the release number and *nnn* is the build number):

   tar -xzvf everRun_upgrade-*x.x.x.x-nnn*.kit *.iso

   After you obtain the correct install ISO, save it or burn it to a DVD. See "Obtaining ever-Run Software" on page 34.

3. Check that a monitor and keyboard are connected to the PM that you are recovering.

4. Check that Ethernet cables are connected from the PM you are recovering to the network or directly to the other PM, if the two everRun system PMs are in close proximity. The Ethernet cable should connect from the first embedded port on the PM you are recovering or from an option (that is, add-on or expansion) port if the PM does not have an embedded port.

To recover a PM

1. Manually power on the PM that you want to recover. As the PM powers on, enter the firmware (BIOS) setup utility and set the Optical Drive as the first boot device.

2. Either mount the ISO image or insert the DVD into the PM.

3. At the **Welcome** screen, select **Recover PM, Join system: Preserving data** and press **Enter**.

4. When prompted, respond to the **Select interface for private Physical Machine connection**, and then respond to the prompt **Select interface for managing the system (ibiz0)**.

5. When prompted to configure **ibiz0**, select **Automatic configuration via DHCP** or **Manual Configuration (Static Address)**. (The installation software configures priv0 automatically.)

6. When installation is complete, the PM ejects the install DVD (if used) and reboots.

7. As the PM boots, you can view its activity on the **Physical Machines** page of the everRun Availability Console. The **Activity** column displays the PM as **recovery (in Maintenance)** and then **running** after recovery is complete.

8. Manually reinstall applications and any other host-level software and reconfigure the PM to match your original settings.

Related Topics

"Maintenance Mode" on page 111

"Managing Physical Machines" on page 111

"The everRun Availability Console" on page 54

"The Physical Machines Page" on page 84

Resetting MTBF for a Failed Physical Machine

Reset the mean time between failures (MTBF) counter for a physical machine (PM) to attempt to restart a failed PM.

If a PM crashes, the everRun software automatically restarts it, unless it has fallen below its MTBF threshold. If the PM is below the MTBF threshold, the everRun software leaves the machine powered off. If necessary, you can reset the MTBF counter and restart the PM.

> **Caution**: Do not reset the MTBF counter unless instructed to do so by your authorized Stratus service representative, as doing so may affect the fault tolerance of your system.

> **Note**: The **Reset Device** button is displayed only if the PM falls below its MBTF threshold.

To reset the MTBF counter for a PM

1. Determine which PM has the MTBF counter you want to reset.

2. In the everRun Availability Console, click **Physical Machines** in the left-hand navigation panel.

3. Select the appropriate PM (node0 or node1) and then click **Work On**, which changes the PM's **Overall State** to **Maintenance Mode** and the **Activity** state to **running (in Maintenance)**.

4. After the PM displays **running (in Maintenance)**, click **Reset Device**.

Related Topics

7

Chapter 7: Managing Virtual Machines

Manage a virtual machine (VM) to control its operation, provision its resources, or configure its guest operating systems and applications.

You can view and manage VMs on the **Virtual Machines** page of the everRun Availability Console, which you access as described in "The Virtual Machines Page" on page 88. To perform specific management tasks, see the following topics.

To manage the operational state of a VM, see:

- "Starting a Virtual Machine" on page 198

- "Shutting Down a Virtual Machine" on page 198

- "Powering Off a Virtual Machine" on page 200

- "Opening a Virtual Machine Console Session" on page 200

- "Renaming a Virtual Machine" on page 202

- "Removing a Virtual Machine" on page 202

To create or configure a VM, see:

- "Planning Virtual Machine Resources" on page 122 (virtual CPUs, memory, storage, and networks)

- "Creating and Migrating Virtual Machines" on page 127

- "Managing Snapshots" on page 219

- "Managing Virtual CDs" on page 215

- "Configuring Windows-based Virtual Machines" on page 190

- "Configuring Linux-based Virtual Machines" on page 194

- "Managing Virtual Machine Resources" on page 204

To complete advanced tasks, see:

- "Assigning a Specific MAC Address to a Virtual Machine" on page 231

- "Selecting a Preferred PM for a Virtual Machine" on page 232

- "Changing the Protection Level for a Virtual Machine (HA or FT)" on page 232

- "Configuring the Boot Sequence for Virtual Machines" on page 233

- "Resetting MTBF for a Failed Virtual Machine" on page 234

Planning Virtual Machine Resources

When creating virtual machines, plan to allocate system resources to maximize system performance and continuous uptime.

To plan for allocating resources to your virtual machines, see:

- "Planning Virtual Machine vCPUs" on page 122

- "Planning Virtual Machine Memory" on page 124

- "Planning Virtual Machine Storage" on page 125

- "Planning Virtual Machine Networks" on page 126

Planning Virtual Machine vCPUs

Allocate virtual CPUs (vCPUs) to assign computing resources to a virtual machine (VM) on your everRun system.

When allocating vCPUs to a VM, consider the following information and restrictions:

- Each vCPU represents a virtual unit of processing power. The total number of vCPUs available on an everRun system is equal to the minimum of the number of hardware threads presented by either physical machine (PM) in the system. For example, in a system where one PM that has 4 cores and 2 threads per core (8 vCPUs) and another PM that has 8 cores and 2 threads per core (16 vCPUs), the total number of vCPUs available is 8 vCPUs (fewest threads of either PM).

- The number of vCPUs available for all VMs is equal to the total number of vCPUs available on the everRun system minus the number of vCPUs allocated to the everRun system software (you can

set system vCPUs to 2 or 4, as described in "Configuring System Resources" on page 71). For example, if the total number of vCPUs is 8, and you allocate 2 vCPUs to the system software, there are 6 vCPUs that can be assigned to running VMs without over-provisioning the system.

- The maximum number of vCPUs you can allocate to any one VM is the total number of vCPUs available to all VMs minus the number of vCPUs allocated to currently running VMs (as described above) within the limits listed in "Virtual Machine Recommendations and Limits" on page 407.

- Windows-based VMs: If you change the number of assigned vCPUs from 1 to *n* or *n* to 1, after restarting the VM at the end of the reprovisioning process (see "Reprovisioning Virtual Machine Resources" on page 204), you must shut down and restart the VM a second time. This allows the VM to correctly reconfigure itself for Symmetric Multiprocessing (SMP). The VM displays odd behavior and is not usable until it is restarted.

- The **System** page of the everRun Availability Console (see "The System Page" on page 57) indicates the total number of vCPUs, the number of vCPUs allocated to the everRun system software, the number of vCPUs consumed by running VMs, and the number of free vCPUs.

- The everRun software allows the over-provisioning of vCPUs. If the number of free vCPUs on the **System** page is less than zero, you have over-provisioned the vCPUs; the console indicates this and displays an estimate of the degree to which vCPUs have been over-provisioned.

- The over-provisioning of vCPUs does not prevent you from creating or starting VMs; however, it is best to avoid running the system in an over-provisioned state.

Considerations When Over-Provisioning Virtual CPUs

> **Note**: In general, avoid over-provisioning VM resources. It is best to isolate each VM's resources to protect the VM against other VMs that might experience resource leaks or unexpected performance peaks. When you create and configure VMs, assign dedicated resources that cannot be used by other VMs.

You should over-provision physical CPUs only under the following conditions:

- The peak vCPU resources consumed by the combined VMs does not exceed the physical resources of the everRun system.

- One or more VMs are used at different times (such as off-peak backups).

- One or more of the VMs will be stopped while the other is running, for example, during VM upgrades or VM point-in-time backup or recovery.

- Peak total CPU use by VMs will not affect service level agreements or required response times.

- Each VM's CPU use is well understood, and its application(s) are not prone to resource leaks. When CPUs are over-provisioned, a leak in one VM can affect the performance of other VMs.

Related Topics

"System Requirements Overview" on page 22

"Creating and Migrating Virtual Machines" on page 127

"Managing Virtual Machine Resources" on page 204

Planning Virtual Machine Memory

Allocate memory to assign physical memory to a virtual machine (VM) on your everRun system.

When allocating memory to a VM, consider the following information and restrictions:

- The total memory you can allocate to the VMs is equal to the total amount of memory available on the everRun system (see "Memory Requirements" on page 24) minus the memory allocated to the everRun system software (which you can set to 1, 2, or 4 gigabytes (GB), as described in "Configuring System Resources" on page 71). For example, if the total amount of memory is 16 GB, and you allocate 2 GB to the system software, there are 14 GB of memory available to the VMs.

- You can provision a single VM with memory up the total amount of memory available to the VMs. Each VM consumes its requested amount of memory plus an additional 20% memory for overhead.

- The minimum memory allocation is 256 MB, but 64-bit operating systems require 600 MB or more. Be sure to verify the memory requirements for your guest operating systems.

- The **System** page of the everRun Availability Console (see "The System Page" on page 57) indicates the total amount of memory, the memory allocated to the everRun system software, the memory consumed by running VMs, and the amount of free memory. Use this page to verify your memory allocations.

- The everRun software does not allow over-provisioning of memory for **running** VMs; it prevents you from starting VMs that would exceed the total physical memory of the physical machines. You may safely allow over-provisioning of memory to occur only if one or more of the VMs is **stopped** while the other is running, for example, during VM upgrades or VM point-in-time backup or recovery.

- If necessary, you can manually redistribute memory by shutting down or reconfiguring one or more under-utilized VMs and then reassigning the available resources to a more heavily-utilized VM.

Related Topics

Planning Virtual Machine Storage

Plan the allocation of storage on your everRun system to ensure that you have space for your virtual machines (VMs) and system management needs.

When you install the everRun software, it forms a storage group from the available space on all logical disks. You allocate VM volumes and virtual CDs (VCDs) from this storage group, the assignment of which can have a dramatic impact on system performance and your ability to fully utilize available storage capacity.

When allocating storage to your virtual machines (VMs), consider the following actions:

- Observe storage maximums

  The everRun software does not allow over-provisioning of storage. The aggregate required storage for all VMs and VCDs must be no more than the total available storage in the everRun system. The system prevents you from creating a volume for a VM from a storage group that does not have enough space.

- Minimize stranded storage

  Ensure that each PM has the same amount of storage capacity. If one PM has more storage than the other, only the minimum amount of space is available in the storage group. For example, if one PM has 3 terabytes (TB) of storage and another PM has 2 TB of storage, the total amount of storage is 2 TB (least storage of either PM).

- Leave storage space for additional VCDs

  Leave at least 5 GB of free space in a storage group to allow room to create VCDs for installing additional VMs and applications. (To conserve this storage space, consider deleting VCDs when you are finished using them.)

- Leave storage space for VM snapshots

When you create each VM volume, you specify its volume size as well as the size of the larger volume container in which the volume and its snapshots are stored. To leave enough space for the snapshots that you plan to create, start by allocating a volume container that is at least two times the size of the volume that it contains; however, your needs may vary depending on VM snapshot activity and Disaster Recovery protection. For more information about estimating the amount of storage needed in a volume container, see "Sizing Volume Containers" on page 16.

To conserve storage space in a volume container, you can remove older or obsolete snapshots as described in "Removing a Snapshot" on page 230. If necessary, you can also expand a volume container as described in "Expanding a Volume Container on the everRun System" on page 213.

- Create separate boot and data volumes for each VM

  Install the guest operating system and applications in the first (boot) volume, and create separate volumes for associated data. Separating the boot and data volumes helps to preserve the data and makes it easier to recover a VM if the boot volume crashes.

- Create a boot volume with enough capacity for the guest operating system plus overhead

  Observe the minimum space requirements of your guest operating system and consider allocating slightly more space to account for the formatted capacity of the volume and usage. For example, if you allocate 5 GB to the boot drive when creating the VM, the formatted capacity of the boot volume starts at approximately 4.8 GB before usage, and this might be insufficient to meet a 5 GB requirement.

Related Topic

"Storage Requirements" on page 23

"Creating and Migrating Virtual Machines" on page 127

"Managing Virtual Machine Resources" on page 204

Planning Virtual Machine Networks

Plan network resources to determine how you will allocate available virtual networks to the virtual machines (VMs) on your everRun system.

When you install the everRun software, it binds pairs of physical network ports across the two physical machines (PMs) to form redundant virtual networks. When you create or reprovision VMs on your everRun system, you connect the VMs to these virtual networks instead of the physical network ports.

When connecting VMs to virtual networks, consider the following information and restrictions:

- You can connect one VM to multiple virtual networks, and you can connect multiple VMs to the same virtual network.

- The everRun software allows unlimited over-provisioning of network resources; therefore, be sure to profile a VM's network bandwidth/response time requirements when allocating virtual networks.

- When multiple VMs share the same virtual network, available network bandwidth is shared equally between the VMs. Unlike vCPU capacity, there is no way to proportionately allocate bandwidth resources. Therefore, high use of network resources by one VM can reduce the performance of all VMs on that network. If a VM has a large bandwidth requirement, consider connecting a dedicated virtual network to that VM.

Related Topics

"General Network Requirements and Configurations" on page 24

"Creating and Migrating Virtual Machines" on page 127

"Managing Virtual Machine Resources" on page 204

Creating and Migrating Virtual Machines

Generate a new virtual machine (VM) on the everRun 7.*x* system by creating a new VM, migrating an existing VM or physical machine (PM) directly over the network , or importing an Open Virtualization Format (OVF) file from an existing everRun or Avance VM.

To create a new VM (without an existing source VM or PM), see "Creating a New Virtual Machine" on page 128.

To migrate or import a system from a non-everRun 7.*x* source, see "Migrating From Avance or everRun MX Systems" on page 143 for considerations, and then see one of the following topics depending on your needs:

- "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133 (most VMs or PMs, including everRun MX- and Avance-based VMs)

  Use the *P2V client* (**virt-p2v**) to transfer a PM or VM directly over the network to a new VM on the everRun system.

- "Importing an OVF File from an everRun MX System" on page 164 (everRun MX-based VMs only)

Use XenConvert to export a VM from the everRun MX system to OVF and Virtual Hard Disk (VHD) files on a network share, and then use everRun Availability Console to import those files to the everRun 7.*x* system.

- "Importing an OVF File from an Avance System" on page 173 (Avance-based VMs only)

  Use Avance Management Console to export a VM from the Avance Unit to OVF and raw tar hard disk files on a management PC or network share, and then use everRun Availability Console to import those files to the everRun 7.*x* system.

To migrate or import a VM from another everRun 7.*x* system, or to duplicate or restore a VM on the same everRun 7.*x* system, see one of the following topics:

- "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133

  Use the *P2V client* (**virt-p2v**) to transfer a VM directly over the network to a new VM on another everRun 7.*x* system or on the same everRun 7.*x* system.

- "Managing Snapshots" on page 219

  Use the everRun Availability Console to create a snapshot of the source VM and export the snapshot to OVF and VHD files on a network share.

- "Importing an OVF File from an everRun 7.x System " on page 181

  Use the everRun Availability Console to import OVF and VHD files to another everRun 7.*x* system or back to the same everRun 7.*x* system.

  "Replacing a Virtual Machine from an OVF File" on page 185

  Use the everRun Availability Console to import OVF and VHD files back to the same everRun 7.*x* system to overwrite and restore an existing VM from a previous backup copy.

Related Topics

"Managing Virtual Machines" on page 121

Creating a New Virtual Machine

Create a new virtual machine (VM) to install a guest operating system on your everRun system. (You can also migrate an existing VM or physical machine (PM), as summarized in "Creating and Migrating Virtual Machines" on page 127.)

Launch the **VM Creation Wizard** by clicking **Create** on the **Virtual Machines** page. The wizard steps you through the process of allocating resources to the VM.

Note:

If you need to create a Windows Server 2003 VM, see "Creating a New Windows Server 2003 Virtual Machine" on page 132. You must perform a different procedure to create a Windows Server 2003 VM.

Prerequisites:

- Review the prerequisites and considerations for allocating CPUs, memory, storage, and network resources to the VM, as listed in "Planning Virtual Machine Resources" on page 122.

- Create a bootable virtual CD (VCD) of the Windows or Linux installation media, as described in "Creating a Virtual CD" on page 216. The bootable VCD must be a single CD or DVD. Multiple CDs or DVDs are not supported.

- Ensure that both PMs of the everRun system are online; otherwise, the system cannot properly create the VM.

- If you want to protect the new VM with Disaster Recovery (DR), wait until after you finish installing the guest operating system. If necessary, open the VM console and verify that the guest is healthy and responsive before enabling DR protection in the One View Console.

To create a new VM

1. On the **Physical Machines** page (see "The Physical Machines Page" on page 84), verify that both PMs are in the **running** state and that neither PM is in maintenance mode or in the process of synchronizing.

2. On the **Virtual Machines** page (see "The Virtual Machines Page" on page 88), click **Create** to open the **VM Creation Wizard**.

3. On the **Name, Description, Protection and OS** page:

   a. Type the **Name** and an optional **Description** for the VM as they will appear in the everRun Availability Console.

    b. Select the level of protection to use for the VM:

         ○ **Fault Tolerant (FT)**—Transparently protects an application by creating a redundant environment for a VM running across two physical machines. Use FT for applications that need greater downtime protection than HA provides.

         ○ **High Availability (HA)**—Provides basic failover and recovery, with some faults requiring an (automatic) VM reboot for recovery. Use HA for applications that can tolerate some downtime and that do not need the downtime protection that FT provides.

      For more information about these levels of protection, see "Modes of Operation" on page 11.

    c. Select the **Boot VCD** that contains the operating system you want to install.

    d. Click **Next**.

4. On the **vCPUs and Memory** page:

    a. Specify the number of **vCPUs** and the amount of **Memory** to assign to the VM. For more information, see "Planning Virtual Machine vCPUs" on page 122 and "Planning Virtual Machine Memory" on page 124.

    b. Click **Next**.

5. On the **Volumes** page:

    a. Type the **Name** of the boot volume as it will appear in the everRun Availability Console.

    b. Type the **Container Size** and **Volume Size** of the volume to create in gigabytes (GB). The container size is the total size for the volume including extra space to store snapshots. The volume size is the portion of the container that is available to the guest operating system. For more information about allocating storage, see "Sizing Volume Containers" on page 16 and "Planning Virtual Machine Storage" on page 125.

    c. Select the **Disk Image** format:

        ■ **RAW**—raw disk format

        ■ **QCOW2**—QEMU Copy On Write (QCOW2) format, which supports snapshots and Disaster Recovery

    d. If applicable, create additional data volumes by clicking **Add New Volume** and specifying the parameters for each volume. (You can also add volumes after you create the VM by

using the **Reprovision Virtual Machine** wizard, as described in "Creating a Volume in a Virtual Machine" on page 207.)

    e. Click **Next**.

6. On the **Networks** page, select the shared networks to attach to the VM (fr more information, see "Planning Virtual Machine Networks" on page 126). To continue, click **Next**.

7. On the **Creation Summary** page:

    a. Review the creation summary. If you need to make changes, click **Back**.

    b. If you want to prevent a console session from automatically starting to observe the software installation, deselect **Launch Console**.

    c. To accept the VM as provisioned and begin the software installation, click **Finish**.

8. If applicable, observe the progress of the installation of the operating system (allow pop-ups in your browser, if necessary) and respond to any prompts in the VM console session.

9. After you install the operating system, configure the additional resources and software necessary for production use, as described in:

    ▪ "Configuring Windows-based Virtual Machines" on page 190

    ▪ "Configuring Linux-based Virtual Machines" on page 194

> ⚠ **Caution**: If the primary PM fails or the VM crashes before the final reboot after the installation process is completed, the installation of the VM may need to be restarted.

The VM may not reboot if installations of any of the following are aborted:

- The guest operating system, including the configuration steps
- Any middleware or applications that manipulate system files

Related Topics

"Renaming a Virtual Machine" on page 202

"Removing a Virtual Machine" on page 202

"Creating and Migrating Virtual Machines" on page 127

"Managing Virtual Machine Resources" on page 204

"Managing the Operation of a Virtual Machine" on page 198

Creating a New Windows Server 2003 Virtual Machine

Follow these instructions to create a new Windows Server 2003 VM on your everRun system. You should understand the following considerations before you create the Windows Server 2003 VM:

- The Windows Server 2003 operating system is no longer supported by Microsoft.

- The **only version** of Windows Server 2003 that everRun systems support is the **Windows Server 2003 R2 Enterprise SP2 32-bit** operating system.

- The network VirtIO driver is not automatically installed as it is when creating VMs with other operating systems. The manual steps required to do this are provided in the procedure below.

> **Note**: The following procedure documents only the unique actions that are required to install this guest OS on your everRun system. You must also respond to other normal installation prompts not documented here (for example choosing a locale).

To create a new Windows Server 2003 VM

1. Create a bootable virtual CD (VCD) of the Windows Server 2003 media as described in .

2. Perform steps 1 through 7 of the procedure as described in .

3. When the dialog box informing you that the software has not passed Windows Logo testing appears click **Yes** to continue the installation.

4. When the dialog box informing you that the RedHat VirtIO SCSI controller driver has not passed Windows Logo testing appears, click **Yes** to continue the installation.

5. When the dialog box informing you that Windows Setup is not complete, click **Cancel**.

6. In the Windows Setup message informing you that you have chosen to not continue Setup, click **OK**.

7. Open **Computer Management** and click **Device Manager**.

8. In the right-hand pane of Computer Manager, under **Other Devices**, right click **Ethernet Controller**. In the pop-up menu click **Update Driver.**

9. In the **Hardware Update Wizard**, select **No, not this time**. Click **Next**.

10. In the **Hardware Update Wizard**, select **Install from a list or specific location (Advanced).** Click **Next**.

11. In the **Hardware Update Wizard**, select **Search removable media (floppy, CD-ROM...)**. Click **Next**.

12. In the **Hardware Update Wizard**, select the top-most Red Hat VirtIO Ethernet Adapter entry. Click **Next**.

13. When the Hardware Installation message informs you that the software has not passed Windows Logo testing click **Continue Anyway**, then click **Finish.**

14. Close **Computer Management**.

15. Shut down the VM that was just installed. This must be done in order to remove the virtual floppy drive that was automatically installed earlier during the installation.

> **Note**: If you need to install optional software from the Windows Server CD2 you must obtain an ISO image of that media. Place that ISO image on a network that the system can access, and run the setup.exe file.

16. After you install the operating system, configure the additional resources and software necessary for production use, as described in "Configuring Windows-based Virtual Machines" on page 190.

Related Topics

"Creating and Migrating Virtual Machines" on page 127

"Managing the Operation of a Virtual Machine" on page 198

Migrating a Physical Machine or Virtual Machine to an everRun 7.*x* System

Migrate a physical machine (PM) or virtual machine (VM) to transfer it over the network to a new VM on the everRun 7.*x* system. (You can also import an Open Virtualization Format (OVF) file to the everRun 7.*x* system, as summarized in "Creating and Migrating Virtual Machines" on page 127.)

To migrate a PM or VM over the network, boot the *P2V client* (**virt-p2v**) on the source PM or VM and use the client to configure, initiate, and monitor the secure network transfer from source side. No configuration steps are required on the everRun system until after the migration is complete, but you can confirm that the migration is in progress on the **Volumes** page of the everRun Availability Console as volumes associated with the new VM begin to appear.

> ⚠ **Caution**: Consider backing up your source PM or VM before preparing to migrate it.

Notes:

- The migration process supports only PMs or VMs running CentOS/RHEL 6, Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Small Business Server 2011, or Ubuntu 12.04 or later. (If you need to migrate a Windows Server 2003 VM, see "Migrating a Windows Server 2003 VM to an everRun 7.x System" on page 161. You must perform a different procedure to migrate a Windows Server 2003 VM.)

- For Linux-based PMs or VMs, consider editing the `/etc/fstab` file before the migration process to comment out entries for data volumes and allow only the boot volume to mount. Because Linux-based VMs use different device names on the everRun system, your new VM may boot into single-user mode if it cannot the mount volumes with their original device names. You can restore the `/etc/fstab` entries with the correct device names after the migration process, as described below in **Troubleshooting**.

- For Ubuntu-based PMs or VMs, you must edit the `/boot/grub/grub.cfg` file and change the `gfxmode` parameter to `text` (for example, `set gfxmode=text`) in the source PM or VM before the migration; otherwise, the new VM's console hangs on the everRun system. You can restore the original setting in the source PM or VM after the migration.

- Your source PM or VM must be offline for the duration of the migration process. Consider scheduling a planned maintenance period for the migration.

- The time required for the PM or VM migration depends on the size and number of volumes on the source system as well as the network bandwidth between the source and the target everRun system. For example, transferring a source system with one 20 GB boot volume over a 1 Gb/s network may take about 30 minutes.

- You can migrate multiple PMs or VMs at one time, but sharing network bandwidth may increase migration times.

- If you will continue to use the source PM or VM after the migration, remember to set a different MAC address and IP address for the new VM on the everRun system.

- If the everRun system switches from the primary PM to the secondary PM during a migration, the migration process fails. This does not affect the continuous uptime of

> your system, but you must reboot the P2V client on the source PM or VM and start over. See **Troubleshooting** below for more information.

> **Prerequisite**: Both PMs of the everRun system must be online for the migration process to function properly. On the **Physical Machines** page of the everRun Availability Console, verify that both PMs are in the **running** state and that neither PM is in maintenance mode or in the process of synchronizing.

To prepare for migrating a PM to the everRun system

1. Download the P2V client ISO file from the **Downloads** page at http://www.stratus.com/go/support/everrun.

   a. On the **Downloads** page, click **everRun** (if it is not already displayed) and then select the appropriate version.

   b. Scroll down to **Drivers and Tools** and then continue scrolling to **everRun P2V Client for Virtual or Physical Machine Migration**.

   c. Select the **P2V Client (virt-p2v)** file.

2. If you want to verify the integrity of the ISO image, use the associated `fciv` checksum file and the Microsoft File Checksum Integrity Verifier (FCIV) executable file, if you have already downloaded these files to your system. Otherwise, use the MD5 checksum hash function.

   Using fciv

   Open a command prompt window. From the directory containing the ISO, executable, and verification files, type a command similar to the following to verify the ISO image:

   fciv -v -xml virt-p2v-n.n.n-n.nnnnnnnn.n.el6.centos.xml

   If the command succeeds (that is, it returns the message `All files verified successfully`), go to the next step. If the command fails, repeat the download.

   Using MD5

   Open a command prompt window as an administrator, and enter the following:

```
CertUtil -hashfile path_to_file MD5
```

The `CertUtil` command displays a message indicating whether or not it com-
pleted successfully. If the command succeeds, continue with the next step. If the
command fails, repeat the download.

3. Burn the P2V client ISO file to a CD-ROM that you will use to boot the physical machine.

4. Insert the P2V client CD into the CD/DVD drive of the source PM.

5. Shut down the PM in preparation to boot the P2V client.

To prepare for migrating a VM to the everRun system

1. Download the P2V client ISO file from the **Drivers and Tools** section of the **Downloads**
   page at http://www.stratus.com/go/support/everrun. Ensure that you download the version
   of the P2V client that matches the version of the everRun system to which you are migrating
   the VM.

2. If you want to verify the integrity of the ISO image, use the associated `fciv` checksum file
   and the Microsoft File Checksum Integrity Verifier (FCIV) executable file, if you have
   already downloaded these files to your system. Otherwise, use the MD5 checksum hash
   function.

   Using fciv

   Open a command prompt window. From the directory containing the ISO, execut-
   able, and verification files, type a command similar to the following to verify the ISO
   image:

   fciv -v -xml virt-p2v-n.n.n-n.nnnnnnnn.n.el6.centos.xml

   If the command succeeds (that is, it returns the message `All files`
   `verified successfully`), go to the next step. If the command fails, repeat
   the download.

   Using MD5

   Open a command prompt window as an administrator, and enter the following:

   ```
   CertUtil -hashfile path_to_file MD5
   ```

> The `CertUtil` command displays a message indicating whether or not it completed successfully. If the command succeeds, continue with the next step. If the command fails, repeat the download.

3. Insert or connect the P2V client ISO file to the source VM and set the virtual CD drive as the boot device in the associated hypervisor.

4. Shut down the VM in preparation to boot the P2V client.

To migrate a PM or VM to the everRun system

1. Power on the source PM or VM to boot the P2V client. After a minute or so, the **virt-p2v** window is displayed.

2. If prompted, configure the network settings to use for the migration process; otherwise, skip to step 3. To configure the network settings:

   a. Select an active network device, if more than one is present.

   b. To specify static network settings, optionally clear the **Automatic configuration** check box and enter your **IP Address**, **Gateway**, and **DNS Servers** settings. Otherwise, keep the default settings to use DHCP.

   c. Click **Use these network settings**.

3. Enter the connection settings for the conversion server (the everRun system). Enter the **Hostname** or IP address of the system and the **Password** for the `root` account. (You must use the `root` account of the everRun host operating system, as described in "Accessing the Host Operating System" on page 20.)

4. Click **Connect**. The **Target properties** page is displayed.

5. Select **EverRun-FT** as the **Destination Profile**. (For information about these levels of protection, see "Creating a New Virtual Machine" on page 128 and "Modes of Operation" on page 11.)

6. Enter the **Name** for the target VM that will be displayed in the everRun Availability Console. (The name must be different from any existing VMs on the everRun system.)

7. The **Number of CPUs** and **Memory(MB)** values are automatically detected and completed, but optionally modify them if you want the VM on the everRun system to have more CPUs or memory than the source PM or VM.

8. Select which **Fixed Storage** devices to include in the migration by activating the check box next to each device.

   You must select at least one volume, including the boot volume. (Because the P2V client is a Linux-based utility, all devices are listed by Linux device names, where **sda** or **vda** represents the boot volume.)

9. The P2V client automatically manages **Removable Media** and **Network Interfaces** for the migration. Only one CD/DVD drive and one network interface is transferred to the new VM on the everRun system, regardless of your selections. You cannot change the CD/DVD configuration in the new VM, but you can provision additional network interfaces to the VM as needed after the migration.

10. When you are ready to migrate the PM or VM to the everRun system, click **Convert**. (If you need to cancel the migration for any reason, see **Troubleshooting** below.)

11. When the migration is complete, the P2V client displays a success message. If applicable, you can eject the CD or virtual CD and click **Power Off** to shut down the source PM or VM.

> **Note**: After the migration, the new VM on the everRun system is located on the primary PM, and it remains in a stopped state. Before starting the VM, complete the migration as described in the next procedure.

To complete the migration on the everRun system

1. Open the **Virtual Machines** page (see "The Virtual Machines Page" on page 88) in the everRun Availability Console.

2. Select the new VM in the top pane and click **Config** to open the **Reprovision Virtual Machine** wizard, as described in "Reprovisioning Virtual Machine Resources" on page 204. Use the wizard to configure the desired vCPUs, memory, storage, and network settings for the VM:

   - If your source PM or VM had more than one network interface, configure the additional network interfaces that were not included in the migration process.

   - If you will continue running the source PM or VM, ensure that the MAC address for each network interface in the new VM is different from the source PM or VM.

   Click **Finish** on the last wizard page to implement the changes.

3. Click **Start** to boot the new VM.

4. Click **Console** to open the console of the VM and log on to the guest operating system. (For information about using the console, see "Opening a Virtual Machine Console Session" on page 200.)

5. For Windows-based VMs only, install the required VirtIO drivers (already installed on Linux-based systems).

> **Note**: You must install two or more drivers, each of which requires the system to restart. When prompted, you can wait until the last driver is installed to restart the guest operating system.

In most cases, Windows either prompts you to install the drivers or automatically installs the drivers. After restarting the system to apply the new drivers, verify that the drivers are present or install them if necessary, as follows:

a. Open **Device Manager** in the guest operating system.

b. Expand **Network adapters** and verify that the **Red Hat VirtIO Ethernet Adapter** is present. There may be more than one adapter present depending on the number of network interfaces in your VM.

If the **Red Hat VirtIO Ethernet Adapter** is not present, expand **Other devices** and right-click the unknown **Ethernet Controller** device. Select **Update Driver Software** and follow the wizard to automatically search for and install the **Red Hat VirtIO Ethernet Adapter** driver. Repeat the driver update for each additional **Ethernet Controller** device.

c. Expand **Storage controllers** and verify that the **Red Hat VirtIO SCSI controller** is present. There may be more than one controller present depending on the number of volumes in your VM.

If the **Red Hat VirtIO SCSI controller** is not present, right-click the unknown **SCSI controller** device. Select **Update Driver Software** and follow the wizard to automatically search for and install the **Red Hat VirtIO SCSI controller** driver. Repeat the driver update for each additional **SCSI controller** device.

d. If applicable, restart the guest operating system to load the updated drivers.

> **Note**: On the **Virtual Machines** page and **Volumes** page of the everRun Availability Console, the **State** column may not accurately reflect the state of the VM or volume until the VirtIO drivers are properly installed.

6. Disable any guest operating system services that are unnecessary for operation on the everRun system:

   - If you migrated from a PM source, disable any services that interact directly with hardware. Examples include:

     - Dell OpenManage (OMSA)

     - HP Insight Manager

     - Diskeeper

   - If you migrated from a VM source, disable any services associated with other hypervisors. Examples include:

     - VMware Tools

     - Hyper-V Tools

     - Citrix Tools for Virtual Machines

   After disabling these services, restart the guest operating system to implement your changes.

7. If necessary, update the network configuration settings in the guest operating system and restart it to enable the settings.

8. Verify that you have configured your guest operating system with the additional Windows- or Linux-based system settings described in:

   - "Configuring Windows-based Virtual Machines" on page 190

   - "Configuring Linux-based Virtual Machines" on page 194

After you verify that the new VM is functioning properly, the migration process is complete; however, the everRun system may continue to synchronize data between PMs to enable High Availability (HA) or Fault Tolerant (FT) operation.

Troubleshooting

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

To cancel the migration process

Power down the source PM or VM running the P2V client.

To clean up after a canceled or failed migration

Open the everRun Availability Console and remove any migrated volumes associated with the source PM or VM. If you want to restart the migration process, reboot the P2V client on the source PM or VM.

To recover from a failed migration

If the migration process fails, an error message is displayed in the P2V client on the source PM or VM. Another message may be displayed on the everRun system. Use these messages to determine the problem.

If the migration continues to fail, and the option is available, enable server-side debugging. After the migration, generate a diagnostic file to send to your authorized Stratus service representative, as described in "Creating a Diagnostic File" on page 74. The diagnostic file includes any server-side debugging messages from the migration process.

To recover when the new VM's console hangs on the everRun **system**

For Ubuntu-based VMs, the VM console hangs in everRun Availability Console if you do not properly set the `gfxmode` parameter before the migration process (as described in **Notes**). If the VM console hangs, keep restarting the VM until the console opens properly in everRun Availability Console and then modify the `gfxmode` parameter to prevent subsequent issues.

For additional VM console troubleshooting, see "Opening a Virtual Machine Console Session" on page 200.

To recover missing data volumes in the VM on the everRun system

If your data volumes do not appear in the VM on the everRun system after the import, you may need to manually restore the volumes, as follows:

- Shut down the VM, run the **Reprovision Virtual Machine** wizard, and verify that you have included the volumes on the **Volumes** page.

- For Windows-based VMs, use **Disk Management** to bring data volumes online.

- For Linux-based VMs, edit the `/etc/fstab` file to reflect the new device names for the storage devices, from Avance (`/dev/xvda` through `/dev/xvdh`) to everRun

(`/dev/vda` through `/dev/vdh`). Device names also may have shifted, for example, if volumes were not included in the import.

To recover missing network devices in the VM on the everRun system

If your network devices do not appear in the VM on the everRun system after the import , you may need to manually restore them, as follows:

- Shut down the VM, run the **Reprovision Virtual Machine** wizard, and verify that you have included the networks on the **Networks** page.

- For Linux-based VMs, reconfigure the network startup script to reflect the new device names for the network interfaces.

Related Topics

"Migrating From Avance or everRun MX Systems" on page 143

"Creating and Migrating Virtual Machines" on page 127

"Configuring Windows-based Virtual Machines" on page 190

"Configuring Linux-based Virtual Machines" on page 194

"Managing Virtual Machine Resources" on page 204

"Managing the Operation of a Virtual Machine" on page 198

Migrating From Avance or everRun MX Systems

If you are migrating from an everRun MX system or an Avance unit to an everRun 7.*x* system, and you want to transfer virtual machines (VMs) from the other system, see "Creating and Migrating Virtual Machines" on page 127.

To learn more about migrating your system-wide configuration to an everRun system, start with one of the following topics, depending on your needs:

- "Planning to Migrate from an everRun MX System" on page 144 (System-to-System Migration)

  Use this planning information to consider the system-wide configuration and settings that are affected when you migrate an everRun MX system and its VMs to an everRun 7.*x* system.

- "Converting an everRun MX System to an everRun 7.x System" on page 147 (In-Place Migration)

  Use this procedure to perform an in-place migration of an everRun MX system and its VMs to the everRun 7.*x* software.

- "Planning to Migrate from an Avance Unit" on page 153 (System-to-System Migration)

  Use this planning information to consider the system-wide configuration and settings that are affected when you migrate an Avance unit and its VMs to an everRun 7.*x* system.

- "Converting an Avance Unit to an everRun 7.x System" on page 155 (In-Place Migration)

  Use this procedure to perform an in-place migration of an Avance unit and its VMs to the everRun 7.*x* software.

Related Topics

"Planning" on page 21

"Software Installation" on page 32

"Post-Installation Tasks" on page 48

"Creating and Migrating Virtual Machines" on page 127

Planning to Migrate from an everRun MX System

If you have an existing everRun MX system, this topic describes some items to consider when migrating to an everRun 7.*x* system.

For all systems, see "Creating and Migrating Virtual Machines" on page 127 for information about migrating your virtual machines (VMs) to the everRun 7.*x* system.

> ℹ **Note**: For best results, contact your authorized Stratus service representative for assistance in evaluating and performing upgrades from an everRun MX system.

Platform Requirements

Whether you reuse the existing everRun MX hardware or migrate to new hardware, the platform must meet the minimum system requirements for everRun 7.*x* systems, as described in "Physical Machine System Requirements" on page 405.

Multi-node XenServer pools are supported by everRun MX, but only two-node configurations are supported for everRun 7.*x* systems.

Planned Outage

The considerations in this help topic assume that an outage can be tolerated throughout the migration process. If you have minimum downtime requirements, contact your authorized Stratus service representative for assistance.

Guest Operating System Support

Verify that the Windows guest operating system running in each of the everRun MX virtual machines is supported by the everRun 7.*x* software. See "Compatible Guest Operating Systems" on page 404.

Also, verify that each Windows guest operating system is supported by the migration process (as described in "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133) or the import process (as described in "Importing an OVF File from an everRun MX System" on page 164).

Network Preparation

Prepare the platform network and the networking environment to conform to the everRun 7.*x* requirements. See "General Network Requirements and Configurations" on page 24.

Management Network Access

The XenServer management network becomes the everRun 7.*x* business network. As in everRun MX, the management console (everRun Availability Console) is accessed over this network.

Bonded network interfaces are recommend for the XenServer management network, but they are not supported for the everRun 7.*x* management network.

In everRun MX, each node in the XenServer pool has an IPv4 address associated with it. The same is true for an everRun 7.*x* system, but a **system IP** address is also required, and it must be a static address (not DHCP). This system IP address provides access to the everRun Availability Console; it is failed-over between everRun 7.*x* nodes as necessary by the everRun 7.*x* software.

Availability Link Networks

The A-Link networks that were in use in everRun MX will continue to be the A-Link networks on the everRun 7.*x* system. In everRun MX, the A-Links could have networking interfaces in each node that were not on the same subnet, but this is not possible on an everRun 7.*x* system. For each of the two possible A-Links, the network interfaces associated with them in each node must exist in the same local network, because IPv6 link local addresses are used to identify them.

Two 10-Gb networks are recommended for the A-Links.

It is not required that the A-Link connections be point-to-point (that is, they can be on a switched network).

Private Network

The everRun private network must be identified. Only one everRun 7.*x* system can be installed and operational on the private network at any one time, so it is recommended that the private network be a point-to-point connection between the two everRun 7.*x* nodes.

On the everRun 7.*x* system, it is typical to share one of the A-Links for the private network when at least one of the A-Link networks is connected point-to-point.

A 10-Gb network is recommended for the private network.

Business Networks

All networks that are not the private network or an A-Link network can also be business networks (that is, networks available for use by the VMs). The management network can be used simultaneously as a business network.

Storage Considerations

everRun MX supported both external storage and redundant-path storage. Neither of these configurations is supported on an everRun 7.*x* system.

everRun MX allowed the storage to be configured into multiple volume groups. The everRun 7.*x* software automatically creates a single storage group out of all the available storage.

For physical storage requirements, see "Storage Requirements" on page 23.

Quorum Support

Prior to everRun MX 6.2, the quorum servers could be available only over the A-Links. As of everRun MX 6.2, the quorum servers could be available over any network in the XenServer pool. On everRun 7.*x* systems, the quorum servers must be available over the business network, which is configured with an IPv4 address and required for quorum.

The Preferred Quorum Server should be configured as the first Quorum Server and the Alternate Quorum Server should be configured as the second Quorum Server in the everRun Availability Console.

Installing everRun

After the nodes in the everRun 7.*x* system are configured, you can install and configure the everRun 7.*x* software, as described in "Software Installation" on page 32.

Migrating Virtual Machines

Using either the P2V client migration process or the OVF import process, migrate the VMs to the everRun 7.x system. For an overview of each process, see "Creating and Migrating Virtual Machines" on page 127.

Converting an everRun MX System to an everRun 7.x System

Convert an everRun MX system to an everRun 7.x system to perform an in-place migration of the everRun MX system and its virtual machines (VMs) to the everRun 7.x software.

To convert an everRun MX system, shut down one physical machine (PM) or *node* in the everRun MX system and install the everRun 7.x software on that node. Use the P2V client to transfer each VM from the everRun MX node to the everRun 7.x node over the network. Then, install the everRun 7.x software on the remaining node.

> **Caution**: Consider backing up the everRun MX system and its VMs and recording its settings before the conversion. Converting an everRun MX system to an everRun 7.x system ultimately overwrites everything on your everRun MX system (after you migrate your VMs to the everRun 7.x node).

> **Notes**:
>
> - For best results, contact your authorized Stratus service representative for assistance in evaluating and performing upgrades from an everRun MX system.
>
> - Before converting an everRun MX system to an everRun 7.x system, verify that your PMs and VMs are supported as described in "Physical Machine System Requirements" on page 405 and "Compatible Guest Operating Systems" on page 404.

To prepare for converting an everRun MX system

1. Plan for converting your everRun MX system by reviewing the information:

   - "Planning to Migrate from an everRun MX System" on page 144

     Describes some items to consider when migrating or converting from an everRun MX system to an everRun 7.x system.

   - "Software Installation" on page 32

     Summarizes the steps for installing the everRun 7.x software.

   - "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page

133

Describes how to use the P2V client to migrate a VM from one system to another. Also describes some steps you may need to complete in your guest operating systems **before** migrating the VMs to ensure that the VMs will function properly on the everRun 7.*x* system.

2. Back up your everRun MX system and VMs.

3. Download the everRun 7.*x* ISO file from the **Downloads** page at http://www.stratus.com/go/support/everrun.

   a. On the **Downloads** page, click **everRun** (if it is not already displayed) and select the appropriate version.

   b. Scroll down to **Product Downloads**, and under **Install**, click the link to the appropriate ISO image (everRun_**install-7.***x.x.x-xxx***.iso**).

   c. Save the ISO image

4. Download the P2V client ISO file from the same **Downloads** page.

   a. On the **Downloads** page, click **everRun** (if it is not already displayed) and then select the appropriate version.

   b. Scroll down to the **Drivers and Tools** bar and then continue scrolling to **everRun P2V Client for Virtual or Physical Machine Migration**.

   c. Select the **P2V Client (virt-p2v)** file.

   d. Save the file.

5. Burn the everRun 7.*x* ISO file to a physical DVD that you will use to install the everRun 7.*x* software on each PM in your system.

6. Burn the P2V client ISO file to a physical CD that you will boot in each everRun MX VM to transfer the VMs to the everRun 7.*x* system.

7. Contact your network administrator to request at least one static IP address to use as the system-wide IP address for your converted everRun 7.*x* system. Request an additional static IP address for each of the two nodes if you do not have a DHCP server to automatically assign these addresses or if you prefer to use only static addresses.

> **Note**: You must maintain unique system IP addresses for the everRun MX system and the everRun 7.*x* system while both systems are online; however, if you want to re-use the original everRun MX system IP address for the everRun 7.*x* system, you can change the network settings of the everRun 7.*x* system after the conversion is complete.

To shut down the master server of the everRun MX system

Starting with both nodes running the everRun MX software, do the following:

1. Log on to the **everRun Availability Center** with the hostname or IP address of your everRun MX master node at:

   http://*everRunMX-address*:8080

2. On left-hand navigation panel, click the **Hosts** tab.

3. Right-click the master server and select **Shutdown**.

4. Allow the server to evacuate the VMs and properly shut down. You can watch its progress on the **everRun Log** tab.

   When the server is shut down, a message describes that you have lost connection to the everRun Availability Center. This is expected.

5. Open **Citrix XenCenter** and connect to remaining server of the everRun MX system, which is now the master server.

6. Make sure the VMs are still running on the remaining server before continuing.

To convert the first node of the everRun MX system to an everRun 7.*x* node

> **Caution**: Converting a node to the everRun 7.*x* software erases all hard drives in that node.

Starting one node shut down and the second node running the everRun MX software, do the following:

1. Insert the everRun 7.*x* DVD into the physical DVD drive of the offline node and boot the node to start the installation program.

2. Follow the instructions in "Installing Software on the First PM" on page 40 to install the

everRun 7.*x* software on the first node. Power on the node, update the necessary settings in the firmware (BIOS) setup utility, and boot the node from the everRun 7.*x* DVD to run the installation program.

When configuring the management network, select a DHCP-assigned address for now and record the IP address as described in "Recording the Management IP Address" on page 45. (You can optionally specify a static IP address for each node later, after converting the second node.)

> **Caution**: Do not convert the remaining node of the everRun MX system at this point; otherwise, all everRun MX data and VMs will be lost.

3. When you finish installing the everRun 7.*x* software on the first node, verify that you can connect to the everRun Availability Console at the IP address of the newly-installed node.

4. Log on to the everRun Availability Console of the newly-installed node as described in "Logging on to the everRun Availability Console for the First Time" on page 49.

   When prompted for the initial configuration settings, type the static IP address you obtained from your network administrator as the **System IP** address. Also, if you want to fully enable the features of your everRun 7.*x* system for testing, upload and activate your product license on the **LICENSE INFORMATION** page.

   > **Notes**:
   >
   > - When specifying the **System IP** address, type the system-wide IP address of the everRun system, and not the node0 or node1 address.
   >
   > - If you want to verify that your VMs work on the first node before you install the everRun 7.*x* software on the remaining node, activate your product license now. You can use the P2V client to migrate your VMs to the everRun 7.*x* system without a product license, but you cannot start and test your VMs on the everRun 7.*x* system unless you activate a valid license.

To migrate VMs from the everRun MX node to the everRun 7.*x* node

With the first node running the everRun 7.*x* software and the second node running the everRun MX software, do the following:

1. If applicable, prepare your VMs for migration as described in "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133. (If you need to migrate a Windows Server 2003 VM, see the specific steps in "Migrating a Windows Server 2003 VM to an everRun 7.x System" on page 161.)

   In some cases, you need to perform steps in the guest operating system before migrating a VM to ensure that the VM will function properly on the everRun 7.x system.

2. Log on to the **everRun Availability Center** on the remaining node of the everRun MX system at:

   http://*everRunMX-system*:**8080**

3. In the left-hand navigation panel, click **Virtual Machines**.

4. Right-click a VM that you want to migrate and click **Unprotect**.

5. When the VM is unprotected and automatically shut down, go back to **XenCenter**.

6. In the left-hand navigation panel of **XenCenter**, locate and expand the entry for the everRun MX system. Click the VM, and click **Start**.

7. After the VM starts, click the **Console** tab and click **Click here to create a DVD Drive**. Shut down the VM to save the change.

8. Insert the P2V client CD into the DVD drive of the remaining everRun MX node.

9. In the **Console** tab, next to **DVD drive** *n*, select the physical P2V client CD in the drop down menu. Click **Start** to begin booting the VM from the P2V client CD.

10. Migrate the VM by following the steps in "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133.

11. After the migration completes, power off the VM and close the VM console window.

12. In the everRun Availability Console connected to the everRun 7.x node, verify that the VM appears on the **Virtual Machines** page.

13. Start the migrated VM and verify that it is functioning properly. Follow the instructions in "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133 to complete any migration steps in the VM. For example, you may need to install drivers or disable certain services.

> **Caution**: The original VM on the everRun MX system must remain shut down when you use the VM on the everRun 7.*x* system; otherwise, the VMs will have network and software licensing conflicts.

> **Note**: You can start a VM on the everRun 7.*x* system only if you have activated your product license. Upload and activate your license as described in "Managing the everRun Product License" on page 62.

14. If necessary, configure and manage your VM as described in "Managing Virtual Machines" on page 121. For guest-specific settings, see:

    - "Configuring Windows-based Virtual Machines" on page 190

    - "Configuring Linux-based Virtual Machines" on page 194

15. Follow steps 1-14 to migrate additional VMs.

16. Verify that all of your VMs are functioning properly, and that you have recorded any additional settings that you need from the remaining everRun MX server, which you will overwrite in the next procedure.

To complete the conversion to the everRun 7.*x* software

> **Caution**: Converting a node to the everRun 7.*x* software erases all hard drives in that node. After you convert the second node, you cannot recover the original VMs except by restoring from exports or third-party backups.

1. Shut down the remaining node of the everRun MX system.

2. Follow the instructions in "Installing Software on the Second PM" on page 46 to install the everRun 7.*x* software on the remaining node. Power on the node, update the necessary settings in the firmware (BIOS) setup utility, and boot the node from the everRun 7.*x* DVD to run the installation program.

   When configuring the management network, select a DHCP-assigned address for now. (You can specify a static IP address after the software installation.)

3. When the installation finishes, connect to the everRun Availability Console at the system IP address of the everRun 7.*x* system.

4. Verify that both PMs reach the **running** state and that the PMs finish synchronizing. The initial synchronization may take minutes or hours depending on your configuration, including the amount of storage and the number of VMs.

5. Optionally, update the network settings for the everRun 7.*x* system:

   - If you want to reuse the static IP address of the everRun MX system as the system IP address of the everRun 7.*x* system, open the **Preferences** page and click **IP Configuration**. On the **System IP** tab, enter the static IP settings that were used by the everRun MX system and click **Save**.

   - If you want to specify a static IP address for each node, click each **Node*n* IP** tab, enter the new settings, and click **Save**.

   If necessary, the everRun Availability Console reloads to reflect the new addresses.

6. Configure the everRun 7.*x* settings summarized in "Post-Installation Tasks" on page 48.

Troubleshooting

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

To resolve network connectivity problems with the everRun 7.*x* system

If you have trouble connecting to the everRun Availability Console after installing the first node, you may have used the same IP address for node0 and for the system IP address of the everRun 7.*x* system To correct the problem, reinstall the everRun 7.*x* software on node0 and ensure that the IP addresses you type for node0 and the system IP address are unique.

Planning to Migrate from an Avance Unit

If you have an existing Avance unit, this topic describes some items to consider when migrating to an everRun 7.*x* system.

For all systems, see "Creating and Migrating Virtual Machines" on page 127 for information about migrating your virtual machines (VMs) to the everRun 7.*x* system.

> ℹ **Note**: For best results, contact your authorized Stratus service representative for assistance in evaluating and performing upgrades from an Avance unit.

Platform Requirements

Whether you reuse the existing Avance hardware or migrate to new hardware, the platform must meet the minimum system requirements for everRun systems, as described in "Physical Machine System Requirements" on page 405.

Planned Outage

The considerations in this help topic assume that an outage can be tolerated throughout the migration process. If you have minimum downtime requirements, contact your authorized Stratus service representative for assistance.

Guest Operating System Support

Verify that the Windows or Linux guest operating system running in each of the Avance VMs is supported by the everRun software. See "Compatible Guest Operating Systems" on page 404.

Also, verify that each guest operating system is supported by the migration process (as described in "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133) or the import process (as described in "Importing an OVF File from an everRun MX System" on page 164).

Network Preparation

Prepare the platform network and the networking environment to conform to the everRun system requirements. See "General Network Requirements and Configurations" on page 24.

Management Network Access

The same network that was used to access the Avance Management Console will be used for the everRun Availability Console.

In Avance, the nodes were available on the management network for management only through the IPv4 system address, which could be failed-over to either node in the system. The everRun software uses the same system address, but it also requires separate IPv4 addresses for each node in the same subnet as the system IP address.

Availability Link Networks

Avance had no Availability Links; therefore, these networks must be added to the hardware configuration.

Two 10-Gb networks are recommended for the A-Links.

It is not required that the A-Link connections be point-to-point (that is, they can be on a switched network).

Private Network

The same network used as the private network on the Avance unit can be used for the private network on the everRun system.

Only one everRun system can be installed and operational on the private network at any one time, so it is recommended that the private network be a point-to-point connection between the two everRun nodes.

It is typical to share one of the A-Links for the private network when at least one of the A-Link networks is connected point-to-point.

A 10-Gb network is recommended for the private network.

Business Networks

All networks that are not the private network or an A-Link network can also be business networks (that is, networks available for use by the VMs). The management network can be used simultaneously with the business network.

Storage Considerations

Avance unit storage can be used as-is in the everRun system; however, there can be only one storage group. For physical storage requirements, see "Storage Requirements" on page 23.

Installing everRun

After the nodes in the everRun system are configured, you can install and configure the everRun software, as described in "Software Installation" on page 32.

Migrating Virtual Machines

Using either the P2V client migration process or the OVF import process, migrate the VMs to the everRun system. For an overview of each process, see "Creating and Migrating Virtual Machines" on page 127.

Converting an Avance Unit to an everRun 7.x System

Convert an Avance unit to an everRun system to perform an in-place migration of the Avance unit and its virtual machines (VMs) to the everRun 7.x software.

To convert an Avance unit, shut down one physical machine (PM) or *node* in the Avance unit and install the everRun software on that node. Use the P2V client to transfer each VM from the Avance node to the everRun node over the network. Then, install the everRun software on the remaining node.

> **Caution**: Consider backing up the Avance unit and its VMs and recording its settings before the conversion. Converting an Avance unit to an everRun system ultimately overwrites everything on your Avance unit (after you migrate your VMs to the everRun node).

> **Notes**:
>
> - For best results, contact your authorized Stratus service representative for assistance in evaluating and performing upgrades from an Avance unit.
>
> - Before converting an Avance system to an everRun system, verify that your PMs and VMs are supported as described in "Physical Machine System Requirements" on page 405 and "Compatible Guest Operating Systems" on page 404.

To prepare for converting an Avance unit

1. Plan for converting your Avance unit by reviewing the following information:

   - "Planning to Migrate from an Avance Unit" on page 153

     Describes some items to consider when migrating or converting from an Avance unit to an everRun system.

   - "Software Installation" on page 32

     Summarizes the steps for installing the everRun software.

   - "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133

     Describes how to use the P2V client to migrate a VM from one system to another. Also describes some steps you may need to complete in your guest operating systems **before** migrating the VMs to ensure that the VMs will function properly on the everRun system.

2. Back up your Avance unit and VMs.

3. Download the everRun ISO file from the **Downloads** page at http://www.stratus.-com/go/support/everrun.

4. Download the P2V client ISO file from the **Drivers and Tools** section of the same support page.

5. Burn the everRun ISO file to a physical DVD that you will use to install the everRun software on each PM in your system.

6. In the Avance Management Console, use the P2V client ISO file to create a VCD that you will boot in each Avance VM to transfer the VMs to the everRun system.

7. Contact your network administrator to request at least one static IP address to use as the system-wide IP address for your converted everRun system. Request an additional static IP address for each of the two nodes if you do not have a DHCP server to automatically assign these addresses or if you prefer to use only static addresses.

> **Note**: You must maintain unique system IP addresses for the Avance unit and the everRun system while both systems are online; however, if you want to reuse the original Avance unit IP address for the everRun system, you can change the network settings of the everRun system after the conversion is complete.

To convert node0 of the Avance unit to an everRun node

> **Caution**: Converting a node to the everRun software erases all hard drives in that node.

Starting with both nodes running the Avance software, do the following:

1. In Avance Management Console, verify that your Avance unit is running properly and that both PMs are online.

2. Enable maintenance mode on **node0** of the Avance unit.

> **Note**: Start with node0 of the Avance unit for consistency, because this first node that you convert will become node0 of the everRun system.

3. Verify that the VMs migrate from node0 to node1.

4. Shut down node0.

5. Follow the instructions in "Installing Software on the First PM" on page 40 to install the everRun software on node0. Power on the node, update the necessary settings in the firmware (BIOS) setup utility, and boot the node from the everRun DVD to run the installation

program.

When configuring the management network, select a DHCP-assigned address for now and record the IP address as described in "Recording the Management IP Address" on page 45. (You can optionally specify a static IP address for each node later, after converting the second node.)

> ⚠ **Caution**: Do not convert the remaining node of the Avance unit at this point; otherwise, all Avance data and VMs will be lost.

6. When you finish installing the everRun software on node0, verify that you can connect to the everRun Availability Console at the IP address of the newly-installed node.

7. Log on to the everRun Availability Console on node0 as described in "Logging on to the everRun Availability Console for the First Time" on page 49.

When prompted for the initial configuration settings, type the static IP address you obtained from your network administrator as the **System IP** address. Also, if you want to fully enable the features of your everRun system for testing, upload and activate your product license on the **LICENSE INFORMATION** page.

> ℹ **Notes**:
>
> - When specifying the **System IP** address, type the system-wide IP address, and not the node0 or node1 address.
>
> - If you want to verify that your VMs work on node0 before you install the everRun software on the remaining node, activate your product license now. You can use the P2V client to migrate your VMs to the everRun system without a product license, but you cannot start and test your VMs on the everRun system unless you activate a valid license.

To migrate VMs from the Avance node to the everRun node

With node0 running the everRun software and node1 running the Avance software, do the following:

1. If applicable, prepare your VMs for migration as described in "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133. (If you need to migrate a Windows Server 2003 VM, see the specific steps in "Migrating a Windows Server 2003 VM to

an everRun 7.x System" on page 161.)

In some cases, you need to perform steps in the guest operating system before migrating a VM to ensure that the VM will function properly on the everRun system.

2. In the Avance Management Console, shut down a VM that you want to migrate.

3. Boot the VM from the P2V client VCD and migrate the VM by following the steps in "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133.

4. After the migration completes, power off the VM and close the VM console window.

5. In the everRun Availability Console connected to the everRun node, verify that the VM appears on the **Virtual Machines** page.

6. Start the migrated VM and verify that it is functioning properly. Follow the instructions in "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133 to complete any migration steps in the VM. For example, you may need to install drivers or disable certain services.

> **Caution**: The original VM on the Avance system must remain shut down when you use the VM on the everRun system; otherwise, the VMs will have network and software licensing conflicts.

> **Note**: You can start a VM on the everRun system only if you have activated your product license. Upload and activate your license as described in "Managing the everRun Product License" on page 62.

7. If necessary, configure and manage your VM as described in "Managing Virtual Machines" on page 121. For guest-specific settings, see:

   - "Configuring Windows-based Virtual Machines" on page 190
   - "Configuring Linux-based Virtual Machines" on page 194

8. Follow steps 1-7 to migrate additional VMs.

9. Verify that all of your VMs are functioning properly, and that you have recorded any additional settings you that need from the remaining Avance node (node1), which you will overwrite in the next procedure.

To complete the conversion to the everRun software

> **Caution**: Converting a node to the everRun software erases all hard drives in that node. After you convert the second node, you cannot recover the original VMs except by restoring from exports or third-party backups.

1. Shut down the Avance unit to power off the remaining Avance node (node1). In the Avance Management Console, on the **Unit** page, click **Shutdown** .

2. Follow the instructions in "Installing Software on the Second PM" on page 46 to install the everRun software on node1. Power on the node, update the necessary settings in the firmware (BIOS) setup utility, and boot the node from the everRun DVD to run the installation program.

   When configuring the management network, select a DHCP-assigned address for now. (You can specify a static IP address after the software installation.)

3. When the installation finishes, connect to the everRun Availability Console at the system IP address of the everRun system.

4. Verify that both PMs reach the **running** state and that the PMs finish synchronizing. The initial synchronization may take minutes or hours depending on your configuration, including the amount of storage and the number of VMs.

5. Optionally, update the network settings for the everRun system:

   - If you want to reuse the static IP address of the Avance unit as the system IP address of the everRun system, open the **Preferences** page and click **IP Configuration**. On the **System IP** tab, enter the static IP settings that were used by the Avance unit and click **Save**.

   - If you want to specify a static IP address for each node, click each **Node*n* IP** tab, enter the new settings, and click **Save**.

   If necessary, the everRun Availability Console reloads to reflect the new addresses.

6. Configure the everRun settings summarized in "Post-Installation Tasks" on page 48.

Troubleshooting

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

To resolve network connectivity problems with the everRun system

If you have trouble connecting to the everRun Availability Console, especially after installing the first node (node0), you may have used the same IP address for node0 and for the system IP address. To correct the problem, reinstall the everRun software on node0 and ensure that the IP addresses you type for node0 and the system IP address are unique.

Migrating a Windows Server 2003 VM to an everRun 7.x System

Follow these instructions to migrate a Windows Server 2003 virtual machine (VM) from an Avance unit or an everRun MX system to a destination everRun 7.2 or later system. You should understand the following considerations before you migrate the Windows Server 2003 VM:

- The Windows Server 2003 operating system is no longer supported by Microsoft.

- The **only version** of Windows Server 2003 that everRun systems support is the **Windows Server 2003 R2 Enterprise SP2 32-bit** operating system.

- The destination system must be running everRun software release 7.2 or later.

To migrate the VM, boot the *P2V client* (**virt-p2v**) in the source Windows Server 2003 VM and use the client to configure, initiate, and monitor a secure network transfer from source side. To begin, follow the appropriate procedure: *To prepare for migrating a Windows Server 2003 VM* from your source system, and then continue with *To migrate a Windows Server 2003 VM from Avance or everRun MX system*.

To prepare for migrating a Windows Server 2003 VM from an Avance unit

1. Download the P2V client ISO file from the **Drivers and Tools** section of the **Downloads** page at http://www.stratus.com/go/support/everrun.

    a. On the **Downloads** page, click **everRun** (if it is not already displayed) and then select the appropriate version.

    b. Scroll down to **Drivers and Tools** and then continue scrolling to **everRun P2V Client for Virtual or Physical Machine Migration**.

    c. Select the **P2V Client (virt-p2v)** file.

2. If you want to verify the integrity of the ISO image, use the associated `fciv` checksum file and the Microsoft File Checksum Integrity Verifier (FCIV) executable file, if you have already downloaded these files to your system. Otherwise, use the MD5 checksum hash function.

    Using fciv

Open a command prompt window. From the directory containing the ISO, execut-
able, and verification files, type a command similar to the following to verify the ISO
image:

fciv -v -xml virt-p2v-n.n.n-n.nnnnnnnn.n.el6.centos.xml

If the command succeeds (that is, it returns the message `All files`
`verified successfully`), go to the next step. If the command fails, repeat
the download.

Using MD5

Open a command prompt window as an administrator, and enter the following:

`CertUtil -hashfile path_to_file MD5`

The `CertUtil` command displays a message indicating whether or not it com-
pleted successfully. If the command succeeds, continue with the next step. If the
command fails, repeat the download.

3. In the Avance Management Console, use the P2V client ISO file to create a VCD that you
   will boot in the Windows Server 2003 VM to transfer it to the everRunsystem.

4. On the **Virtual Machines** page, select the Windows Server 2003 VM and click **Shutdown**.

5. When the Windows Server 2003 VM is stopped, click **Boot from CD**.

6. In the **Boot from a CD** dialog box, select the P2V client VCD and click **Boot**.

To prepare for migrating a Windows Server 2003 VM from an everRun MX system

1. Download the P2V client ISO file from the **Drivers and Tools** section of the **Downloads**
   page at http://www.stratus.com/go/support/everrun.

2. Burn the P2V client ISO file to a physical CD that you will boot in the Windows Server 2003
   VM to transfer it to the everRun 7.2 or later system.

3. Perform steps 1 through 9 in the *To migrate VMs from the everRun MX node to the everRun*
   7.x node section of "Converting an everRun MX System to an everRun 7.x System" on page
   147 to shut down the Windows Server 2003 VM and boot it from the P2V client CD.

To migrate a Windows Server 2003 VM from an Avance or everRun MX system

1. In the **virt-p2v** window, fill in the destination everRun system's host name (or host
   IP address) and password. Click **Connect**.

2. In the next **virt-p2v** window, click **Convert**.

   You can monitor the progress of the migration in the **virt-p2v** window and on the **Volumes** page of the destination everRun system's everRun Availability Console as volumes associated with the new VM begin to appear.

3. When the migration is complete, the **virt-p2v** window displays a success message. Click **Power Off** to shut down the source VM.

4. In the destination everRun system's everRun Availability Console, click **Virtual Machines**.

5. Select the newly created VM and click **Start**.

6. Log on to the Windows Server 2003 guest operating system.

7. A service control manager warning about a driver failing during system startup appears. Click **OK**.

8. In the **Found New Hardware** wizard, select **No, not this time** and click **Next**.

9. Select **Install the software automatically**. Click **Next**.

10. A warning about the RedHat VirtIO Ethernet Adapter not passing Windows Logo testing appears. Click **Continue Anyway**.

11. When the **Found New Hardware** wizard completes, click **Finish**.

12. A warning about the RedHat VirtIO SCSI Adapter not passing Windows Logo testing appears. Click **Continue Anyway.**

13. The **Found New Hardware** wizard displays **a Cannot Install this Hardware** message. Select **Don't prompt me again to install this software** and click **Finish**.

14. At the prompt to restart the computer, click **Yes**.

15. A service control manager warning about a driver failing during system startup appears again. Click **OK**.

16. If necessary, update the network configuration settings in the guest operating system and restart it to enable the settings.

After you verify that the new VM is functioning properly, the migration process is complete; however, the everRun system may continue to synchronize data between PMs to enable High Availability (HA) or Fault Tolerant (FT) operation.

Related Topics

Importing an OVF File from an everRun MX System

Import an Open Virtualization Format (OVF) file from an everRun MX system if you want to transfer a
VM to the everRun 7.*x* system for deployment. (To migrate a physical machine (PM) or virtual machine
(VM) to the everRun 7.*x* system without using an OVF file, see "Migrating a Physical Machine or Virtual
Machine to an everRun 7.x System" on page 133.)

To import a VM from an everRun MX system, first use XenConvert 2.1 to export OVF and Virtual Hard
Disk (VHD) files from the everRun MX system to a network share, and then use the everRun Availability
Console to import the OVF and VHD files from the network share to the everRun 7.*x* system.

> ⚠️ **Caution**: Consider backing up your source VM before preparing it for export from the everRun
> MX system.

Notes:

- You can import only VMs running Windows Server 2008 from everRun MX systems. Importing a Windows Server 2003 VM from an OVF file is not supported. If you need to transfer a Windows Server 2003 VM to an everRun 7.*x* system, see "Migrating a Windows Server 2003 VM to an everRun 7.x System" on page 161.

- For Windows-based VMs, you must install VirtIO drivers in the guest operating system **before** exporting the VM from the everRun MX system, as described in this topic. If you do not install the VirtIO drivers, the imported VM crashes while booting on the everRun 7.*x* system.

- You need to map a network share that is accessible from the source VM on the everRun MX system and also accessible by the management PC running the everRun Availability Console. You use XenConvert to export the VM to this share, then you import the VM to the everRun 7.*x* system from this share.

- In preparation for exporting the OVF file from the everRun MX system, you must unprotect the VM in the everRun Availability Center, which automatically shuts down the VM. Consider scheduling a planned maintenance period for this process.

- The time required for the export and import depends on the size and number of volumes in the source VM as well as network bandwidth. For example, transferring a VM with one 20 GB boot volume over a 1 Gb/s network may take about 30 minutes each way, export and import.

- When you import the VM on the everRun 7.x system, the import wizard creates a new instance of the VM with unique hardware IDs. The import wizard does not offer the Restore option that creates an identical VM with the same hardware IDs (SMBIOS UUID, system serial number, and MAC addresses), because the export files from everRun MX systems do not include this information.

- If you will continue to use the source VM on the everRun MX system after the import, remember to set a different IP address and hostname for the VM on the everRun 7.*x* system.

- If the everRun 7.*x* system switches from the primary PM to the secondary PM during an import, the import process fails. This does not affect the continuous uptime of your

> ℹ️   system, but you must delete the incomplete VM and associated volumes on the ever-Run 7.*x* system, and import them again.

Exporting an OVF File from the everRun MX System

Exporting a VM from the everRun MX system exports the VM's configuration in an OVF file along with a copy of the selected volumes on your management PC.

To prepare for exporting a VM from the everRun MX system

1. Log on to the **everRun Availability Center** with the hostname or IP address of your ever-Run MX master node at:

   http://*everRunMX-system*:**8080**

2. In the left-hand navigation panel, click **Virtual Machines**.

3. Right-click a VM that you want to export and click **Unprotect**.

4. When the VM is unprotected and automatically shut down, open **Citrix XenCenter**.

5. In the left-hand navigation panel of **XenCenter**, locate and expand the entry for the everRun MX system. Click the VM that you want to export, and click **Start**.

6. Click the **Console** tab to open the console of the VM and log on to the Windows guest operating system.

7. Ensure that all volumes are labeled accurately, as summarized in "Managing Windows Drive Labels" on page 189.

8. Run the Windows System Preparation Tool (`Sysprep`) to prepare the guest operating system for redeployment.

9. Install the VirtIO drivers and the XenConvert utility in the Windows guest operating system:

   a. Download the **VirtIO.exe** driver installation utility from the **Drivers and Tools** section of the **Downloads** page at http://www.stratus.com/go/support/everrun to the guest operating system. This installation utility installs the VirtIO drivers and also the XenConvert utility required for an export from the everRun MX system.

   If you want to verify the integrity of the VirtIO.exe file, also download the associated fciv (Windows) or md5sum (Linux) checksum file and execute similar commands to those described in "Obtaining everRun Software" on page 34.

b. Right-click the installation utility and click **Run as administrator**.

c. Click **OK** to install the software, and monitor the progress in the command prompt window.

d. Click **Restart Later** when Windows prompts you to restart the guest operating system.

> **Note**: Windows prompts you to restart while the installation utility is still working. **Do not restart the VM** until you complete the following steps; otherwise, the driver installation fails and your imported VM will not boot on the everRun 7.*x* system.

e. Wait until the command prompt window indicates that the installation is finished and prompts you to **Press any key to continue**.

f. Click the command prompt window to make it the active window, then press any key and wait for command prompt window and WinZip window to close.

g. Restart the guest operating system to load the new drivers.

You can optionally uninstall the VirtIO drivers and the XenConvert utility after a successful import, as described later in this topic.

To export the VM and boot volume from the everRun MX system

1. In the Windows guest operating system on the everRun MX system, map a network share to which you will export the VM. For example, you can access a network share on your management PC that runs the everRun Availability Console.

2. Start **Citrix XenConvert** in the source VM.

3. Verify that **From: This machine** is selected.

4. Select **To: Open Virtualization Format (OVF) Package**. Click **Next**.

5. Select only the **(Boot)** volume to export. Explicitly deselect other volumes by clicking the **Source Volume** pulldown menu and selecting **None**. Do not change any other settings on this page. Click **Next**.

> ⓘ **Note**: You can export only one volume at a time; otherwise, the export fails. See the next procedure to export additional volumes.

6. Specify a path in the **Please choose a folder to store the Open Virtualization (OVF) package** text area. Click **Browse** and select a new, empty folder on the network share that you mounted for the export.

7. Ensure that the following XenConvert options are disabled. These options are not supported, and they can prevent a successful import:

   - Include a EULA in the OVF package

   - Create Open Virtual Appliance (OVA)

   - Compress Open Virtual Appliance (OVA)

   - Encrypt

   - Sign with Certificate

8. Click **Next**.

9. Optionally modify the name of the target OVF file. Click **Next**.

10. Click **Convert**.

> ⓘ **Note**: During the export process, if Windows displays a message indicating that you need to format a hard disk to use it, you can click **Cancel** to dismiss this message. The export continues normally.

To export each additional volume from the VM on the everRun MX system

1. Restart **Citrix XenConvert** on the source VM.

2. Verify that **From: This machine** is selected.

3. Select **To: XenServer Virtual Hard Disk (VHD)**. Click **Next**.

4. Select only **one** volume to export. Explicitly deselect other volumes by clicking the **Source Volume** pulldown menu and selecting **None**.

   Do not change any other settings on this page. Click **Next**

5. Specify a path in the **Please choose a folder to store the Open Virtualization (OVF)**

package text area. Click **Browse** and select a new, empty folder on the network share that you mounted for the export. Click **Next**.

> **Note**: XenConvert does not give the option of specifying VHD file names, so each VHD export must initially be stored in a different folder to avoid overwriting the previous files.

6. Click **Convert**. This creates a VHD file and a PVP file.

7. After the VHD export, rename the new VHD file to give it a new, unique name and move it to the folder with the boot volume OVF and VHD. The PVP file is not used.

8. Repeat this procedure for each additional volume.

Importing the OVF file to the everRun 7.*x* System

Importing a VM to the everRun 7.*x* system imports the VM's configuration and any associated volumes that you select from your exported files.

> **Prerequisites**:
>
> - The selected OVF file (boot volume) and all associated VHD files (additional volumes) must be in the same directory, and no other VHD files can be in that directory.
>
> - Both PMs of the everRun 7.*x* system must be online for the import process to function properly.

To import a VM to the everRun **7.*x* system**

1. If applicable, on your management PC, map the network share containing the exported OVF and VHD files.

2. Log on to the everRun 7.*x* system with the everRun Availability Console.

3. On the **Physical Machines** page (see "The Physical Machines Page" on page 84), verify that both PMs are in the **running** state and that neither PM is in maintenance mode or in the process of synchronizing.

4. On the **Virtual Machines** page (see "The Virtual Machines Page" on page 88), click **Import/Restore** to open the import wizard.

5. If prompted, allow the required Java™ plugins to load in your web browser. For information about enabling Java for the everRun Availability Console, see "Compatible Internet Browsers" on page 30.

6. Click **Browse**. In the file browser, select the **.ovf** file that you want to import from your management PC and click **Import**.

7. Click **Import** to create a new instance of the VM with unique hardware IDs.

8. Review the information and make any desired edits, if necessary:

   ■ **Name, CPU, and Memory**

     Change the name of the virtual machine, edit the number of vCPUs, or allocate the total memory it can use.

   ■ **Storage**

     Shows all of the volumes. Select the **Create** box for a volume to allocate a storage container for the volume on the everRun 7.*x* system (the boot volume is required). Select the **Restore Data** box to import data for a volume from the OVF file.

   ■ **Network**

     Displays all of the available networks. You can remove a network or add one that is not already allocated. A minimum of one network is required. If you will continue running the source VM on the everRun MX system, ensure that the MAC address for each network interface in the new VM is different from the source VM.

9. Optionally, clear the check box for **Auto start Virtual Machine after import** if you need to reprovision the VM before starting it for the first time on the everRun 7.*x* system.

10. Click **Import** to begin importing the VM. When the transfer is complete, click **Done** to close the import wizard.

> **Note**: Imported volumes begin to appear on the **Volumes** page of the everRun Availability Console while the import is still in progress. Do not attach or remove any of these imported volumes until the import window reports that the process is complete; otherwise, the import fails.

11. If applicable, use the **Reprovision Virtual Machine** wizard to allocate additional resources

to the VM, as described in "Reprovisioning Virtual Machine Resources" on page 204.

When you are finished reprovisioning the VM, click **Start** to boot the VM.

12. Click **Console** to open the console of the VM and log on to the guest operating system.

13. Allow the guest operating system to automatically install the VirtIO drivers and other required drivers, which may take several minutes. When a notification icon indicates that **Your device is ready to use** and you are prompted to restart, restart the guest operating system to load the drivers.

14. If necessary, update the network settings in the guest operating system.

After you verify that the new VM is functioning properly, the import process is complete; however, the everRun 7.*x* system continues to synchronize data between PMs to enable High Availability (HA) or Fault Tolerant (FT) operation.

> **Note**: Your new VM and its associated volumes may be marked with warning symbols until the data has been synchronized and the VirtIO drivers are running.

To optionally uninstall the VirtIO drivers from the source VM on the everRun MX system (Windows-based VMs only)

After you successfully import the new VM to the everRun 7.*x* system, you can uninstall the VirtIO drivers and the XenConvert utility from the Windows-based source VM on the everRun MX system. However, uninstalling this software is optional, as it does not interfere with the operation of the VM.

1. In the console of the source Windows-based VM, locate the **VirtIO.exe** installation utility. (This same utility is used to uninstall the VirtIO drivers if they are present.)

2. Right-click the installation utility and click **Run as administrator**.

3. Click **OK** to uninstall the VirtIO drivers, and monitor the progress in the command prompt session.

4. When prompted, press any key to close the utility. No restart is necessary.

Troubleshooting

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

To clean up after a canceled or failed export from the everRun MX system

In the Windows guest operating system, consider saving log file information from XenConvert, then close the utility. Remove all of the files from the export folder on your network share, or create a new folder for a subsequent export. You must select an empty folder for each new export.

To clean up after a canceled or failed import on the everRun 7.*x* system

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

To recover from a failed export from the everRun MX system

The export fails if you export more than one volume at a time. Run XenConvert again and be careful to explicitly deselect all but one volume for the export. Also, ensure that you use an empty folder for each new export.

To recover from a failed import to the everRun 7.*x* system

The imported VM crashes if the VirtIO drivers are not present in a Windows-based VM. Before running the XenConvert export again, ensure that you install the VirtIO drivers in the VM on the everRun MX system.

To recover missing data volumes in the VM on the everRun 7.*x* system

If your data volumes do not appear in the VM on the everRun 7.*x* system after the import, you may need to manually restore the volumes, as follows:

- Shut down the VM, run the **Reprovision Virtual Machine** wizard, and verify that you have included the volumes on the **Volumes** page.
- Use **Disk Management** to bring data volumes online.

To recover missing network devices in the VM on the everRun 7.*x* system

Shut down the VM, run the **Reprovision Virtual Machine** wizard, and verify that you have included the networks on the **Networks** page.

Related Topics

"Migrating From Avance or everRun MX Systems" on page 143

"Creating and Migrating Virtual Machines" on page 127

"Configuring Windows-based Virtual Machines" on page 190

"Configuring Linux-based Virtual Machines" on page 194

"Managing Virtual Machine Resources" on page 204

Importing an OVF File from an Avance System

Import an Open Virtualization Format (OVF) file from an Avance unit if you want to transfer a VM to the everRun 7.*x* system for deployment. (To migrate a physical machine (PM) or virtual machine (VM) to the everRun 7.*x* system without using an OVF file, see "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133.)

To import a VM from an Avance unit, first use the Avance Management Console to export OVF and hard disk files to a management PC, and then use the everRun Availability Console to import the OVF and hard disk files from the management PC to the everRun system.

When you import a VM image in the everRun Availability Console, the import wizard allows you to choose between *importing* or *restoring* the VM. Importing a VM creates a new instance of the VM with unique hardware IDs. Restoring a VM creates an identical VM with the same hardware IDs (SMBIOS UUID, system serial number, and MAC addresses, if provided in the VM image) that your guest operating system and applications may require for software licensing. To prevent conflicts with the original VM, restore a VM only if you want to transfer it to the everRun system and stop using it on the source system.

> **Caution**: Consider backing up your source VM before preparing it for export from the Avance unit.

Notes:

- You can import only VMs running CentOS/RHEL 6, Windows 7, Windows Server 2008, or Ubuntu 12.04 or later from Avance units.

- If you need to transfer a Windows Server 2003 VM to an everRun system, see "Migrating a Windows Server 2003 VM to an everRun 7.x System" on page 161. Importing a Windows Server 2003 VM from an OVF file is not supported.

- For Windows-based VMs, you must install VirtIO drivers in the guest operating system **before** exporting the VM from the Avance unit, as described in this topic. If you do not install the VirtIO drivers, the imported VM crashes while booting on the everRun 7.*x* system.

- For Linux-based VMs, before exporting the VM from the Avance unit, consider editing the `/etc/fstab` file to comment out entries for data volumes and allow only the boot volume to mount. Because Linux-based VMs use different device names on the everRun system, your new VM may boot into single-user mode if it cannot mount the volumes with their original device names. You can restore the `/etc/fstab` entries in the new VM with the correct device names after the import process, as described below in **Troubleshooting**.

- For Ubuntu-based VMs, you must edit the `/boot/grub/grub.cfg` file and change the `gfxmode` parameter to `text` (for example, `set gfxmode=text`) before exporting the VM from the Avance unit; otherwise, the new VM's console hangs on the everRun system. You can restore the original setting in the source VM after the migration.

- Your source VM must be shut down while you are exporting the OVF file or creating a snapshot on the Avance unit. Consider scheduling a planned maintenance period for this process.

- The time required for the export and import depends on the size and number of volumes in the source VM as well as network bandwidth. For example, transferring a VM with one 20 GB boot volume over a 1 Gb/s network may take about 30 minutes each way, export and import.

- • If you will continue to use the source VM on the Avance unit after the import, remember to set a different MAC address and IP address for the VM on the everRun system.

- • If the everRun system switches from the primary PM to the secondary PM during an import, the import process fails. This does not affect the continuous uptime of your system, but you must delete the incomplete VM and associated volumes on the everRun system, and import them again.

Exporting an OVF File from the Avance Unit

Exporting a VM from the Avance unit exports the VM's configuration in an OVF file along with a copy of the selected volumes on your management PC.

To prepare for exporting a VM from the Avance unit (Windows-based VMs only)

1. Log on to the Avance unit with the Avance Management Console.

2. On the **Virtual Machines** page, select the VM to export.

3. Click **Console** to open the console of the VM and log on to the Windows guest operating system.

4. Ensure that all volumes are labeled accurately, as summarized in "Managing Windows Drive Labels" on page 189.

5. Run the Windows System Preparation Tool (`Sysprep`) to prepare the guest operating system for redeployment.

6. Install the VirtIO drivers in the Windows guest operating system:

   a. Download the **VirtIO.exe** driver installation utility from the **Drivers and Tools** section of the **Downloads** page at http://www.stratus.com/go/support/everrun to the guest operating system.

   If you want to verify the integrity of the VirtIO.exe file, also download the associated fciv (Windows) or md5sum (Linux) checksum file and execute similar commands to those described in "Obtaining everRun Software" on page 34.

   b. Right-click the installation utility and click **Run as administrator**.

   c. Click **OK** to install the VirtIO drivers, and monitor the progress in the command prompt window.

   d. Click **Restart Later** when Windows prompts you to restart the guest operating

system.

> **Note**: Windows prompts you to restart while the installation utility is still working. **Do not restart the VM** until you complete the following steps; otherwise, the driver installation fails and your imported VM will not boot on the everRun system.

   e. Wait until the command prompt window indicates that the VirtIO driver installation is finished and prompts you to **Press any key to continue**.

   f. Click the command prompt window to make it the active window, then press any key and wait for command prompt window and WinZip window to close.

   g. Restart the guest operating system to load the new drivers.

Installing the VirtIO drivers also installs the XenConvert utility required for exports from everRun MX systems; however, this utility is not used on Avance units. You can optionally uninstall the VirtIO drivers and the XenConvert utility after a successful import, as described later in this topic.

To export a VM from the Avance unit

The following procedure describes how to export a VM from Avance, but you can also create a snapshot and export the snapshot to reduce downtime for the source VM. To create a snapshot, see the Avance online help.

   1. Log on to the Avance unit with the Avance Management Console.

   2. On the **Virtual Machines** page, select the VM to export.

   3. With the VM selected, click **Shutdown** and wait for the VM to power off.

   4. Click **Export** to display the export wizard.

   5. If prompted, allow the required Java™ plugins to load in your web browser.

   6. Click **Export VM**. (Click **Export Snapshot** if you created a snapshot.)

   7. Click **Browse**. Select a location for the export on your management PC running the Avance Management Console and click **Save**.

   8. Select the volumes you want capture, or click **VM Configuration Only** to include only the

configuration details of each volume in the export file, but not the data.

9. Click **Export**.

Importing the OVF file to the everRun System

Importing a VM to the everRun system imports the VM's configuration and any associated volumes that you select from the OVF export on your management PC.

> **Prerequisite**: Both PMs of the everRun system must be online for the import process to function properly.

To import a VM to the everRun system

1. Log on to the everRun system with the everRun Availability Console.

2. On the **Physical Machines** page (see "The Physical Machines Page" on page 84), verify that both PMs are in the **running** state and that neither PM is in maintenance mode or in the process of synchronizing.

3. On the **Virtual Machines** page (see "The Virtual Machines Page" on page 88), click **Import/Restore** to open the import wizard.

4. If prompted, allow the required Java plugins to load in your web browser. For information about enabling Java for the everRun Availability Console, see "Compatible Internet Browsers" on page 30.

5. Click **Browse**. In the file browser, select the **.ovf** file that you want to import from your management PC and click **Import**.

6. Select **Import** or **Restore**. Import creates a new instance of the VM with unique hardware IDs. Restore creates an identical VM with the same hardware IDs that are provided in the OVF file.

7. Review the information and make any desired edits, if necessary:

   - **Name, CPU, and Memory**

     Change the name of the virtual machine, edit the number of vCPUs, or allocate the total memory it can use.

   - **Storage**

Shows all of the volumes. Select the **Create** box for a volume to allocate a storage container for the volume on the everRun system (the boot volume is required). Select the **Restore Data** box to import data for a volume from the OVF file.

- **Network**

    Displays all of the available networks. You can remove a network or add one that is not already allocated. A minimum of one network is required. If you will continue running the source VM on the Avance unit, ensure that the MAC address for each network interface in the new VM is different from the source VM.

8. Optionally, clear the check box for **Auto start Virtual Machine after import** if you need to reprovision the VM before starting it for the first time on the everRun system.

9. Click **Import** to begin importing the VM. When the transfer is complete, click **Done** to close the import wizard.

> **Note**: Imported volumes begin to appear on the **Volumes** page of the everRun Availability Console while the import is still in progress. Do not attach or remove any of these imported volumes until the import window reports that the process is complete; otherwise, the import fails.

10. If applicable, use the **Reprovision Virtual Machine** wizard to allocate additional resources to the VM, as described in "Reprovisioning Virtual Machine Resources" on page 204.

    When you are finished reprovisioning the VM, click **Start** to boot the VM.

11. Click **Console** to open the console of the VM and log on to the guest operating system.

12. For Windows-based VMs, allow the guest operating system to automatically install the VirtIO drivers and other required drivers, which may take several minutes. When a notification icon indicates that **Your device is ready to use** and you are prompted to restart, restart the guest operating system to load the drivers.

13. If necessary, update the network settings in the guest operating system.

After you verify that the new VM is functioning properly, the import process is complete; however, the everRun system may continue to synchronize data between PMs to enable High Availability (HA) or Fault Tolerant (FT) operation.

> ℹ️ **Note**: Your new VM and its associated volumes may be marked with warning symbols until the data has been synchronized and the VirtIO drivers are running.

To optionally uninstall the VirtIO drivers from the source VM on the Avance unit (Windows-based VMs only)

After you successfully import the new VM to the everRun system, you can uninstall the VirtIO drivers and the XenConvert utility from the Windows-based source VM on the Avance unit. However, uninstalling this software is optional, as it does not interfere with the operation or continuous uptime of the Avance unit.

1. In the console of the source Windows-based VM, locate the **VirtIO.exe** installation utility. (This same utility is used to uninstall the VirtIO drivers if they are present.)

2. Right-click the installation utility and click **Run as administrator**.

3. Click **OK** to uninstall the VirtIO drivers, and monitor the progress in the command prompt session.

4. When prompted, press any key to close the utility. No restart is necessary.

Troubleshooting

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

To clean up after a canceled or failed export from the Avance unit

On your management PC, remove all of the files from the export folder or create a new folder for a subsequent export.

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.

To recover from a failed import to the everRun system

The imported VM crashes if the VirtIO drivers are not present in a Windows-based VM. Before running the export again, ensure that you install the VirtIO drivers in the VM on the Avance unit.

To recover when the new VM's console hangs on the everRun system

For Ubuntu-based VMs, the VM console hangs in everRun Availability Console if you do not properly set the `gfxmode` parameter before the import process (as described in **Notes**). If the

VM console hangs, keep restarting the VM until the console opens properly in everRun Availability Console and then modify the `gfxmode` parameter to prevent subsequent issues.

For additional VM console troubleshooting, see "Opening a Virtual Machine Console Session" on page 200.

To recover missing data volumes in the VM on the everRun system

If your data volumes do not appear in the VM on the everRun system after the import, you may need to manually restore the volumes, as follows:

- Shut down the VM, run the **Reprovision Virtual Machine** wizard, and verify that you have included the volumes on the **Volumes** page.

- For Windows-based VMs, use **Disk Management** to bring data volumes online.

- For Linux-based VMs, edit the `/etc/fstab` file to reflect the new device names for the storage devices, from Avance (`/dev/xvda` through `/dev/xvdh`) to everRun (`/dev/vda` through `/dev/vdh`). Device names also may have shifted, for example, if volumes were not included in the import.

To recover missing network devices in the VM on the everRun system

If your network devices do not appear in the VM on the everRun system after the import , you may need to manually restore them, as follows:

- Shut down the VM, run the **Reprovision Virtual Machine** wizard, and verify that you have included the networks on the **Networks** page.

- For Linux-based VMs, reconfigure the network startup script to reflect the new device names for the network interfaces.

Related Topics

"Migrating From Avance or everRun MX Systems" on page 143

"Creating and Migrating Virtual Machines" on page 127

"Configuring Windows-based Virtual Machines" on page 190

"Configuring Linux-based Virtual Machines" on page 194

"Managing Virtual Machine Resources" on page 204

"Managing the Operation of a Virtual Machine" on page 198

Importing an OVF File from an everRun 7.*x* System

Import an Open Virtualization Format (OVF) file from an everRun system if you want to transfer a VM from one everRun 7.*x* system to another, or if you want to transfer an image that you created back to the same everRun 7.*x* system to restore or duplicate the original VM. (To migrate a physical machine (PM) or virtual machine (VM) to the everRun 7.*x* system without using an OVF file, see "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133.)

To import a VM image from an everRun system, first use the everRun Availability Console on the source everRun system to create a VM snapshot (see "Creating a Snapshot" on page 220) and export that snapshot (see "Exporting a Snapshot" on page 224) to OVF and Virtual Hard Disk (VHD) files on a supported network share. Mount the network share on your management PC, and then open the everRun Availability Console on the target everRun system to import the OVF and VHD files from your management PC.

When you import a VM image in the everRun Availability Console, the import wizard allows you to choose between *importing* or *restoring* the VM. Importing a VM creates a new instance of the VM with unique hardware IDs. Restoring a VM creates an identical VM with the same hardware IDs (SMBIOS UUID, system serial number, and MAC addresses, if provided in the VM image) that your guest operating system and applications may require for software licensing. To prevent conflicts with the original VM, restore a VM only if you want to transfer it to the everRun system and stop using it on the source system.

If you want to restore an existing VM on the same everRun system to overwrite the VM and recover it from a previous backup copy, see "Replacing a Virtual Machine from an OVF File" on page 185.

Notes:

- You can import VMs only if they are running supported guest operating systems, as described in "Compatible Guest Operating Systems" on page 404.

- The time required for the import depends on the size and number of volumes in the source VM as well as network bandwidth. For example, transferring a VM with one 20 GB boot volume over a 1 Gb/s network may take about 30 minutes.

- When you import or restore an everRun VM, the original container size for each volume you include is not preserved. For example, if your source VM has a 20 GB boot volume in a 40 GB volume container, the target VM will have a 20 GB boot volume in a 20 GB volume container. If necessary, you can expand the volume containers on the target system as described in "Expanding a Volume Container on the everRun System" on page 213.

- If you are importing a VM back to the same everRun system to duplicate the VM, you must rename the VM and duplicate volumes during either the export or import process.

- If you are restoring a VM back to the same everRun system, the VM can be started only if the original VM is stopped or removed from that system. If you are restoring a VM from a different system, you must stop the original VM on the source system before you start it on the target system to prevent conflicts.

- If you will continue to use the source VM after the import or restore process, remember to set a different MAC address and IP address for the VM on the target system.

- If the everRun system switches from the primary PM to the secondary PM during an import, the import process fails. This does not affect the continuous uptime of your system, but you must delete the incomplete VM and associated volumes on the everRun system, and import them again.

Prerequisite: Both PMs of the everRun system must be online for the import process to function properly.

To import a VM to the everRun **system**

1. Create and export a VM snapshot on the source everRun system. For more information, see "Managing Snapshots" on page 219.

2. On the management PC that you use to run the everRun Availability Console, do the following:

    a. Map the network share that contains the exported OVF and VHD files.

    b. Log on to the everRun Availability Console on the target everRun system.

3. On the **Physical Machines** page (see "The Physical Machines Page" on page 84), verify that both PMs are in the **running** state and that neither PM is in maintenance mode or in the process of synchronizing.

4. On the **Virtual Machines** page (see "The Virtual Machines Page" on page 88), click **Import/Restore** to open the import wizard.

5. If prompted, allow the required Java plugins to load in your web browser. For information about enabling Java for the everRun Availability Console, see "Compatible Internet Browsers" on page 30.

6. Click **Browse**. In the file browser, locate the exported files. Select the **.ovf** file that you want to import, and click **Import**.

7. Select **Import** or **Restore**. Import creates a new instance of the VM with unique hardware IDs. Restore creates an identical VM with the same hardware IDs that are provided in the OVF file.

8. Review the information and make any desired edits, if necessary:

    -   **Name, CPU, and Memory**

        Change the name of the virtual machine, edit the number of vCPUs, or allocate the total memory it can use.

    -   **Storage**

        Shows all of the volumes. Select the **Create** box for a volume to allocate a storage container for the volume on the everRun system (the boot volume is required). Select the **Restore Data** box to import data for a volume from the VHD file.

    -   **Network**

        Displays all of the available networks. You can remove a network or add one that is not already allocated. A minimum of one network is required. If you will continue running the

source VM on the source everRun system, ensure that the MAC address for each network interface in the new VM is different from the source VM.

9. Optionally, clear the check box for **Auto start Virtual Machine after import** if you need to reprovision the VM before starting it for the first time on the everRun system.

10. Click **Import** to begin importing the VM. When the transfer is complete, click **Done** to close the import wizard.

> ℹ️ **Note**: Imported volumes begin to appear on the **Volumes** page of the everRun Availability Console while the import is still in progress. Do not attach or remove any of these imported volumes until the import window reports that the process is complete; otherwise, the import fails.

11. If applicable, use the **Reprovision Virtual Machine** wizard to allocate additional resources to the VM, as described in "Reprovisioning Virtual Machine Resources" on page 204. Also, if you want to allocate additional space in each volume container for snapshots, see "Expanding a Volume Container on the everRun System" on page 213.

    When you are finished reprovisioning the VM, click **Start** to boot the VM.

12. Click **Console** to open the console of the VM and log on to the guest operating system.

13. If necessary, update the network settings in the guest operating system.

After you verify that the new VM is functioning properly, the import process is complete; however, the everRun system may continue to synchronize data between PMs to enable High Availability (HA) or Fault Tolerant (FT) operation.

> ℹ️ **Note**: Your new VM and its associated volumes may be marked with warning symbols until the data has been synchronized and the VirtIO drivers are running.

Troubleshooting

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

To clean up after a canceled or failed import

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

To recover missing data volumes in the target VM

If your data volumes do not appear in the VM on the target everRun system after the import, you may need to manually restore the volumes, as follows:

- Shut down the VM, run the **Reprovision Virtual Machine** wizard, and verify that you have included the volumes on the **Volumes** page.

- For Windows-based VMs, use **Disk Management** to bring data volumes online.

- For Linux-based VMs, edit the `/etc/fstab` file to reflect the new device names for the storage devices. Device names may have shifted, for example, if volumes were not included in the import.

To recover missing network devices in the VM on the everRun system

If your network devices do not appear in the VM on the target everRun system after the import , you may need to manually restore them, as follows:

- Shut down the VM, run the **Reprovision Virtual Machine** wizard, and verify that you have included the networks on the **Networks** page.

- For Linux-based VMs, reconfigure the network startup script to reflect the new device names for the network interfaces.

Related Topics

"Migrating From Avance or everRun MX Systems" on page 143

"Creating and Migrating Virtual Machines" on page 127

"Configuring Windows-based Virtual Machines" on page 190

"Configuring Linux-based Virtual Machines" on page 194

"Managing Virtual Machine Resources" on page 204

"Managing the Operation of a Virtual Machine" on page 198

Replacing a Virtual Machine from an OVF File

Replace a virtual machine (VM) from an Open Virtualization Format (OVF) file if you want to restore a VM on your everRun system by overwriting the VM with a previous backup copy. (If you want to import a VM from a different system, see the overview in "Creating and Migrating Virtual Machines" on page 127.)

Typically, importing a VM creates a new instance of the VM with unique hardware IDs. Restoring a VM creates an identical VM with the same SMBIOS UUID, system serial number, and MAC addresses, if

provided in the VM image, that your guest operating system and applications may require for software licensing. The hardware ID, though, of the restored VM is unique. If an identical VM already exists on the everRun system, restoring the VM allows you to replace the VM and overwrite it with your previous copy.

You can restore a VM that already exists on an everRun system only if you have previously created a VM snapshot (see "Creating a Snapshot" on page 220) and exported that snapshot (see "Exporting a Snapshot" on page 224) to OVF and Virtual Hard Disk (VHD) files on a supported network share. You must mount that network share on your management PC, and then open the everRun Availability Console on the target everRun system to restore the OVF and VHD files from your management PC.

> **Caution**: Consider backing up your existing VM on the everRun system before overwriting and restoring it. If you create and export another snapshot, ensure that you do not overwrite the OVF and VHD files that you want to restore.

Notes:

- The time required to restore a VM depends on the size and number of volumes in the source VM as well as network bandwidth. For example, transferring a VM with one 20 GB boot volume over a 1 Gb/s network may take about 30 minutes.

- If you overwrite and restore an existing VM, the everRun system removes the existing VM and its volumes, but the system does not remove any of the VM's snapshots or the volume containers in which the snapshots are stored. The volume containers continue to use storage space on your everRun system until you remove the VM's snapshots (see "Removing a Snapshot" on page 230). If storage space is limited, you may want to remove the snapshots before starting the restore process to ensure that there will be enough storage space for the operation.

- If you previously expanded the volume containers of your VM to allow enough space for snapshots, you may want to note the current size of each volume container before you overwrite and restore the VM. Because the everRun system creates all new volume containers for a restored VM and does not preserve the expanded container sizes, you need to manually expand the volume containers of the restored VM after the restore process is finished (see "Expanding a Volume Container on the everRun System" on page 213).

- If the everRun system switches from the primary PM to the secondary PM while restoring a VM, the restore process fails. This does not affect the continuous uptime of your system, but you must delete the incomplete VM and associated volumes on the everRun system, and restore them again.

Prerequisite: Both PMs of the everRun system must be online for the restore process to function properly.

To overwrite and restore a VM on the everRun system

1. Create and export a VM snapshot on the source everRun system. For more information, see "Managing Snapshots" on page 219.

2. On the management PC that you use to run the everRun Availability Console, do the following:

    a. Map the network share that contains the exported OVF and VHD files.

    b. Log on to the everRun Availability Console on the target everRun system.

3. On the **Physical Machines** page (see "The Physical Machines Page" on page 84), verify that both PMs are in the **running** state and that neither PM is in maintenance mode or in the process of synchronizing.

4. On the **Virtual Machines** page (see "The Virtual Machines Page" on page 88), select the VM that you want to restore from your previous backup copy.

5. Click **Restore** to open the restore wizard.

6. If prompted, allow the required Java plugins to load in your web browser. For information about enabling Java for the everRun Availability Console, see "Compatible Internet Browsers" on page 30.

7. Click **Browse**. In the file browser, locate the network share with the exported files. Select the **.ovf** file that you want to restore, and click **Restore**.

8. Confirm that you will overwrite the existing VM and data and proceed by clicking **Continue**.

> **Caution**: Restoring a VM overwrites all of its data and configuration details.

9. Review the information and make any desired edits, if necessary:

    ▪ **Name, CPU, and Memory**

       Change the name of the virtual machine, edit the number of vCPUs, or allocate the total memory it can use.

    ▪ **Storage**

       Shows all of the volumes. Select the **Create** box for a volume to allocate a storage container for the volume on the everRun system (the boot volume is required). Select the **Restore Data** box to import data for a volume from the VHD file.

    ▪ **Network**

       Displays all of the available networks. You can remove a network or add one that is not already allocated. A minimum of one network is required.

10. Optionally, clear the check box for **Auto start Virtual Machine after restore** if you need to repro-
    vision the VM before starting it for the first time.

11. Click **Restore** to begin restoring the VM. When the transfer is complete, click **Done** to close the
    restore wizard.

> ℹ️ **Note**: Restored volumes begin to appear on the **Volumes** page of the everRun Avail-
> ability Console while the restore process is still in progress. Do not attach or remove
> any of these restored volumes until the restore window reports that the process is com-
> plete; otherwise, the restore process fails.

12. If applicable, use the **Reprovision Virtual Machine** wizard to allocate additional resources to the
    VM, as described in "Reprovisioning Virtual Machine Resources" on page 204. Also, if you want to
    allocate additional space in each volume container for snapshots, see "Expanding a Volume Con-
    tainer on the everRun System" on page 213.

    When you are finished reprovisioning the VM, click **Start** to boot the VM.

After you verify that the restored VM is functioning properly, the restore process is complete; however, the
everRun system may continue to synchronize data between PMs to enable High Availability (HA) or Fault
Tolerant (FT) operation.

> ℹ️ **Note**: Your restored VM and its associated volumes may be marked with warning symbols
> until the data has been synchronized and the VirtIO drivers are running.

Troubleshooting

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

To clean up after a canceled or failed restore process

In the everRun Availability Console on the target system, remove the restored VM and any
volumes associated with the restored VM.

Related Topics

"Creating and Migrating Virtual Machines" on page 127

"Managing Virtual Machine Resources" on page 204

"Managing the Operation of a Virtual Machine" on page 198

Managing Windows Drive Labels

Label volumes in a Windows-based virtual machine to ensure that they are correctly mapped before you export the virtual machine or create a snapshot of it.

> ⚠ **Caution**: Ensure that each volume has a unique identifiable label before running **Sysprep** (to prepare for an export or snapshot). This process requires administrator privileges.

To set a label from the command prompt, type:

```
C:\>label C:c-drive
```

To list and verify all volume labels, use the **diskpart** utility:

```
C:\> diskpart

DISKPART> list volume

...

DISKPART> exit
```

After importing the virtual machine, use **Disk Manager** to reassign the drive letters. The labels you assigned before the export or snapshot will help to identify the drives. For instructions on reassigning drive letters on a Windows system, search for the Microsoft Support web site.

Related Topics

"Creating and Migrating Virtual Machines" on page 127

"Configuring Windows-based Virtual Machines" on page 190

"Managing Snapshots" on page 219

Configuring Windows-based Virtual Machines

After installing a Windows-based virtual machine, configure the additional resources and software necessary for production use, as described in:

- "Creating and Initializing a Disk (Windows-based VMs)" on page 191

- "Installing Applications (Windows-based VMs)" on page 192

If you plan to create VM snapshots (see "Managing Snapshots" on page 219), consider installing the QEMU guest agent and configuring the Microsoft Shadow Volume Copy Service (VSS), as described in:

- "Installing the QEMU Guest Agent for Application-Consistent Snapshots (Windows-based VMs)" on page 192

In addition, ensure that you configure the following settings:

- Change the time zone in the guest operating system to correspond to the time zone configured on the **Date and Time** preference page in the everRun Availability Console (see "Configuring Date and Time" on page 70); otherwise, the VM's time zone changes whenever VMs restart or migrate. Network Time Protocol (NTP) is recommended for both the VM and the everRun system.

- Disable hibernation (enabled by default in some cases) to prevent the guest operating system from going into a power-saving state.

- Configure the power button action in the guest operating system to shut down the guest (and not to hibernate it) to allow the **Shutdown** VM button in the everRun Availability Console to work properly (see "Shutting Down a Virtual Machine" on page 198).

> **Note**: For Disaster Recovery (DR)-protected VMs, ensure that you configure the power button action in the guest operating system to shut down the guest. 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.

- Configure the guest operating system to generate a crash dump file if the operating system crashes. Follow the instructions in the Microsoft article, *How to generate a complete crash dump file or a kernel crash dump file by using an NMI on a Windows-based system* (Article ID: 927069). Follow the instructions in the **More Information** section.

Related Topics

"Managing Virtual Machines" on page 121

Creating and Initializing a Disk (Windows-based VMs)

Create and initialize a disk to prepare it for partitioning into volumes in a Windows-based virtual machine.

To create and initialize a disk in a Windows-based virtual machine

1. Use the everRun Availability Console to create a new volume in a storage group on the everRun system, as described in "Creating a Volume in a Virtual Machine" on page 207.

2. In the Windows guest operating system, open **Disk Management** or a similar utility.

3. Initialize the newly-added disk. (You may be prompted to do so automatically.)

4. Convert the disk to a dynamic disk.

5. Create one or more simple volumes on the disk.

6. Restart the Windows guest operating system.

See your Windows documentation for complete instructions.

> **Note**: Because the everRun software already mirrors data at the physical level, volume redundancy is not required in the Windows guest operating system.

Related Topics

"Opening a Virtual Machine Console Session" on page 200

"Configuring Windows-based Virtual Machines" on page 190

"Creating and Migrating Virtual Machines" on page 127

"Managing the Operation of a Virtual Machine" on page 198

Installing Applications (Windows-based VMs)

Install an application in a Windows-based virtual machine over the network. For example, map a network share that contains the installation program or download the installation program to the guest operating system as an executable file or ISO file.

> **Note**: You cannot use virtual CDs to install applications.

Related Topics

"Opening a Virtual Machine Console Session" on page 200

"Configuring Windows-based Virtual Machines" on page 190

"Creating and Migrating Virtual Machines" on page 127

"Managing the Operation of a Virtual Machine" on page 198

Installing the QEMU Guest Agent for Application-Consistent Snapshots (Windows-based VMs)

Install the Quick EMUlator (QEMU) guest agent in your Windows-based guest operating system if you want to create application-consistent snapshots of your virtual machine (VM). For an overview of everRun snapshots, see "Managing Snapshots" on page 219.

Typically, while applications are running, they process transactions, open and write files, hold information in memory, and more. If you take a VM snapshot while your applications are still working, it is similar to restarting your system after a power outage. Although most modern file systems are designed to recover from this type of outage, it is possible that some data will be corrupted or lost in the process, especially while transaction-intensive applications are running. In this case, taking a snapshot without preparing your applications results in a *crash-consistent* snapshot, as if you took the snapshot after a crash or power outage.

Microsoft Windows provides the Volume Shadow Copy Service (VSS) that can inform the file system and your applications when they must temporarily *quiesce* or freeze their operations during a snapshot or backup. If your applications support VSS, the everRun software can signal your applications through the QEMU guest agent and VSS to quiesce during a user or Disaster Recovery (DR) snapshot on your everRun system, thus ensuring an application-consistent snapshot.

> **Caution**: Before installing the QEMU guest agent, contact your application vendor(s) to determine if they support Microsoft VSS and if any additional configuration steps are necessary to support VSS operations. You can create application-consistent snapshots only if your applications support VSS and the QEMU guest agent is properly installed and running.

> **Notes**:
>
> - By default, all snapshots are considered crash-consistent snapshots unless you install the QEMU guest agent and explicitly configure your applications to quiesce when signaled by Microsoft VSS.
>
> - When you install the QEMU guest agent, you may need to restart your VMs. If your VMs are in use, schedule a maintenance period for this procedure.

To install the QEMU guest agent

1. Log on to the everRun system with the everRun Availability Console.

2. Select a VM on the **Virtual Machines** page.

3. Click **Console** and log on to the Windows guest operating system.

4. To transfer the QEMU guest agent installer to your system, do one of the following:

   ▪ Open a web browser and download the installer from the **Drivers and Tools** section of the **Downloads** page at http://www.stratus.com/go/support/everrun.

   ▪ Mount a local network share that contains the installer and either copy it to your system or prepare to run it from the share.

5. Start the installer by double-clicking the icon. The QEMU Guest Agent Setup wizard is displayed.

6. Read the license information. If appropriate, click the check box next to **I agree to the license terms and conditions**.

7. Click **Install** to begin the software installation.

8. If Windows prompts that it cannot verify the publisher of the driver software, click **Install** to continue installing the software.

9. If prompted, click **Restart** to restart the guest operating system.

   When Windows restarts, you may see a message indicating that the driver software was installed.

10. If prompted, click **Restart** to restart the guest operating system again.

To verify that the QEMU guest agent is properly installed and running

Open **Services**. For example, click **Start** and **Run**, then type **services.msc** and click **Run**. Verify that the following services are present and running:

- QEMU Guest Agent (always runs)

- QEMU Guest Agent VSS Provider (may run only during quiesce)

Open **Device Manager**. For example, click **Start**, **Control Panel**, **Hardware**, and **Device Manager**. Verify that the following driver is installed and running:

- VirtIO Serial Driver (under System devices)

Related Topics

"Configuring Windows-based Virtual Machines" on page 190

"Creating and Migrating Virtual Machines" on page 127

"Managing the Operation of a Virtual Machine" on page 198

Configuring Linux-based Virtual Machines

After installing a Linux-based virtual machine, configure the additional resources and software necessary for production use, as described in:

- "Creating and Initializing a Disk (Linux-based VMs)" on page 196

- "Installing Applications (Linux-based VMs)" on page 196

If you plan to create VM snapshots (see "Managing Snapshots" on page 219), consider installing the QEMU guest agent, as described in:

- "Installing the QEMU Guest Agent for Application-Consistent Snapshots (Linux-based VMs)" on page 197

In addition, ensure that you configure the following settings:

- Disable hibernation (enabled by default in some cases) to prevent the guest operating system from going into a power-saving state.

- Configure the power button action in the guest operating system to shut down the guest (and not to hibernate it) to allow the **Shutdown** VM button in the everRun Availability Console to work properly. For the minimal server version of **Ubuntu Linux**, optionally install the `acpid` package to enable the **Shutdown** button. See "Shutting Down a Virtual Machine" on page 198.

> **Note**: For Disaster Recovery (DR)-protected VMs, ensure that you configure the power button action in the guest operating system to shut down the guest. 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.

- Install the `kexec-tools` package and configure the guest operating system to generate a crash dump file if the system crashes.

- For **Ubuntu Linux** guest operating systems, to prevent a problem where the VM console hangs in everRun Availability Console, edit the `/boot/grub/grub.cfg` file and change the `gfxmode` parameter to `text` (for example, `set gfxmode=text`). If the VM console hangs before you can set the parameter, see the troubleshooting information in "Opening a Virtual Machine Console Session" on page 200 to resolve the issue.

For more information about these settings, see your Linux documentation.

Related Topics

Creating and Initializing a Disk (Linux-based VMs)

Create and initialize a disk to make it available for storing data in a Linux-based virtual machine.

To create and initialize a disk in a Linux-based virtual machine

1. In the everRun Availability Console, create a new volume in a storage group, as described in "Creating a Volume in a Virtual Machine" on page 207.

2. In the Linux-based virtual machine, use the volume management tool or edit files as needed to initialize and mount the volume. See your Linux documentation for complete instructions.

The disk device names for a Linux-based virtual machine are `/dev/vda` through `/dev/vdh`, not the standard `/dev/sda` through `/dev/sdh`. The everRun virtual disk volumes appear in the guest operating system and are used as if they were physical disks.

Related Topics

"Opening a Virtual Machine Console Session" on page 200

"Configuring Linux-based Virtual Machines" on page 194

"Creating and Migrating Virtual Machines" on page 127

"Managing the Operation of a Virtual Machine" on page 198

Installing Applications (Linux-based VMs)

Install an application in a Linux-based virtual machine over the network. For example, mount a network drive that contains the installation package or download the installation package to the guest operating system as an executable file or ISO file.

> **Note**: You cannot use virtual CDs (VCDs) to install applications.

Related Topics

"Opening a Virtual Machine Console Session" on page 200

"Configuring Linux-based Virtual Machines" on page 194

"Creating and Migrating Virtual Machines" on page 127

"Managing the Operation of a Virtual Machine" on page 198

Installing the QEMU Guest Agent for Application-Consistent Snapshots (Linux-based VMs)

Install the Quick EMUlator (QEMU) guest agent in your Linux-based guest operating system if you want to create application-consistent snapshots of your virtual machine (VM). For an overview of everRun snapshots, see "Managing Snapshots" on page 219.

Typically, while applications are running, they process transactions, open and write files, hold information in memory, and more. If you take a VM snapshot while your applications are still working, it is similar to restarting your system after a power outage. Although most modern file systems are designed to recover from this type of outage, it is possible that some data will be corrupted or lost in the process, especially for transaction-intensive applications. In this case, taking a snapshot without preparing your applications results in a *crash-consistent* snapshot, as if you took the snapshot after a power outage.

If your applications support QEMU signaling, the everRun software can signal your applications through the QEMU guest agent to ensure that your applications *quiesce* or freeze during a user or Disaster Recovery (DR) snapshot on your everRun system, thus ensuring an application-consistent snapshot.

Most Linux distributions already include a QEMU guest agent (usually in the `qemu-guest-agent` package). For information about installing and configuring the QEMU guest agent, see the documentation for your particular Linux distribution.

> **Caution**: Before installing a QEMU guest agent, contact your application vendor(s) to determine if they support QEMU signaling and if any additional configuration steps are necessary to quiesce your applications. You can create application-consistent snapshots only if your applications support QEMU signaling and the QEMU guest agent is properly installed and running.

> **Notes**:
>
> - By default, all snapshots are considered crash-consistent snapshots unless you explicitly install the QEMU guest agent and configure your applications to quiesce when signaled by the everRun software.
>
> - When you install the QEMU guest agent, you may need to restart your VMs. If your VMs are use, schedule a maintenance period for the installation.

Related Topics

"Configuring Linux-based Virtual Machines" on page 194

"Creating and Migrating Virtual Machines" on page 127

Managing the Operation of a Virtual Machine

Manage the operation of a virtual machine as described in:

- "Starting a Virtual Machine" on page 198

- "Shutting Down a Virtual Machine" on page 198

- "Powering Off a Virtual Machine" on page 200

- "Opening a Virtual Machine Console Session" on page 200

- "Renaming a Virtual Machine" on page 202

- "Removing a Virtual Machine" on page 202

For additional information configuration and troubleshooting information, see "Advanced Topics (Virtual Machines)" on page 231.

Starting a Virtual Machine

Start a virtual machine (VM) to boot the VM's guest operating system.

To start a virtual machine

1. On the **Virtual Machines** page, select a VM.

2. Click **Start**.

Related Topics

"Shutting Down a Virtual Machine" on page 198

"Powering Off a Virtual Machine" on page 200

"Managing the Operation of a Virtual Machine" on page 198

Shutting Down a Virtual Machine

Shut down a virtual machine (VM) to begin an orderly shutdown of the guest operating system.

> ℹ️ **Note**: You can shut down a VM with guest operating system commands. Some guests allow (or can be configured to allow) you to shut down a VM using the everRun Availability Console.

To shut down a VM in everRun Availability Console

1. On the **Virtual Machines** page, select a VM.

2. Click **Shutdown**.

   A warning message appears, asking you to confirm the shutdown. Click **Yes** to shutdown or **No** to discontinue the shutdown.

If the VM is not responding, you can also **Power Off** the VM to stop it without properly shutting down the guest operating system.

Shutting down a VM in the everRun Availability Console is similar to pressing the power button on a physical machine, which typically results in an orderly shutdown of the operating system. In some cases, you may need to explicitly enable this feature in the guest operating system. For example:

- For any guest, verify that the power button action is set to shut down the guest operating system and not to hibernate it. If you click **Shutdown** in the everRun Availability Console for a guest that is set to hibernate, the VM remains in a **stopping** state and never properly shuts down.

- On some guests, the power button does not shut down the system unless a user is logged on to the operating system. You may be able to update security settings to enable the power button even in the absence of a login session.

- On some minimal server versions of Ubuntu Linux, the `acpid` package that enables the power button is not included in the default installation. You can manually install this package to enable the power button.

> **Note**: For Disaster Recovery (DR)-protected VMs, ensure that you configure the power button action in the guest operating system to shut down the guest. 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.

See the documentation for your guest operating system to configure the behavior of the system power button, thus enabling the **Shutdown** button to work in the everRun Availability Console.

Related Topics

"Starting a Virtual Machine" on page 198

"Powering Off a Virtual Machine" on page 200

"Managing the Operation of a Virtual Machine" on page 198

Powering Off a Virtual Machine

Power off a virtual machine (VM) to stop it without properly shutting down guest operating system.

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

To power off a virtual machine

1. On the **Virtual Machines** page, select a VM.

2. Click **Power Off**.

Related Topics

Opening a Virtual Machine Console Session

Open a virtual machine (VM) console 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 everRun Availability Console, but you can also use a remote desktop application for this purpose.

To open a VM console

1. On the **Virtual Machines** page, select a VM.

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 for the everRun Availability Console, see "Compatible Internet Browsers" on page 30.

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 in the everRun Availability Console if you do not properly set the `gfxmode` parameter. In the guest operating system, edit the `/boot/grub/grub.cfg` file and change the `gfxmode` 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 in the everRun Availability Console.

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 in everRun Availability 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.

Related Topics

Renaming a Virtual Machine

Rename a virtual machine (VM) to change its name as it appears on the **Virtual Machines** page.

If you need to change the host name of the guest operating system running in a VM, use guest operating system tools.

To rename a virtual machine

1. On the **Virtual Machines** page, select a VM.

2. Double-click the name of the VM.

3. Type the new name and press **Enter**.

Related Topics

Removing a Virtual Machine

Remove a virtual machine (VM) to permanently delete it and optionally delete associated volumes from the everRun system.

> **Notes**:
>
> - When you remove a VM, any snapshots associated with the VM and the volume containers in which the snapshots are stored remain on the everRun system. To remove a VM snapshot and all of its associated volume snapshots, see "Removing a Snapshot" on page 230.
>
> - When all volume and volume snapshot contents have been removed from a volume container, the system automatically removes the container from the system, which frees up space in the storage group.

> **Prerequisite**: Both PMs of the everRun system must be online to properly remove a VM. On the **Physical Machines** page of the everRun Availability Console, verify that both PMs are in the **running** state and that neither PM is in maintenance mode or in the process of synchronizing.

To remove a virtual machine

1. On the **Virtual Machines** page, select a VM.

2. Click **Shutdown**.

3. When the VM has stopped, click **Remove**.

4. In the **Remove Virtual Machine** dialog box, activate the check box next to volumes that you want to delete. Clear the check box for volumes to save as archives or save for attachment to another VM.

   > **Caution**: Make sure that you select the correct VM and volumes for removal. When you click **Delete VM**, these items are permanently removed.

5. Click **Delete VM** to permanently delete the VM and any selected volumes.

Related Topics

"Renaming a Virtual Machine" on page 202

"Creating and Migrating Virtual Machines" on page 127

Managing Virtual Machine Resources

Manage virtual machine resources to reconfigure the vCPUs, memory, storage, or network resources of an existing virtual machine.

To reconfigure virtual machine resources, use the **Reprovision Virtual Machine** wizard, as described in:

- "Reprovisioning Virtual Machine Resources" on page 204

To reconfigure virtual machine volumes, see the following task-specific topics:

- "Creating a Volume in a Virtual Machine" on page 207

- "Attaching a Volume to a Virtual Machine" on page 208

- "Detaching a Volume from a Virtual Machine" on page 210

- "Removing a Volume from a Virtual Machine" on page 211

- "Expanding a Volume Container on the everRun System" on page 213

To recover virtual machine resources, freeing space for new volumes or virtual CDs, see:

- "Recovering Virtual Machine Resources" on page 214

Reprovisioning Virtual Machine Resources

Reprovision a virtual machine (VM) to change its allocation of virtual CPUs (vCPUs), memory, storage, or network resources.

Launch the **Reprovision Virtual Machine** wizard by clicking **Config** in the bottom pane of the **Virtual Machines** page. The wizard steps you through the process of reallocating resources to the VM.

> **Prerequisites**:
>
> - Review the prerequisites and considerations for allocating vCPUs, memory, storage, and network resources to the VM, as listed in "Planning Virtual Machine Resources" on page 122. For more information about storage resources, see "Planning Virtual Machine Storage" on page 125.
>
> - To reprovision a VM, you must shut down the VM.

> **Note**: You cannot reprovision a VM while it is protected with Disaster Recovery. If necessary, you can unprotect the VM, reprovision it, and then protect it again.

To reprovision a virtual machine

1. Open the **Virtual Machines** page (see "The Virtual Machines Page" on page 88).

2. Select a VM and click **Shutdown**.

3. When the VM has stopped, click **Config** to display the **Reprovision Virtual Machine** wizard.

4. On the **Name, Description, and Protection** page:

   a. Type the **Name** and an optional **Description** for the VM as they will appear in the everRun Availability Console.

   b. Select the level of protection to use for the VM:

      ○ **Fault Tolerant (FT)**

      ○ **High Availability (HA)**

      For information about these levels of protection, see "Creating a New Virtual Machine" on page 128 and "Modes of Operation" on page 11.

   c. Click **Next**.

5. On the **vCPUs and Memory** page:

   a. Specify the number of **vCPUs** and the amount of **Memory** to assign to the VM. For more information, see "Planning Virtual Machine vCPUs" on page 122 and "Planning Virtual Machine Memory" on page 124.

   b. Click **Next**.

6. On the **Volumes** page, you can:

   > **Notes**:
   >
   > - You cannot modify the VM boot volume, only data volumes
   >
   > - To expand a volume container, see "Expanding a Volume Container on the everRun System" on page 213.

- Click **Detach** to disconnect a volume from a VM and keep it for future use.

- Click **Delete** to permanently remove a volume from the everRunsystem.

- Select an unattached volume from a pulldown menu (if displayed) and click **Attach**.

- Add a new volume:

    a. Type the **Name** of the boot volume.

    b. Type the **Container Size** and **Volume Size** of the volume in gigabytes (GB). The container size is the total size for the volume including extra space to store snapshots. The volume size is the portion of the container that is available to the guest operating system. For more information about allocating storage, see "Sizing Volume Containers" on page 16 and"Planning Virtual Machine Storage" on page 125.

    c. If applicable, click **Add New Volume** to create a new data volume. (If the button is not visible, scroll down to the bottom of the wizard page.) Specify the parameters for the new volume.

    d. If applicable, click **Attach** to connect a volume to a VM.

    To continue, click **Next**.

7. On the **Networks** page, activate the check box for each shared network that you want to attach to the VM.

    For each shared network that you attach, you can also optionally:

    - Set a custom MAC address (for details, see "Assigning a Specific MAC Address to a Virtual Machine" on page 231).

    - Set the **State** to **Enabled** or **Disabled**, which allows you to allow or block network traffic to the selected network.

    For more information, see "Planning Virtual Machine Networks" on page 126. To continue, click **Next**.

8. On the **Configuration Summary** page:

    > **Caution**: Make sure that any volumes marked for removal are correct. When you click **Finish**, permanent data loss occurs on disks marked for removal.

    a. Review the configuration summary. If you need to make changes, click **Back**.

    b. To accept the VM as provisioned, click **Finish**.

9. Click **Start** to restart the VM.

10. For Windows-based VMs, if you changed the number of assigned virtual CPUs in a Windows-based VM from 1 to *n* or or *n* to 1, after restarting the VM at the end of the re-provisioning process you must shut down and restart the VM a second time. This allows the VM to correctly reconfigure itself for Symmetric Multiprocessing (SMP). The VM displays odd behavior and is not usable until it is restarted.

Related Topics

"Managing Virtual Machine Resources" on page 204

"Planning Virtual Machine Resources" on page 122

"Managing Virtual Machines" on page 121

Creating a Volume in a Virtual Machine

Create a volume to attach a new, blank volume to a virtual machine (VM). (You can also attach an existing, unattached volume as described in "Attaching a Volume to a Virtual Machine" on page 208.)

> ℹ **Note**: You cannot create a volume for a VM if the VM is protected with Disaster Recovery. If necessary, you can unprotect the VM, create the volume, and then protect the VM again.

> ✅ **Prerequisite**: Before creating a volume for a VM, you must shut down the VM.

To create a new volume in a VM

1. Open the **Virtual Machines** page (see "The Virtual Machines Page" on page 88).

2. Select a VM and click **Shutdown**.

3. When the VM has stopped, click **Config** to display the **Reprovision Virtual Machine** wizard.

4. Click **Next** on each wizard page until the **Volumes** page is displayed. (If applicable, see "Reprovisioning Virtual Machine Resources" on page 204 to configure additional VM resources.)

5. On the **Volumes** page, click **Add a new volume**. (If the button is not visible, scroll down to the bottom of the wizard page.)

6. Under **To Be Created**, do the following:

   a. Type the **Name** of the volume as it will appear in the everRun Availability Console.

   b. Type the **Container Size** and **Volume Size** of the volume to create in gigabytes (GB). The container size is the total size for the volume including extra space to store snapshots. The volume size is the portion of the container that is available to the guest operating system. For more information about allocating storage, see "Sizing Volume Containers" on page 16 and "Planning Virtual Machine Storage" on page 125.

   c. Select the **Disk Image** format:

      ■ **RAW** – raw disk format

      ■ **QCOW2** – QEMU Copy On Write (QCOW2) format, which supports snapshots and Disaster Recovery

   d. Select the **Storage Group** in which to create the volume.

7. Click **Next** on each wizard page until the **Configuration Summary** page is displayed. Verify the configuration changes.

8. Click **Finish** to create the volume.

9. Start the VM and prepare the volume for use in the Windows or Linux guest operating system, as described in:

   ■ "Creating and Initializing a Disk (Windows-based VMs)" on page 191

   ■ "Creating and Initializing a Disk (Linux-based VMs)" on page 196

Related Topics

"Detaching a Volume from a Virtual Machine" on page 210

"Removing a Volume from a Virtual Machine" on page 211

"Managing Virtual Machine Resources" on page 204

"Planning Virtual Machine Resources" on page 122

"Managing Virtual Machines" on page 121

Attaching a Volume to a Virtual Machine

Attach a volume to connect a currently unused volume to a virtual machine.

Note: You cannot attach a volume to a VM if the VM is protected with Disaster Recovery. If necessary, you can unprotect the VM, attach the volume, and then protect the VM again.

Prerequisite: Before attaching a volume to a virtual machine, you must shut down the virtual machine.

To attach a volume to a virtual machine

1. Ensure that the volume you want to attach is not in use by another virtual machine; otherwise, you cannot attach it. Open the **Volumes** page, locate the volume, and ensure that the value in the **Used By** column is **None**.

2. Open the **Virtual Machines** page (see "The Virtual Machines Page" on page 88).

3. Select a VM and click **Shutdown**.

4. When the VM has stopped, click **Config** to display the **Reprovision Virtual Machine** wizard.

5. Click **Next** on each wizard page until the **Volumes** page is displayed. (If applicable, see "Reprovisioning Virtual Machine Resources" on page 204 to configure additional VM resources.)

6. On the **Volumes** page, locate the pulldown menu next to the **Add a new volume** button. Select an unattached volume from the pulldown menu and click **Attach**.

   (If the pulldown menu is not visible, scroll down to the bottom of the wizard page. The pulldown menu is displayed only if there are unattached volumes on the everRun system.)

7. Click **Next** on each wizard page until the **Configuration Summary** page is displayed. Verify the configuration changes.

8. Click **Finish** to attach the selected volume.

Related Topics

"Creating a Volume in a Virtual Machine" on page 207

"Detaching a Volume from a Virtual Machine" on page 210

"Removing a Volume from a Virtual Machine" on page 211

"Managing Virtual Machine Resources" on page 204

"Planning Virtual Machine Resources" on page 122

"Managing Virtual Machines" on page 121

Detaching a Volume from a Virtual Machine

Detach a volume to disconnect it from a virtual machine and keep it for future use. (You can also per-manently delete the volume from the everRun system, as described in "Removing a Volume from a Virtual Machine" on page 211.)

> **Notes**:
>
> - When you detach a volume from a VM, both the volume and its volume container exist separately from the VM. They remain on the system even if you remove the VM.
>
> - If you decide to remove the volume, and you also want to remove its volume container to reclaim space in the storage group, you must remove any snapshots stored in the volume container; otherwise, the volume container remains on the system. For more information, see "Removing a Volume from a Virtual Machine" on page 211.
>
> - You cannot detach a volume from a VM that is protected with Disaster Recovery. If necessary, you can unprotect the VM, detach the volume, and then protect the VM again.

> **Prerequisite**: Before detaching a volume from a virtual machine, you must shut down the vir-tual machine.

To detach a volume from a virtual machine

1. Open the **Virtual Machines** page (see "The Virtual Machines Page" on page 88).

2. Select a VM and click **Shutdown**.

3. When the VM has stopped, click **Config** to display the **Reprovision Virtual Machine** wizard.

4. Click **Next** on each wizard page until the **Volumes** page is displayed. (If applicable, see "Repro-visioning Virtual Machine Resources" on page 204 to configure additional VM resources.)

5. On the **Volumes** page, locate the volume to detach. (If the volume is not visible, scroll down on the wizard page.)

6. Click **Detach** beside the volume name to mark the volume for detachment.

> ⚠️ **Caution**: Be careful to mark the correct volume to detach, avoiding any volumes that are currently in use.

7. Click **Next** on each wizard page until the **Configuration Summary** page is displayed. Verify the configuration changes.

8. Click **Finish** to detach the selected volume.

Related Topics

Removing a Volume from a Virtual Machine

Remove a virtual machine (VM) volume to permanently delete it from the everRun system. (You can also detach a volume from the VM but keep it for future use, as described in .)

> 🛈 **Notes**:
>
> - If you remove a volume, and you also want to remove its volume container to reclaim space in the storage group, you must remove any volume snapshots stored in the volume container; otherwise, the container remains on the system. To remove a VM snapshot and all of its associated volume snapshots, see .
>
> - When all volume and volume snapshot contents have been removed from a volume container, the system automatically removes the container from the system, which frees up space in the storage group.
>
> - You cannot remove a volume that is attached to a VM if the VM is protected with Disaster Recovery. If necessary, you can unprotect the VM, remove the volume, and then protect the VM again.

> ✓ **Prerequisite**: Before removing a volume attached to a virtual machine, you must shut down the virtual machine.

To remove a volume that is attached to a virtual machine

1. Open the **Virtual Machines** page (see "The Virtual Machines Page" on page 88).

2. Select a VM and click **Shutdown**.

3. When the VM has stopped, click **Config** to display the **Reprovision Virtual Machine** wizard.

4. Click **Next** on each wizard page until the **Volumes** page is displayed. (If applicable, see "Reprovisioning Virtual Machine Resources" on page 204 to configure additional VM resources.)

5. On the **Volumes** page, locate the volume to delete. (If the volume is not visible, scroll down on the wizard page.)

6. Click **Delete** beside the volume name to mark the volume for deletion.

> ⚠ **Caution**: Be careful to mark the correct volume to remove, avoiding any volumes that are currently in use.

7. Click **Next** on each wizard page until the **Configuration Summary** page is displayed. Verify the configuration changes.

8. Click **Finish** to permanently delete the selected volume.

To remove an unattached volume

> ⚠ **Caution**: Before removing a volume, ensure that it is no longer needed by other administrators.

1. Open the **Volumes** page.

2. Select an unattached volume. (The **VM** column must read **None**, otherwise, the **Remove** button is not displayed.)

3. Click **Remove**.

Related Topics

Renaming a Volume on the everRun System

Rename a volume on the everRun system to change its name as it appears on the **Volumes** page.

If you need to change the name of a disk or volume in the guest operating system running in a virtual machine, use guest operating system tools.

To rename a volume on the everRun system

1. Locate the volume on the **Volumes** page.

2. Double-click the name of the volume.

3. Specify the new name and press **Enter**.

Related Topics

Expanding a Volume Container on the everRun System

Expand a virtual machine (VM) volume container to allocate more space in the container for snapshots or for the guest operating system volume. (Expand the portion of a volume container that is available to the guest operating system by executing the "volume-resize" on page 403 command in the everRun host operating system.)

You can expand the volume container, but you cannot reduce the size of a container. Use the following procedure to expand a volume container whether the VM is running or stopped. To estimate the amount of storage to allocate to a volume container, see "Sizing Volume Containers" on page 16.

> **Prerequisite**: Ensure that both PMs of the everRun system are online; otherwise, the system cannot properly expand a volume container.

To expand a volume container

1. On the **Physical Machines** page (see "The Physical Machines Page" on page 84), verify that both PMs are in the **running** state and that neither PM is in maintenance mode or in the process of synchronizing.

2. On the **Volumes** page (see "The Volumes Page" on page 93), click **Expand Container**.

3. Next to **Expand By**, type the amount of storage space to add to the volume container (in gigabytes (GB)). When you type the number, the dialog box displays the **Expanded Container Size** that will result if you complete the operation.

    > **Note**: Consider the **Expand By** entry carefully, because after expanding a container, you cannot undo the change or reduce the size of the volume container; you can only expand the volume further.

4. Click **Expand Container** to commit the change and expand the container. The dialog box displays the expansion progress and automatically closes when the operation is complete.

Related Topics

"Creating a Volume in a Virtual Machine" on page 207

"Detaching a Volume from a Virtual Machine" on page 210

"Removing a Volume from a Virtual Machine" on page 211

"Managing Virtual Machine Resources" on page 204

"Planning Virtual Machine Resources" on page 122

"Managing Virtual Machines" on page 121

Recovering Virtual Machine Resources

To conserve storage space, remove VM resources when they are no longer needed. You may also need to immediately recover storage space when there is insufficient space for certain tasks, such as creating a volume or VCD.

To recover storage space, remove unused resources as described in the following topics:

- "Removing a Virtual Machine" on page 202

- "Removing a Volume from a Virtual Machine" on page 211

- "Removing a Virtual CD" on page 219

You can also remove unused snapshots from a VM to free space for new snapshots on an existing volume, but doing so does not recover storage space for new volumes or VCDs:

- "Removing a Snapshot" on page 230

Related Topics

"Managing Virtual Machine Resources" on page 204

"Planning Virtual Machine Resources" on page 122

"Managing Virtual Machines" on page 121

Managing Virtual CDs

Create and manage virtual CDs (VCDs) to make software installation media available to the virtual machines on your everRun system in ISO format.

A VCD is a read-only ISO image file that resides on a storage device of the everRun system. Use the **Virtual CD Creation Wizard** (in everRun Availability Console) to upload an existing ISO file, as described in "Creating a Virtual CD" on page 216.

After you create a VCD, you can boot from it to install a Windows or Linux guest operating system, or start a VM from a bootable recovery VCD.

> **Note**: To ensure continuous uptime, the everRun software prevents you from inserting a VCD after guest installation because it would prevent the system from migrating VMs in the event of a failure. However, you can still boot a virtual machine from a VCD for troubleshooting purposes.

You manage VCDs as described in:

Creating a Virtual CD

Create a virtual CD (VCD) to make software installation media available to the virtual machines (VM) on your everRun system.

To create a VCD, use the **Virtual CD Creation Wizard** to upload or copy an ISO file to a storage device on the everRun system. Thereafter, you can boot from it (see "Booting from a Virtual CD" on page 218) to install a guest operating system or start a VM from a bootable recovery VCD..

> **Notes**:
>
> 1. You cannot use VCDs to install applications in virtual machine. If necessary, mount a network drive or ISO image in the guest operating system to access application media.
>
> 2. Each VCD consumes disk space in the storage group in which it is stored. Unless you use a VCD on a regular basis, remove it when it is no longer needed.
>
> 3. If you create a bootable VCD for installation, it must be a single CD or DVD. Multiple CDs or DVDs are not supported.

To create a VCD

1. If necessary, create ISO files of any physical media for which you will create VCDs.

2. Open the **Virtual CDs** page in the everRun Availability Console.

3. Click **Create VCD** to open the **Virtual CD Creation Wizard**.

4. In the wizard, select a storage group with sufficient free space for the VCD.

5. Type a name for the VCD.

6. Select a source for the VCD:

- **Upload ISO file** uploads a file from your remote system running the everRun Availability Console.

- **Copy CD ISO from network source** copies the file from a Web URL.

7. If you selected **Upload ISO file**, click **Next** and select the ISO file to upload.

8. Click **Finish** to upload or copy the ISO file from the specified source.

The **Virtual CD Creation Wizard** reports that the VCD has been successfully added, but transferring the image may take several more minutes depending on the size of the image.

You can determine the status of a VCD by checking the **State** column on the **Virtual CDs** page:

- A syncing icon ( ) indicates that the VCD is still being created.

- A broken icon ( ) indicates that the VCD creation failed. Remove the VCD and try creating it again.

- A normal icon ( ) indicates that the transfer is complete and that the VCD is ready to use.

Related Topics

"Burning a CD or DVD for a Virtual CD" on page 217

"Managing Virtual CDs" on page 215

"Creating and Migrating Virtual Machines" on page 127

Burning a CD or DVD for a Virtual CD

If you need to burn a physical CD or DVD that you will subsequently use to create a virtual CD on the ever-Run system (see "Creating a Virtual CD" on page 216), note the following guidelines:

- Use only media-burning software and CD-R or DVD-R media and drives that support the Disk At Once (DAO) method. Using software that defaults to DAO mode, like ImgBurn from http://img-burn.com/, provides more assurance that you will use DAO mode.

- Always use new media.

- To minimize the probability of having buffer under-runs during the burn process, download the ISO image to the same computer on which you are burning the media.

- Always verify the newly burned disc. You can use the verification feature of your media-burning software.

Related Topics

Booting from a Virtual CD

Boot a virtual machine from a virtual CD (VCD) to install a guest operating system or to perform maintenance.

Before booting from a VCD, you must shut down the virtual machine.

To boot a virtual machine from a VCD

1. If necessary, create a VCD from a bootable CD/DVD (see "Creating a Virtual CD" on page 216).

2. On the **Virtual Machines** page, select a virtual machine.

3. If the virtual machine is running, click **Shutdown**.

4. When the virtual machine status shows **stopped**, click **Boot from CD** in the lower pane.

5. Select the bootable VCD, then click **Boot**.

> **Note**: A Windows-based virtual machine booted from a VCD boots as a hardware virtual machine (HVM), and it can access only the first three disk volumes.

Related Topics

Renaming a Virtual CD

Rename a virtual CD (VCD) to change its name as it appears on the **Virtual CDs** page.

To rename a VCD

1. Locate the VCD on the **Virtual CDs** page.

2. Double-click the name of the VCD.

3. Specify the new name and press **Enter**.

Related Topics

Removing a Virtual CD

Remove a virtual CD (VCD) to permanently delete it from the everRun system.

To remove a VCD

1. In the everRun Availability Console, click **Virtual CDs**.

2. Locate the VCD you want to remove in the list.

3. Ensure that the **Can Remove** column displays **Yes** for the VCD. If the value is **No**, the VCD is currently in use.

4. Select the VCD and click **Remove** in the lower panel.

Related Topics

Managing Snapshots

Snapshots allow you to save an image of a virtual machine (VM) at a particular point in time. If you export a snapshot, you can use the exported files to import the VM to another system or back to the same everRun system to restore or duplicate the original VM.

> **Notes**:
>
> - You cannot revert to a snapshot or create a VM directly from a snapshot. You can create VM snapshots only to export files that you use to restore or duplicate the original VM.
>
> - When you create a VM snapshot, all volumes attached to the VM are automatically included in the snapshot; however, you can exclude volumes if you export the snapshot to another system. You cannot create individual volume snapshots.

You manage snapshots as described in:

- "Creating a Snapshot" on page 220

- "Exporting a Snapshot" on page 224

- "Removing a Snapshot" on page 230

To view the snapshots that you have created in the everRun Availability Console:

- Open the **Snapshots** page (see "The Snapshots Page" on page 93)

- On the **Virtual Machines** page (see "The Virtual Machines Page" on page 88), click a VM and click the **Snapshots** tab.

When you create a VM snapshot, the everRun system saves a snapshot image that includes any data that has changed in the VM since the previous snapshot, or, if no snapshots exist, since you originally created the VM. Because each snapshot contains only the changed data, some snapshots may take a small amount of storage space, and other snapshots may take more space depending on the level of VM activity and the amount of time that has passed since the previous snapshot.

Because snapshots are stored in the volume containers for each volume, ensure that you reserve enough storage space in the volume container for each volume you want to include in your VM snapshots, as described in "Sizing Volume Containers" on page 16. You can also remove older or obsolete snapshots to recover storage space.

You can create a snapshot of a VM whether the VM is running or shut down; however, if you want to create an *application-consistent* snapshot, where supported applications *quiesce* or freeze their operations to ensure data consistency, you must prepare your guest operating system as described in one of the following topics:

- "Installing the QEMU Guest Agent for Application-Consistent Snapshots (Windows-based VMs)" on page 192

- "Installing the QEMU Guest Agent for Application-Consistent Snapshots (Linux-based VMs)" on page 197

Related Topics

"Creating and Migrating Virtual Machines" on page 127

"Managing the Operation of a Virtual Machine" on page 198

Creating a Snapshot

Create a snapshot to save an image of a virtual machine (VM) at a particular point in time. If you export the snapshot as described in "Exporting a Snapshot" on page 224, you can use the exported files to import the VM to another system or back to the same everRun system to restore or duplicate the original VM. For an overview of snapshots, see "Managing Snapshots" on page 219.

You can create a snapshot of a VM whether the VM is running or shut down; however, if you want to create an *application-consistent* snapshot, where supported applications *quiesce* or freeze their operations to ensure data consistency, you must prepare your guest operating system as described in one of the following topics:

- "Installing the QEMU Guest Agent for Application-Consistent Snapshots (Windows-based VMs)" on page 192

- "Installing the QEMU Guest Agent for Application-Consistent Snapshots (Linux-based VMs)" on page 197

The number of snapshots you can create depends on the amount of storage space you have allocated in the volume container for each VM volume, as described in "Sizing Volume Containers" on page 16. If necessary, you can expand a volume container as described in "Expanding a Volume Container on the everRun System" on page 213.

> **Notes**:
>
> - For Linux-based VMs, if you want to create a snapshot of the VM to export to another system, consider editing the `/etc/fstab` file to comment out entries for data volumes and allow only the boot volume to mount. Because Linux-based VMs may use different device names on another system, your new VM may boot into single-user mode if it cannot mount the volumes with their original device names. You can restore the `/etc/fstab` entries in the new VM with the correct device names after the import process.
>
> - If you want to shut down the source VM while creating a snapshot, consider scheduling a planned maintenance period for this process.
>
> - When you create a VM snapshot, all volumes attached to the VM are automatically included in the snapshot; however, you can exclude volumes if you export a snapshot to another system as described in "Exporting a Snapshot" on page 224.
>
> - If you want to use a snapshot to duplicate a VM, and you will continue to use the source VM after the export, remember to set a different MAC address and IP address for the VM when you import it on the target system.
>
> - If the everRun system switches from the primary PM to the secondary PM during the snapshot, the snapshot fails. This does not affect the continuous uptime of your system, but the snapshot is automatically deleted, and you need to start a new snapshot.

> **Prerequisite**: Both PMs of the everRun system must be online for the snapshot process to function properly. If only one PM is online, the snapshot is written only to the online PM, and that same PM must be primary if you export the snapshot later.

To prepare for creating a snapshot (Windows-based VMs only)

1. If you want to create an application-consistent snapshot, ensure that the QEMU guest agent is installed and running, as described in "Installing the QEMU Guest Agent for Application-Consistent Snapshots (Windows-based VMs)" on page 192.

2. Ensure that all volumes are labeled accurately, as summarized in "Managing Windows Drive Labels" on page 189.

3. Run the Windows System Preparation Tool (Sysprep) if you need to prepare the guest
   operating system for redeployment.

To prepare for creating a snapshot (Linux-based VMs only)

If you want to create an application-consistent snapshot, ensure that the QEMU guest agent is
installed and running, as described in "Installing the QEMU Guest Agent for Application-Consistent
Snapshots (Linux-based VMs)" on page 197.

To create a snapshot

1. Log on to the everRun system with the everRun Availability Console.

2. On the **Physical Machines** page (see "The Physical Machines Page" on page 84), verify that both
   PMs are in the **running** state and that neither PM is in maintenance mode or in the process of syn-
   chronizing.

3. On the **Virtual Machines** page, select a VM.

4. With the VM selected, click the **Snapshot** button in the bottom pane.

5. In the **Snapshot Virtual Machine** dialog box, optionally type a **Snapshot Name** and **Description**
   for the snapshot.

   The default **Snapshot Name** for each new snapshot is the name of the VM, but you can type a
   more descriptive name. (The snapshot name does not need to be unique.)

6. Click **Create Snapshot**. The snapshot begins, and the dialog box closes automatically.

Creating a snapshot typically takes a few seconds, but it may take longer depending on the level of
VM activity and the amount of time that has passed since the previous snapshot. You can determine the
status of a snapshot by checking the **State** column on the **Snapshots** page:

- A broken icon (✖) indicates that a snapshot is still in progress, or that is written to only one node in
  the everRun system.

- A normal icon (✔) indicates that a snapshot is complete.

If you want to export a completed snapshot, see "Exporting a Snapshot" on page 224.

Related Topics

"Managing Snapshots" on page 219

"Creating and Migrating Virtual Machines" on page 127

"Managing the Operation of a Virtual Machine" on page 198

Exporting a Snapshot

Export a snapshot to transfer a virtual machine (VM) image from an everRun system to a network-mounted folder (that is, directory). Exporting a snapshot makes the VM image available for importing to another system or for importing back to the same everRun system to restore or duplicate the original VM. (For an overview of snapshots, see "Managing Snapshots" on page 219.)

You prepare for exporting snapshots by creating a network-mounted folder to store an exported VM in your environment. Create a folder for either a Windows share (also known as a Common Internet File System (CIFS) share) or a Network File System (NFS) export. After creating the folder, you mount it in the host operating system of the everRun system, as described in this topic. When you initiate an export in the everRun Availability Console, the everRun system saves the VM image to the network-mounted folder as standard Open Virtualization Format (OVF) and Virtual Hard Disk (VHD) files.

Notes:

- When you create a snapshot that you intend to export, you must follow steps to prepare the guest operating system; otherwise, the VM image that you create may not function as expected. For details, see "Creating a Snapshot" on page 220.

- When you export a snapshot, you export a fully coalesced snapshot of the VM from that point in time, not only the changed data. If you want to create differential backups of a VM, enable Disaster Recovery or use a third-party backup solution.

- You can export a snapshot that you created in the everRun Availability Console or a snapshot created by Disaster Recovery, but you cannot remove or otherwise manage Disaster Recovery snapshots.

- When you export a snapshot to import a VM to another everRun system, the original container size for each volume you include is not preserved. For example, if your source VM has a 20 GB boot volume in a 40 GB volume container, the target VM will have a 20 GB boot volume in a 20 GB volume container. If necessary, you can expand the volume containers on the target everRun system as described in "Expanding a Volume Container on the everRun System" on page 213.

- The time required for the export depends on the size and number of volumes in the source VM as well as network bandwidth. For example, transferring a VM with one 20 GB boot disk over a 1 Gb/s network may take about 30 minutes.

- If you will continue to use the source VM after the export, remember to set a different MAC address and IP address for the VM when you import it on the target system.

- If the everRun system switches from the primary PM to the secondary PM during an export, the export process fails. This does not affect the continuous uptime of your system. You can delete the partially exported files from your system running the everRun Availability Console and export the files again.

> **Prerequisite**: Both PMs of the everRun system must be online for the export process to function properly. You can export a snapshot from a single-node system only if all of the volume snapshots that you select to include in the export are present on the primary node, as displayed in the **Export Snapshot** dialog box. In most cases, snapshots are replicated on both nodes, but a snapshot may be unavailable if a node was offline when the snapshot was taken.

To create and mount an NFS export or Windows CIFS share

Before you can export a snapshot, you must create and mount the folder to which the export(s) will be transferred, as follows:

1. Create a network-mounted folder for a Windows/CIFS share or an NFS export in your environment where you can store VM exports.

   Ensure that you have enough storage for the VMs that you want to export. Also, set full read/write permissions on the network-mounted folder to permit file transfers, or, for a Windows/CIFS share only, assign read/write permissions to a specific user on the system/domain that hosts the share. Record the location and settings of the NFS export or CIFS share, which you will specify in a later step.

2. Log on to the everRun system with the everRun Availability Console.

3. On the **Physical Machines** page, verify that both PMs are in the running state and that neither PM is in maintenance mode or in the process of synchronizing. See "The Physical Machines Page" on page 84. Also, make note of which PM is the **primary** node. In the list in the top pane, the primary node is marked as **node*n* (primary)**.

4. Obtain the IP address of the primary node, if you do not already know it. For example, on the **Preferences** page, click **IP Configuration**. Click the **Node*n* IP** tab for the primary node and record the **IP Address** value.

5. Use a secure shell (`ssh`) utility to log on to the host operating system (host OS) of the primary node of the everRun system, where you will mount the folder. Log on as the `root` user.

   The next step shows how to use the `ftxmnt` script to automatically mount the folder. The script should work in most cases, but you can also manually mount the folder by executing standard mount commands if needed.

> **Notes**:
>
> - If you manually mount the NFS export or Windows/CIFS share in the host OS of the everRun system, you must create the mount point at `/mnt/ft-export`, where the export process expects to find it. (If you use the `ftxmnt` script, it automatically creates this mount point.)
>
> - If you want the mount to persist when you reboot the everRun system, manually add an entry to the `/etc/ftstab` file in the host OS of the everRun system. (The `ftxmnt` script does not modify the `/etc/ftstab` file.)
>
> - You need to mount the NFS export or Windows/CIFS share only on the primary node of the everRun system, but you can optionally add the mount to the `/etc/ftstab` file on both nodes so it is always available even if the primary node changes.
>
> - If you mount a Windows/CIFS share that requires a password, and the password changes after the mount, you need to unmount the folder and mount it again with the new password; otherwise, the export may fail unexpectedly.

6. To automatically mount the NFS export or Windows/CIFS share, execute the `ftxmnt` script and respond to the interactive prompts. For example, the following output shows how to mount a Windows/CIFS share (\\192.168.0.111\ExportVMs) that is accessible by a specific user account:

```
[root@node0 /]# ftxmnt

This script is meant to mount a Network Attached Storage
location to use for exporting everRun virtual machines.
Enter Ctrl-C to exit


Enter n if you are mounting an nfs share, enter w if you
are entering a windows share: w
What is the IP address or the computer name of the file
```

```
server?
```

192.168.0.111

```
What is the name of the share you wish to mount?
```

ExportVMs

```
Does this share require authentication? (y/n):
```

Respond **y** to the prompt above if the share requires authentication. When you respond **y**, the following prompts appear:

- ```
  What is your username?
  ```

  Enter your *domain\username*.

If the share does not require authentication, you must type **y** (if you type **n**, you will be unable to mount a CIFS share). For Username, enter a guest username, and for Password, enter an empty password.

The following message appears:

```
Successfully mounted folder \\192.168.0.111\ExportVMs
at path /mnt/ft-export/
```

7. Switch to the /mnt/ft-export directory in the everRun host OS and create a file to verify that the export or share is present and that you have read/write permissions. For example:

touch test

ls

test

Confirm that the file also appears in the export or share on the remote system. If the file is not present or the everRun host OS displays an error, verify your mount settings and permissions.

8. Remove the test file.

rm test

Later, you want to unmount the export or share after exporting your virtual machines, switch out of the /mnt/ft-export directory and execute the umount command, as follows:

cd /

```
# umount /mnt/ft-export
```

To export a snapshot

1. Log on to the everRun system with the everRun Availability Console.

2. On the **Physical Machines** page (see "The Physical Machines Page" on page 84), verify that both PMs are in the **running** state and that neither PM is in maintenance mode or in the process of synchronizing.

3. If you have not already done so, create a snapshot, as described in "Creating a Snapshot" on page 220.

4. On the **Snapshots** page, select the snapshot to export.

   Snapshots are usually in a normal state (✓) the **State** column. If a snapshot is broken (✗), it may indicate that one or more volumes in the snapshot are unavailable for export. You can check volume availability in step 7.

5. Click **Export**.

6. In the **Export Snapshot** dialog box, type the path in **/mnt/ft-export** where you want the snapshot to be exported.

   For example, if you want the export process to create a new directory named `ocean1` to store the OVF and VHD files, type `ocean1`. If you want the export process to create the `ocean1` directory inside an existing directory named `TestVMs`, type `TestVMs/ocean1`.

7. Review the list of **Captured Volumes** and select the volumes to include in the export.

   In most cases, the dialog box shows that **All Captured Volumes are available for Export on node***n* , the primary node. You can select any snapshots for export.

   If one or more snapshots are unavailable on the primary node (usually because the node was offline when the snapshot was taken), the dialog box allows you to select only the available snapshots. If necessary, you can cancel the export, ensure that both nodes are in the **running** state , and create a new snapshot for export.

8. Click **Export Snapshot**. The export begins, and the dialog box closes automatically.

You can monitor the **Export Status** in the **Summary** tab for the snapshot that you are exporting. Progress is reported as the percentage (%) completed. When the process is complete, the status changes to **Export completed successfully**.

The everRun system exports the VHD files (volumes) first, then it exports the OVF file. You can confirm that the process is finished when the OVF file appears in the folder.

After the export process, if you want to import or restore the OVF and VHD files on an everRun system, see "Importing an OVF File from an everRun 7.x System " on page 181

Troubleshooting

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

To clean up after a canceled or failed export from the everRun system

Remove the VM files from the export folder or create a new folder for a subsequent export.

Related Topics

"Managing Snapshots" on page 219

"Creating and Migrating Virtual Machines" on page 127

"Managing the Operation of a Virtual Machine" on page 198

Removing a Snapshot

Remove a snapshot to permanently delete it from the everRun system.

> **Notes**:
>
> - When you remove a VM snapshot, you also remove all of its associated volume snapshots, which frees up storage space in the volume containers that contain those volume snapshots.
>
> - If you remove all volume and volume snapshot contents from a volume container, the system automatically removes the container from the system, which frees up space in the storage group.
>
> - You can remove snapshots only if they were created by users of the everRun Availability Console. You cannot remove Disaster Recovery (DR) snapshots unless you unprotect the VM.

To remove a snapshot

1. On the **Snapshots** page, select a snapshot to remove.

2. Click **Delete**.

3. A confirmation window appears. Click **Yes** to continue deleting the snapshot or click **No** to stop the deletion.

Related Topics

"Managing Snapshots" on page 219

"Creating and Migrating Virtual Machines" on page 127

"Managing the Operation of a Virtual Machine" on page 198

Advanced Topics (Virtual Machines)

The following topics describe procedures and information for advanced users:

- "Assigning a Specific MAC Address to a Virtual Machine" on page 231

- "Selecting a Preferred PM for a Virtual Machine" on page 232

- "Changing the Protection Level for a Virtual Machine (HA or FT)" on page 232

- "Configuring the Boot Sequence for Virtual Machines" on page 233

- "Resetting MTBF for a Failed Virtual Machine" on page 234

- "Locating a Dump File in a Virtual Machine" on page 235

To manage the operation of a virtual machine, see "Managing the Operation of a Virtual Machine" on page 198.

Assigning a Specific MAC Address to a Virtual Machine

Assign a specific Media Access Control (MAC) address to a virtual machine (VM) if you need to override its default MAC address.

> **Prerequisite**: Before modifying the MAC address for a virtual machine, you must shut down the VM.

To assign a specific MAC address to a VM

1. Open the **Virtual Machines** page (see "The Virtual Machines Page" on page 88).

2. Select a VM and click **Shutdown**.

3. When the VM has stopped, click **Config** to display the **Reprovision Virtual Machine** wizard.

4. Click **Next** on each wizard page until the **Networks** page is displayed. (If applicable, see "Repro-visioning Virtual Machine Resources" on page 204 to configure additional VM resources.)

5. On the **Networks** page, locate the network to modify and make a note of the current MAC address in case you need to restore it.

6. Type the new address in the **MAC address** column, or leave the text area blank to allow the ever-Run software to automatically assign the MAC address.

7. Click **Finish**.

Related Topics

"Advanced Topics (Virtual Machines)" on page 231

"Managing Virtual Machine Resources" on page 204

"Managing the Operation of a Virtual Machine" on page 198

Selecting a Preferred PM for a Virtual Machine

Select a preferred physical machine to ensure that a virtual machine runs on a particular physical machine in the everRun system.

> **Note**: By default, the system automatically balances the load of virtual machines over the two physical machines. Do not modify this setting unless you have specific load balancing require-ments .

To select a preferred physical machine

1. On the **Virtual Machines** page, select a virtual machine.

2. In the bottom pane, click the **Load Balance** tab.

3. Choose your preference from the pulldown list and click **Save**.

Related Topics

"Advanced Topics (Virtual Machines)" on page 231

"Managing the Operation of a Virtual Machine" on page 198

Changing the Protection Level for a Virtual Machine (HA or FT)

You can change the protection level of guest VMs from high availability (HA) to fault tolerance (FT), or vice versa.

To change the protection level

1. On the **Virtual Machines** page, select a stopped VM (marked "stopped" in the **Activity** column). (See "Shutting Down a Virtual Machine" on page 198 for information about stopping a VM.)

2. In the bottom pane, click **Config** to open the **Reprovision Virtual Machine** wizard

3. On the **Name, Description and Protection** page, select the **HA** or **FT** button.

4. Continue clicking through the wizard pages to the last page. Press **Finish** and then **OK** (if the recon-figuration was successful).

Related Topics

"Modes of Operation" on page 11 (HA or FT)

"Advanced Topics (Virtual Machines)" on page 231

"Managing the Operation of a Virtual Machine" on page 198

Configuring the Boot Sequence for Virtual Machines

Configure the boot sequence of virtual machines to set the order in which guest operating systems and applications are started on the everRun system.

Determine the required boot sequence, then configure the boot settings for each virtual machine accordingly.

To set the boot sequence for a virtual machine

1. On the **Virtual Machines** page, select a virtual machine.

2. In the bottom pane, click the **Boot Sequence** tab.

3. Configure the boot settings, as described below.

4. Click **Save**.

The boot settings are as follows:

- **Priority Group** enables users to specify the order in which virtual machines boot after powering on the everRun system or after a failover, which requires restarting virtual machines. Some business solutions require specific virtual machines to be running before starting others. Group **1** is the

highest priority and **none** is the lowest. The everRun software waits for the **OS and Application Start Time** to elapse before starting virtual machines in the next priority group.

Boot sequence example:

VM	Priority Group	OS and Application Start Time
DNS	1	2 mins
App	2	30 secs
DB	2	10 mins
Web	3	0

    1   everRun boots the DNS VM.

    2   2 minutes after the DNS VM is started, everRun starts the App and DB servers in group 2.

    3   10 minutes after the DB VM is started, everRun starts the Web VM in group 3.

- **OS and Application Start Time** should be set to the time it takes from starting the virtual machine until the guest operating system and applications are fully functional.

Related Topics

"Advanced Topics (Virtual Machines)" on page 231

"Managing the Operation of a Virtual Machine" on page 198

Resetting MTBF for a Failed Virtual Machine

Reset the mean time between failure (MTBF) counter for a virtual machine to attempt to restart a failed virtual machine.

If a virtual machine's guest OS crashes, everRun automatically restarts it, unless it has fallen below its MTBF threshold. If the virtual machine is below the MTBF threshold, everRun leaves it in the crashed state. If necessary, you can reset the MTBF counter and restart the virtual machine.

> **Caution**: Do not reset the MTBF counter unless instructed to do so by your authorized Stratus service representative, as doing so may affect the continuous uptime of your system.

> **Notes**:
>
> 1. The **Reset Device** button is displayed only if the virtual machine falls below its MBTF threshold.
>
> 2. The **Clear MTBF** button is displayed only if the system software supporting a VM on one physical machine falls below its MBTF threshold.

To reset the MTBF counter for a virtual machine

1. On the **Virtual Machines** page, select a virtual machine.

2. Click **Reset Device**.

If the system software supporting a VM on one physical machine fails too often, perform the steps below to reset its MTBF counter.

To reset the MTBF counter for a VM on one physical machine

1. On the **Virtual Machines** page, select a virtual machine.

2. Click **Clear MTBF**.

Related Topics

"Advanced Topics (Virtual Machines)" on page 231

"Managing the Operation of a Virtual Machine" on page 198

"Creating a Diagnostic File" on page 74

Locating a Dump File in a Virtual Machine

Locate a dump file in a virtual machine (VM) if the VM has crashed and you need to collect the dump file for troubleshooting purposes.

To collect a dump file for your service representative

- For Windows-based VMs—Retrieve the file from **C:\WINDOWS\MEMORY.DMP** (by default) in the file system of the VM.

- For Linux-based VMs—Retrieve the dump file from the `/var/crash` directory (by default) in the file system of the VM.

If you cannot locate a dump file, ensure that you configured the guest operating system to generate a crash dump file when the operating system hangs:

- Windows-based VMs: Follow the instructions in the Microsoft article, *How to generate a complete crash dump file or a kernel crash dump file by using an NMI on a Windows-based system* (Article ID: 927069). Follow the instructions in the **More Information** section.

- Linux-based VMs: Install the `kexec-tools` package and enable crash dumps. For more information, see your Linux documentation.

Related Topics

"Advanced Topics (Virtual Machines)" on page 231

"Managing the Operation of a Virtual Machine" on page 198

"Creating a Diagnostic File" on page 74

8

Chapter 8: Maintaining Physical Machines

You can maintain PMs in an everRun system by adding or replacing various components or even the entire PM.

> ✅ **Prerequisite**: Before you add, replace, or upgrade a component, see "Physical Machine Hardware Maintenance Restrictions" on page 237.

Determine what component needs to be replaced and then read the topic for the appropriate procedure:

- To add or replace PM components, see:

  - "Adding or Replacing Hot-Swappable Components" on page 238 for hot-swappable components such as network cables, fans, and power supplies

  - "Adding or Replacing Components That Are Not Hot-Swappable" on page 239 for components such as CPUs and memory or any other component that is not hot-swappable.

  - "Adding a New NIC" on page 240 for adding new network interface cards (NICs).

- To replace a PM or a failed motherboard, NIC, or RAID controller, see "Replacing Physical Machines, Motherboards, NICs, or RAID Controllers" on page 242.

- To upgrade both PMs in a running system, see "Upgrading Both Physical Machines In a Running System" on page 244.

For information on disks, see "Logical Disks and Physical Disks" on page 15.

Physical Machine Hardware Maintenance Restrictions

When you replace physical machines (PMs), motherboards, or RAID controllers, you should ensure compatibility by complying with these restrictions:

- New PMs must have processors that are from the same processor family as the existing PM, in order to support live migration. If the processors in the new and existing PMs are from different processor families, you must stop the VMs to migrate them from the existing PM to the new PM.

- CPUs on a replacement PM must be compatible with the CPUs on the original PM.

- In the replacement PM, the quantity of the following resources must be the same or greater than in the original PM:

    - Number of processor cores.

    - Total memory.

    - Total logical disk capacity.

    - Total number of network ports; each port must support, at a minimum, the speed of the existing ports, and all add-on NICs within a particular PM must have the same vendor/model number.

    - Total number of network ports; each port must support, at a minimum, the speed of the existing ports.

In addition, check "System Requirements Overview" on page 22 for information about system hardware and software requirements before performing hardware maintenance on a PM, to confirm that the maintenance you are planning complies with any system restrictions.

Related Topics

"Maintenance Mode" on page 111

"Maintaining Physical Machines" on page 237

"The everRun Availability Console" on page 54

"Physical Machines and Virtual Machines" on page 8

"The Physical Machines Page" on page 84

Adding or Replacing Hot-Swappable Components

Use this procedure to add or replace a component that is hot-swappable. Such components may include network cables, fans, and power supplies. In this procedure, the PM continues to run.

> **Prerequisite**: Before you add, replace, or upgrade a component, see "Physical Machine Hardware Maintenance Restrictions" on page 237.

To add or replace a hot-swappable component

1. Determine which PM (node0 or node1) requires the component.

2. In the everRun Availability Console, click **Physical Machines** in the left-hand navigation panel.

3. Select the appropriate PM (node0 or node1) and then click **Work On**, which changes the PM's **Overall State** to **Maintenance Mode** and the **Activity** state to **running (in Maintenance)**.

4. Follow vendor instructions for adding or replacing a hot-swappable component in the PM.

5. Select the repaired PM on the **Physical Machines** page. Click **Finalize** and then click **OK**.

If you add a cable to both PMs and if they are on the same subnet, everRun detects the connectivity and pairs the NICs in a newly created shared network. You have the option of renaming the newly created shared network on the **network** page.

Related Topics

"Maintenance Mode" on page 111

"Maintaining Physical Machines" on page 237

"The everRun Availability Console" on page 54

"Physical Machines and Virtual Machines" on page 8

"The Physical Machines Page" on page 84

Adding or Replacing Components That Are Not Hot-Swappable

Use this procedure to add or replace a component that is not hot-swappable. Such components may include CPUs and memory as well as fans and power supplies that are not hot-swappable.

In this procedure, you gracefully shut down a running PM.

> **Prerequisite**: Before you add, replace, or upgrade a component, read "Physical Machine Hardware Maintenance Restrictions" on page 237.

To add or replace a component that is not hot-swappable

1. Determine which PM (node0 or node1) or if each PM requires the replacement component.

2. In the everRun Availability Console, click **Physical Machines** in the left-hand navigation panel.

3. Select the appropriate PM (node0 or node1) and then click **Work On**, which changes the PM's **Overall State** to **Maintenance Mode** and the **Activity** state to **running (in Maintenance)**.

4. After the PM displays **running (in Maintenance)**, click **Shutdown** and then **OK**.

5. Add or replace the component.

6. If you disconnected any network cables, reconnect them. Do not add cables to any new network ports in this step.

7. On the PM that is shutdown, press the power button. As the PM powers on, everRun also powers on and begins synchronizing the PM's storage (appears).

8. On the **Networks** page, click the **Fix** button, if it is highlighted, which may occur when network cables have been moved on the upgraded PM.

9. Select the repaired PM on the **Physical Machines** page. Click **Finalize** and then click **OK**.

10. When synchronization is complete (disappears), perform steps 3 through 9 for the other PM, if necessary.

> **Note**: To avoid data loss, do not power down the primary PM while the disks are synchronizing.

Related Topics

Adding a New NIC

When adding new NICs, you must add NICs to both physical machines (PMs) and then cable the NICs to the appropriate switch on both sides in order to establish connectivity and to form one or more shared networks that you can then assign to VMs or use as A-links.

> ✓ **Prerequisite**: Before you add a NIC, see "Physical Machine Hardware Maintenance Restrictions" on page 237.

To add new NICs

> ℹ **Note**: You can begin this procedure with **node0** or **node1** and then continue with the other node. The procedure below begins with **node0** for simplicity.

1. In the everRun Availability Console, click **Physical Machines** in the left-hand navigation panel.

2. Perform the following for **node0**:

   a. Select the appropriate node and then click **Work On**.

   b. After the node displays **running (in Maintenance)**, click **Shutdown** and then **OK**.

   c. Insert the new NIC in the desired slot.

   d. Press the power button to power on the node.

   Wait for the PM to boot and for the everRun Availability Console to display **running** as the **Activity** state for the appropriate node under **Physical Machines**.

   e. Click **Finalize** for and then click **OK**, which exits the node from maintenance mode.

   Wait while storage synchronization completes (↻ disappears).

3. Perform Step 2 for **node1**.

   In node1 insert the new NIC in the slot that corresponds to the slot where you inserted the new NIC in the PM that is node0 (Step c, above).

4. Connect network cables to the new NICs, as needed, and configure the new network as an A-Link or a business network. See "Connecting Additional Networks" on page 50.

5. Reconfigure and start any VMs that need to use the new networks. See "Managing Virtual Machines" on page 121.

Related Topics

"Maintenance Mode" on page 111

"Maintaining Physical Machines" on page 237

"The Physical Machines Page" on page 84

Replacing Physical Machines, Motherboards, NICs, or RAID Controllers

You replace motherboards, NICs, RAID controllers, and a physical machine (PM) in an everRun system while the system is running. You can remove PMs to upgrade a PM or to replace a failed PM. You can replace motherboards, NICs, or RAID controllers. Several types of hardware faults can hang or crash a PM in an everRun system, including a failure of the motherboard, CPU, mid-plane, or storage controller. (If you want to recover a failed PM instead of replacing it, see "Recovering a Failed Physical Machine" on page 116.)

You remove a PM using the everRun PM **Remove** function, which deletes a PM from the everRun system's database. The everRun system then waits while an additional PM completes the process of joining the system.

If you replace a PM or a component, use vendor instructions, but first read "Physical Machine Hardware Maintenance Restrictions" on page 237.

> **Warning**: This procedure deletes all software you may have installed on the PM and all PM configuration information you may have entered before the replacement procedure. After you complete this procedure, you must manually re-install all your software and reconfigure the PM to match your original settings.

> **Prerequisite**: Obtain installation software for the everRun release that the PM has been running using one of the following methods:
>
> - Download an install ISO from your authorized Stratus service representative.
>
> - Extract an install ISO into the current working directory from the most recently used upgrade kit by executing a command similar to the following (*x.x.x.x* is the release number and *nnn* is the build number):
>
>   tar -xzvf everRun_upgrade-x.x.x.x-*nnn*.kit *.iso
>
> After you obtain the correct install ISO, save it or burn it to a DVD. See "Obtaining everRun Software" on page 34.

> **Prerequisites**: If you are replacing a PM, prepare the new PM:
>
> 1. Configure networks. See "Network Architecture Overview" on page 18.
>
> 2. Configure storage. See "Storage Requirements" on page 23.
>
> 3. Connect power. See "Connecting Power" on page 33.
>
> 4. Configure the firmware (BIOS). See "Configuring Settings in the Firmware Setup Utility" on page 36.

To remove and replace a failed PM, motherboard, NIC, or RAID controller

1. In the everRun Availability Console, click **Physical Machines** in the left-hand navigation panel.

2. Select the appropriate PM (node0 or node1) and then click **Work On**, which changes the PM's **Overall State** to **Maintenance Mode** and the **Activity** state to **running (in Maintenance)**.

3. After the PM displays **running (in Maintenance)**, click **Shutdown** and then **OK**.

4. After the PM has shut down, click **Remove** ( ) and respond appropriately to the confirmation message. An alert message appears if removal conditions are not met.

   If you confirm that you want to remove the PM, the everRun software deletes the PM from the ever-Run system, and displays a message that the system has successfully deleted the PM.

   To replace the PM, continue with the steps below.

5. Manually power off the old PM.

6. Install the new PM or component. If you are replacing a motherboard, NIC, or RAID controller, do so now. If you are replacing the PM, disconnect and remove it now, and then install the new PM. Check that a monitor and keyboard are connected to it.

7. Reconnect any network cables to their original positions. Check that Ethernet cables are connected from the new PM (or new NIC) to the network or directly to the running (primary) PM, if the two everRun system PMs are in close proximity. One Ethernet cable should connect from the first embedded port on the new PM or from a NIC port if the new PM does not have an embedded port.

8. Manually power on the PM. As the PM powers on, enter the firmware (BIOS) setup utility, and set

the Optical Drive as the first boot device.

9. Either mount the ISO image or insert the DVD into the PM.

10. At the **Welcome** screen, select **Replace PM, Join system: Initialize data** and press **Enter**.

> **Note**: If necessary, see "Installing Software on the Second PM" on page 46 for reference. Although that topic refers to the "second PM," in this instance, it applies to the replacement PM.

11. When prompted, respond to the **Select interface for private Physical Machine connection**, and then respond to the prompt **Select interface for managing the system (ibiz0)**.

12. When prompted to configure **ibiz0**, select **Automatic configuration via DHCP** or **Manual Configuration (Static Address)**. (The installation software configures priv0 automatically.)

13. When installation is complete, the PM ejects the install DVD (if used) and reboots.

14. As the PM boots up, the everRun Availability Console displays its activity on the **Physical Machines** page. The **Activity** column displays the new PM as **recovery (in Maintenance)** and then **running (in Maintenance)**.

15. When you are ready to bring the replacement PM online, click **Finalize** to exit maintenance mode. Verify that both PMs return to the **running** state and that the PMs finish synchronizing. The initial synchronization may take minutes or hours depending on your configuration, including the amount of storage and the number of VMs.

16. Manually reinstall applications and any other host-level software and reconfigure the PM to match your original settings.

Related Topics

Upgrading Both Physical Machines In a Running System

> ✓ **Prerequisite**: Before you upgrade to new physical machines, see "Physical Machine Hardware Maintenance Restrictions" on page 237.

To upgrade to new physical machines

1. Upgrade everRun software if required to support the new PM. See the everRun **Release Notes** and the help on the **everRunUpgrade Kits** page of the everRun Availability Console

2. Upgrade the first PM; see "Replacing Physical Machines, Motherboards, NICs, or RAID Controllers" on page 242.

3. Repeat for the second PM. The everRun software then migrates the VMs to the other PM.

4. If you added additional NIC ports, see "Network Architecture Overview" on page 18.

Related Topics

"Maintenance Mode" on page 111

"Maintaining Physical Machines" on page 237

"The everRun Availability Console" on page 54

"Physical Machines and Virtual Machines" on page 8

"The Physical Machines Page" on page 84

Part 2: Supporting Documents

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

9

Chapter 9: everRun Release 7.2.2.0 Release Notes

These release notes are for everRun release 7.2.2.0 (updated at 1:37 PM on 4/22/2021). See the following sections:

- Important Considerations

- Known Issues

- New Features, Enhancements, and Bug Fixes

- Getting Help

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

Important Considerations

Upgrading from Previous Releases of everRun

You can upgrade from any prior everRun release (listed on the **Downloads** page at http://www.stratus.-com/go/support/everrun) to everRun release 7.2.*x* **with no VM downtime** by following the instructions in "Upgrading everRun Software" on page 103.

If you are upgrading from a release not listed on the everRun Support page (for example, a beta release) you must perform a complete system re-install.

> **Caution**: All PMs and VMs must be in good health prior to performing an upgrade of everRun software. Before starting an upgrade, examine the everRun Availability Console to verify that there are no alerts indicating PM or VM problems.

> **Notes**:
>
> 1. The everRun Availability Console may not automatically refresh after an everRun upgrade completes, giving the impression that the upgrade has not completed. Periodically refresh the everRun Availability Console during the upgrade to see if the upgrade has completed. To do this, click the browser's reload or refresh button. Pressing the F5 key also accomplishes this on many browsers. If you encounter problems during an upgrade, contact Stratus support for assistance at http://www.stratus.com/services-support/customer-support.
>
> 2. everRun releases prior to release 7.2.*x* did not support VM disks larger than 2 terabytes. If you have such a disk, contact Stratus support at http://www.stratus.com/services-support/customer-support before you attempt to upgrade to everRun release 7.2.*x*.

A DR-Protected VM Cannot Be Deleted

A DR-protected VM cannot be deleted. After shutting down a DR-protected VM, the **Remove** button will not appear. To delete such a VM, use the One View Console to disable DR protection for that VM. After DR protection is removed, the **Remove** button will be enabled and you can use the everRun Availability Console to shut down and remove the VM.

Updating Guest VM Software After Installing a VM

After installing a VM, check to see if updates to the guest OS are available. If updates are available, install them.

> **Caution**: RHEL7 and CentOS7 Virtual Machines must use kernel version 3.10.0-123.8.1 or later. If using an earlier kernel version there is a risk that the VM may hang.

Do Not Update CentOS Host OS Directly from CentOS

Do not update the CentOS host OS software directly from CentOS. Use only the CentOS release that is installed along with everRun software.

Optimizing Performance of A-Link Networks

Stratus recommends that you enable jumbo frames on A-Link networks by setting their Ethernet frame MTU size to 9000 bytes (by default, they are set to 1500 bytes). Doing so improves VM performance and reduces host processing overhead.

The A-Link networks must:

- Be a single Ethernet cable, point-to-point connection, or

- Have intermediate components (for example, switches) that are all fully capable of passing jumbo frame traffic

Use AVCLI commands to enable jumbo frames. AVCLI is installed on the host system along with everRun software. You can run AVCLI by logging onto the host through a remote console using the system IP address. Alternatively, you can install AVCLI on a remote management computer. For information about how to install AVCLI on a remote computer, see "AVCLI Command Overview" on page 260.

To set A-Links to use jumbo frames:

1. From a remote console, issue the `network-info` command to determine the name(s) of the A-Link network(s). In the command's output, look for the names of networks that have **role = A-Link** . See "network-info" on page 334 for an example.

2. Issue the "network-change-mtu" on page 332 command to change the MTU size to the maximum value of 9000 bytes. The change takes effect immediately. The following example changes the `sync_2003` and `sync_2004` A-Link networks to use jumbo frames.

        avcli network-change-mtu sync_2003 sync_2004 9000

3. Issue the `network-info` command to verify that the A-Links now have MTU values of 9000.

> **Caution**: After you issue the `network-change-mtu` command, do not issue another `network-change-mtu` command until after the new MTU settings have taken effect. Use the `network-info` command as described in step 3 above, to verify that the new MTU settings have taken effect.

Migrating a PM or VM to an everRun System

Migrating Windows 2012 R2 or Windows 8.*x* PMs or VMs from a non-everRun system to an everRun system is not supported. For a list of PM and VM operating systems that you can migrate, see "Migrating a Physical Machine or Virtual Machine to an everRun 7.x System" on page 133.

Status of RAID Physical Disks Is Not Monitored

everRun software does not monitor the state of physical disks in a RAID set. You must use the tools supplied by the RAID controller vendor to monitor the health and status of individual physical disks in a RAID set.

Other Important everRun Considerations

For important considerations about everRun systems, see "Important Physical Machine and Virtual Machine Considerations" on page 407.

Known Issues

Windows 2008 (pre-R2) Guests May Crash

Windows Server 2008 (pre-R2) VMs are at risk of crashing and can exhibit the following symptoms:

- Bug Check 0x19: BAD_POOL_HEADER (see http://msdn.microsoft.com/en-us/library/windows/hardware/ff557389(v=vs.85).aspx for more information).

- Bug Check 0x3B: SYSTEM_SERVICE_EXCEPTION (see http://msdn.microsoft.com/en-us/library/windows/hardware/ff558949(v=vs.85).aspx for more information).

Under heavy disk loads, such as during a back up, Windows Server 2008 x64 pre-R2 (NT 6.0, Vista kernel) crashes with the symptoms listed above.

Guest VMs running other Windows versions, including Windows Server 2008 R2 and Linux do **not** exhibit these symptoms.

Do not install or import Windows Server 2008 pre-R2 guests on everRun systems. Instead install one of the following supported Windows types which do not exhibit these symptoms:

- Windows Server 2008 R2 (NT6.1, Windows 7 kernel) x64

- Windows Server 2012 (NT6.2, Windows 8 kernel) x64

- Windows Server 2012 R2 (NT6.3, Windows 8.1 kernel)

If you already use Windows Server pre-R2 guests, monitor them for the symptoms described above. Install a replacement VM of one of the Windows types mentioned above for any VM that must run reliably. If crashes do not impact you, it is likely that crashes will occur as load on your VM increases.

Simplex PM Does Not Reboot After an everRunUpgrade

When upgrading a simplex system (single PM) from everRunRelease 7.2.0.0, the upgrade process completes but the system does not reboot. To reboot a simplex system after it's upgrade completes, click **System** in the left-hand navigation panel then click **Reboot**.

VMs May Not Boot If One Node is Removed From System

If you remove one PM from the system (by clicking **Work On** and then clicking **Remove**), do **not** place the remaining PM into maintenance and then bring it back into service by just using the **Finalize** button. Doing so will prevent all VMs from being able to boot. If you must place the remaining PM into maintenance mode, reboot it before you return it to service. See "Rebooting a Physical Machine" on page 113 for details.

The VM Console Button Does Not Work With Java 8

The **Console** button on the **Virtual Machines** page does not work when Java 8 is installed on the remote management computer running the everRun Availability Console. To avoid this problem, do not install Java 8 on the remote management computer. Instead use Java 7.

Uploading an Upgrade Kit Will Fail If The User Session Times Out

Uploading an upgrade kit will fail if the user session on the everRun Availability Console times out during the upload process. This might occur, for example, when upgrading a DR PM through the primary PM's site over a low-bandwidth or heavily congested DR link. If the upload process is taking a long time, you can avoid the problem by performing an action in the everRun Availability Console (like clicking to view a different page) before the session times out. Alternatively you can perform the upload locally at the site of the system being upgraded.

A VM Exported With Only Some of its Snapshotted Volumes Cannot be Imported

During a VM export operation, be sure to select all of the VMs volumes. Doing so exports a VM that can then be imported at a later time.

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

When either a user or the Disaster Recovery (DR) software removes a snapshot on an everRun system, 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. 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.

- A user cannot enable or resume DR protection for a VM. An alert on the **Alerts** page of the everRun Availability 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 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. This is unlikely to happen on systems with moderate work load and RPOs in the 1 - 6 hour range but should this occur, it is necessary to increase the RPO time to avoid falling out of RPO.

The ftxmt Script Does Not Work With CIFS as Documented

When creating and mounting an export share on a Windows (CIFS) share, type **y** in response to the question **Does this share require authentication?**. Then enter the guest user name (usually **guest**) and password.

Moving an everRun System to a Different Subnet

Use the following procedure to prepare the management IP configuration of an everRun system to work on a different subnet (for example when shipping to another location or when reconfiguring network subnets).

> **Notes**: This procedure requires:
>
> 1. A **management computer**, connected to the same subnet the everRun system is currently on, to view the everRun Availability Console.
>
> 2. A **VGA console** connected directly to the primary node of everRun system. See "Site and System Preparation" on page 33.

1. In the everRun Availability Console, click **Physical Machines** in the left-hand navigation panel, and note which node is the primary node.

2. Connect a VGA console directly to the primary node.

3. On the VGA console, press **Enter**. The console displays several addresses. Note the PM's link-local IPv6 address (it is the one that begins with **fe80::**).

4. In the management computer's browser, enter the URL of the link-local IPv6 address in the form http://[*ipv6-link-local-address*]. Be sure to include the address within brackets, for example: http://[fe80::21c:23ff:fedd:30ed].

5. Place both nodes into maintenance mode. Log on to the everRun Availability Console and in the left-hand navigation panel, click **Physical Machines**.

   a. Select the secondary node (the one not marked primary) and click **Work On**.

   b. Select the primary node and click **Work On**.

6. Click **Preferences** in the left-hand navigation panel, and click **IP Configuration**.

   a. Change the IP configuration settings to match the addresses for the new subnet to which the system will be moved.

   b. Click **Save**.

7. Click **System** in the left-hand navigation panel, then click **Shutdown**.

8. Move the everRun system to the new location and/ or connect it to the new subnet.

9. Power on both PMs.

10. On a management computer, connect to the everRun Availability Console using the IPv4 management address you specified in step 6.

11. Remove both nodes from maintenance mode. In the left-hand navigation panel, click **Physical Machines**.

    a. Select one node and click **Finalize**.

    b. Select the other node and click **Finalize**.

Under Certain High Workloads Windows VM Snapshots May Not Be Application-Consistent

In some high workload situations, the Windows QEMU guest agent may become unresponsive, preventing snapshots of Windows VMs from being application-consistent (instead they are only crash consistent as indicated on the **Summary** tab of the **Snapshots** page). If this occurs, application-consistent snapshots will not longer be possible until the Windows QEMU quest agent is restarted. Perform the following procedure to restore application-consistent snapshot capability.

1. In the Windows Task Manager stop the **QEMU Guest Agent** (qemu-ga.exe) process.

2. In the Windows Services user interface, start the **QEMU Guest Agent** service.

Specifying a Log File While Installing the Windows QEMU Guest Agent May Cause VM Timeouts

Do not specify a log file while installing qemu-ga.exe. Doing so may cause VSS timeouts when snapshots are being taken.

Replacing Physical Machines, Motherboards, NICs, or RAID Controllers

In the event of a hardware failure requiring replacement of an entire PM, everRun supports PM replacement while VMs continue to run on the other PM, thereby avoiding any guest downtime. The procedure for doing this is documented in "Replacing Physical Machines, Motherboards, NICs, or RAID Controllers" on page 242. After completing this procedure, perform the following steps to avoid any potential subsequent problems.

> **Notes**:
>
> 1. The physical machine **Remove** operation is used for a variety of reasons. After implementing the procedure described below, contact Stratus Support for guidance if there is any issue that does not resolve automatically, including any questionable indicators on the everRun Availability Console. For contact information, see the **everRun Support** page at http://www.stratus.com/services-support/customer-support.
>
> 2. Verify that the guest operating systems are running, then contact Stratus with all relevant status and questions, before attempting resolution on your own.

1. The preferred PM setting can get corrupted after replacing a PM. It is not possible to tell which VMs may be impacted by this, so you must perform steps **a.** and **b.** below for **each** VM.

    a. In the everRun Availability Console, change the preferred PM setting to the node that the VM is **not** currently on. See "Load Balancing" on page 115 and "Selecting a Preferred PM for a Virtual Machine" on page 232 for information about how to do this.

    b. Then change the preferred PM of each VM back to the desired setting.

2. If, after performing the previous step, an alert appears saying that a rebalance must be performed, on the everRun Availability Console masthead, click **Rebalance** (⚖).

Unsupported Network Adapter Card and Chip

Due to the issue outlined at http://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=migr-5093183, everRun does not support the following network adapter card and chip:

- The Broadcom NetXtreme II Dual Port 10GBase-T Network Adapter, IBM part number 49Y7910

- Any other NICs that use the Broadcom BCM57712 Ethernet hardware chip

Do Not Use the `ifdown` Command

Do not issue the `ifdown` command from an everRun physical machine's host OS to temporarily bring down a VM's business (ibiz$x$) network connection. Doing so will disconnect the physical interface from its bridge and cause the VM to become unreachable over the network. Instead, use the `ifconfig down` command.

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 everRun Release 7.2.2.0

- bz-29135 - Modules fail to recompile when upgrading base OS.

- bz-29069 - Unable to Grant Access to User using active directory

- bz-28948 - The SNMP OID var sraSiOverallSystemStatus is not correctly set and is a regression from the previous release.

- bz-28927 - Node crashes running scenarios on Dell 630 and Dell 730 Haswell platforms

- bz-28907 - VM is stuck in snapshot state after powering off and powering on

- bz-29027 - Date and Time not updated correctly on secondary node

- bz-29014 - Fix to 26664 overrides much of the AX's split-brain protection

- bz-29255 - VMs cannot start on SuperMicro server (AES bit)

- bz-29248 - Address glibc GHOST security hole CVE-2015-0235

- bz-29211 - Available memory calculations for VM creation, reconfiguration, and startup are incorrect

- bz-29259 - CPU ucode update causes problems on IBM Haswell servers

- bz-29065 - Address NTP vulnerabilities CVE-2014-9296, CVE-2014-9295, CVE-2014-9294, CVE-2014-9293

Fixed in everRun Release 7.2.1.0

- bz-28701 - Selecting the **Identify** button for a NIC that does not support the identify feature during everRun software installation, causes the installation to abort (and the physical machine to reboot).

New in everRun Release 7.2.0.0

- Disaster Recovery (optional feature, requires separate license)

- Virtual machine snapshots

- Import and Restore snapshots

- Export virtual machine snapshot

- Simplex everRun system (in DR configurations only)

- Support for 24 VMs (up to 4 of these can be FT VMs)

- In-place upgrade of Avance and everRun MX systems to everRun

- Reset MTBF of VMs

- Parallel Redundancy Protocol (PRP)

- Active Directory

- Support for disks larger than 2 terabytes

Getting Help

If you have a technical question about everRun software, you can find the latest documentation at the **Downloads** 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 **everRun Support** page at http://www.stratus.com/services-support/customer-support.

10

Chapter 10: everRun Command Line Interface Reference

You can use the everRun command-line interface to control the system from a remote console. The following topics describe how to administer and use the command-line interface:

- "AVCLI Command Overview" on page 260
- "AVCLI Command Descriptions" on page 272

AVCLI Command Overview

You can use the everRun command-line interface (AVCLI) to control the system from a remote console.

The following topics explain how to install the AVCLI client:

- "Prerequisites" on page 261
- "Installing the Linux Client" on page 261
- "Installing the Windows Client" on page 262

The following topics explain how to use the AVCLI command interface:

- "Using AVCLI" on page 263
- "Executing a Command" on page 263
- "Using AVCLI Help" on page 264

The following topics are helpful for programmers using the AVCLI command interface:

- "AVCLI Error Status" on page 265
- "XML Encapsulated Errors" on page 265

- "Error Checking" on page 266

- "Asynchronous Command Delay" on page 266

- "Output Formatting" on page 267

- "AVCLI Exceptions" on page 271

Related Topics

"AVCLI Command Descriptions" on page 272

Prerequisites

Before you use AVCLI, these prerequisites apply:

- Verify that the client computer has Java Runtime Environment (JRE), version 1.6, update 14 or later, installed by typing:

    ```
    java -version
    ```

    If the client computer already has this version of JRE installed, the output looks similar to this:

    ```
    java version "1.6.0_16" Java(TM) SE Runtime Environment
    (build 1.6.0_16-b01) Java HotSpot(TM) Server VM (build
    14.2-b01, mixed mode)
    ```

    If the output shows that the client computer has an older version of JRE installed, download the correct version from http://www.java.com/en/download/manual.jsp.

- You need a valid username and password. The default username/password is `admin`/`admin`. AVCLI scripts embed the username/password, so use access control lists (ACLs) to safeguard your new credentials. AVCLI commands are encrypted using SSL.

Installing the Linux Client

To download the AVCLI client for Linux:

1. Download the Linux client:

    a. Go to the **Downloads** page at http://www.stratus.com/go/support/everrun.

    b. On the **Downloads** page, click **everRun** (if it is not already displayed) and then select the appropriate version.

      c. Scroll down to **Drivers and Tools** and then continue scrolling to **everRun Command Line Interface (AVCLI)**.

      d. Select the **RHEL (64-bit) avcli client** and save the file.

2. Log on as the root user.

3. Add the directory `/usr/bin,` if it does not exist.

4. Install the client by typing:

```
rpm -i avcli*.rpm
```

Your Linux system can contain only one copy of AVCLI at one time. If another version is already installed, you receive an error message similar to the following:

```
file /usr/bin/avcli.bat from install of avcli-2.1.1-0
conflicts with file from package avcli-1.0-0 file
/usr/lib/ImportExportLibs.jar from install of avcli-2.1.1-0
conflicts with file from package avcli-1.0-0
```

If you receive the preceding message, remove the previous version of AVCLI by typing:

```
rpm -e avcli-1.0-0
```

Then repeat step 4.

Installing the Windows Client

To download the AVCLI client for Windows:

1. Download the Windows client:

      a. Go to the **Downloads** page at http://www.stratus.com/go/support/everrun.

      b. On the **Downloads** page, click **everRun** (if it is not already displayed) and then select the appropriate version.

      c. Scroll down to **Drivers and Tools** and then continue scrolling to **everRun Command Line Interface (AVCLI)**.

      d. Click **Windows avcli client**. Save the file.

2. Double-click `avcli.msi.` Follow the onscreen instructions.

3. Click **Run**. When prompted, accept the EULA.

4. If prompted to remove a previous version of AVCLI, click `Start` > `All Programs` > `everRun` > `Uninstall AVCLI`. Then repeat steps 1- 3.

Using AVCLI

To use AVCLI:

- On Windows, click `Start Menu` > `All Programs` > `everRun` > `Command Prompt`.

- On Linux, type the **avcli** command, followed by one or more commands. For example:

  `# avcli -H localhost -u admin -p admin vm-info`

> **Note**: In the preceding example, typing the **-H**, **-u**, and **-p** options automatically saves the host-name, username, and password, respectively, so that subsequent commands do not require them. You can also create a shortcut to avoid the need to prefix all commands with the host-name, username, and password, as described in "Executing a Command" on page 263.

From the command line, use the **help** command to list all AVCLI commands or to display information for a specific command. See "Using AVCLI Help" on page 264.

Executing a Command

Commands must include the DNS name or IPv4 address of the everRun system. If you specify incorrect syntax, a message displays the correct syntax.

Create a shortcut to avoid the need to prefix all commands with the hostname, username, and password.

To create a shortcut:

Windows

The `avcli` command executes the batch file `avcli.bat` in `%Program Files%\everRun`. You can add login credentials to this file:

1. Open `avcli.bat` with a text editor.

2. Search for this string:

   `-jar "%AVCLI_HOME%\avcli.jar"`

3. Append login info. For example:

   `-jar "%AVCLI_HOME%\avcli.jar" -u admin -p admin -H everrun`

If you manage several everRun systems with the same username and password, specify the
domain names of the individual systems in the command line:

```
$ avcli -H everrun1 node-info node0
```

or

```
$ avcli -H everrun2 node-info node0
```

Linux

Create an alias in your login `.cshrc` file. For example:

```
alias avcli='/usr/bin/avcli -u admin -p admin -H everrun'
```

In the example, `avcli` is the alias name, `admin/admin` is the username/password, and
`everRun` is the everRun system's domain name. You can then use this alias to log on and spe-
cify commands. For example, you could specify `unit-info` as follows:

```
$ avcli unit-info
```

Using AVCLI Help

This topic describes how to use AVCLI help.

Listing All Commands

To list all available AVCLI commands, type:

```
$ avcli help
```

The output follows:

```
[root@node0 zoneinfo]# avcli help

Usage: avcli [OPTION]... [COMMAND]

-u, --username username to login with

-p, --password password to login with

-H, --hostname hostname to login to

--log log file to capture debug information in

-x, --xml format output in XML

-V, --version display the version and exit
```

```
-h, --help display this message and exit

.

.

.
```

If you type a command that AVCLI does not recognize, AVCLI displays the preceding output.

Displaying Help for a Specific Command

To display help for a specific command, type:

```
$ avcli help command_name
```

For example, if you type:

```
$ avcli help vm-create
```

The output is:

```
Usage: avcli vm-create[--interfaces] [--shared-storage]

Create a new VM.

.

.

.
```

If you type a valid command with an invalid argument, AVCLI displays the same output as if you had specified help for the command.

AVCLI Error Status

AVCLI does not follow the Linux convention of returning 0 on successful execution and 1 for an error.

XML Encapsulated Errors

To display all errors as encapsulated XML suitable for processing with an XML parser, specify $-x$ on the command line.

The following example displays errors associated with a bad username/password:

```
$ avcli -x -H eagles -u admin -p foo node-info
```

The following example displays errors associated with a bad host address for the everRun system:

```
$ avcli -x -H foo -u admin -p foo node-info

foo
```

The following example attempts an operation using a nonexistent VM:

```
$ avcli -H eagles -x vm-delete eagles23

Cannot find a resource that matches the identifier eagles23.
```

Error Checking

To cleanly catch all errors while developing scripts, always specify output in XML format. This returns an error with any reply that does not return valid XML or any XML document with an error attribute.

The following example is from a PERL subroutine `_cli` that provides a shell for executing AVCLI commands. The code that checks for errors does a simple pattern match on `$stdout`.

```
my $error = 0

$error = 1 unless ($stdout =~ /xml version/);

$error = 1 if ($stdout =~ /\/);
```

If no error occurs, `$stdout` is cast into a PERL hash using the standard PERL `XML::Simple Library`. Otherwise, this error appears:

```
unless ($error) {

    my $xs = XML::Simple->new();

    $stdout_hash = $xs->XMLin($stdout,forceArray=>0);

    return 0;

}

return 1;
```

Asynchronous Command Delay

Commands that invoke an action on the everRun system are called *asynchronous* because the command completes before the action completes. This allows for complex scripting.

If you want a command to complete inline before proceeding to the next command, create a simple script and use the —wait option. For example:

```
$ cli -x -H eagles node-workon --wait node0
```

In this example, `cli` does not complete until VMs and the management port are failed over from node0 to node1, and node0 is in maintenance mode. Without the `—wait` option, the command completes when acknowledged but before the resources are migrated.

Output Formatting

AVCLI can create user-friendly command output and program-friendly XML output.

User-Friendly Command Output

AVCLI output is formatted for easy readability. For example:

```
$ avance -u admin -p admin -H avance -x node-info

node:

-> name : node0

-> id : host:o14

-> state: running

-> sub-state : nil

-> standing-state : maintenance

-> mode : maintenance

-> primary : false

-> manufacturer : Dell

-> model : Dell PowerEdge 2950

-> maintenance-allowed : true

-> maintenance-guest-shutdown : false

-> cpus : 8

-> memory : 4,288,675,840

virtual machines:

node:

-> name : node1
```

```
-> id : host:o406

-> state : running

-> sub-state : nil

-> standing-state : warning

-> mode : normal

-> primary : true

-> manufacturer : Dell

-> model : Dell PowerEdge 2950

-> maintenance-allowed : true

-> maintenance-guest-shutdown : true

-> cpus : 8

-> memory : 4,288,675,840

virtual machines:

virtual machine:

-> name : eagles1

-> id : vm:o1836
```

> ℹ **Note**: The output format of these commands may vary between releases.

Program-Friendly XML Output

You can create program-friendly XML output by using the `-x` or `--xml` global option. For example:

```
$ avcli -u admin -p admin -H localhost -x node-info

<?xml version="1.0" encoding="utf-8" standalone="no"?>

<avance>

<node>

<name>node1</name>

<id>host:o55</id>
```

```
<state>running</state>

<manufacturer>Intel Corporation</manufacturer>

<model>S5520UR</model>

<memory>25706889216</memory>

</node>

<node>

<name>node0</name>

<id>host:o23</id>

<state>running</state>

<manufacturer>Intel Corporation</manufacturer>

<model>S5520UR</model>

<maintenance-allowed>true</maintenance-allowed>

<maintenance-guest-shutdown>false</maintenance-guest-shutdown>
```

```
<cpus>2</cpus>

<memory>25706889216</memory>

<virtual-machines>

<virtual-machine>

<name>MyVM</name>

<id>vm:o6417</id>

</virtual-machine>

</virtual-machines>

</node>

</avance>
```

> ℹ **Note**: The schema definition is maintained between releases.

If you do **not** specify -X or --XML and the command returns an error, a verbose message appears. For example:

```
$ cli -H eagles vm-delete eagles23

%Error: Cannot find a resource that matches the identifier
eagles23. com.avance.yak.cli.exceptions.CommandLineException:
Cannot find a resource that matches the identifier eagles23.

at

com.avance.yak.cli.ResourceDisambiguateServiceProvider.throwNo
nExistentResource(ResourceDisambiguateServiceProvider.java:56)


at

com.avance.yak.cli.ResourceDisambiguateServiceProvider.getReso
urceId(ResourceDisambiguateServiceProvider.java:81)

at

com.avance.yak.cli.Command.findResourceId(Command.java:80)
```

```
at
com.avance.yak.cli.CommandWithUnparsedAmbiguousResourcesInvoke
Each.execute
(CommandWithUnparsedAmbiguousResourcesInvokeEach.java:65)
at
com.avance.yak.cli.Command.execute(Command.java:194)
at
com.avance.yak.cli.CommandLine.execute(CommandLine.java:649)
at
```

AVCLI Exceptions

If you do not specify `-X` or `--XML` and the command returns an error, a verbose message appears. For example:

```
$ cli -H eagles vm-delete eagles23
%Error: Cannot find a resource that matches the identifier
eagles23. com.avance.yak.cli.exceptions.CommandLineException:
Cannot find a resource that matches the identifier eagles23.
at
com.avance.yak.cli.ResourceDisambiguateServiceProvider.throwNo
nExistentResource(ResourceDisambiguateServiceProvider.java:56)

at
com.avance.yak.cli.ResourceDisambiguateServiceProvider.getReso
urceId(ResourceDisambiguateServiceProvider.java:81)
at
com.avance.yak.cli.Command.findResourceId(Command.java:80)
at
```

```
com.avance.yak.cli.CommandWithUnparsedAmbiguousResourcesInvoke

Each.execute

(CommandWithUnparsedAmbiguousResourcesInvokeEach.java:65)

at

com.avance.yak.cli.Command.execute(Command.java:194)

at

com.avance.yak.cli.CommandLine.execute(CommandLine.java:649)

at

com.avance.yak.cli.Program.main(Program.java:94)
```

AVCLI Command Descriptions

Click each heading to see the full list of AVCLI commands in that group.

> **Note**: The Examples section for each command assumes that you have set up a command shortcut as described in .

Help

Basic System Information

System Configuration

System User Management

Managing Physical Machines

Managing Alerts

Managing Virtual Machines

Related Topics

ad-disable

Usage

```
avcli ad-disable
```

Description

The `ad-disable` command disables Active Directory support.

ad-enable

Usage

```
avcli ad-enable
```

Description

The `ad-enable` command enables Active Directory support.

ad-info

Usage

```
avcli ad-info
```

Description

The `ad-info` command displays information about the Active Directory.

ad-join

Usage

```
avcli ad-join --username name [--password password] domain
```

Description

The `ad-join` command joins the everRun system to the specified Active Directory domain and enables Active Directory support.

Options

`--username` *name*	The user with rights to join to the specified domain.
`--password` *password*	The password of the user with rights to join to the specified domain. If you do not give the password, you are automatically prompted for it.
domain	The name of the Active Directory domain to join.

Examples

```
$ avcli ad-join --username domain\administrator --password
secret domain
```

```
$ avcli ad-join --username domain\administrator domain
```

ad-remove

Usage

```
avcli ad-remove --username name [--password password] domain
```

Description

The `ad-remove` command removes the everRun system from the specified Active Directory domain and disables Active Directory support.

Options

`--username` *name*	The user with rights to remove the everRun system from the specified domain.
`--password` *password*	The password of the user with rights to remove the ever-Run system from the specified domain. If you do not give the password, you are automatically prompted for it.
domain	The name of the Active Directory domain from which the everRun system is to be removed.

Examples

```
$ avcli ad-remove --username domain\administrator --password
secret domain
```

```
$ avcli ad-remove --username domain\administrator domain
```

---

alert-delete

Usage

```
avcli alert-delete [alerts... | purge]
```

Description

The `alert-delete` command deletes specific alerts or optionally, all alerts.

Options

alerts	One or more alerts to be deleted.
`purge`	Delete all alerts.

Examples

```
$ avcli alert-delete alert:o10
```

```
$ avcli alert-delete alert:o10 alert:o11
```

```
$ avcli alert-delete purge
```

alert-info

Usage

```
avcli alert-info [alerts...]
```

Description

The `alert-info` command displays information about all alerts or only those specified.

Options

alerts	The alert information to be displayed.

audit-export

Usage

```
avcli audit-export
```

Description

The `audit-export` command exports all of the audit logs.

audit-info

Usage

```
avcli audit-info [number-of-audit-logs]
```

Description

The `audit-info` command displays either the last 50 audit logs or the specified number of audit logs.

Options

number-of-audit-logs	The number of audit logs to display. The default value is 50.

Examples

```
$ avcli audit-info
```

```
$ avcli audit-info 25
```

callhome-disable

Usage

```
avcli callhome-disable
```

Description

The `callhome-disable` command disables call home.

callhome-enable

Usage

```
avcli callhome-enable
```

Description

The `callhome-enable` command enables call home.

callhome-info

Usage

```
avcli callhome-info
```

Description

The `callhome-info` command displays information about call home.

datetime-config

Usage

```
avcli datetime-config date time [timezone]
```

Description

The `datetime-config` command sets the date, time, and time zone on everRun systems.

Options

date	The date, formatted as *YYYY-MM-DD*.
time	The time, formatted as *HH*:*MM*:*SS,* in a 24-hour format.
timezone	The time zone. By default, it is the currently configured time zone.

You can specify the following values for *timezone*.

Africa/Cairo	Africa/Casablanca	Africa/Harare
Africa/Lagos	Africa/Monrovia	Africa/Nairobi
Africa/Windhoek	America/Adak	America/Anchorage
America/Asuncion	America/Bogota	America/Buenos_Aires
America/Caracas	America/Chicago	America/Chihuahua
America/Cuiaba	America/Denver	America/Godthab
America/Goose_Bay	America/Grand_Turk	America/Guyana
America/Halifax	America/Havana	America/Indianapolis
America/Los_Angeles	America/Managua	America/Manaus
America/Mexico_City	America/Miquelon	America/Montevideo

America/New_York	America/Noronha	America/Phoenix
America/Regina	America/Santiago	America/Sao_Paulo
America/St_Johns	America/Tijuana	America/Winnipeg
Asia/Amman	Asia/Baghdad	Asia/Baku
Asia/Bangkok	Asia/Beijing	Asia/Beirut
Asia/Bishkek	Asia/Calcutta	Asia/Colombo
Asia/Damascus	Asia/Dhaka	Asia/Gaza
Asia/Hong_Kong	Asia/Irkutsk	Asia/Jerusalem
Asia/Kabul	Asia/Kamchatka	Asia/Karachi
Asia/Katmandu	Asia/Krasnoyarsk	Asia/Magadan
Asia/Novosibirsk	Asia/Rangoon	Asia/Riyadh
Asia/Seoul	Asia/Singapore	Asia/Taipei
Asia/Tashkent	Asia/Tbilisi	Asia/Tehran
Asia/Tokyo	Asia/Vladivostok	Asia/Yakutsk
Asia/Yekaterinburg	Asia/Yerevan	Atlantic/Azores
Atlantic/Cape_Verde	Atlantic/Stanley	Australia/Adelaide
Australia/Brisbane	Australia/Darwin	Australia/Hobart
Australia/Lord_Howe	Australia/Melbourne	Australia/Perth
Australia/Sydney	Etc/GMT	Etc/GMT+1
Etc/GMT+10	Etc/GMT+11	Etc/GMT+12

Etc/GMT+2	Etc/GMT+3	Etc/GMT+4
Etc/GMT+5	Etc/GMT+6	Etc/GMT+7
Etc/GMT+8	Etc/GMT+9	Etc/GMT-1
Etc/GMT-10	Etc/GMT-11	Etc/GMT-12
Etc/GMT-13	Etc/GMT-14	Etc/GMT-2
Etc/GMT-3	Etc/GMT-4	Etc/GMT-5
Etc/GMT-6	Etc/GMT-7	Etc/GMT-8
Etc/GMT-9	Europe/Athens	Europe/Belgrade
Europe/Berlin	Europe/Helsinki	Europe/Istanbul
Europe/Kaliningrad	Europe/London	Europe/Minsk
Europe/Moscow	Europe/Paris	Europe/Samara
Europe/Sarajevo	Japan	Pacific/Auckland
Pacific/Chatham	Pacific/Easter	Pacific/Fiji
Pacific/Guam	Pacific/Marquesas	Pacific/Norfolk
Pacific/Tongatapu		

Examples

```
$ avcli datetime-config 2010-12-31 6:03:10

$ avcli datetime-config 2010-12-31 20:09:22 America/New_York
```

diagnostic-create

Usage

```
avcli diagnostic-create [minimal | medium | stats | full]
```

Description

The `diagnostic-create` command creates a new diagnostic of the specified type.

Options

minimal	The smallest diagnostic (approximately 2 to 10 MB).
medium	A medium diagnostic (approximately 10 MB).
full	A large diagnostic (approximately 60 MB).

diagnostic-delete

Usage

```
avcli diagnostic-delete diagnostics...
```

Description

The `diagnostic-delete` command deletes the specified diagnostic files.

Options

diagnostics	One or more diagnostic files to be deleted.

diagnostic-extract

Usage

```
avcli diagnostic-extract diagnostics.zip...
```

Description

The `diagnostic-extract` command extracts the specified diagnostic files.

Options

diagnostics	One or more diagnostic files to be extracted.

diagnostic-fetch

Usage

```
avcli diagnostic-fetch [--file name] diagnostics...
```

Description

The `diagnostic-fetch` command downloads the specified diagnostics to the current directory. If the diagnostic's status is busy, `diagnostic-fetch` waits for the diagnostic to complete and then downloads it. The default diagnostic file name is `diagnostic-`*type-name_ YYYYMMDD_HHMMSS*`.zip`:

- *type*: The type of diagnostic: minimal, medium, stats, full.

- *name*: The name of the everRun system, as displayed by `unit-info`.

- *YYYY*: The year the diagnostic was created.

- *MM:* The month the diagnostic was created.

- *DD*: The day of the month the diagnostic was created.

- *HH*: The hour the diagnostic was created.

- *MM*: The minute the diagnostic was created.

- *SS*: The second the diagnostic was created.

Options

diagnostics	One or more diagnostic files to be downloaded.
`--file` *name*	The name of the file written to the current directory. This option is valid if only one diagnostic is downloaded.
`--extract`	Extract the downloaded diagnostic files.

Examples

```
$ avcli diagnostic-fetch buggrab:o10

$ avcli diagnostic-fetch --file buggrab.zip buggrab:o10

$ avcli diagnostic-fetch buggrab:o10 buggrab:o11 buggrab:o12
```

diagnostic-info

Usage

```
avcli diagnostic-info diagnostics...
```

Description

The `diagnostic-info` command displays information about all diagnostics or only about those specified.

Options

diagnostics	One or more diagnostic files about which to display information.

dialin-disable

Usage

```
avcli dialin-disable
```

Description

The `dialin-disable` command disables dial-in.

dialin-enable

Usage

```
avcli dialin-enable
```

Description

The `dialin-enable` command enables dial-in.

dialin-info

Usage

```
avcli dialin-info
```

Description

The `dialin-info` command displays information about dial-in configuration.

disk-move-to-group

Usage

```
avcli disk-move-to-group disk... storage-group
```

Description

The `disk-move-to-group` command moves one or more logical disks to a storage group.

Options

disk	One or more disks to be moved.
storage-group	A storage group.

ealert-config

Usage

```
avcli ealert-config [--ssl] [--username username] [--password
password] --host host recipients...
```

Description

The `ealert-config` command configures e-Alert support in everRun systems. If you do not provide a user name, the command assumes that authentication is not required to access the SMTP server. If you provide a user name but not a password, the command prompts you for the password.

Options

`--ssl`	Use SSL when communicating with the SMTP server.
`--username` *username*	Use this name for authentication on the specified SMTP host.
`--password` *password*	Use this password for authentication on the specified SMTP host.
`--host` *host*	The DNS or IP address of the SMTP server.
recipients	The list of email addresses to receive eAlert emails; required only when e-Alerts are enabled.

Examples

The following command configures email alerts to use the SMTP server `mail.my-domain.com` and to send alerts to the recipient `admin@my-domain.com`:

```
$ avcli ealert-config --host mail.my-domain.com admin@my-
domain.com
```

The following command configures email alerts to use the SMTP server `mail.my-domain.com` and to send alerts the recipients `admin@my-domain.com` and `bob@my-domain.com`:

```
$ avcli ealert-config --host mail.my-domain.com admin@my-
domain.com bob@my-domain.com
```

The following command configures email alerts to use the protocol SSL and the SMTP server `mail.my-domain.com`, and to send alerts to the recipient `bob@my-domain.com`, using the username `admin` and the password `secret` for authentication:

```
$ avcli ealert-config --ssl --username admin --password secret
--host mail.my-domain.com bob@my-domain.com
```

The following command configures email alerts to use the protocol SSL and the SMTP server `mail.my-domain.com`, and to send alerts to the recipient `bob@my-domain.com`, using the username `admin` and no password for authentication:

```
$ avcli ealert-config --ssl --username admin --host mail.my-
domain.com bob@my-domain.com
```

ealert-disable

Usage

```
avcli ealert-disable
```

Description

The `ealert-disable` command disables e-Alert.

ealert-enable

Usage

```
avcli ealert-enable
```

Description

The `ealert-enable` command enables e-Alert.

ealert-info

Usage

```
avcli ealert-info
```

Description

The `ealert-info` command displays information about the e-Alert configuration.

help

Usage

```
avcli help [command] [-all]
```

Description

The `help` command provides help about a specific command or lists all AVCLI commands.

Options

`-all`	Display detailed information for all commands.

Examples

To display general command usage and a list of all commands for which `help` provides information:

```
$ avcli help
```

To display information about a specific command (`storage-info`, in this example):

```
$ avcli help storage-info
```

To display detailed information about all commands for which `help` provides information:

```
$ avcli help -all
```

image-container-info

Usage

```
image-container-info [image-container]
```

Description

The `image-container-info` command displays information about all image containers (also known as *volume containers*) or optionally, about only the specified image containers. Specifically, the command displays information about the portion of the image container that is available to the guest operating system.

Options

image-container	The name of the image container. If you do not provide this argument, the command displays information about all image containers.

Examples

```
$ avcli image-container-info

image-container:

-> name : root

-> id : imagecontainer:o58

-> hasFileSystem : false

-> isLocal : true

-> size : 21,479,030,784

-> size-used : 21,479,030,784

-> storage-group : none

image-container:

-> name : root

-> id : imagecontainer:o31

-> hasFileSystem : false
```

```
-> isLocal : true

-> size : 21,479,030,784

-> size-used : 21,479,030,784

-> storage-group : none

image-container:

-> name : swap

-> id : imagecontainer:o36

-> hasFileSystem : false

-> isLocal : true

-> size : 2,151,677,952

-> size-used : 2,151,677,952

-> storage-group : none

image-container:

-> name : swap

-> id : imagecontainer:o66

-> hasFileSystem : false

-> isLocal : true

-> size : 2,151,677,952

-> size-used : 2,151,677,952

-> storage-group : none

image-container:

-> name : shared.fs_image_container

-> id : imagecontainer:o77

-> hasFileSystem : false

-> isLocal : false
```

```
-> size : 1,073,741,824

-> size-used : 1,073,741,824

-> storage-group : none

image-container:

-> name : win7_ent_x86_32_sp1

-> id : imagecontainer:o1360

-> hasFileSystem : false

-> isLocal : false

-> size : 2,684,354,560

-> size-used : 2,684,354,560

storage-group:

-> name : Initial Storage Group

-> id : storagegroup:o21

image-container:

-> name : boot-chom1

-> id : imagecontainer:o1690

-> hasFileSystem : true

-> isLocal : false

-> size : 42,949,672,960

-> size-used : 37,787,627,192

storage-group:

-> name : Initial Storage Group

-> id : storagegroup:o21
```

image-container-resize

Usage

```
image-container-resize --new-size size image-container
```

Description

The `image-container-resize` command increases the size of the image container; specifically, the portion that is available to the guest operating system. (An *image container*, also known as a *volume container*, is a system-wide container that holds volumes and snapshots.) You might want to increase the image container's size if you need to take snapshots and the container lacks sufficient free space to do so.

Options

`--new-size size`	The new image-container size. By default, *size* is in megabytes, but you can specify standard qualifiers (for example, KB, K, MB, M, GB, or G).
image-container	The name of the image container.

Examples

```
$ avcli image-container-resize --new-size 40G boot-chom1
```

kit-delete

Usage

```
avcli kit-delete kit_id
```

Description

The `kit-delete` command deletes the specified kit(s).

Options

kit_id	One or more upgrade kits to be deleted. The value is the kit ID.

For information on obtaining the value for *kit_id*, see the command description.

Example

```
kit-delete kit:o24
```

kit-info

Usage

```
avcli kit-info [kit_id...]
```

Description

The `kit-info` command displays information about all kits (the default) or only the specified kits.

Options

kit_id	One or more upgrade kits about which to display information. The value is the kit ID.

Examples

You can issue the `kit-info` command to obtain the *kit-id* value for the "kit-delete" on page 311 command. In the command output, the `id` field displays the *kit-id* value. In the following sample output of the `kit-info` command, the `id` field displays the value `kit:o24`:

```
[root@node0 ~]# avcli kit-info
-> name : unspecified
-> id : kit:o24
-> description : unspecified
-> version : 7.5.0-127
-> locked : false
```

license-info

Usage

```
avcli license-info
```

Description

The `license-info` command displays information about the license.

license-install

Usage

```
avcli license-install license-file
```

Description

The `license-install` command installs the specified license file.

Options

license-file	The file containing the license-key definitions.

Examples

```
$ avcli license-install avance.key
```

local-group-add

Usage

```
avcli local-group-add --name name --permissions permission-
type
```

Description

The `local-group-add` command adds a new local user group.

Options

`--name` *name*	Local group name.
`--permissions` *permission-type*	Local group permissions, in the form of a comma-separated list.

Examples

```
$ avcli local-group-add --name unprivileged_users --
permissions ADD_USER
```

local-group-delete

Usage

```
avcli local-group-delete groups...
```

Description

The `local-group-delete` command deletes the specified local user groups. You cannot delete default groups (`admin`, `platform_admin`, `read_only`).

Options

groups	Local user groups.

Examples

```
$ avcli local-group-delete unprivileged_users
```

local-group-edit

Usage

```
avcli local-group-edit [--name] [--permissions] group-name-or-
sid
```

Description

The `local-group-edit` command edits an existing local user group. You cannot edit default
groups (`admin`, `platform_admin`, `read_only`).

Options

`--name` *name*	New local group name.
`--permissions` *permission-type*	Local group permissions, in the form of a comma-separated list.
group-name-or-sid	The name or security ID.

Examples

```
$ avcli local-group-edit --name privileged_users --permissions
ADD_USER unprivileged_users
```

local-group-info

Usage

```
avcli local-group-info [groups...]
```

Description

The `local-group-info` command displays information about all local user groups, or only those specified.

Options

groups	Local user groups.

local-user-add

Usage

```
avcli local-user-add --username name --realname name --email
address [--password password] [--new-password password] [--
local-groups groups] [--permissions permission-types]
```

Description

The `local-user-add` command adds a new local user to the everRun system. If the user's password is not given, the user is automatically prompted for it. The user is prompted twice to verify that the password was entered correctly.

Options

`--username` *name*	everRun local user name.
`--password` *password*	Boolean flag that indicates whether the user should be prompted for a new password.
`--new-password` *password*	Specify the password as a command-line option instead of being prompted in the same way as `--password`.
`--realname` *name*	The user's real name.
`--email` *address*	The user's email address.
`--local-groups` *groups*	Local groups for the user to join, in the form of a comma-separated list.
`--permissions` *permission-types*	Local user permissions, in the form of a comma-separated list.

Examples

```
$ avcli local-user-add --username bsmith --realname "Bob
Smith" --email bsmith@example.com --password secret --local-
groups admin
```

```
$ avcli local-user-add --username bsmith --realname "Bob
Smith" --email bsmith@example.com --local-groups users1,users2
--permissions ADD_USER,UPDATE_USER
```

local-user-delete

Usage

```
avcli local-user-delete users...
```

Description

The `local-user-delete` command deletes the specified local users.

Options

users	One or more local users.

Examples

```
$ avcli local-user-delete afjord
```

```
$ avcli local-user-delete afjord bsmith tkirch
```

local-user-edit

Usage

```
avcli local-user-edit user [--username name]  [--realname
name] [--email address]  [--password password] [--new-password
password] [--local-groups groups] [--permissions permission-
types] user-name-or-sid
```

Description

The `local-user-edit` command edits an existing user. If you do not give the `--password` option, the password is not changed. If you give the `--password` option, the command prompts the user twice to verify that the password was entered correctly.

Options

`--username` *name*	The user name to assign.
`--password` *password*	Boolean flag that indicates whether the user should be prompted for a new password.
`--new-password` *password*	Specify the password as a command-line option instead of being prompted in the same way as `--password`.
`--realname` *name*	The user's real name.
`--email` *address*	The user's email address.
`--local-groups` *groups*	Local groups for the user to join, in the form of a comma-separated list.
`--permissions` *permission-types*	Local user permissions, in the form of a comma-separated list.
group-name-or-sid	The name or security ID.

Examples

```
$ avcli local-user-edit --email bsmith@example.net bsmith

$ avcli local-user-edit --realname "Robert Smith" --email
rsmith@example.com bsmith

$ avcli local-user-edit --email bsmith@example.net --local-
groups read_only --permissions ADD_USER,UPDATE_USER bsmith

$ avcli local-user-edit --password bsmith

$ avcli local-user-edit --new-password secret bsmith
```

local-user-info

Usage

```
avcli local-user-info [user...]
```

Description

The `local-user-info` command displays information about all users (by default) or only about the specified users.

Options

user	One or more users about which to display information.

localvm-clear-mtbf

Usage

```
avcli localvm-clear-mtbf
```

Description

The `localvm-clear-mtbf` command brings half of a VM back into service after it has been

removed from service for failing too many times.

media-create

Usage

```
avcli media-create [--storage-group storage] [--name name]
url...
```

Description

The `media-create` command loads an ISO image into an everRun system from the specified URL.

Options

`--storage-group` *group*	The storage volume to carve from. If you do not specify this option, the storage group with the most free space is automatically selected.
`--name` *name*	The name of the carved volume. If you do not specify this option, the name is determined from the URL.
url	The URL where the ISO file is located.
`--wait`	Wait for the ISO(s) to be created.

Examples

```
avcli media-create --storage-group Pool-0001 --name cd.iso
http://hostname/cd.iso

avcli media-create http://hostname/cd.iso

avcli media-create http://hostname/cd1.iso
http://hostname/cd2.iso
```

media-delete

Usage

```
avcli media-delete media...
```

Description

The `media-delete` command deletes the specified media.

Options

media	The media to be deleted.

media-eject

Usage

```
avcli media-eject [--cdrom name] [vm...]
```

Description

The `media-eject` command ejects media from the specified virtual machines.

Options

`--cdrom` *name*	The CD-ROM device to eject. This value is optional if the VM has only a single CD-ROM device.
vm	The name of the VM containing the media to be ejected.

media-import

Usage

```
avcli media-import [--storage-group storage] [--name name] [--
throttle] [--silent] file...
```

Description

The `media-import` command loads an ISO image into an everRun system from the specified
file.

Options

`--storage-group` *group*	The storage volume to carve from. If you do not specify this option, the shared storage with the most free space is automatically selected.
`--name` *name*	The name of the carved volume. If you do not specify this option, the name is determined from the file. This option is valid only if one ISO is specified.
`--throttle`	Slow down the import/export operation. Valid values are: • `none`: Do not use throttling. This is the default value. • `low`: Slow down by about 25%. • `medium`: Slow down by about 50%. • `high`: Slow down by about 75%.
`--silent`	Suppress output.
file	The file(s) containing an ISO image.

Examples

```
avcli media-import --storage-group Pool-0001 --name cd.iso
cd.iso
avcli media-import cd.iso
```

```
avcli media-import cd1.iso cd2.iso
```

media-info

Usage

```
avcli media-info [media...]
```

Description

The `media-info` command displays information about all media, or optionally, only the specified media.

Options

media	The media about which to display information.

network-change-mtu

Usage

```
avcli network-change-mtu name size
```

Description

The `network-change-mtu` command changes the MTU size of the specified A-Link network on everRun systems.

Options

name	The name of the A-link network
size	The MTU size. Valid values are 1500 - 9000.

Examples

The following commands change the MTU size on the A-Link `priv0`.

```
$ avcli network-change-mtu priv0 4000
```

```
$ avcli network-change-mtu priv0 9000
```

network-change-role

Usage

```
avcli network-change-role networks... role
```

Description

The `network-change-role` command changes the role of the specified network to the specified role.

Options

networks	One or more networks whose role is to be changed.
role	The new role. Specify either `business` or `a-link`.

network-info

Usage

```
avcli network-info [networks...]
```

Description

The `network-info` command displays information about all shared networks, or optionally, about only the specified networks.

Options

networks	One or more networks.

Output

The following example shows the settings for four networks, including the default MTU value of 1500 for A-Links.

```
avcli network-info
shared network:
     -> name           : sync_2003
     -> id             : sharednetwork:o2334
     -> fault-tolerant : ft
     -> role           : a-link
     -> bandwidth      : 10 Gb/s
     -> mtu            : 1500
shared network:
     -> name           : network0
     -> id             : sharednetwork:o64
     -> fault-tolerant : ft
     -> role           : business
     -> bandwidth      : 1 Gb/s
     -> mtu            : 1500
```

```
shared network:

     -> name          : sync_2004

     -> id            : sharednetwork:o2333

     -> fault-tolerant : ft

     -> role          : a-link

     -> bandwidth     : 10 Gb/s

     -> mtu           : 1500

shared network:

     -> name          : priv0

     -> id            : sharednetwork:o65

     -> fault-tolerant : ft

     -> role          : private

     -> bandwidth     : 1 Gb/s

     -> mtu           : 1500
```

node-add

Usage

```
avcli node-add [--wait]
```

Description

The `node-add` command adds a PM to an everRun system.

Options

--wait -w	Wait for the command to complete.

node-cancel

Usage

```
avcli node-cancel pm
```

Description

The `node-cancel` command cancels a PM that is being imaged.

Options

pm	The PM to cancel.

node-config-prp

Usage

```
avcli node-config-prp --nic1 adapter --nic2 adapter node
```

Description

The `node-config-prp` command configures a PRP adapter on the specified PM with two physical adapters.

You must run this command twice: once to configure the adapter on the first PM, and once to configure the adapter on the second PM.

Options

`--nic1 adapter`	The name of a physical adapter.
`--nic2 adapter`	The name of a physical adapter.
node	The PM containing the PRP adapter to be configured.

Examples

```
$ avcli node-config-prp --nic1 eth0 --nic2 eth1 node0
```

node-delete

Usage

```
avcli node-delete pm [--wait]
```

Description

The `node-delete` command deletes a PM.

Options

pm	The PM to be deleted. It must be in maintenance mode.
--wait -w	Wait for the command to complete.

node-delete-prp

Usage

```
avcli node-delete-prp --name adapter node
```

Description

The `node-delete-prp` command deletes a PRP adapter on the specified PM.

You must run this command twice: once to delete the adapter on the first PM, and once to delete the adapter on the second PM.

Options

`--name adapter`	The name of the adapter to delete.
node	The PM containing the adapter to delete.

Examples

```
$ avcli node-delete-prp --name ad0 node0
```

node-info

Usage

```
avcli node-info [pm...]
```

Description

The `node-info` command displays information about all PMs (by default) or only about the specified PMs.

Options

pm	The PM about which to display information.

node-reboot

Usage

```
avcli node-reboot [--wait] pm
```

Description

The `node-reboot` command reboots the specified PM.

Options

`--wait`
 	
`-w`
	Wait for the command to complete.

pm	The PM to reboot.

node-recover

Usage

```
avcli node-recover [--wipe] pm [--wait]
```

Description

The `node-recover` command recovers the specified PM.

Options

pm	The PM to recover.
`--wipe`	Wipe the disks off the PM prior to recovery.

`--wait`
 	
`-w`
	Wait for the command to complete.

node-shutdown

Usage

```
avcli node-shutdown [--force] [--wait] pm
```

Description

The `node-shutdown` command shuts down the specified PM. Before issuing `node-shutdown`, you must first place the node in maintenance mode. To do so, you can issue `"node-workon" on page 346` or use the everRun Availability Console.

Options

`--force`
 	
`-f`
	Override the shutdown warning.

`--wait`
 	
`-w`
	Wait for the command to complete.

pm	The PM (for example, `node1`) to shut down.

Examples

```
$ avcli node-workon node0
$ avcli node-shutdown --force node0
```

node-workoff

Usage

```
avcli node-workoff [--wait] pm
```

Description

The `node-workoff` command takes the specified PM out of maintenance mode.

Options

`--wait`
 	
`-w`
	Wait for the command to complete.

pm	The PM to remove from maintenance mode.

node-workon

Usage

```
avcli node-workon pm
```

Description

The `node-workon` command places the specified PM in maintenance mode.

Options

pm	The PM to place into maintenance mode.

Examples

```
$ avcli node-workon node0
```

ntp-config

Usage

```
avcli ntp-config servers...
```

Description

The `ntp-config` command enables and configures NTP support using the specified list of servers.

Options

servers	The list of servers to configure.

Examples

```
$ avcli ntp-config 1.2.3.4
$ avcli ntp-config 1.2.3.4 2.4.6.8
```

ntp-disable

Usage

```
avcli ntp-disable
```

Description

The `ntp-disable` command disables NTP in your everRun system.

ova-info

Usage

```
avcli ova-info filename.ova...
```

Description

The `ova-info` command displays information about the specified OVA files.

Options

filename`.ova`	One or more OVA files.

ovf-info

Usage

```
avcli ovf-info filename.ovf...
```

Description

The `ovf-info` command displays information about the specified OVF files.

Options

filename`.ovf`	One or more OVF files.

owner-config

Usage

```
avcli owner-config [--email address] [--name name] [--phone
number]
```

Description

The `owner-config` command configures the everRun system's owner information.

Options

`--email` *address*	The owner's email address.
`--name` *name*	The owner's name.
`--phone` *number*	The owner's phone number.

Examples

```
$ avcli owner-config --email "Bob Smith" --email
bsmith@example.org --phone 800-555-1234
```

```
$ avcli owner-config --phone 800-555-1234
```

owner-info

Usage

```
avcli owner-info
```

Description

The `owner-info` command displays information about the owner of the everRun system.

pm-clear-mtbf

Usage

```
avcli pm-clear-mtbf
```

Description

The `pm-clear-mtbf` command clears a PM's MTBF from the user interface.

proxy-config

Usage

```
avcli proxy-config --port name [--username name] [--password
password] host
```

Description

The `proxy-config` command configures the everRun system to use a proxy server. If you do not specify a user name, AVCLI assumes that authentication is not required to access the proxy server. If you specify a user name but not a password, you are prompted for the password.

Options

`--port` *number*	The port number.
`--username` *name*	The user's name.
`--password` *password*	The user's password.
host	The host name.

Examples

```
$ avcli --port 8080 proxy.my-domain.com
```

```
$ avcli --port 8080 --username user --password secret
proxy.my-domain.com
```

```
$ avcli --port 8080 --username user proxy.my-domain.com
```

proxy-disable

Usage

```
avcli proxy-disable
```

Description

The `proxy-disable` command disables proxy.

proxy-enable

Usage

```
avcli proxy-enable
```

Description

The `proxy-enable` command enables proxy.

proxy-info

Usage

```
avcli proxy-info
```

Description

The `proxy-info` command displays information about the proxy configuration.

snmp-config

Usage

```
avcli snmp-config [--enable-requests] [--enable-traps] [--port
number] [--community name] [recipients...]
```

Description

The `snmp-config` command configures SNMP for use in an everRun system.

Options

--enable-requests	Enable SNMP requests. If you do not specify the option, requests are disabled.
--enable-traps	Enable SNMP traps. If you do not specify the option, traps are disabled.
--community *name*	The name of the SNMP community.
--port *number*	The port to use for SNMP. The default is 162.
recipients	The list of hosts to which to send traps; required only when traps are enabled.

Examples

The following example enables SNMP requests, and then traps and sends them to `localhost` and `snmp.my-domain.com`.

```
$ avcli snmp-config --enable-requests --enable-traps --
community public localhost snmp.my-domain.com
```

The following example disables SNMP requests, enables traps, and sends them to `localhost`.

```
$ avcli snmp-config --enable-traps --community public
localhost
```

snmp-disable

Usage

```
avcli snmp-disable
```

Description

The `snmp-disable` command disables SNMP.

snmp-info

Usage

```
avcli snmp-info
```

Description

The `snmp-info` command displays information about SNMP configuration.

storage-group-info

Usage

```
avcli storage-group-info [--disks] [--volumes] [storage-
group...]
```

Description

The `storage-group-info` command displays information about all storage groups, or option-
ally, only about those specified.

Options

`--disks`	Show the logical disks belonging to a storage group.
`--volumes`	Show the volumes using a storage group.
storage-group	One or more storage groups about which to display inform-ation.

storage-info

Usage

```
avcli storage-info [--disks] [--volumes] [storage-group...]
```

Description

The `storage-info` command displays information about all storage groups, or optionally, only about those specified.

Options

`--disks`	Show the logical disks belonging to a storage group.
`--volumes`	Show the volumes using a storage group.
storage-group	One or more storage groups about which to display information.

timezone-config

Usage

```
avcli timezone-config timezone
```

Description

The `timezone-config` command sets the time zone.

Options

timezone	The time zone.

Examples

```
$ avcli timezone-config America/New_York
```

timezone-info

Usage

```
avcli timezone-info
```

Description

The `timezone-info` command displays the list of configurable time zones.

unit-change-ip

Usage

```
avcli unit-change-ip IP_address
```

Description

The `unit-change-ip` command changes the IP configuration of the management network for the everRun system specified by *IP_address*.

Options

IP_address	The IP address of the everRun system.

unit-configure

Usage

```
avcli unit-configure
```

Description

The `unit-configure` command configures the everRun system.

unit-eula-accept

Usage

```
avcli unit-eula-accept [--deny]
```

Description

The `unit-eula-accept` command accepts or denies the EULA.

Options

`--deny`	Deny acceptance of the EULA.

unit-eula-reset

Usage

```
avcli unit-eula-reset
```

Description

The `unit-eula-reset` command resets the EULA acceptance state on an everRun system.

unit-info

Usage

```
avcli unit-info
```

Description

The `unit-info` command displays information about the specified everRun system.

unit-shutdown

Usage

```
avcli unit-shutdown
```

Description

The `unit-shutdown` command shuts down an everRun system.

unit-shutdown-cancel

Usage

```
avcli unit-shutdown-cancel
```

Description

The `unit-shutdown-cancel` command cancels a pending shutdown for an everRun system.

unit-shutdown-state

Usage

```
avcli unit-shutdown-state
```

Description

The `unit-shutdown-state` command returns the everRun system's shutdown state.

unit-synced

Usage

```
avcli unit-synced [--wait]
```

Description

The `unit-synced` command returns true if the everRun system is synchronized between all

PMs; otherwise, it returns false.

Options

`--wait`
 	
`-w`
	Wait for the command to complete.

vm-boot-attributes

Usage

```
avcli vm-boot-attributes --priority priority --application-
start-time minutes [vm...]
```

Description

The `vm-boot-attributes` command sets the boot attributes for the specified VMs.

Options

`--priority` *priority*	The boot priority; values are 1 to 1000.
`--application-start-time` *minutes*	The estimated start time of the VM and application, in minutes. The minimum value is one minute.
vm	One or more VMs whose boot attributes are being set.

Examples

```
$ avcli vm-boot-attributes --priority 1 --application-start-
time 1 vm1
```

```
$ avcli vm-boot-attributes --priority 1 --application-start-
time 1 vm:o100
```

vm-cd-boot

Usage

```
avcli vm-cd-boot --iso iso [--wait] [vm...]
```

Description

The `vm-cd-boot` command starts the specified VMs and boots from the specified ISO image.

Options

--iso *iso*	The ISO image to boot.
--wait	Wait for the VM to boot.
vm	One or more VMs that are being started.

Examples

```
$ avcli vm-cd-boot --iso MyISO vm1

$ avcli vm-cd-boot --iso MyISO vm:o100

$ avcli vm-cd-boot --iso MyISO --wait vm1
```

vm-create

Usage

```
avcli vm-create --name name --cpu number --memory memory --
cdrom cd-name | --kickstart template [--interfaces networks]
[--disabled-interfaces networks] [--storage-group group] --
volumes volumes [--wait]
```

Description

The `vm-create` command creates a new VM.

Options

`--name` *name*	The name of the VM to create.
`--cpu` *number*	The number of virtual CPUs to assign to the VM.
`--memory` *memory*	The amount of memory, in megabytes, to assign to the VM.
`--cdrom` *cd-name*	The CD-ROM from which you initially boot the VM. You cannot specify this option with `--kickstart`.
`--kickstart` *template*	The kickstart template to use when booting the VM. You cannot specify this option with `--cdrom`.
`--interfaces` *networks*	The list of networks to attach to the VM. Specify a network only once. The attached network must not be private.
`--storage-group` *group*	The storage group to use to carve VM volumes from. If you do not specify this value, the storage group with the most free space is automatically selected.
`--volumes` *volumes*	List of volumes to attach to this VM. A *volume* is made up of four components, separated by commas:

	• Size of the volume; required. By default, the volume size is specified in megabytes, but you can use standard qualifiers such as KB, MB, GB, and TB. • Storage-group name or ID from which to carve storage. • Volume name. • Volume disk image format (raw or qcow2).

`--wait`
 	
`-w`
	Wait for the command to complete.

Examples

Create a VM named `vm001` with a CPU, 512 MB of memory, a 1,024 MB volume, and that is attached to `network0`.

```
$ avcli vm-create --name vm001 --cpu 1 --memory 512 --
cdrom linux.iso \
--interfaces network0 --volumes 1024
```

Create a VM named `vm001` with a CPU, 512 MB of memory, a 1,024 MB volume, and that is attached to `network0`. Then allocate storage from `Pool-0001` for the volume.

```
$ avcli vm-create --name vm001 --cpu 1 --memory 512 --
cdrom linux.iso \
--interfaces network0 --volumes 1024 \
--storage-group Pool-0001
```

Create a VM named `vm001` with a CPU, 512 MB of memory, a 1,024 MB volume, and that is attached to `network0`. Then allocate storage from `Pool-0001` for the volume. The volume is named `vm001_vol0`.

```
$ avcli vm-create --name vm001 --cpu 1 --memory 512 --
cdrom linux.iso \
--interfaces network0 --volumes 1024,Pool-0001,vm001_vol0
```

Create a VM named `vm001` with a CPU and 512 MB of memory, and that is attached to network0 and network1. Create two volumes, where the first is 10 GB and the second is 50 GB. Allocate storage for these volumes from `Pool-0001` and `Pool-0002`, respectively.

```
$ avcli vm-create --name vm001 --cpu 1 --memory 512 --
cdrom linux.iso \
--interfaces network0 network1 \
--volumes 10GB,Pool-0001 50GB,Pool-0002
```

Create a VM based on a kickstart template.

```
$ avcli vm-create --name vm001 --cpu 1 --memory 512 --
kickstart template:o81 \
--interfaces network0 --volumes 10GB
```

vm-delete

Usage

```
avcli vm-delete [--volumes volumes] [--wait] vm...
```

Description

The `vm-delete` command deletes the specified VMs, and optionally, the volumes attached to the VMs.

Options

`--volumes` *volumes*	Delete the volumes attached to the VM.
`--wait` `-w`	Wait for the command to complete.
vm	One or more VMs to be deleted.

Examples

```
avcli vm-delete vm1

avcli vm-delete --volumes vm1

avcli vm-delete --volumes vm1 vm2
```

vm-export

Usage

```
avcli vm-export --name name [--folder name] [--use-snapshot]
[--silent] [--config-only] [--data][--description] [--
throttle] [--compress] [--use-https]
```

Description

The `vm-export` command exports the VM.

Options

`--name` *name*	The name or ID of the VM to export.
`--folder` *name*	The destination folder. By default, this is the name of the VM.
`--use-snapshot`	Export using the VM's pre-existing snapshot. When you use a snapshot to export, the complete snapshot is exported, and you cannot specify `--config-only` or `--data`.
`--silent`	Suppress output.
`--config-only`	Export the VM's configuration without any data. You cannot specify this option with `--use-snapshot`.
`--data`	Export data only for the specified volumes. You cannot specify this option with `--use-snapshot`.
`--description`	The user-specified description for this export.
`--throttle`	Slow down the import/export operation. Valid values are: • `none`: Do not use throttling. This is the default value. • `low`: Slow down by about 25%. • `medium`: Slow down by about 50%. • `high`: Slow down by about 75%.

`--compress`	Enable server side compression (such as `gzip`) of the exported volume data. By default, compression is off. ℹ **Note**: Compression is very CPU-intensive and can slow down your export by a factor of 3 or more in some cases.
`--use-https`	Use secure HTTPS transport instead of the default streaming method (HTTP transport). Streaming over HTTPS provides slower performance than HTTP but is much more secure.

Examples

```
$ avcli vm-export --name vm1

$ avcli vm-export --folder /path/exported-vms/vm1 --name vm1

$ avcli vm-export --config-only --name vm1

$ avcli vm-export --compress --use-https --throttle low --name
vm1

$ avcli vm-export --use-snapshot --throttle high --name vm1

$ avcli vm-export --data volume1 volume2 --name vm1
```

vm-import

Usage

```
avcli vm-import --archive filename.ova [--no-auto-start] [--
cpu number] [--memory size] [--name vm-name] [--storage-groups
groups] [--interfaces networks] [--remap-volumes] [--volumes
volumes] [--volume-prefix prefix] [--data] [--force] [--
silent] [--dry-run] [--throttle amount] [--use-https] [--
protection-level level]
```

Description

The `vm-import` command imports a VM from an OVA or OVF VM archive file.

Options

`--archive` *filename.ova*	The OVA or OVF file archive to import.
`--no-auto-start`	Do not start the VM after the import has finished.
`--cpu` *number*	The number of CPUs to assign to the VM. This defaults to the value in the archive.
`--memory` *size*	The size of memory, in megabytes, to assign to the VM. This defaults to the value in the archive.
`--name` *vm-name*	The name to assign to the VM. This defaults to the value in the archive.
`--storage-groups` *groups*	The list of storage groups to use for allocating the VM's volumes. By default, all available storage groups are used. Allocation occurs in a round-robin fashion.
`--interfaces` *networks*	The list of shared networks to assign to the VM's interfaces. By default, values in the archive or available shared networks are assigned.

`--remap-volumes`	First attempt to remap all volumes to the shared-mirrors as defined in the archive, after that the `--volumes` and `--storage-groups` rules are in effect.
`--volumes` *volumes*	Import only these volumes. By default, all available volumes from the OVF are imported.
`--volume-prefix` *prefix*	Adds the specified *prefix* to the beginning of the newly imported volume names to prevent conflicts with existing volumes on the system. For example, if a source volume is `ocean_boot`, and you specify `--volume-prefix new`, the imported volume would be `new-ocean_boot`.
`--data`	Import data only for the specified volumes.
`--force`	When the OVF file is missing the `isBootable` flag (a known issue for Windows XP), assume that the VHD pointed to by OVF is the bootable one.
`--silent`	Suppress output.
`--dry-run`	Show the interface to the shared network and volume-to-storage-group assignments without actually importing or restoring a VM.
`--throttle` *amount*	Slow down the import/export operation. Valid values are: • `none`: Do not use throttling. This is the default value. • `low`: Slow down by about 25%. • `medium`: Slow down by about 50%. • `high`: Slow down by about 75%.

`--use-https`	Use secure HTTPS transport instead of the default streaming method (HTTP transport). Streaming over HTTPS provides slower performance than HTTP but is much more secure.
`--protection-level` *level*	The protection level to assign to the VM. Valid options are `HA` and `FT` (default).

Examples

```
$ avcli vm-import --archive vm1.ova

$ avcli vm-import --archive vm1.ovf

$ avcli vm-import --name myVM --throttle low --archive vm1.ovf

$ avcli vm-import --cpu 2 --memory 1024 --archive vm1.ovf

$ avcli vm-import --interfaces network0 network1 --archive
vm1.ovf

$ avcli vm-import --remap-volumes --archive vm1.ovf

$ avcli vm-import --storage-groups sm-0000 sm-0001 --archive
vm1.ovf

$ avcli vm-import --volumes boot_vol vol3 --data vol3 --
archive vm1.ovf

$ avcli vm-import --name myVM --protection-level HA --archive
vm1.ovf
```

vm-info

Usage

```
avcli vm-info [vm...]
```

Description

The `vm-info` command displays information about all VMs, or optionally, about specific VMs.

Options

vm	One or more VMs for which to display information.

Examples

```
$ avcli vm-info
```

```
$ avcli vm-info vm1
```

```
$ avcli vm-info vm1 vm:o100
```

vm-poweroff

Usage

```
avcli vm-poweroff [vm...] [--wait]
```

Description

The `vm-poweroff` command powers off the specified VMs.

Options

vm	One or more VMs to power off. Specify a VM either by name or ID.
`--wait` `-w`	Wait for the command to complete.

Examples

```
$ avcli vm-poweroff vm1

$ avcli vm-poweroff vm1 vm2

$ avcli vm-poweroff vm1 vm:o100
```

vm-poweron

Usage

```
avcli vm-poweron [vm...] [--wait]
```

Description

The `vm-poweron` command powers on the specified VMs.

Options

vm	One or more VMs to power on. Specify a VM either by name or ID.

`--wait`
 	
`-w`
	Wait for the command to complete.

Examples

```
$ avcli vm-poweron vm1

$ avcli vm-poweron vm1 vm2

$ avcli vm-poweron vm1 vm:o100
```

vm-reprovision

Usage

```
avcli vm-reprovision --name name [--cpu number] [--memory
size] [--addVolumes volumes] [--deleteVolumes volumes] [--
keepVolumes volumes] [--interfaces networks] [--disabled-
interfaces networks]
```

Description

The `vm-reprovision` command reprovisions the specified VM.

Options

`--name` *name*	Specify the VM to reprovision. Reprovision only one VM at a time. Specify a VM either by name or ID.
`--cpu` *number*	The number of virtual CPUs. This defaults to the VM's current amount.
`--memory` *size*	The size of memory, in megabytes. This defaults to the VM's current amount.
`--addVolumes` *volumes*	The list of volumes to attach to this VM. A *volume* is made up of four components, separated by commas: • Size of the volume; required. By default, the volume size is specified in megabytes, but you can use standard qualifiers such as KB, MB, GB, and TB. • Storage-group name or ID from which to carve storage. • Volume name. • Volume disk image format (raw or qcow2).
`--deleteVolumes` *volumes*	The list of volume(s) that are currently attached to the spe-

	cified VM to be deleted. Specify a volume either by name or ID.
`--keepVolumes` *volumes*	The list of volume(s) that are currently attached to the specified VM to be kept attached to the VM. If you specify a volume that is currently attached but not specified in this list, the volume is detached (not destroyed) from the VM. Specify a volume either by name or ID.
`--interfaces`*networks*	The list of networks to attach to the VM. Specify a network only once. The attached network must not be private.
`--disabled-interfaces` *networks*	A list of networks to attach to the VM, but which should not be enabled. Specify a network only once. The attached network must not be private.

Examples

```
$ avcli vm-reprovision --cpu 2 --name vm1

$ avcli vm-reprovision --cpu 2 --name vm:o100

$ avcli vm-reprovision --cpu 2 --memory 2048 --name vm:o100
```

Reprovision a VM named `vm001` that has a CPU, 512 MB of memory, a 1,024 MB volume and is attached to network0, and then allocate storage from `Pool-0001` for the volume. The volume is named `vm001_vol0`.

```
$ avcli vm-reprovision --cpu 1 --memory 512 --interfaces
network0 \

--addVolumes 1024,Pool-0001,vm001_vol0 --name vm1
```

Reprovision VM `vm1`, and then delete the volumes `volume:o411`, `data-vm1`, and `data-vm2` associated with it.

```
$ avcli vm-reprovision --deleteVolumes volume:o411 data-
vm1 data-vm2 --name vm1
```

Reprovision VM `vm1` with the new data volume `data-1-7`, delete volume `volume:o1043`, keep volumes `volume:o1`, `volume:o2`, `volume:o4`, and attach network interfaces `sharednetwork:o129` and `sharednetwork:o130`.

```
$ avcli vm-reprovision --cpu 3 --memory 3359 --addVolume
2500,storagegroup:o54,data-1-7 --deleteVolumes
volume:o1043 --keepVolumes volume:o1 volume:o2 volume:o4 -
-interfaces sharednetwork:o129 sharednetwork:o130 --name
vm1
```

vm-restore

Usage

```
avcli vm-restore --archive filename.ova [--no-auto-start][--
cpu number][--memory size][--name vm-name][--storage-groups
groups][--interfaces networks][--volume-prefix prefix][--data]
[--silent][--dry-run] [--throttle][--use-https]
```

Description

The `vm-restore` command restores a VM from an OVA or OVF file.

Options

`--archive` *filename*`.ova`	The OVA or OVF file archive to restore.
`--no-auto-start`	Do not start the VM after the restore has finished.
`--cpu` *number*	The number of CPUs to assign to the VM. This defaults to the value in the archive.
`--memory` *size*	The size of memory, in megabytes, to assign to the VM. This defaults to the value in the archive.
`--name` *vm-name*	The name to assign to the VM. This defaults to the value in the archive.
`--storage-groups` *groups*	The list of storage groups to use for allocating the VM's volumes. By default, all available storage groups are used. Allocation occurs in a round-robin fashion.
`--interfaces` *networks*	The list of shared networks to assign to the VM's interfaces. By default, values in the archive or available shared networks are assigned.
`--volume-prefix` *prefix*	Adds the specified *prefix* to the beginning of the

	newly imported volume names to prevent conflicts with existing volumes on the system. For example, if a source volume is `ocean_boot`, and you specify `--volume-prefix new`, the imported volume would be `new-ocean_boot`.
`--data`	Restore data only for the specified volumes.
`--silent`	Suppress output.
`--dry-run`	Show the interface to the shared network and volume-to-storage-group assignments without actually restoring a VM.
`--throttle`	Slow down the operation. Valid values are: • `none`: Do not use throttling. This is the default value. • `low`: Slow down by about 25%. • `medium`: Slow down by about 50%. • `high`: Slow down by about 75%.
`--use-https`	Use secure HTTPS transport instead of the default streaming method (HTTP transport). Streaming over HTTPS provides slower performance than HTTP but is much more secure.

Examples

```
$ avcli vm-restore --archive vm1.ova

$ avcli vm-restore --archive vm1/vm1.ovf

$ avcli vm-restore --name myVM --throttle low --archive
vm1.ovf

$ avcli vm-restore --cpu 2 --memory 1024 --archive vm1.ovf
```

```
$ avcli vm-restore --interfaces network0 network1 --archive
vm1.ovf

$ avcli vm-restore --storage-groups sm-0000 sm-0001 --archive
vm1.ovf

$ avcli vm-restore --data vol1 vol3 --archive vm1.ovf
```

vm-shutdown

Usage

```
avcli vm-shutdown [vm...][--wait]
```

Description

The `vm-shutdown` command shuts down the specified VMs.

Options

vm	One or more VMs to shut down. Specify a VM either by name or ID.

`--wait`
 	
`-w`
	Wait for the command to complete.

Examples

```
$ avcli vm-shutdown vm1

$ avcli vm-shutdown vm1 vm2

$ avcli vm-shutdown vm1 vm:o100
```

vm-snapshot-create

Usage

```
avcli vm-snapshot-create [--volumes | --no-data][--
description] [--desire] [--require] vm-name
```

Description

The `vm-snapshot-create` command creates a VM snapshot.

Two snapshot consistency levels are supported:

- *Crash consistency*: The restored data is in the same state that it would have been if the system had crashed at the exact moment that the snapshot was taken. A crash-consistent snapshot does not capture the contents of memory or any pending I/O operations.

- *Application consistency*: Before the snapshot is taken, cooperating applications are briefly frozen so that transactions are complete, buffers flushed, files closed, and so on. This ensures that cooperating applications start from a consistent state. This is the highest level of consistency.

Options

`--volumes | --no-data`	The names of volumes to include in the snapshot. By default, all volumes are included in the snapshot unless you specify `--volumes` with individual volume names or you specify `--no-data`. If you specify `--no-data`, no volumes are included in the snapshot. These arguments are mutually exclusive.
`--description`	The user-specified description for this snapshot.
`--desire`	The highest consistency level to attempt in order to declare the snapshot a success. If this attempt fails, attempts are made at successively lower levels (but no lower than the level specified by `--require`). Values are `crash` and `application` (the default value).
`--require`	The minimum consistency level needed to declare the snapshot a

	success. Values are `crash` and `application` (the default value).
vm-name	The VM's ID.

Examples

```
$ avcli vm-snapshot-create --volumes volume:o100
volume:o101 vm1
```

vm-snapshot-delete

Usage

```
avcli vm-snapshot-delete snapshot...
```

Description

The `vm-snapshot-delete` command deletes the specified snapshots.

Options

snapshot	One or more snapshots of the VM. Specify a snapshot by ID.

Examples

```
$ avcli vm-snapshot-delete vmsnapshot:o100 vmsnapshot:o101
```

vm-snapshot-export

Usage

```
avcli vm-snapshot-export [--wait][--silent][--volumes volumes
| --no-data] --path pathname snapshot
```

Description

The `vm-snapshot-export` command exports a VM in OVF/VHD format to the directory specified by *pathname*. The command first exports VHD files, followed by the OVF file. When the OVF file appears in *pathname*, the export is complete.

> **Note**: Before you can start an export, you must mount a target Windows/CIFS or NFS share (from another system) in the everRun host operating system. For details, see "Exporting a Snapshot" on page 224.

Options

`--wait`	Wait for the export operation to complete. Specify this option to view the export progress.
`--silent`	Suppress progress output.
`--volumes` *volumes*	Restrict the exported volumes to those specified; otherwise, all volumes will be created. Specify volumes by configuration name or ID, boot volume first. You cannot specify this option with the `--no-data` option.
`--no-data`	Do not include any volumes in the exported snapshot. You cannot specify this option with the `--volumes` option.
`--path` *pathname*	A pathname relative to the export mount point to where the exported OVF is written.
snapshot	The name of the snapshot to export.

Examples

Export a snapshot with all captured volumes:

```
$ avcli vm-snapshot-export --path exports/ex1 ex1
```

Export a snapshot without any volume data:

```
$ avcli vm-snapshot-export --no-data --path exports/ex1 ex1
```

Export a snapshot with just one captured volume:

```
$ avcli vm-snapshot-export --volumes boot-ex1 --path
exports/ex1 ex1
```

vm-snapshot-info

Usage

```
avcli vm-snapshot-info [snapshot...]
```

Description

The `vm-snapshot-info` command displays information about all snapshots, or optionally, only about those specified.

Options

snapshot	One or more snapshots of the VM. Specify a snapshot either by name or ID.

vm-unlock

Usage

```
avcli vm-unlock [vm...]
```

Description

The `vm-unlock` command unlocks the specified VMs. For example, VM import operations set the lock to prevent a VM from being started or modified while the operation is occurring. If an operation fails unexpectedly, leaving the VM locked, use this command to unlock that VM.

Options

vm	One or more VMs to unlock. Specify a VM either by name or ID.

Examples

```
$ avcli vm-unlock vm1

$ avcli vm-unlock vm:o100
```

volume-info

Usage

```
avcli volume-info [volume...]
```

Description

The `volume-info` command displays information about all volumes, or optionally, only about those specified.

Options

volume	A volume about which to display information.

volume-resize

Usage

```
avcli volume-resize --new-size size volume
```

Description

The `volume-resize` command resizes a volume. The image container (also known as a *volume container*) must be large enough to allow this. You must stop the VM before specifying this command.

Options

`--new-size` *size*	The new volume size. By default, *size* is in megabytes, but you can specify standard qualifiers (for example, KB, K, MB, M, GB, or G).
volume	The volume to be resized.

Examples

```
# avcli volume-resize --new-size 79G boot-airplane1
```

11

Chapter 11: System Reference Information

See the following topics for reference information

-

-

-

-

Compatible Guest Operating Systems

The following are compatible as guest operating systems for virtual machines (VMs) running on everRun systems.

Operating System	Version
CentOS 7	CentOS 7.064-bit
CentOS 6	CentOS 6.4, 6.5, 6.6 (all 64-bit)
Microsoft Windows Server 2012 (Foundation, Essentials, Standard, Data-center)	64-bit, 64-bit R2
Microsoft Windows Small Business Server 2011 (Standard, Essential, Premium Add-On)	64-bit

Operating System	Version
Microsoft Windows Server 2008 (Web, Small Business, Standard, Enterprise, Datacenter)	32-bit, 64-bit R2 only
Microsoft Windows Server 2003 (Enterprise)	32-bit R2 SP2 [1]
Microsoft Windows 8.1 Desktop Enterprise)	64-bit
Microsoft Windows 8 Desktop (Enterprise)	64-bit
Microsoft Windows 7 Desktop	32-bit, 64-bit
Red Hat Enterprise Linux 7 (Workstation, Server)	Red Hat 7.0 64-bit
Red Hat Enterprise Linux 6 (Workstation, Server)	Red Hat 6.4, 6.5, 6.6 (all 64-bit)
SUSE Linux Enterprise Server	SLES 11 SP3 64-bit
Ubuntu	12.04, 13.10, 14.04 (all 64-bit)

[1]For specific installation and migration procedures, see "Creating a New Windows Server 2003 Virtual Machine" on page 132 and "Migrating a Windows Server 2003 VM to an everRun 7.x System" on page 161.

Physical Machine System Requirements

The following table presents the minimum and maximum capacities of the listed devices for physical machines running on everRun systems.

Physical Device	Minimum	Maximum Tested	Architected	Notes
Processors/CPUs: Intel Xeon E5-2*XXX* v3	1	2	No Practical Limit	

Physical Device	Minimum	Maximum Tested	Architected	Notes
Intel Xeon E5-2*XXX* v2 Intel Xeon E5-*2XXX* Intel Xeon E5-1*XXX* v3 Intel Xeon E5-1*XXX* v2 Intel Xeon E5-1*XXX* Intel Xeon E3-1*XXX* v3 Intel Xeon E3-1*XXX* v2 Intel Xeon E3-1*XXX*				
Number CPU Sockets per Physical Machine	1	2	No Practical Limit	
Physical Memory	8 GB	384 GB	No Practical Limit	
Internal Disk Count per Physical Machine	2	24	No Practical Limit	Minimum 2 drives per PM for FT. VM disks/volumes are replicated on both PMs.
Total Disk Capacity	36 GB	9.4 TB	No Limit	

Physical Device	Minimum	Maximum Tested	Architected	Notes
Management ENET Ports	1	1	1	1 per system required.
A-Link ENET Ports	1 on each PM	8 on each PM		2 recommended. No VM can have more than 2. Maximum of 8 (for 4 or more guests).
Business ENET Ports	1	20		Can be shared with Management link.
Quorum Servers	0	2		

Important Physical Machine and Virtual Machine Considerations

For optimal implementation of physical machines and virtual machines, be aware of the configuration maximums and requirements described in the following sections:

- "Physical Machine System Requirements" on page 405

- "Virtual Machine Recommendations and Limits" on page 407

- "Combined Virtual Machine Maximums" on page 409

- "Important Considerations" on page 410

Virtual Machine Recommendations and Limits

Virtual machines (VMs) require certain CPU core resources and have and other limits for memory, networks, and storage.

Recommended Number of CPU Cores

The number of cores recommended for everRun workloads depends upon the number of vCPUs in each VM and the types of the VMs as described below:

Item	Number of Physical Threads
Fixed system overhead (host and system management)	2
Each FT guest with *n* vCPUs	*n* + 2 (typical)
Each HA guest with *n* vCPUs	*n* + 1 (typical)

> **Note**: A non-hyperthreaded physical CPU core can handle 1 physical thread. A hyper-threaded physical CPU core can handle 2 physical threads.

The actual number of required threads depends upon the workload. The guidelines above should cover most workloads. Since any given workload may require fewer or more threads, it's good practice to test and characterize your specific workload.

Examples

A single 4-vCPU FT guest typically requires:

- 2 threads for host/system management
- 6 threads for guest
  - **8 threads total** (a single socket 4-core hyper-threaded system)

Four 5-vCPU FT guests typically require:

- 2 threads for host/system management
- 7 threads for first guest
- 7 threads for second guest
- 7 threads for third guest
- 7 threads for fourth guest
  - **30 threads total** (a dual socket 8-core hyper-threaded system)

Virtual Machine Limits

For systems with many or large virtual machines (VMs), configure everRun with 10 Gb sync links, and for the everRun software itself, 4 vCPUs and 4096 MB. Refer to the **Preferences -> Systems Resources**

page in the everRun Availability Console for instructions on setting the everRun system resources to the maximum.

The following table lists everRun system VM limits.

Item	Limits
Maximum VCPUs per FT VM	8
Maximum VCPUs per HA VM	16
Maximum Memory per FT VM	213.33 GB
Maximum Memory per HA VM	213.33 GB
Maximum Availability Links per VM	2
Maximum Virtual Networks per VM	20
Maximum Storage Volumes per VM	12
Guest Volume Size	Tested up to 2.2 TB. There are no known limitations other than those imposed by the guest operating system.
Max. Snapshots per VM	16 (72 total per system)

Combined Virtual Machine Maximums

The following table presents the combined maximums of virtual machines (VMs) and virtual NICs that can run on everRun systems.

Virtual Device	Maximum
Total FT VMs	4
Total VMs (FT and HA combined)	24
Total Virtual Network Interface cards (NICs)	20

Important Considerations

Note the following important considerations.

Feature	Comment
everRunSystem Disk	Recommended minimum configuration for physical machines: - One logical volume protected by RAID1, RAID 5, RAID 6, or RAID 10 or - Two non-RAID or RAID 0 volumes. When using multiple volumes per RAID set, the RAID set should set a type that provides redundancy, such as RAID1, RAID5, or RAID10.
USB CD/DVD Drive	USB CD/DVD drives are supported on all platforms for everRun installation.
Direct-Attach Tape Drives	Access to direct-attach tape drives by the guests is not supported. Stratus recommends using network-attach tape drives.
Console Connectivity	Each PM's text console is available for a CentOS operating system. However, VGA mode is not supported; that is, the PM must be at run-level 3 and cannot run at run-level 5. See "System Management" below.

Feature	Comment
SSD Support	everRun supports solid state drives according to the storage controller vendor specifications.
System Management	everRun system management **does not work** at run-level 5.

Accessing Knowledge Base Articles

The **Stratus Customer Service Portal** provides a searchable **Knowledge Base** with technical articles about all Stratus products, including everRun. In some cases, the online Help directly references these Knowledge Base articles (for example, KB-*nnnn*). You can access the Customer Service Portal and Knowledge Base by using your existing service portal credentials, or by creating a new user account, as follows.

To access the Knowledge Base

1. Log on to the **Stratus Customer Service Portal** at https://support.stratus.com.

   If needed, create a new account as follows:

   a. Click **Register Account**.

   b. Enter your company email address and contact info, and click **Register**.

      Your company email address must include a domain name (for example, stratus.com) for a company that is a registered customer of Stratus.

   c. Click the link in the email that you receive from Stratus.

   d. Enter a new password and finish configuring your account.

   If you need assistance creating an account, contact your authorized Stratus service representative.

2. In the service portal, click **Knowledge Base** in the left pane.

3. In the **Keyword Search** box, enter keywords associated with the information you need, and then click **Search**.

   To search for an article by its KB-*nnnn* number, click **Advanced Search**. Next to **Search by ID**, type the article ID number (*nnnn*) and click **Display**.

Related Topics

"Supporting Documents" on page 247

12

Chapter 12: SNMP

Simple Network Management Protocol (SNMP) is a standard protocol for receiving alarms, sending traps, and monitoring system status. SNMP draws upon system-defining information that is stored in hierarchically configured management information bases (MIBs).

To configure an everRun system to use SNMP, see "Configuring SNMP Settings" on page 78.

You can download a copy of the MIB file from the **Drivers and Tools** section of the **Downloads** page at http://www.stratus.com/go/support/everrun.